Julio/Agosto 2017 - nº 25

it User

TECH & BUSINESS

Seguridad en dispositivos móviles: un nuevo campo de batalla

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

Entrevista a Laurent Allard, vicepresidente de OVH

IBM explica cómo aprovechar la Ciencia de Datos y GDPR

La digitalización aumenta los riesgos de fraude

Mesa Redonda IT: Movilidad y seguridad, ¿una quimera?

Securización de dispositivos móviles

Juan Ramón Melara
juanramon.melara@itdmgroup.es

Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, David Marchal

Diseño y maquetación revistas digitales
Contracorriente

Diseño y maquetación proyectos especiales
Eva Herrero

Producción audiovisual
Antonio Herrero, Ismael González

Fotografía
Ania Lewandowska

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

Hablar de seguridad cuando los medios de comunicación generalistas, la radio y la televisión han abierto sus informaciones más de dos y tres veces en estas semanas con ataques informáticos es muy sencillo. La parte de concienciación se facilita mucho, porque todas las empresas han visto los efectos que un ataque puede causar, y no solo en sus datos, sino en su capacidad operativa.

Pero lo cierto es que estos ataques son solo una muestra de lo que puede pasarle a una empresa si no pone especial interés en su seguridad. El enfoque tradicional ha dejado de ser efectivo, porque, tal y como nos recuerdan los profesionales en la Mesa Redonda IT y en nuestro En Portada, la red actual ha dejado de tener límites. Ya no se trata, por tanto, de poner un muro alrededor de la empresa, porque la empresa no tiene límites físicos que poder asegurar.

Los límites de la empresa están allí donde lleguen sus empleados y clientes, porque desde allí accederán a datos críticos para el negocio, y hay que tenerlo en cuenta a la hora de definir la forma de protegerla.

Hay otros vectores de ataque, cierto, pero todos los profesionales apuntan a los dispositivos móviles como el próximo campo de batalla contra el malware. Además, a estas alturas en casi imposible encontrar una empresa que no haya apostado en mayor o menor medida por la movilidad, con lo que contar con una política de seguridad adecuada y completa es vital para todas las compañías.

Así que si no queremos llevarnos un disgusto cuando llegue el próximo ataque, más vale que nos pongamos manos a la obra, porque ya vamos tarde.

Juan Ramón Melara
IT Digital Media Group

Más tiempo de actividad.
Menos tiempo de inactividad.

HPE Just Right IT proporciona tecnología sencilla y fiable que le ayudará a generar oportunidades a la velocidad que marcan las empresas de hoy en día. Con el respaldo de nuestros partners locales y décadas de experiencia, estas soluciones, productos y servicios correctamente dimensionados se han diseñado para ayudar a las empresas en crecimiento a producir resultados sólidos. Vea todas estas soluciones en la revista online haciendo click aquí

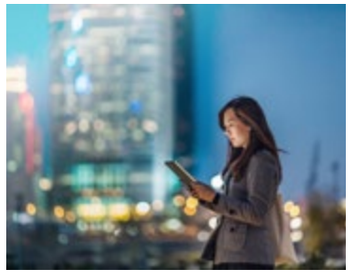
HPE Just Right IT, para empresas de cualquier tamaño.

Accelerating next

Hewlett Packard Enterprise

Sumario

Especial IT



Reimagine 2017: Transformación Digital, de la teoría a la práctica

Hewlett Packard Enterprise

intel

Automatización de procesos y servicios, primer paso hacia la Transformación Digital

serem

Cyberday 2017: Una visión de la seguridad de nueva generación

Check Point SOFTWARE TECHNOLOGIES LTD.

Mesa Redonda IT

Movilidad y seguridad: ¿una quimera?

R S C

No son solo médicos

NO SOLO it

Índice de anunciantes

Hewlett Packard Enterprise Just Right IT

Comparex Oracle Database Appliance

Kaspersky CiberSafety Games

Board Toma de decisiones

OVH Infraestructura dedicada

Serem DevOps

GMV Transformación Digital

Hewlett Packard Enterprise Flexible Capacity

Tecnología para tu empresa

IT Whitepapers

Ninja Twitter

Yes Management

IT Televisión

Actualidad

Entrevista a Laurent Allard, vicepresidente de OVH

IBM explica en Fast Track Your Data cómo aprovechar la ciencia de datos y GDPR

La Inteligencia artificial, clave de la jornada Europa y España ante la Transformación Digital

La Transformación Digital no es posible sin la automatización de procesos y tareas

La digitalización favorece el incremento del fraude

El mercado interior empuja los datos del negocio de consultoría en 2016

De WannaCry a Petya: cómo el ransomware puede 'paralizar el mundo'

COMPAREX
Software · Consulting · Services

Oracle Database Appliance

Sencilla, optimizada y asequible

ORACLE Platinum Partner

Simplifique la complejidad del centro de datos con un sistema moderno, convergente y con poco uso de recursos.

- Gran ahorro de costes en hardware, almacenamiento... frente a un sistema en que el usuario se encarga de todo.
- Increíble rendimiento y fiabilidad que ayuda al usuario a ser más productivo y al personal de TI a cumplir los acuerdos de nivel de servicio (SLA).
- El personal de TI ahorra tiempo en el mantenimiento y puede centrarse en servicios estratégicos beneficiosos para el negocio.
- ODA como solución comercial para distintos entornos de aplicaciones

---

Con más de **40 años de presencia en el mercado**, desde **COMPAREX** damos servicio tanto al sector público, como a medianas y pequeñas empresas así como a grandes corporaciones internacionales. Expertos en datacenter, COMPAREX es proveedor global de TI especializado en la gestión completa del ciclo de vida del software comercial, la transformación de las infraestructuras IT y la consultoría técnica de productos y servicios basados en cloud. Nuestro portfolio incluye licencias de software de más de 3.000 fabricantes, así como consultoría y servicios profesionales.

Contáctenos sin compromiso y le daremos más información en **info@comparex.es**

Laurent Allard, vicepresidente de OVH

“Las líneas de desarrollo van según lo planeado, y tendremos los diez nuevos centros de datos previstos en este año”

En pleno proceso de ampliación y desarrollo global, OVH anunciaba hace unos meses su intención de adquirir VCloud Air de VMware. Para conocer todos los detalles y repasar los planes de la firma para este año, hemos conversado con Laurent Allard, vicepresidente y antiguo CEO de OVH.

El pasado mes de abril, VMware y OVH hicieron públicos los planes de la primera para adquirir vCloud Air. Los detalles financieros de la transacción no se hicieron públicos, pero se esperaba que la transacción se cerrase durante el segundo trimestre de 2017, un paso que, según Octave Klaba, CEO de OVH, permitirá a su compañía “ofrecer una proposición de valor única para despliegues empresariales aún mayores, incluyendo capacidades enriquecidas de migración y funcionalidades híbridas para centros de datos virtuales. Creemos que esto será muy beneficioso para todos nuestros clientes a nivel global”.

Para Pat Gelsinger, CEO de VMware, “los clientes tendrán acceso a la infraestructura global de OVH, su gran servicio de soporte y conservarán toda la tecnología SDDC de VMware y su innovación tal y como están acostumbrados”, y añadía que “seguimos comprometidos en la entrega de nuestra arquitectura Cross-Cloud que extenderá nuestra estrategia de cloud híbrida, permitiendo a los clientes hacer funcionar, gestionar, conectar y asegurar sus aplicaciones a través de diferentes nubes y dispositivos en un sistema operativo común”.

Una operación con dos razones principales

Para complementar la información acerca de las razones de la compra y las consecuencias de la misma,

Nuestra tecnología no es propietaria y cualquier vuelta atrás que quiera hacer el cliente es totalmente transparente

Laurent Allard, vicepresidente de OVH

IT User pudo conversar con Laurent Allard, vicepresidente y antiguo CEO de OVH, quien nos explicaba que "esta operación se ha realizado en base a dos razones, principalmente. La primera de ellas es acelerar los planes que ya teníamos sobre la mesa de desarrollar el negocio en Estados Unidos. Con este paso, vamos a ser capaces de acelerar este desarrollo de nuestro negocio cloud en Estados Unidos. Por otra parte, y aprovechando el desarrollo que ha estado haciendo tanto el pasado año como éste VMware, vamos a poder migrar centros de datos con una arquitectura más tradicional a una arquitectura más puntera sin necesidad de parar la producción en el proceso de migración tanto de los procesos de trabajo como de los datos, que se realizará de forma totalmente transparente para los clientes, sin necesidad de que tengan que ver interrumpidos sus procesos de negocio".

Por tanto, la aceleración de los planes de desarrollo en Estados Unidos ha sido una de las bases para dar este paso. Tal y como nos explica Allard, "nuestra tecnología cloud es muy competitiva en Estados Unidos y seguimos trabajando en la construcción de dos grandes centros de datos en el país norteamericano, uno en la costa éste y otro en la costa oeste. Ambos centros de datos van a tener una capacidad de escalado de hasta 80.000 servidores y nuestra intención no solo es trasladar allí las cargas de trabajo de empresas estadounidenses, sino seguir creciendo y desarrollando ese negocio local".

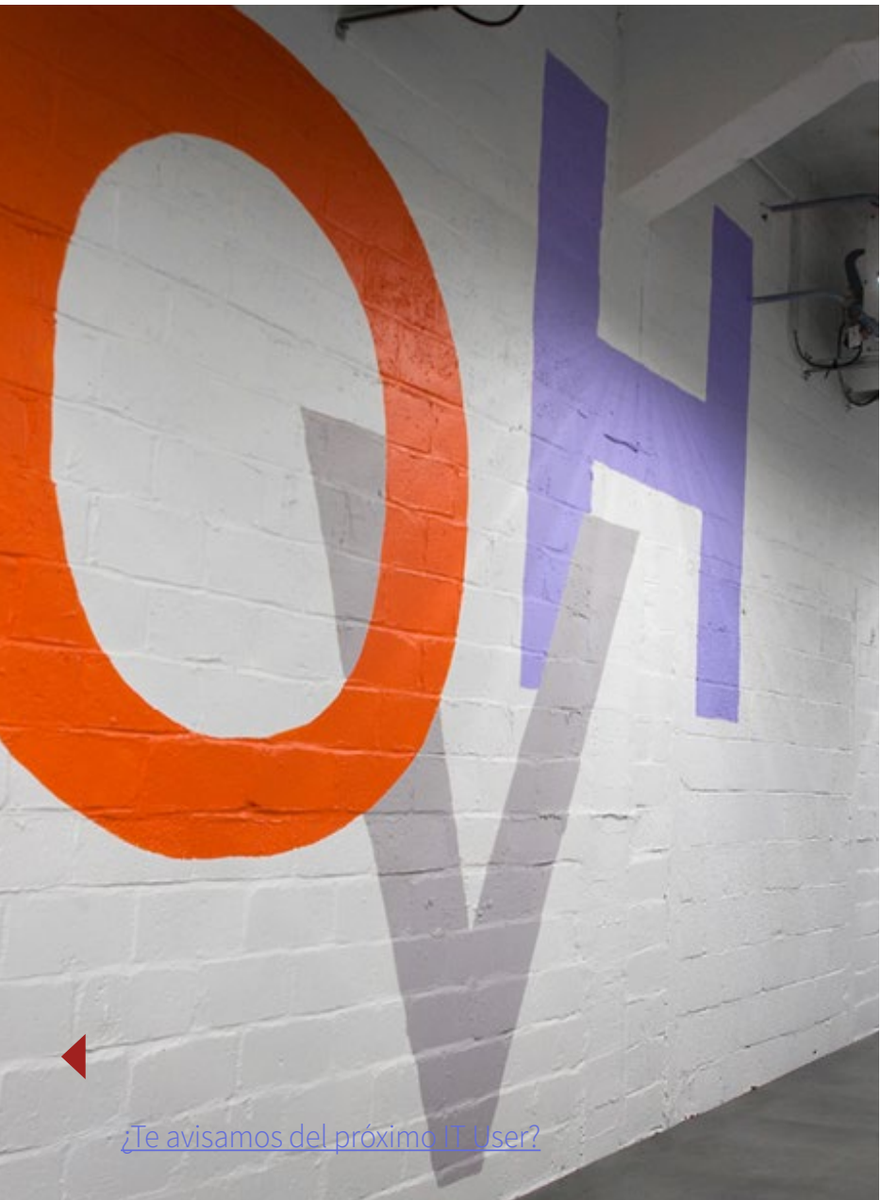
Estados Unidos, un mercado particular

De hecho, este desarrollo en Estados Unidos va a tener una particularidad, y es que se va a crear una estructura de personal específica y va a considerarse como un negocio aislado para proteger los intereses de otras compañías de los posibles efectos de la denominada Ley Patriota. En este sentido, nos apunta que "un cliente español o francés, al no ser una compañía norteamericana, no está sujeto al cumplimiento de la Ley Patriota, sino a las leyes locales que se aplique en cada uno de los países. De ahí que queramos mantenerlo totalmente aislado, porque cualquier otro proveedor norteamericano puede llegar a verse afectado por la Ley Patriota. Todos los recursos, tanto tecnológicos como de personal u organizativos de OVH en Estados Unidos serán totalmente independientes del resto de los negocios de OVH en el mundo, sin ningún tipo de accesos mutuos ni intercambios de datos, con lo que si un cliente español, por ejemplo, con contrato con OVH en Europa quiere iniciar un negocio con nosotros en Estados Unidos, deberá firmar un nuevo contrato independiente".

"Con esto", continúa, "dividimos en dos el negocio, por una parte, Estados Unidos y, por otra, el resto, y nos aseguramos de que nuestros clientes del resto del mundo, bajo ninguna circunstancia, están expuestos a la Ley Patriota".

La relación entre OVH y VMware ha sido muy sólida y fructífera los últimos años, y así nos lo asegura Laurent Allard. "Desde 2011, hemos tenido una muy buena relación y hemos sido en varias ocasiones reconocidos por ello. Además, durante este tiempo hemos trabaja-

Con este paso, vamos a ser capaces de acelerar este desarrollo de nuestro negocio cloud en Estados Unidos



¿Te avisamos del próximo IT User?

do muy estrechamente a la hora de innovar e investigar. Además, somos el principal Cloud as a Service de VMware. Hemos trabajado mucho desarrollando juntos y nos hemos esforzado mucho en este tiempo para ser capaces de dar el mejor servicio a sus clientes".

Expansión internacional y planes de desarrollo

Junto con esta novedad, quisimos preguntar a Laurent Allard por el proceso de expansión global de la compañía iniciado el pasado año con el anuncio de la apertura de 10 nuevos centros de datos en diferentes países. Tal y como nos confirma, "los planes se están desarrollando según lo previsto. Por el momento, ya tenemos tres de ellos en producción. Ahora estamos ultimando la puesta en marcha y la comercialización de otros dos, en Reino Unido y Alemania, manteniendo la agenda. Durante este verano, deberán estar operativos los dos centros de datos de Estados Unidos y en el próximo trimestre avanzaremos con los de España, Italia y Holanda, que deberían estar funcionando antes de 2018. Entre medias, vamos a incrementar también nuestra capacidad en Francia con la apertura de otro datacenter".

Por último, quisimos valorar con este directivo los puntos fuertes de su compañía en el mercado, y nos explicaba que los criterios de selección de los clientes, ya sean grandes, medianos o pequeños con diferentes, así como su cuota de mercado, pero que, principalmente, lo que define a OVH es "la apuesta por los estándares; Nuestra tecnología no es propietaria y cualquier vuelta atrás que quiera hacer el cliente es totalmente transparente. Otro punto fuerte es nuestra eficacia en costes y la predictibilidad de los mismos, dado que nuestros costes incluyen todo, no tenemos extra-costes ocultos. El tercer punto es que no exponemos, como ya he explicado, a ninguno de nuestros clientes de ninguna manera a la Ley Patriota, ni trasladamos los datos de nuestros clientes de un país a otro. El siguiente es que nosotros diseñamos y desarrollamos nuestros propios servidores, lo que nos permite controlar mejor los costes y ofrecer a los clientes un servicio a menor precio. Y, finalmente, la innovación, tenemos una propuesta más amplia que muchos de nuestros competidores".

Enlaces relacionados

- Cloud dedicada como base de la Transformación Digital
- OVH
- Cloud Privada
- Casos de éxito

KASPERSKY lab

KASPERSKY SECURITY AWARENESS

FORMACIONES DE CONCIENCIACIÓN EN CIBERSEGURIDAD

La firma quiere ayudar a las empresas a sacar el máximo partido de los datos

IBM explica en Fast Track Your Data cómo aprovechar la ciencia de datos y GDPR

La nueva normativa europea de protección de datos es uno de los principales cambios a los que se van a tener que enfrentar las compañías que operan en la Unión Europea. Consciente de esta realidad, IBM ha celebrado en Munich (Alemania) su evento Fast Track Your Data, en el que ha explicado la importancia de los datos y cuál es su propuesta para ayudar a las empresas a cumplir con GDPR. Además, también ha realizado anuncios que buscan ayudar a las empresas a sacar provecho de los datos, el principal valor de cualquier compañía.

Bárbara Madariaga. Munich (Alemania)

IBM cree firmemente que, en su transformación digital, las empresas deben poner foco fundamentalmente en los datos, pero el problema radica en saber cómo y para qué utilizar los datos. Así lo han asegurado diferentes directivos durante la jornada Fast Track Your Data que la firma ha celebrado en Munich y en la que se ha explicado que, para que las empresas aprovechen esta nueva realidad, es necesario disponer de una cultura empresarial que se filtre a todas las áreas de la empresa, de manera que todo el mundo entienda que es crítico tomar decisiones de negocio basadas en los datos; contar con profesionales de los datos que realmente tengan el conocimiento necesario para hacer el análisis correcto y den a las empresas la información que necesitan; y contar con servicios y plataformas que lo facilite.

Algo que se presenta como crucial, más si se tiene en cuenta que, en la actualidad "solamente el 15% de las organizaciones son capaces de tomar decisiones sacando el máximo valor de los datos".

Simplificar la gestión de los datos

Durante la sesión general, Rob Thomas, director general de IBM Analytics, ha explicado la importancia que tienen los datos para cualquier compañía. "La ciencia de los datos y el machine learning van a hacer lo mismo en el Siglo XXI que lo que hizo la revolución industrial por el Siglo XIX". En este sentido,

"La ciencia de los datos y el machine learning van a hacer lo mismo en el Siglo XXI que lo que hizo la revolución industrial"

Rob Thomas, director general de IBM Analytics

Thomas ha animado a las empresas a no quedarse atrás y aprovechar "las grandes oportunidades de negocio que se presentan ante nosotros". Y es que, para el directivo, la "ciencia de los datos es la nueva TI", con lo que esto representa. "Los científicos de datos, los desarrolladores y los profesionales van a trabajar de manera conjunta para hacer frente a los principales problemas".

En este punto, IBM se ha propuesto ayudar a las empresas "simplificando la gestión de datos". Para IBM "la analítica de datos, el machine learning y la inteligencia cognitiva" son tres tendencias que, aunque ya son el presente, "también marcarán el futuro", y ya están transformando industrias como las finanzas, la salud, las aseguradoras, el retail o el comercio electrónico.

"Nos encontramos en un momento apasionante en el que hay que dar respuestas a preguntas como de qué manera utilizamos los datos y cuál es el valor que sacamos de ellos". Rob Thomas ha destacado que el objetivo de su compañía es "simplificar la ciencia de los datos", para utilizarlos de la forma correcta, algo que, si se logra "tendrá la capacidad de leer mentes". Thomas también ha aprovechado su participación para destacar que "nos movemos hacia un mundo multi-cloud" donde la nube híbrida no es sólo el futuro "sino también el presente".

Ante esta realidad, IBM ha aprovechado la jornada para anunciar novedades en IBM Db2, su software de base de datos que busca facilitar la gestión de los mismos a las empresas. Así, y entre éstas, acaba de presentar Db2 Developer Community Edition, con la que permite a los desarrolladores crear "de una forma rápida" prototipos de aplicaciones "que aprovechan todas las capacidades de Enterprise Edition".

"Nos encontramos ante una nueva generación de desarrolladores", ha señalado Rob Thomas. "Ésta busca una forma más ágil de desarrollar aplicaciones de tal

QUÉ PASÓ EN FAST TRACK YOUR DATA

CLICAR PARA VER EL VÍDEO

manera que permitan el crecimiento de sus compañías. Con las novedades en Db2 estamos facilitando el trabajo a los desarrolladores y permitiendo que se involucren en un entorno en claro crecimiento".

La firma también ha anunciado que la nueva versión de Db2 on Cloud ya está disponible en la nube de IBM, además de que ya "soporta JSON".

GDPR

La nueva normativa europea de protección de datos (GDPR) ha copado gran parte del evento de IBM. No en vano, será de obligado cumplimiento el próximo mes de mayo y, a menos de un año vista, "la mayoría de las empresas no están preparadas".

"GDPR es un viaje", han señalado los principales directivos de la firma, quienes han destacado que éste es uno de los principales retos a los que se enfrentan las compañías que operan en la Unión Europea, "aunque también supone una gran oportunidad".

En Munich, IBM ha anunciado una serie de iniciativas como IBM Unified Governance Software Platform, Information Governance Catalog Download & Go, o StoreIQ, que ayudan a las empresas a cumplir con la nueva normativa de protección de datos. Las mejoras "han sido diseñadas para ayudar tanto a los desarrolladores como a los analistas a que aprovechen el poder de la computación cognitiva de tal forma que puedan obtener una mayor compresión, y control, de sus datos al mismo tiempo que cumplen con la GDPR".

"El gran volumen de datos, su continua distribución y las regulaciones como la GDPR han hecho que cada vez sea más importante organizar, analizar y gobernar una información en continuo crecimiento", ha señalado Rob Thomas. "Nuestro objetivo es ayudar a las empresas a entender que no sólo tienen datos, sino que tienen que aprovecharlos para adoptar las mejores decisiones para sus negocios, además de que queremos facilitar su cumplimiento".

Open Data Government Consortium para Apache Atlas

Una de las novedades más importantes que ha anunciado IBM durante el marco de Fast Track Your Data es Open Data Government Consortium para Apache Atlas, con el que la firma busca simplificar la gobernabilidad de los datos y cumplir con la GDPR.

Aunque el proyecto se encuentra en fase inicial, el consorcio trabaja para que éste esté en "un nivel superior" lo antes posible.

El consorcio, de carácter internacional (en él participan empresas como el Grupo ING, Hadoop o Hortonworks, entre otros), busca ayudar a las empresas a adoptar prácticas de gestión de datos "diligentes e integrales" que garanticen la seguridad, integridad, usabilidad y disponibilidad de los datos.

Enlaces relacionados

- Tres mejores prácticas para reducir los riesgos del incumplimiento normativo
- Ideas para cumplir con GDPR
- Descubre la información para cumplir con GDPR
- El coste de incumplir el gobierno de la información

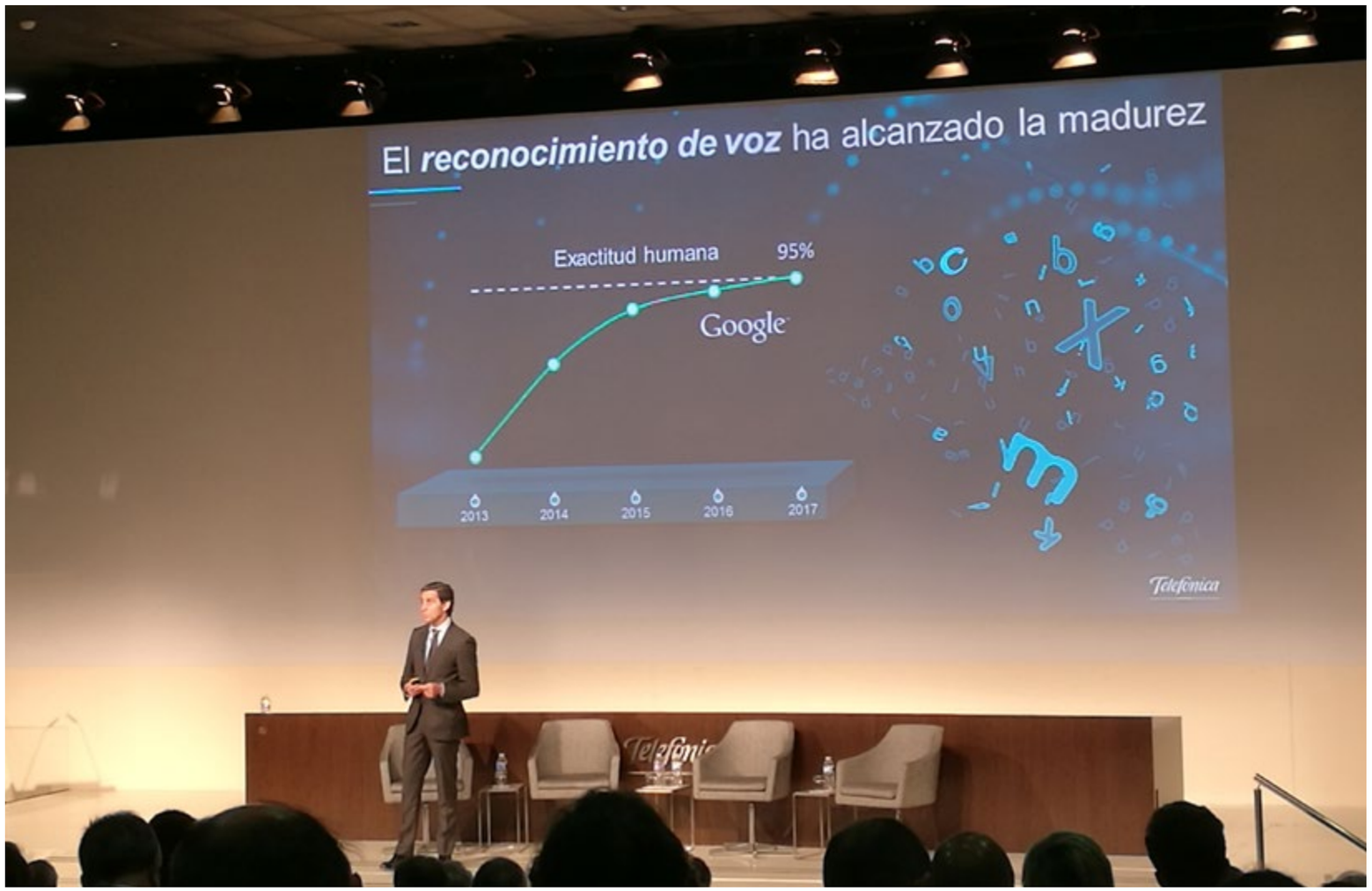
El Futuro de la Toma de Decisiones

Análizar. Simular. Planificar.
Todo en uno

La plataforma número 1 para la toma de decisiones

Actualmente se pueden encontrar muchas soluciones para la visualización de datos, la planificación, la previsión y el análisis avanzado, pero cuando se trata de tomar decisiones necesitas que todo esté perfectamente integrado y que sea capaz de compartir los mismos datos, las mimas métricas y la misma visión de los clientes, productos y mercados. **Aquí llega BOARD.**

www.board.com



“El mundo camina hacia la Inteligencia Artificial”

José María Álvarez-Pallete, presidente de Telefónica

Durante la jornada Europa y España ante la Transformación Digital, organizada por ESYS, José María Álvarez Pallete, presidente de Telefónica, ha analizado el presente y futuro de la digitalización en España, así como ha explicado qué es lo que está haciendo la operadora española para adaptarse a los nuevos tiempos.

Durante su intervención, José María Álvarez-Pallete, presidente de Telefónica, ha ofrecido una serie de datos que muestran la importancia de lo digital. Así, ha destacado que en los próximos años el volumen de datos se va a multiplicar por 11 con la llegada de 5G, la velocidad de conexión será 100 veces superior a la actual y la capacidad se multiplicará por 100. “Los recursos más valiosos serán los datos”, ha explicado Álvarez-Pallete, quien también ha destacado que en la actualidad “más de la mitad del tráfico en Internet no está generado por humanos”.

Ante esta nueva realidad, “los ciudadanos ya están empezando a reaccionar”, sobre todo desde que “se ha disparado el uso de adblockers”. Álvarez-Pallete también ha recordado que “el reconocimiento de voz ha alcanzado la madurez” y “ya empieza a detectar emociones”, con lo que eso significa. “Entramos en una era

"Ninguna empresa tiene garantizada su supervivencia"

en el que las máquinas empiezan a emular los comportamientos humanos y los sistemas cognitivos ya tienen la capacidad de perfeccionarse a sí mismos". En este sentido, Álvarez-Pallete ha reconocido que el mundo camina hacia la era de "la inteligencia artificial y los datos cognitivos" y ha recordado que "estamos hablando de cerebros capaces de pensar y sentir emociones".

La llegada de la Inteligencia Artificial ha provocado que "se tenga que crear un nuevo marco de valores", ante la creciente preocupación "sobre algunos aspectos éticos". Y es que las máquinas "empiezan a tener inteligencia, y vamos a tener que saber qué hacer con ella".

Importancia de la digitalización

Álvarez-Pallete ha asegurado que al día se envían 220.000 millones de mensajes de correo electrónico, 50.000 millones mensajes de WhatsApp (o de cualquier otra plataforma de mensajería instantánea), realiza 5.000 millones de búsquedas en Google, 1.400 millones de contactos en Tinder o 1.000 millones de accesos a LinkedIn. "Nuestra vida cada vez se digitaliza más".

La importancia que están adquiriendo las redes sociales también ha copado parte de la presentación de Álvarez-Pallete, quien ha asegurado que Facebook tiene más "habitantes" que China, LinkedIn más que Rusia y Brasil y Twitter más que Estados Unidos. "Las redes sociales tiene una gran influencia", ha recordado Álvarez Pallete quien ha puesto como ejemplo el caso de Katy Perry. La cantante ha sido la primera en alcanzar los 100 millones de seguidores en Twitter, "tiene más capacidad para comunicarse con sus seguidores que muchos presidentes". Esto también ha llevado a plantearse "los códigos de conducta que tienen que tener las redes sociales".

"La adopción de la tecnología está siendo exponencial", ha afirmado el presidente de Telefónica, destacando que "la telefonía fija tardó 75 años en alcanzar los 100 millones de usuarios, mientras que la telefonía móvil sólo necesitó 16 años, Facebook 4 años y Pokemon GO 4 días".

"No hay aspecto en la vida humana que no sea susceptible de ser alterado por la tecnología. Uber es la primera empresa de transportes pese a no tener coches, Facebook es el primer generador de contenidos pese a no generar contenido propio y Airbnb es la primera empresa de alojamiento pese a no tener casas".

"Nos hemos reinventado y crecemos en todas las partidas"

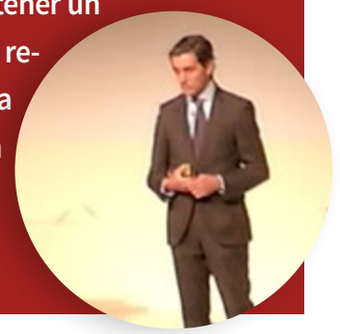
La Junta General de Accionistas de Telefónica ha aprobado todos los acuerdos propuestos por el Consejo de Administración de la compañía, entre ellos la distribución de un dividendo de 0,40 euros por acción en efectivo en 2017, con cargo a reservas de libre distribución. El primer pago, de 0,20€ por acción se realizará el 16 de junio, y el segundo, también de 0,20€ por acción, se hará efectivo el 14 de diciembre de 2017. José María Álvarez-Pallete, presidente ejecutivo de Telefónica, reiteró ante la Junta el compromiso de la compañía con una retribución atractiva para el accionista y con la generación de una rentabilidad por dividendo consistente con el mercado y un pay-out sostenible.

La Junta aprobó igualmente los resultados y la gestión del Consejo de Administración durante 2016, un ejercicio del que Álvarez-Pallete hizo balance en su discurso ante la Junta. "El tiempo nos ha dado la razón. Hoy podemos decir que es una satisfacción depender de nosotros mismos para conseguir los objetivos que nos hemos marcado. Nos hemos reinventado y crecemos en todas las partidas. Eso prueba que vamos en la buena dirección", explicó. En este contexto, hizo hincapié en el reconocimiento del mercado y en la revalorización de la acción un 14% desde que comenzó el año, más del doble del índice telco europeo de referencia.

Por otro lado, Álvarez-Pallete detalló la inversión de cerca de 50.000 millones de euros realizada desde 2012 en las distintas plataformas, y explicó cómo este esfuerzo ha situado a Telefónica en una posición destacada en cuestiones tan relevantes como en el despliegue de redes de ultra banda ancha o en la iniciativa pionera de dotar de Inteligencia Artificial y Sistemas Cognitivos a las redes y servicios de la compañía, que permitirá al cliente gestionar sus experiencias digitales con Telefónica en tiempo real.

Esta transformación significa, a juicio de José María Álvarez-Pallete, que Telefónica ha pasado de vender minutos a vender gigabytes, y que los ingresos de banda ancha y servicios sobre conectividad han superado por primera vez a los de acceso y voz. En su discurso ante los accionistas, destacó también el crecimiento de las principales magnitudes financieras, una buena evolución que se ha trasladado al beneficio neto y que ha generado un flujo de caja libre que crece por primera vez en cinco años, hasta un 24%, junto con una inversión también récord, de hasta el 16,5% de los ingresos.

Precisamente en relación con los objetivos previstos para 2017, el presidente de Telefónica reiteró que será un año de crecimiento sostenible sobre las sólidas bases ya consolidadas y con unas prioridades muy claras: crecer en generación de caja, con expansión de márgenes y manteniendo unos niveles de inversión elevados. Recordó igualmente el éxito de la venta parcial de Telxius el pasado febrero, así como el objetivo de mantener un rating de grado de inversión sólido, reforzando el balance de la compañía a través de la mencionada generación de caja y un progresivo desapalancamiento orgánico.



"Los operadores también nos hemos tenido que transformar"

Álvarez-Pallete ha recordado la influencia que está teniendo la tecnología en sectores como la banca, con blockchain a la cabeza. "Esta tecnología se va a extender a otras áreas".

Transformación digital

Los operadores "también nos hemos tenido que transformar". En este sentido, el presidente de Telefónica ha recordado que hace no mucho tiempo el grueso de su negocio provenía de la voz, algo que ha sido sustituido por los datos. "La digitalización también ha afectado a sectores como el entretenimiento, con Netflix, o a la automoción, con Tesla". No en vano, esta última compañía "ya vale más que General Motors". La Biotecnología y la medicina son otros dos sectores que ya están comprobando los beneficios de la digitalización.

Nueve de las 10 compañías "con mayor valor son de base tecnológica" (Apple, Google, Tesla, Microsoft, Amazon, Netflix, Samsung, Toyota, Facebook e IBM). En este punto, Álvarez Pallete ha recordado

"No hay aspecto en la vida humana que no sea susceptible de ser alterado por la tecnología"

que la importancia de la innovación, destacando que, entre ellas, no hay ninguna compañía europea. "La innovación es básica, algo estamos haciendo mal en Europa y tenemos que cambiar".

"Ninguna empresa tiene garantizada su supervivencia", ha destacado Álvarez Pallete quien ha aprovechado su intervención para recordar que "el 52% de las compañías que se encontraban en el S&P 500 en el año 2000 han desaparecido. "En 1955, la media de supervivencia de una empresa era de 61 años, ahora es de 17 años".

Asimismo, ha animado a las compañías a abordar procesos de digitalización. "Las empresas que no sean capaces de transformase van a tenerlo muy complicado".

Qué está haciendo Telefónica

A este respecto, Álvarez-Pallete también se ha referido a la labor que está haciendo Telefónica para continuar creciendo. "Ésta es una compañía que nació para la voz fija", que se ha tenido que transformar "y adaptarnos a la nueva realidad para añadir más dimensiones".

Álvarez Pallete ha asegurado que Telefónica ha trabajado "para ser una compañía de plataformas" y, para ello, ha invertido más de 50.000 millones de euros.

La primera plataforma consiste en los activos físicos, la segunda en las TI y sistemas, la tercera en proveer servicios financieros, de cloud, conectividad y seguridad, y la cuarta en la Inteligencia Artificial y cognitiva.

Precisamente, la operadora española aprovechó la celebración del Mobile World Congress el pasado mes de febrero para presentar Aura, con la que "los usuarios podrán gestionar su experiencia digital con la compañía, al tiempo que controlar de forma transparente y segura los datos que generan por el uso de sus productos y servicios".

El objetivo es "dotar de Inteligencia Artificial a todos los negocios", ya que "todas las compañías van a tener que aplicar Inteligencia Artificial a sus procesos de negocio en los próximos meses o años".

Con Aura "queremos utilizar la Inteligencia cognitiva para ofrecer experiencias diferenciales", asegurando que "los datos son propiedad de los clientes".

Enlaces relacionados

- Telefónica apuesta por la inteligencia cognitiva con Aura
- Primera Plataforma, la estrategia de Telefónica para reinar en 5G
- Barómetro de emprendimiento de éxito en España
- Bankia Índicex. La digitalización de las empresas en España
- Plan Digital 2020. La digitalización de la sociedad española

¡Despliegue su proyecto cloud!

OVH.es

Lo mejor de la virtualización de VMware en una infraestructura 100% dedicada

La potencia del hardware dedicado, la flexibilidad del cloud

Powered by vmware®

Más información >

Pedro Ligero, director general de ServiceNow para España y Portugal

“La Transformación Digital no es posible sin la automatización de procesos y tareas”

ServiceNow ha presentado los resultados de su informe Today’s State of Work: At the Breaking Point, que evalúa el uso y el impacto de la automatización de las tareas laborales rutinarias en las empresas, cómo afecta al volumen de trabajo y la visión de la alta dirección sobre el futuro de los empleados. Aprovechando esta presentación, hemos conversado con Pedro Ligero, director general de ServiceNow para España y Portugal.

- *El 40% de las empresas afirma que, para 2018, necesitarán estar más automatizadas para poder gestionar el volumen de tareas. Para 2020, el 83% estará en ese punto crítico.*
- *El 75% afirma que los datos procedentes de dispositivos móviles e Internet de las cosas contribuirán a la sobrecarga de trabajo.*
- *El 91% considera que la automatización inteligente puede incrementar la productividad. Esto implica también la adopción de la inteligencia artificial y el aprendizaje automatizado para optimizar los procesos de toma de decisiones con el fin de mejorar los plazos y la precisión de los procesos empresariales.*

El informe se basa en una encuesta a 1.850 ejecutivos con puestos de alta dirección de siete países, de los que más de un tercio son europeos, y revela que la mayoría de las empresas ya han implantado procesos de automatización avanzada en sus departamentos y que casi la mitad de los directivos considera que, en 2018, la automatización será aún más necesaria para gestionar los crecientes volúmenes de trabajo.

El análisis también señala que la automatización de tareas en el trabajo diario impulsa el crecimiento de los beneficios, genera nuevas oportunidades de empleo e incrementa la eficiencia de los equipos, permitiendo que los empleados se centren más en las actividades de valor añadido.

- *La mitad de los directivos (50%) ya ha empezado a utilizar la automatización inteligente en uno o varios de sus procesos y el 84% prevé implantarla en un futuro cercano.*

- *Las empresas europeas con un alto nivel de automatización tienen la probabilidad de incrementar un 15% sus ingresos, seis veces superior respecto a aquellas cuyo grado de automatización es reducido. Por ejemplo, las compañías que aumentaron sus ingresos más del 20% cuentan, de media, con una automatización del 59%, mientras que aquellas que registraron un crecimiento plano o negativo de los ingresos tienen un nivel de automatización del 36%.*

- *De media, únicamente el 38% de los procesos de las empresas están automatizados, algo que afecta directamente a la alta dirección, que dedica 15 horas semanales –lo que corresponde a dos jornadas de trabajo completas– a tareas administrativas manuales.*

- *El área de TI muestra los mejores resultados en términos de eficiencia en los procesos empresariales a diferencia del de recursos humanos que, según los directivos, es el que necesita una transformación digital más profunda.*

Eficacia y eficiencia de mano de la automatización

Para complementar los datos de este estudio, hemos conversado con Pedro Ligero, director general de ServiceNow para España y Portugal, quien nos explicaba que la Automación "es un conjunto de tecnologías que permite a las maquinas funcionar de forma automática, sin la necesidad de la intervención humana. En este sentido, el principal objetivo y beneficio de este proceso es que reemplaza al trabajador en la ejecución de tareas repetitivas o peligrosas, asegurando unos resultados eficientes y precisos. A día de hoy, las empresas necesitan moverse más rápido, pero muchas veces se ven ralentizadas por unas herramientas anticuadas y procesos manuales que las frenan. Este retraso en el flujo de trabajo hace que el empleado medio se distraiga a menudo y necesite un promedio de casi media hora para volver a centrarse en las tareas. Para compensar estas distracciones, muchas veces los trabajadores acaban desempeñando sus funciones con más prisa, aunque esto implique riesgos en términos de eficiencia, y experimentan mayores niveles de estrés y frustración por la presión que supone la falta de tiempo. Por el contrario, al automatizar el trabajo, las empresas pueden optimizar el rendimiento de sus empleados, aumentar los niveles de servicio y lograr un modelo de negocio innovador, en el marco de un funcionamiento más eficiente".

> *"A día de hoy, las empresas necesitan moverse más rápido, pero muchas veces se ven ralentizadas por unas herramientas anticuadas y procesos manuales que las frenan"*
>
> *Pedro Ligero, director general de ServiceNow para España y Portugal*

Para este responsable, "la automación de servicios y proceso y la Transformación Digital van de la mano. El incremento de la eficiencia y productividad que la Transformación Digital aporta a las empresas no sería posible sin la automatización de las tareas y procesos habituales que se llevan a cabo diariamente en las ofi-

CLAVES PARA LA AUTOMATIZACIÓN DE PROCESOS Y SERVICIOS IT CON SERVICENOW

CLICAR PARA VER EL VÍDEO

"El incremento de la eficiencia y productividad que la Transformación Digital aporta a las empresas no sería posible sin la automatización de las tareas y procesos habituales que se llevan a cabo diariamente en las oficinas y que requieren un elevado número de recursos tanto humanos como tecnológicos"

- *Solo el 33% de las tareas de recursos humanos y el 29% de las tareas de atención al cliente están automatizadas, en comparación con el 48% de las tareas del área de TI. Por lo tanto, existe margen de mejora en estos aspectos.*
- *El 72% de los directivos cree que la automatización puede fomentar la creación de nuevos empleos.*
- *El 88% afirma que a los empleados les preocupa que la automatización elimine puestos de trabajo.*
- *Los tres principales obstáculos para acometer la automatización son los recursos necesarios, tanto en términos de presupuesto como de personal, la resistencia de los empleados al cambio y la preocupación acerca de la eliminación de puestos de trabajo.*

cinas y que requieren un elevado número de recursos tanto humanos como tecnológicos.

Pero, ¿pueden automatizarse todos los procesos de la empresa? Preguntado Pedro Ligero nos comenta que, "a día de hoy, probablemente los procesos industriales son los que más avances han conseguido gracias a la implantación de la automación, ya que muchas fábricas utilizan esta tecnología. Aun así, también las oficinas más tradicionales están aprendiendo a aprovechar los sistemas de automación inteligente para desarrollar sus tareas de forma más eficiente. Con servicios orientados a facilitar las actividades, tareas y procesos laborales de todos los días, las empresas de hoy en día pueden operar de manera más rápida y ser más escalables que nunca. Por ejemplo, la tecnología de automación inteligente

de ServiceNow permite la gestión de los servicios en el marco de todos los departamentos de una empresa, incluidas las áreas de TI, Recursos humanos, Instalaciones y Servicios externos, entre otros. Así, los clientes utilizan nuestros servicios para definir, estructurar y automatizar su flujo de trabajo y, de esta forma, logran reducir su dependencia al correo electrónico y las hojas de cálculo de cara a transformar la prestación y gestión de los servicios".

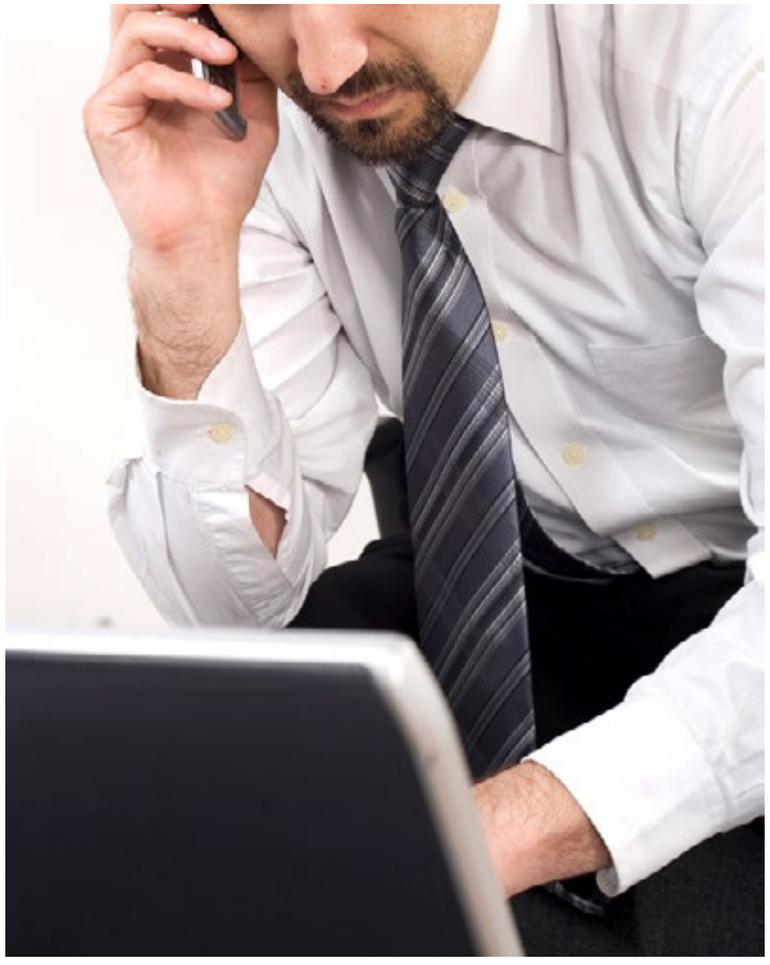
Mucho trabajo por hacer

Según nos explica Pedro Ligero, "la situación de España está línea con la de otros países de la UE, donde las empresas se acercan a un punto crítico y precisan implantar automación inteligente con urgencia para poder gestionar el cada vez más elevado volumen de tareas, que sigue incrementándose debido también a la creciente utilización de dispositivos móviles y de Internet de las cosas. Según nuestro reciente estudio sobre la automatización de las tareas rutinarias en las

oficinas, únicamente el 38% de los procesos de las empresas europeas están automatizados, algo que afecta directamente a la alta dirección, que dedica 15 horas semanales a tareas administrativas manuales. En particular, los departamentos de RR.HH. y servicios de atención al cliente son los que necesitan una mayor transformación digital, ya que actualmente sólo el 33% de las tareas rutinarias de recursos humanos y el 29% de las de atención al cliente están automatizados".

Surge al hilo de estos comentarios otra pregunta: ¿cómo puede afectar esta automatización a la fuerza laboral de la compañía? Para nuestro interlocutor, "aunque muchos empleados miran con preocupación el incremento de la automatización inteligente en las oficinas, ya que perciben que el quitar tareas reduce las necesidades de trabajadores, en realidad está comprobado que los directivos creen que la automación inteligente puede generar puestos de trabajo y de mejor calidad. De hecho, el 72% de los directivos encuestados en nuestro estudio cree que la automatización puede fomentar la creación de nuevos empleos. La ventaja de reducir sensiblemente el tiempo que cada empleado tiene que dedicar a las tareas rutinarias hace que los empleados puedan dedicarse a trabajos más proactivos y de valor añadido para la empresa. Esto, además, tiene un valor positivo en los trabajadores, ya que fomenta su creatividad y les permite desarrollar trabajos más interesantes y con mayores posibilidades de crecimiento profesional. En este sentido, es muy probable que en los próximos años la automación de las tareas rutinarias permita a las empresas incrementar la demanda de perfiles con competencias y capacidades más sociales, como la colaboración, la resolución creativa de problemas y la comunicación".

- *Más de un tercio (38%) de los directivos afirma que el flujo de trabajo ha aumentado un 20% o más en el último año; y un 91% señala que sus empleados más capacitados dedican demasiado tiempo a tareas administrativas.*
- *El 93% considera que la reducción de las tareas rutinarias aumenta la creatividad de los trabajadores.*
- *El 82% de ellos encuentra dificultades para contratar a personas con las capacidades necesarias para hacer crecer sus empresas.*
- *El 92% afirma que la automatización aumentará la demanda de competencias sociales, como la colaboración, la resolución creativa de problemas y la comunicación.*



Enlaces relacionados

- Informe sobre el estado actual del trabajo
- Cómo automatizar procesos y servicios IT con ServiceNow
- Ranking Global de Cloud Computing de la BSA
- Hábitos sobre una TI híbrida
- Barómetro de emprendimiento de éxito en España

serem®

Expertos en Automatización de Procesos.

Now it´s time to do it. Make it easy and simple.

www.serem.com

¿Quiere aplicar DevOps en su empresa?

Descubra con **serem** toda la potencia de servicenow®

Solicite Demo DevOps 120 horas

Implantar DevOps en 120 horas con serem y ServiceNow es posible.

DevOps 120 horas es una aplicación creada por **serem** que nos permite controlar y medir todos los pasos de gestión de proyecto en modo **DevOps**, del desarrollo al despliegue. **ServiceNow 120h Automatizacion**, **Continous delivery**, **Continous integration**... todo es posible con **ServiceNow** y las interfaces que hemos desarrollado.

Según el Estudio anual sobre Tendencias del Fraude 2016

La digitalización aumenta los riesgos de fraude

Según un estudio de la Asociación Española de Empresas contra el Fraude (AEECF) a pesar de los beneficios que conlleva la digitalización de las empresas, también supone un mayor riesgo fraude. Desde AEECF se insta a reforzar los mecanismos existentes para luchar contra este tipo de prácticas.

Siete de cada diez empresas (68,2%) del sector de telecomunicaciones, financieras, automóvil y de créditos al consumo, considera que el fraude ha aumentado durante el último año, mientras que el 18,2% considera que ha permanecido en los mismos niveles, y tan sólo el 13,6% afirma que ha disminuido levemente. Ésta es una de las principales conclusiones de un estudio presentado por la Asociación Española de Empresas contra el Fraude, que también destaca la necesidad de aunar esfuerzos contra el fraude en España.

Según palabras de Felipe Fernández Altea, presidente de la AEECF, "es necesario aunar esfuerzos contra el fraude en España. Desde la Asociación estamos trabajando para crear y cultivar una cultura de intercambio de datos".

La digitalización, ¿problema para el fraude?

Uno de los datos más relevantes del Estudio anual sobre Tendencias del Fraude 2016 tiene a la Transformación Digital como protagonista. Y es que el 91% de los encuestados asegura que una mayor digitalización supone también un reto añadido a la gestión del fraude. "A pesar de que el desarrollo digital ha tenido un impacto muy positivo, el fraude online ha crecido", asegura Diego Azorín Durruty, director general de Bigbank en España, quien insta a adoptar medidas para evitar que los cibercriminales se aprovechen del anonimato propio de Internet.

No en vano, la importancia de los canales digitales queda reflejado en el hecho de que un tercio de los en-

cuestados considera que su negocio online crecerá un 15% o menos, otro tercio estima una subida de entre un 15% y un 30%, y un 22,7% cifra el incremento entre un 30% y un 45%. Estas previsiones "demuestran la necesidad de reforzar los mecanismos existentes en la actualidad para hacer frente al fraude", asegura Felipe Fernández Altea.

Evolución del fraude

En cuanto a la evolución de las tipologías del fraude, cabe destacar que todos los sectores encuestados detectan fraude en primera y tercera persona en su actividad empresarial, con una importante variedad en cuanto a la tipología más comúnmente detectada. "Esta realidad es fiel reflejo de las dificultades a las que se enfrentan las empresas a la hora de detectar el fraude de primera persona y demostrar que ha existido fraude por parte de un tercero".

El fraude en primera persona incide especialmente en el sector financiero, ya que sus miembros son los que más han señalado que la presencia de este tipo de fraude en su sector es superior al 75%.

Qué hacer para reducir el fraude

A tenor de los resultados de la "Estudio Anual sobre Tendencias del Fraude 2016", desde la Asociación Española de Empresas contra el Fraude, se solicita:

- **Reducir las barreras legales para compartir información:** La concienciación sobre la importancia de compartir información como vía para reducir la incidencia del fraude es una realidad incuestionable, sin embargo, todavía existen barreras legales que impiden generar flujos de información entre sectores. Reformar las leyes de protección de datos y permitir la generación de espacios de intercambio de información entre sectores permitirá reducir la incidencia del fraude.
- **Reforzar la colaboración público-privada:** Los flujos de información sobre el fraude no sólo se deben generar en el sector privado, sino que cada vez resulta más relevante generar espacios de intercambio de información entre el sector privado y el público. Por ello, desde la AEECF quieren promover un sistema triangular que facilite el intercambio de información entre empresas del mismo sector; empresas de diferentes sectores que se puedan ver afectadas por fraude en sus diferentes formas; y entre el sector empresarial y el sector público.

Barreras

El estudio también analiza cuáles son las principales barreras que impiden compartir información sobre el fraude entre diferentes sectores. "La barrera legal es el principal impedimento", explica Diego Azorín Durruty. "En mi opinión, la superprotección es un error. Si el mercado fuera más transparente, se reduciría el fraude y tendría consecuencias positivas para los clientes".

Cataluña (72,7%), Comunidad Valencia (68,2%), Andalucía (63,2%), y Madrid (54,5%) son las regiones donde se detecta un mayor fraude

El estudio explica que en 2016 un 50% señalaba la barrera legal como la barrera más relevante, porcentaje que ha ascendido hasta el 77,3% este año.

"Un defraudador va a atacar diferentes sectores. Tenemos la oportunidad de gestionar los datos de manera que podamos luchar contra el fraude", se destaca desde la asociación, que recuerda que "cada entidad dispone de sus propios datos y si luchan solos y no comparten información eres más vulnerable".

Si se comparten los datos "se previene en un 75% el riesgo de sufrir fraude".

Luis Díez Vega, director general comercial en Experian, considera que "el marco de protección de datos es restrictivo al ser garantista" y reclama una "mayor colaboración entre las empresas públicas y privadas para evitar suplantaciones".

Desde la Asociación "estamos trabajando en un entorno de prevención del fraude en el entono multisectorial".

Comunidades con más fraude

A la hora de identificar aquellas regiones españolas donde mayor fraude se ha detectado, cerca del 60% coincide en destacar que el fraude no es un fenómeno localizado en España, aunque mayoritariamente destacan 4 regiones como las más comunes en materia de fraude.

En este sentido, Cataluña (72,7%), Comunidad Valencia (68,2%), Andalucía (63,2%), y Madrid (54,5%) son las regiones donde se detecta un mayor fraude. Les siguen las Islas Canarias (22,7%), la Región de Murcia (18,3%), y Galicia (4,5%).

En esta línea, todos los representantes de los sectores de la automoción y telecomunicaciones han señalado a Cataluña como la región donde más fraude perciben. Además, todos los encuestados del sector de las telecomunicaciones coinciden en señalar a la Comunidad Valenciana como la región donde más sufren las diferentes tipologías de fraude. Por otro lado, el 72% de los encuestados pertenecientes al sector financiero también coincide en señalar esta región como un foco común de fraude.

Enlaces relacionados

- Estudio anual sobre tendencias del fraude
- Big Data, un gran aliado contra el fraude bancario
- Soluciones tecnológicas frente al fraude financiero
- Informe sobre la responsabilidad de las entidades financieras ante el fraude electrónico
- El perfil del defraudador global
- Perspectivas de la pequeña empresa en España
- II Termómetro del Mercado de mediana empresas en España

PREPARADOS, LISTOS, ¡YA!

PARA LA TRANSFORMACIÓN DIGITAL

Ser líder requiere de esfuerzo, innovación, experiencia, calidad y del mejor equipo de profesionales.

En GMV llevamos 30 años entrenando en los mercados más evolucionados tecnológicamente, para conseguir aportar soluciones avanzadas a empresas que desean utilizar la tecnología como vehículo para transformar digitalmente su negocio.

GMV, LIDERANDO LOS PROCESOS DE TRANSFORMACIÓN DIGITAL DEL SECTOR FINANCIERO, SANIDAD, CIBERSEGURIDAD, AAPP Y GRANDES EMPRESAS.

GMV
OFICINAS CENTRALES
Isaac Newton, 11 P.T.M. 28760 Tres Cantos Madrid

www.gmv.es marketing.TIC@gmv.com

www.facebook.com/infoGMV
@infoGMV_es

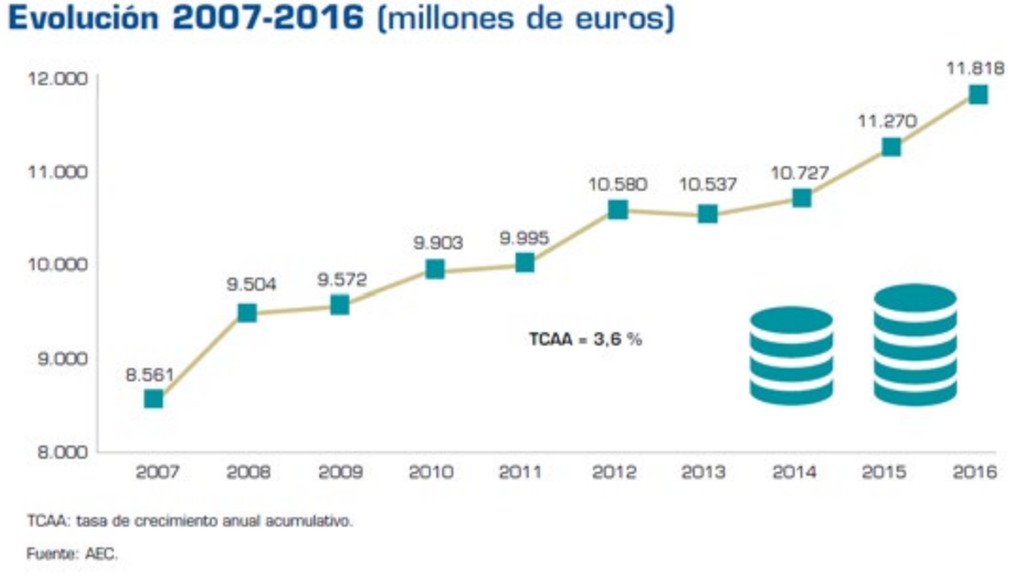
gmv®
INNOVATING SOLUTIONS

AERONÁUTICA I ESPACIO I DEFENSA I SANIDAD I CIBERSEGURIDAD I TRANSPORTE I TELECOMUNICACIONES I TECNOLOGÍAS DE LA INFORMACIÓN

El negocio de la consultoría creció un 4,9% en 2016 gracias al incremento del mercado nacional

El mercado interior empuja los datos del negocio de consultoría en 2016

Por tercer año consecutivo, el negocio de la consultoría en España se ha incrementado, en este caso un 4,9%, hasta alcanzar una facturación de 11.818 millones de euros, según se desprende del informe anual La consultoría española. El sector en cifras en 2016, que ha hecho público la Asociación Española de Empresas de Consultoría (AEC).



Evolución de los ingresos del negocio de la consultoría (en miles de millones)

Elaborado a partir de la información proporcionada por las principales empresas de consultoría que operan en España, el informe refleja que, por tercer año consecutivo, el negocio de consultoría en nuestro país se ha incrementado, y las previsiones apuntan a que el crecimiento para 2017 será algo superior, pudiendo alcanzar el 5,5%.

Al hilo de estas cifras, la presidenta de la AEC, Elena Salgado, se mostraba satisfecha por lo que definía como una tendencia positiva. Para Salgado, además de los datos del propio negocio de la consultoría, conviene recordar "el

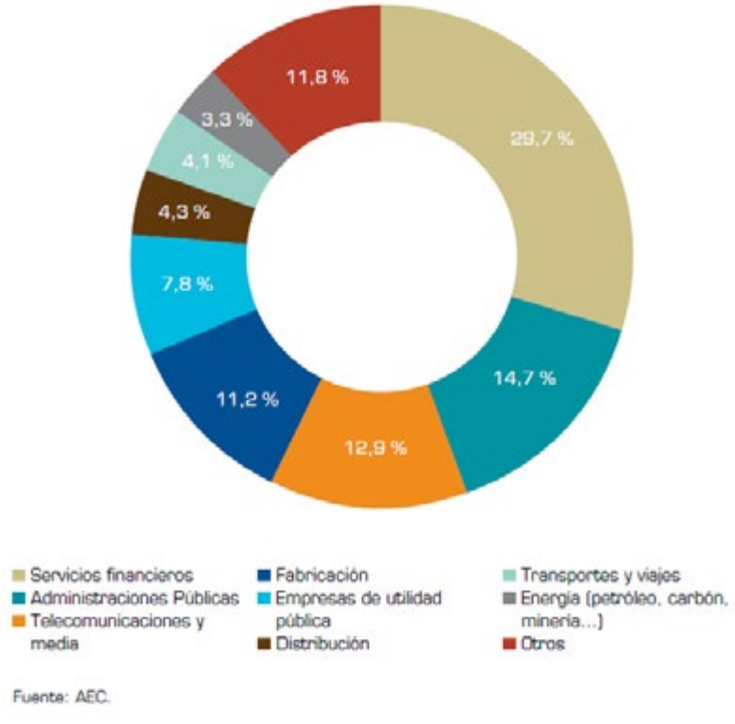
efecto multiplicador" qué ésta tiene sobre el crecimiento de las empresas.

Destacaba Salgado, además, que el incremento del negocio este año se apoya, principalmente, en el incremento del negocio interior, dado que la cifra de negocio exterior, 3.146 millones, ha sido muy similar a la de los últimos años. En este sentido, preguntada por IT User, señalaba que "tiene mucho valor que, en un contexto de ralentización de la economía latinoamericana, la consultoría española siga manteniendo un nivel de ingresos estable".

Volviendo al negocio doméstico, éste se ha incrementado un 6,5% hasta los 8.672 millones de euros, lo que eleva la cifra acumulada hasta los 11.818 millones de euros, frente a los 11.270 de 2015. Si miramos la última década, en 2007 el negocio de la consultoría alcanzó los 8.561 millones, lo que supone un incremento anual acumulado del 3,6 por ciento, años de crisis económica incluidos, para llegar a los datos actuales.

Tal y como lo analizan desde la asociación, el ejercicio de 2016 evidencia la consolidación de una etapa de expansión, que se diferencia de otras etapas anteriores en que las tasas de crecimiento son más moderadas que antes de la crisis, que el incremento tiene su base especialmente en el mercado español y que la productividad del sector aumenta ligeramente.

Evolución de los puestos de trabajo en el sector de la consultoría



Distribución de los ingresos de consultoría en 2016 por sector de actividad

El ejercicio de 2016 evidencia la consolidación de una etapa de expansión, que se diferencia de otras etapas anteriores en que las tasas de crecimiento son más moderadas que antes de la crisis

A nivel de empleo, también son positivos los números que maneja la asociación, dado que la cifra de empleados se situó en 150.547 profesionales, un 4,4% más que el año anterior. Se trata de otra cifra que ha ido creciendo de forma más o menos significativa desde 2009. De hecho, destacan desde la ACE, el papel de las consultoras como origen de empleos de calidad brilla entre el conjunto de sectores intensivos en conocimiento, que son los que se han mostrado más resistentes a los efectos de la crisis.

Así, el sector invirtió en torno a 48 millones de euros en formación de empleados, lo que supone una inversión por empleado de 319 euros, dato muy por encima de los 94 euros invertidos de media por las empresas en España.

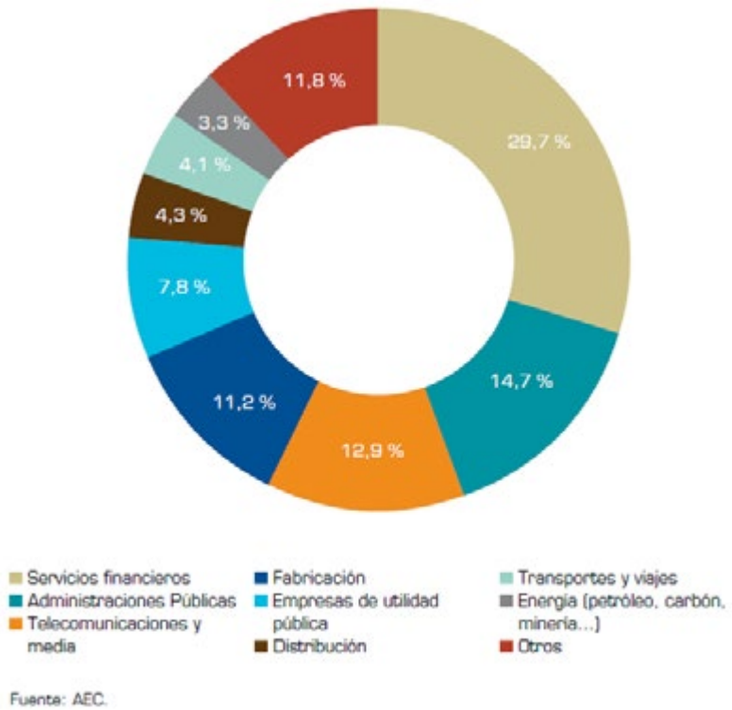
Distribución de ingresos

Tres son las partidas en las que la AEC reparte el total de los ingresos en el negocio de la consultoría en nuestro país. Por un lado, y como partida más importante, Outsourcing o TI as a Service, que supone el 44,8% del negocio, un porcentaje similar al que viene suponiendo en los últimos años. Le sigue el desarrollo e integración, que concentra el 37,2% del negocio, porcentaje al que ha descendido desde porcentajes superiores al 42% desde finales de la década pasada. Por último, consultoría, que sube levemente hasta alcanzar un 18% del total del negocio.

Si nos fijamos en los datos de los diez últimos años, la consultoría ha crecido a ritmos del 1,1% anual, desarrollo e integración al 5,1% y outsourcing el 8,8%.

Por sectores, la principal partida viene proporcionada por los servicios financieros, que suponen el 29,7% del total, seguidos por la Administración Pública con el 14,7%, Telecomunicaciones y Media con

En 2017 el negocio podría crecer un 5,5% hasta situarse en niveles cercanos a los 12.500 millones de euros



Distribución de los ingresos de consultoría en 2016 por tipo de servicio

el 12,9%, Fabricación con el 11,2%, Empresas de utilidad pública con el 7,8%, Distribución con el 4,3%, Transportes y viajes con el 4,1%, y Energía con el 3,3%, quedando un 11,8% restante para el resto de sectores productivos.

El peso de estos servicios financieros ha ido incrementándose levemente desde el año 2004, siendo Administración Pública el segundo sector en este tiempo, si bien tuvo un peso mucho más significativo en el cambio de década, y cierra el podio Telecomunicaciones y Media, que tras un repunte en torno a 2010 y 2011, vuelve a presentar un peso similar al de los últimos años.

Previsiones para 2017

Justo en el ecuador de este ejercicio, y tras presentar los datos de 2016, la AEC ha querido mostrar sus previsiones para 2017, un año en el que el negocio podría crecer un 5,5% hasta situarse en niveles cercanos a los 12.500 millones de euros.

Por líneas, Outsourcing seguiría siendo la más significativa, con un 43,5%, seguida de desarrollo e integración, con un 37,4%, y consultoría, con un 19,1%. En cuanto a los sectores, la previsión es similar a los datos de este año, con servicios financieros, Administración Pública y Telecomunicaciones y Media como las tres primeras fuentes de ingresos.

Enlaces relacionados

- Asociación Española de Empresas de Consultoría
- La consultoría española 2016. El sector en cifras

Accelerating next

Hewlett Packard Enterprise

¿Por qué elegir?
Con HPE Flexible Capacity puede tenerlo todo

HPE Flexible Capacity es un servicio que ofrece las ventajas económicas del modelo de “pago por uso” y la escalabilidad de la nube pública en su propio centro de datos.

Para más información puede consultar el informe de IDC sobre Modelos de consumo de TI

Descargar informe

El mundo sufre el segundo ciberataque masivo en mes y medio

De WannaCry a Petya: cómo el ransomware puede 'paralizar el mundo'

Un ransomware ha vuelto a poner en jaque a organizaciones de todo el mundo. Se trata de Petya, un ciberataque que, al igual que WannaCry, secuestra los ordenadores para exigir, más tarde, el pago de un rescate en bitcoins. Pero, ¿cómo funciona? ¿Cómo nos podemos proteger?

Un mes y medio después de que WannaCry mostrase el poder del ransomware para paralizar el mundo (afectó a grandes empresas como Telefónica, Renault, PetroChina, Nissan o Hitachi, además de a servicios esenciales como el sistema de salud del Reino Unido o 4.000 instituciones de educación de China), llega un nuevo ciberataque a escala global. Se trata de Petya, otro ransomware que utiliza técnicas similares a WannaCry (secuestra los ordenadores y exige el pago de un rescate de 300 dólares) que ha atacado a empresas de todo el mundo, entre las que se encuentran Maersk, Rosneft, Mondelez o Merck. No obstante, ha sido Ucrania, el país que se ha visto más afectado (ha atacado a sus infraestructuras críticas, como aeropuertos, el metro de Kiev, la compañía estatal de energía o el Banco Nacional).

Ninguna empresa española afectada

Petya no ha afectado ni al sector público ni a ninguna empresa estratégica española. Así lo ha hecho saber el CCN-CERT, quien no obstante reconoce que sí que se han visto afectadas multinacionales con sede en España.

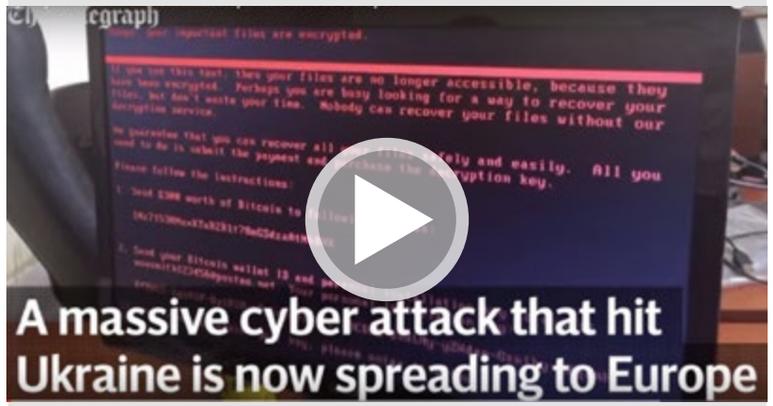
¿Te avisamos del próximo IT User?

"El código dañino utilizado es más sofisticado que en el caso de WannaCry y, en esta ocasión, podría tratarse de un ataque más dirigido ya que la detección inicial del mismo fue localizada con una rápida expansión posterior", asegura el Centro Criptológico Nacional. Además, "da la sensación de que el agresor no parece pretender obtener un beneficio económico, sino perjudicar a las víctimas, ya que no ha adoptado las medidas habituales para conseguir el anonimato y la disponibilidad del servicio de cobro propia de otras campañas de cibercrimen".

Cabe señalar que el proveedor de servicio de Internet ha bloqueado la dirección de correo utilizada para el pago del rescate, por lo que las víctimas no pueden obtener las claves de recuperación al inhabilitar la vía de comunicación con el atacante.

Los sistemas operativos objetivo son los sistemas Windows. En este sentido, Microsoft asegura en un blog que sólo en Ucrania se han visto afectadas más de 12.500 ordenadores. "Posteriormente hemos observado ataques en otros 64 países entre los que se incluyen Bélgica, Brasil, Alemania, Rusia y Estados Unidos.

EL CIBERATAQUE DE PETYA SE EXTIENDE POR EUROPA



CLICAR PARA VER EL VÍDEO

La multinacional estadounidense afirma que esta variedad de ransomware es más sofisticada que las anteriores y explica que ya ha lanzado parches de seguridad para proteger a los equipos. "Las actualizaciones ya están disponibles en todos nuestros productos anti-malware, incluidos Windows Defender Antivirus y Microsoft Security Essentials".

¿Similar a WannaCry?

"Este brote no parece ser tan grande como WannaCry pero el número de organizaciones que han sido afectadas es considerable. Según los datos que tenemos hasta ahora, parece que se está usando el mismo método de propagación que WannaCry. Cualquiera que ejecute sistemas operativos que no hayan sido parcheados con motivo de la aparición de WannaCry, podría ser vulnerable a este ataque", destaca Raj Samani, Head of Strategic Intelligence en McAfee LLC.

Kaspersky Lab, por su parte, considera que este ransomware no es una variante de Petya, sino "un nuevo ransomware que no se ha visto antes" al que ha bautizado como NotPetya. "Nuestros datos de telemetría

Petya ha atacado a empresas de todo el mundo, entre las que se encuentran Maersk, Rosneft, Mondelez o Merck.

El impacto económico de los ciberataques se prolonga en el tiempo

El riesgo de ser víctima de un ciberataque crece. No hay más que ver que, en poco más de mes y medio, se han producido dos ciberataques a nivel global: WannaCry, el pasado mes de mayo, y Petya, ayer mismo.

Lloyd´s advierte de las consecuencias que puede tener ser víctima de un ciberataque, entre las que se encuentran la pérdida de clientes, la caída de acciones o el pago del rescate de los archivos, si se ha sido víctima de un ciberataque como los anteriormente mencionados.

A pesar de esto, las empresas europeas no son conscientes de las consecuencias que puede conllevar ser víctima de un ciberataque. "Hay una falta de comprensión de lo que pueden significar los ataques cibernéticos", ha asegurado a Reuters Inga Beale, directora ejecutiva de Lloyd´s en Londres. "Las empresas necesitan estar preparadas para los costes totales que conlleva ser víctima de un ataque de este tipo".

Un ejemplo de las consecuencias que puede tener un ciberataque lo encarna la compañía británica TalkTalk, la cual sufrió una brecha de seguridad que le costó 52 millones de dólares, a los que se les une otros 44 millones de dólares que tuvo que afrontar "a largo plazo". Lloyd´s explica en su informe que los costes van más allá de los primeros días y se prolongan en el tiempo.

Más allá de ataques como WannaCry o Petya, Lloyd´s advierte del incremento de ciberataques que están "enmascarados" en correos electrónicos de directivos de las compañías a los departamentos financieros, los cuales están causando importantes pérdidas económicas al desencadenar "pagos fraudulentos".

indican que, hasta la fecha, el ataque ha afectado a unos 2.000 usuarios. Las organizaciones de países como Rusia y Ucrania han sido las más afectadas. Además, hemos registrado impactos de este ataque en Polonia, Italia, Reino Unido, Alemania, Francia, Estados Unidos, España y en otros países".

Ataques cada vez más comunes

"Este último ciberataque de ransomware es solo otro ejemplo de las amenazas reales que afectan a empresas, administraciones públicas y países de todo el mundo. Estos ataques están siendo cada vez más agresivos, dirigiéndose a servicios que afectan a la actividad cotidiana de las personas, tales como salud, servicios postales o transporte. Puede parecer que pedir 300 dólares por liberar los datos cifrados no es tanto, pero, sin duda, esta cantidad va a ir aumentando muy rápidamente. El aspecto más preocupante es cómo estos ataques están impactando en infraestructuras críticas. No hay una solución sencilla para erradicar el ransomware, pero sería necesario poner en marcha las acciones necesarias para poder determinar quién está detrás de cada ataque", destaca Álex López, director general de F5 Networks España.

WannaCry o Petya no van a ser casos aislados. "A medida que nos orientamos hacia un mundo de dispositivos conectados y dependientes de las aplicaciones, el área en la que pueden producirse este tipo de ataques es cada vez mayor. Esto proporciona a los hackers más oportunidades para tener éxito en sus actividades. Se necesita un mayor foco en la protección de las aplicaciones y de los datos. Además, por supuesto, de una mayor educación de la gente en todo lo relacionado con la ciberseguridad".

Cómo funciona

A grandes rasgos, este ransomware puede sobrescribir el registro de arranque principal, también conocido como registro de arranque maestro (MBR) del sistema afectado con el fin de bloquear el acceso a los usuarios, y puede llegar a las víctimas que

Este ransomware puede sobrescribir el registro de arranque principal, también conocido como registro de arranque maestro (MBR) del sistema afectado con el fin de bloquear el acceso a los usuarios

utiliza un servicio de almacenamiento cloud legítimo (en este caso lo hace a través de Dropbox).

El equipo de investigación de Trend Micro ha observado que no se trata de la primera vez que el malware abusa de un servicio legítimo para su propio beneficio; sin embargo, ésta es la primera vez (desde hace un largo período de tiempo) que provoca la infección por crypto-ransomware. También es una desviación de la cadena de infección típica, en la que los archivos maliciosos están asociados a mensajes de correo electrónico o alojados en sitios maliciosos y son entregados por kits de exploits.

Check Point explica que los hackers utilizan Loki Bot para el robo de las credenciales. "Nuestro análisis muestra que Petya se propaga lentamente, explotando las vulnerabilidades de las PYMES".

El CCN-CERT destaca que Petya, que se propaga a través de mensajes de correo electrónico, puede explotar una vulnerabilidad de Microsoft Office para propagarse a través de infecciones en las carpetas compartidas en la red de la organización afectada. "Además, intenta utilizar las vías de infección del exploit que aprovecha la vulnerabilidad de Microsoft MS 17-010. En el caso de que el sistema estuviera parcheado ante esta vulnerabilidad, el malware utiliza una alternativa basada en la ejecución de la aplicación propietaria del sistema Windows "Psexec" en carpetas compartidas sobre el sistema víctima".

Cómo protegerse

Como medidas de prevención y mitigación, InnoTec recomienda actualizar el sistema operativo y todas las soluciones de seguridad, así como el cortafuegos personal habilitado; utilizar sólo protocolos seguros en los accesos administrativos desde fuera de la organización; mantener una conducta de navegación segura, empleando herramientas y extensiones de navegador web completamente actualizado; activar la visualización de las extensiones de los ficheros para evitar ejecución de código dañino camuflado como ficheros legítimos no ejecutables; y deshabilitar las macros en los documentos de Microsoft Office y otras aplicaciones similares. En el caso de haberse visto afectados por esta campaña y no dispusieran de copias de seguridad, se recomienda "conservar los ficheros que hubieran sido cifrados por la muestra de ransomware antes de desinfectar la máquina, ya que no es descartable que en un futuro apareciera una herramienta que permitiera descifrar los documentos que se hubieran visto afectados". it

Enlaces relacionados

- Cómo sobrevivir al ransomware cifrado
- Soluciones tecnológicas frente al fraude financiero
- Big Data, un gran aliado contra el fraude bancario
- Ataques con exploits. De las amenazas diarias a las campañas dirigidas
- La paradoja tras la experiencia del usuario con el Criptornsomware

Tecnología para tu Empresa

Encuentra en este centro de recursos de IT User las últimas propuestas tecnológicas para hacer que tu empresa funcione.

Algunos de los documentos que podrás leer son:

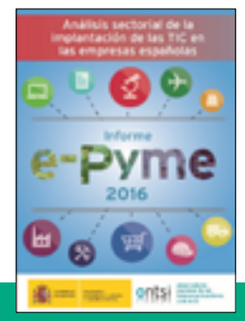
Patrocinado por: Hewlett Packard Enterprise · intel

>> 15 ideas para la transformación digital de tu negocio >>

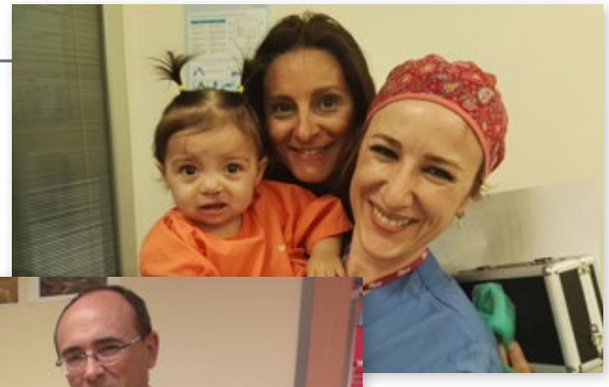
>> Análisis estratégico para el desarrollo de la Pyme en España >>

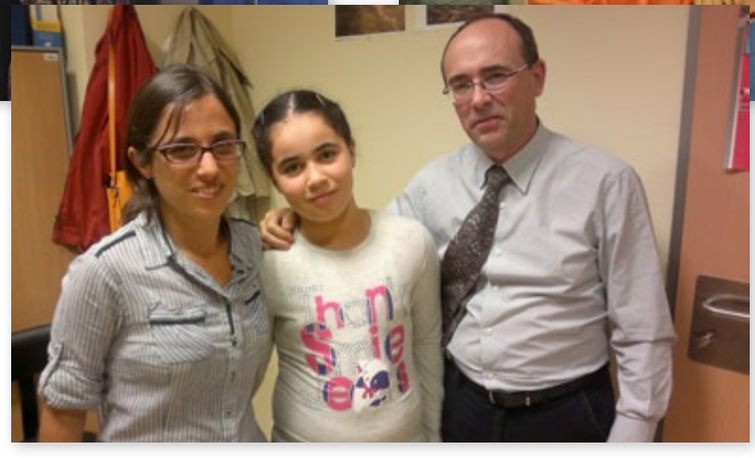
>> Inspiración para pymes: innovar para ahorrar tiempo y dinero >>

>> Informe e-Pyme 2016 >>



No son solo médicos





Muchas veces hablamos de los personajes anónimos que dan su tiempo o su dinero por una buena causa, y que son responsables directos de aliviar un problema o colaborar en la resolución de un problema. Pero, en esta ocasión, Samira Brigüech, presidenta de la Fundación Adelias, quiere poner el foco sobre el personal médico que lleva ya varios años aportando su tiempo, su conocimiento y su esfuerzo al trabajo que hace la fundación.

No son solo médicos, son unos seres que reparan lo físico y los dolores del alma. El dolor que produce estar sufriendo por una enfermedad que no tienen medios para pagar y curarse. Son los médicos y enfermeras de Sanitas que cumplen 8 años donando su talento, su tiempo, su conocimiento y su cariño a miles de niños sin recursos.

Vamos a conocerlos un poco mejor, ahora que cumplimos 10 años y 10.000 niños diagnosticados.

Dr. Jiménez, Jefe del Servicio de Pediatría del Hospital de la Moraleja. Por sus manos han pasado cientos y cientos de niños. Con enfermedades raras, con dolencias que no les dejaban caminar, oír, hablar, ir al baño o simplemente respirar con normalidad. Es uno de los líderes del Pasillo Verde humanitario que Sanitas ha construido con nuestra Fundación.

Ejecutivo, pediatra, padre, un ser humano que ha luchado para arrojar luz sobre cientos de casos com-

Fundación Adelias

La Fundación Adelias nace de la mano de empresarios, ejecutivos de multinacionales 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

plejos, de niños que hoy viven su vida alejados de un padecimiento permanente.

Dr. Larraya, Jefe del Servicio de Cardiología Pediátrica de Sanitas y de la Paz. Un cardiólogo especializado en cardiopatía congénita y que ha colaborado activamente a arrancarle al destino la vida de muchos niños que hoy no tendrían voz en nuestro mundo.

No solo ha valorado, diagnosticado y medicado a cientos de cardiópatas, sino que también ha realizado cateterismos a muchos pequeños que vivían encerrados en una burbuja por riesgo a una muerte prematura. Un médico con una agenda abarrotada de compromisos y que siempre encuentra el momento para meterse en el quirófano con fines humanitarios.

Dr. Greco, cirujano cardiaco, especializado en cardiopatía congénita. Ha operado a decenas de bebés y niños a corazón abierto, a menudo durante 5-6 horas. Enmendando sus corazones rotos y aliviando un sufrimiento extremo. Dándoles la extraordinaria oportunidad de correr, saltar, ir al cole… en resumen, de Vivir, con mayúsculas, una infancia que el destino les quería arrebatar.

No son solo médicos, son unos seres que reparan lo físico y los dolores del alma. El dolor que produce estar sufriendo por una enfermedad que no tienen medios para pagar y curarse

Dra. Arias. Jefa del Servicio de Pediatría del Hospital de la Zarzuela. Una mujer líder, comprometida con los niños más vulnerables, los que viven en una pobreza tal que hasta la vida se les escapa con cada respiración. Ella ha conseguido analizar y valorar casos de niños y adolescentes que ya no deseaban vivir con la carga de su enfermedad. Ha luchado por ellos, involucrando a decenas de especialistas de Sanitas para combatir con la ciencia y una enorme voluntad, unas enfermedades crueles.

Dra. Petersen. Una ginecóloga cuya misión es ayudar a que los bebés nazcan en las mejores condiciones físicas para tener un desarrollo normal. Que cuida a las madres para que sus embarazos progresen sin riesgos y la nueva vida que traen al mundo no llegue con una maleta cargada de problemas. Ha ayudado con su tesón y dedicación a cumplir muchos de los objetivos que nos marcamos con los recién nacidos de las familias más humildes

Dr. Lujan. Pediatra Nefrólogo que ha tratado a cientos de niños con problemas de riñón. Les ha ayudado combatiendo su dolor mediante cirugía, tratamientos locales y dándoles pautas para aliviar su sufrimiento físico y el social, ése que te estigmatiza cuando no controlas tus esfínteres, pero aun así tienes que ir al colegio y hacer como que no pasa nada.

Dr. López. Cardiólogo infantil del Hospital de la Zarzuela. Un hombre fuerte que ha lidiado con decenas de casos sobrecogedores por lo que ha luchado, infatigablemente, para mejorar su salud y arrancar esa sonrisa que tanto les gusta a los médicos ver después de tantos meses de sufrimiento.

Dra. Urcelay. Una especialista en ciruguía plástica y cirugía reparadora. ¿Qué le pasa a la vida un niño cuando su carita, sus labios, su nariz o sus ojos son defor-

mes? ¿Qué pasa, además, cuando eres muy pobre y la prioridad no es que tu aspecto sea normal? Pero sí la pierden un poquito cada día que se miran en el espejo, o en el patio en el colegio cuando te señalan con el dedo. La Dra. Urcelay ha hecho extraordinarias cirugías reparadoras y estéticas para que muchos niños puedan mirarse a sí mismos sin rechazarse. Una mezcla de ciencia, tecnología y tesón han conseguido unos resultados extraordinarios.

Dres. Sanz y Martí. Piernas rotas, caderas destrozadas, pies despedazados por el paso de un furgón sobre sobre ellos. Un trabajo duro para un equipo de traumatólogo y cirujano que ha conseguido que muchos niños vuelvan a caminar. A veces con una cirugía no es suficiente, hay que volver y volver a operar porque las secuelas de los accidentes son terribles. Ellos son los artífices de que haya menos niños minusválidos pululando por el mundo.

Dr. Rodriguez de Alarcón, un cirujano con un talento extraordinario para operar a niños con terribles do-

lencias en los riñones y genitales que hacían de su vida un auténtico infierno físico y anímico. Un hombre que se ha comprometido durante años con niños que jamás podrían abonar sus honorarios, cirugías enormemente complejas y que requieren el máximo compromiso médico y humano. Nos ha donado su excepcional talento, su tiempo y una bondad que ha permanecido durante 8 largos años.

El Dr. German Blanco, un hombre que ha lidiado con adolescentes con mamas de 25 kilos, que les provocaban dolores de espalda, dificultad de movimiento, auto-rechazo físico y a veces terribles deseos de suicidio ante la falta de esperanza de verse como niñas normales. Un hombre que ha luchado durante años con una dedicación titánica para salvarlas de su propio destino.

Las enfermeras. Esos seres mágicos que son la clave de la recuperación de cualquier niño, que hacen curas, administran la medicación, se aseguran de que los niños estén bien alimentados y puedan salir por su propio pie. Son las responsables directas de que los pequeños pacientes reciban toda la atención para su recuperación, son esas personas que siempre están entrando y saliendo de las habitaciones preguntando "¿qué tal estamos hoy?"… y se enciende la luz.

Y hay otros muchos más especialistas, porque la lista acaba en el aire de larga que es…

¿Quieres colaborar?

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

¿Te ha gustado este reportaje?

Compártelo en tus redes sociales

Twitter Facebook LinkedIn beBee

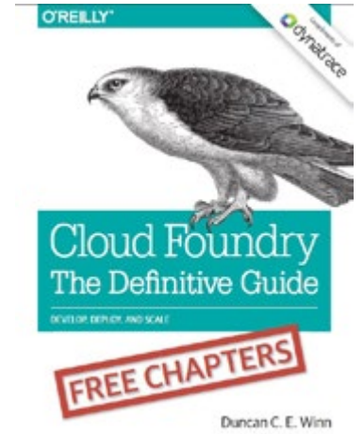
Enlaces relacionados

Fundación Adelias

Internacionalización de Startups Españolas de Base Tecnológica

Empresas como Uber o Airbnb, por citar las más famosas, se han convertido en algunas de las mayores exportadoras de servicios mundiales, generando ingresos millonarios. El Informe de Internacionalización de Startups Españolas de Base Tecnológica elaborado por IE Business School, mide el ritmo y los destinos de las startups españolas, muchas de las cuales se pueden llamar directamente empresas tecnológicas debido al tamaño e importancia que han adquirido a la hora de internacionalizarse y exportar sus servicios.

Guía sobre Cloud Foundry



Disponer de una plataforma cloud nativa es la opción por la que se están decantando las empresas que quieren desarrollar y entregar software de forma rápida y constante. Este informe explica las capacidades de las plataformas cloud nativas y examina los cambios fundamentales que las empresas deben acometer en sus procesos, organización y cultura si quieren aprovechar este planteamiento. Presta especial atención a la plataforma de código abierto Cloud Foundry, una de las más prominentes en el mercado.
Descarga este documento y conoce cómo las aplicaciones cloud nativas están diseñadas para ser "agnósticas a la infraestructura", por lo que pueden prosperar y moverse a voluntad en el entorno cloud altamente distribuido y en constante evolución.

Estrategias para la implementación de infraestructura hiperconvergente

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

Análisis del éxito de las soluciones de gestión del rendimiento empresarial e Inteligencia de negocio

Las empresas que invierten en BI y en gestión del rendimiento, normalmente ven los mayores beneficios después de los dos primeros años. Para llegar a ese punto, los compradores necesitan elegir a un proveedor capaz de proporcionarle ese éxito a largo plazo. Este informe explora las principales características para obtener de la analítica valor tanto a corto como a largo plazo.

La Documentación TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

Hewlett Packard Enterprise | intel

Reimagine 2017

Transformación Digital, de la teoría a la práctica

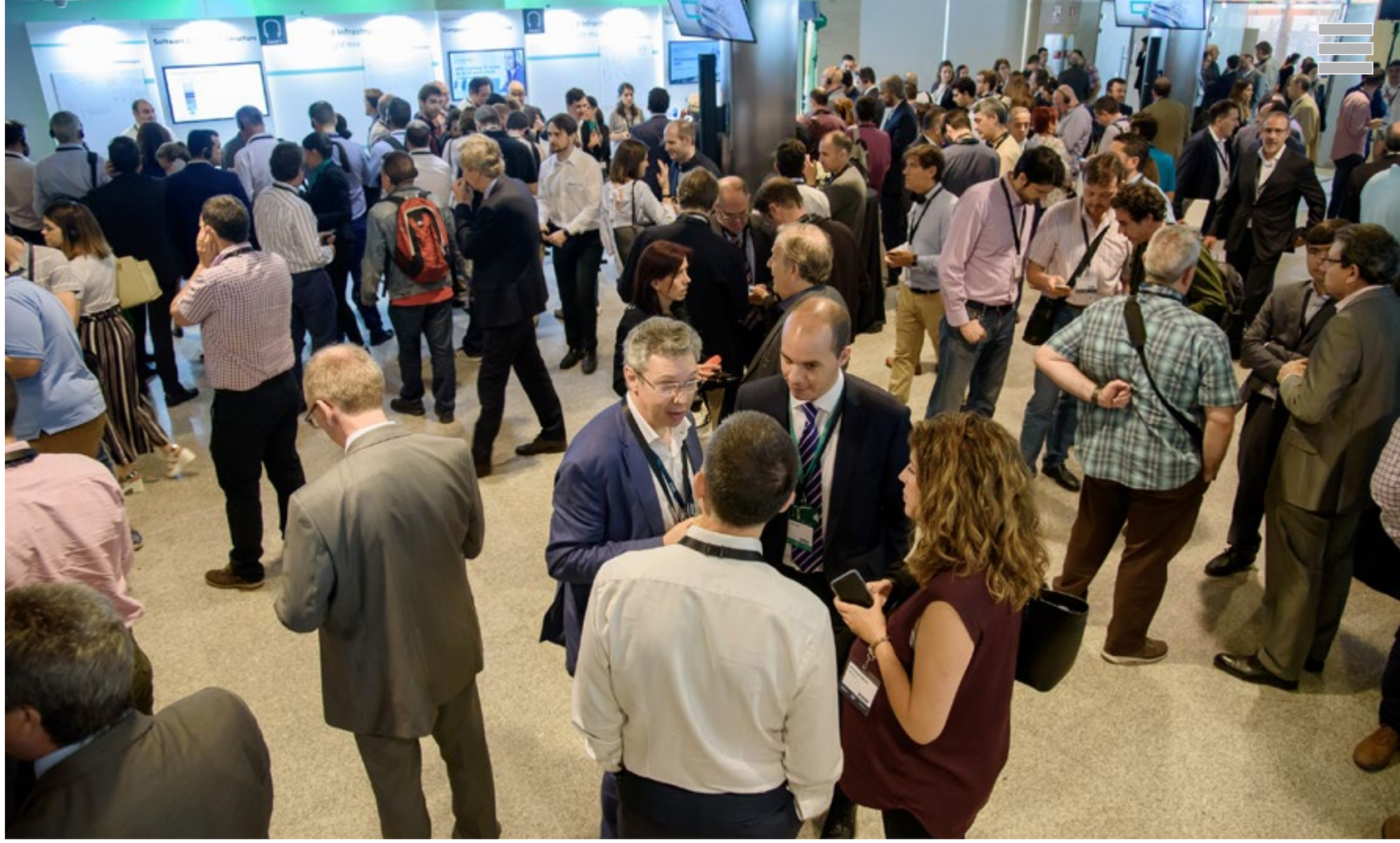
Reimagine 2017: Transformación Digital, de la teoría a la práctica

Hybrid IT: La base tecnológica para la Transformación Digital

IoT: Convirtiendo el desafío en oportunidades

Servicios IT: Simplificando la transformación

HPE celebró en el Santiago Bernabéu una nueva edición de Reimagine, un evento en el que quiso mostrar cuál es su estrategia para ayudar a las empresas en sus procesos de Transformación Digital, una estrategia que se articula sobre tres pilares: tecnología híbrida, servicios IT e Internet de las Cosas, y cómo se implementan en el mundo de los negocios.



Reimagine 2017: Transformación Digital, de la teoría a la práctica

Y es que, y tal y como destacó José María de la Torre, Managing Director HPE VP & General Manager Enterprise Group Iberia, "nos encontramos en medio de un proceso de cambio el cual ofrece numerosas oportunidades". De la Torre aprovechó su intervención para señalar que "la Transformación Digital es también una transformación de la sociedad y cualquier estrategia tiene que pensar en su cliente" y recordó que "el futuro es para los más rápidos y para los que mejor se adapten a los cambios".

En este sentido, José María de la Torre remarcó la importancia que está adquiriendo el dato, "el elemento más disruptivo de la Transformación Digital". Nos encontramos en un momento "de explosión del dato" con las oportunidades que eso significa. "La

“La Transformación Digital es también una transformación de la sociedad y cualquier estrategia tiene que pensar en su cliente”

José María de la Torre, Managing Director HPE VP & General Manager Enterprise Group Iberia

explosión de los datos no sólo es evidente, es imparable y se supera día tras día”. Asimismo, recordó que “en tecnología no hay que buscar reducción de costes inmediata sino optimización, el aumento de capacidades y el retorno de la inversión”.

En este punto, José María de la Torre aseguró que “el mundo será híbrido” y que su compañía está invirtiendo “para facilitar a las empresas la tecnología híbrida”. La estrategia de Hewlett Packard Enterprise “se apoya en tres pilares: un mundo y una TI híbrida, con inteligencia en el extremo y un papel de los servicios cada vez más crítico”. En el apartado de los servicios, tanto De la Torre como otros directivos de HPE explicaron cuáles son los beneficios de HPE Pointnext, la nueva organización de servicios de la compañía que, aunque nueva, “cuenta con un bagaje de más de 75 años de experiencia”. Es más “lideramos el ranking de satisfacción de cliente en España”. IoT es otra de las grandes tendencias del mercado y, para José María de la Torre, es imperativo “empezar a desarrollar la TI del IoT”.

HPE “articula la Transformación Digital alrededor de las soluciones”, aseguró José María de la Torre, quien también hizo hincapié en la importancia de las asociaciones. “Es el momento de establecer alianzas para facilitar la Transformación Digital”. Es más, “para HPE, la política de alianzas es clave”.

“Queremos ser vuestros socios de confianza en la Transformación Digital y ayudaros a abordar vuestros proyectos, independientemente de la fase en la que se encuentren”, remarcó José María de la Torre, quien concluyó su intervención destacando que “sabemos muy bien hacia dónde nos dirigimos. Hemos adoptado decisiones para ser el mejor socio para las empresas”.

La TI híbrida y los servicios son, junto a Internet de las Cosas, las tres grandes áreas de futuro de HPE, tal y como se mostró durante toda la jornada de Reimagine. En el evento, también se analizaron los beneficios de las últimas adquisiciones de HPE, como Niara o Nimble, ambas enfocadas a completar la oferta de la firma y a ayudar en el objetivo de ayudar a las empresas en sus procesos de digitalización.

No se pierda ningún detalle de Reimagine 2017

La TI híbrida y los servicios son, junto a Internet de las Cosas, las tres grandes áreas de futuro de HPE, tal y como se mostró durante toda la jornada de Reimagine.

Plataforma digital

Jorge Fernández, Director de Tecnología de Hewlett Packard Enterprise, quiso mostrar la plataforma digital sobre la que la compañía quiere plantar toda su estrategia, una plataforma que se apoya en una infraestructura definida por software, tanto on premise como en modelo cloud.

Sobre esta infraestructura, piezas fundamentales, como la virtualización, la hiperconvergencia, el mundo físico (cada vez con una presencia más destacada), HDI, contenedores, sistemas operativos para el centro de datos y software en modelo cloud.

Con todo, esta plataforma se despliega sobre cuatro grandes puntos que le hacen ideal para el desarrollo hacia el futuro: análisis y Big Data, IoT, movilidad y desarrollo ágil.

Hablando de desarrollo ágil, ésta es la base sobre la que crear las nuevas aplicaciones, porque ya no podemos ver TI y aplicaciones como elementos ajenos al negocio: “Apps y TI son el negocio”, aseguraba José Antonio Fernández Modero, Responsable de Consultoría Hybrid IT.

El desarrollo de las apps, tradicionalmente, partía de la planificación y el análisis y pasaba por múltiples fases intermedias hasta llegar al despliegue, mientras que de la mano de DevOps, hablamos de un continuo entre el desarrollo, el testeo y el despliegue, reduciendo de forma considerable el tiempo hasta el despliegue, que se realiza de forma constante, con nuevas implementaciones rápidas que van mejorando el desarrollo de la aplicación, adecuándolo a las necesidades del negocio.

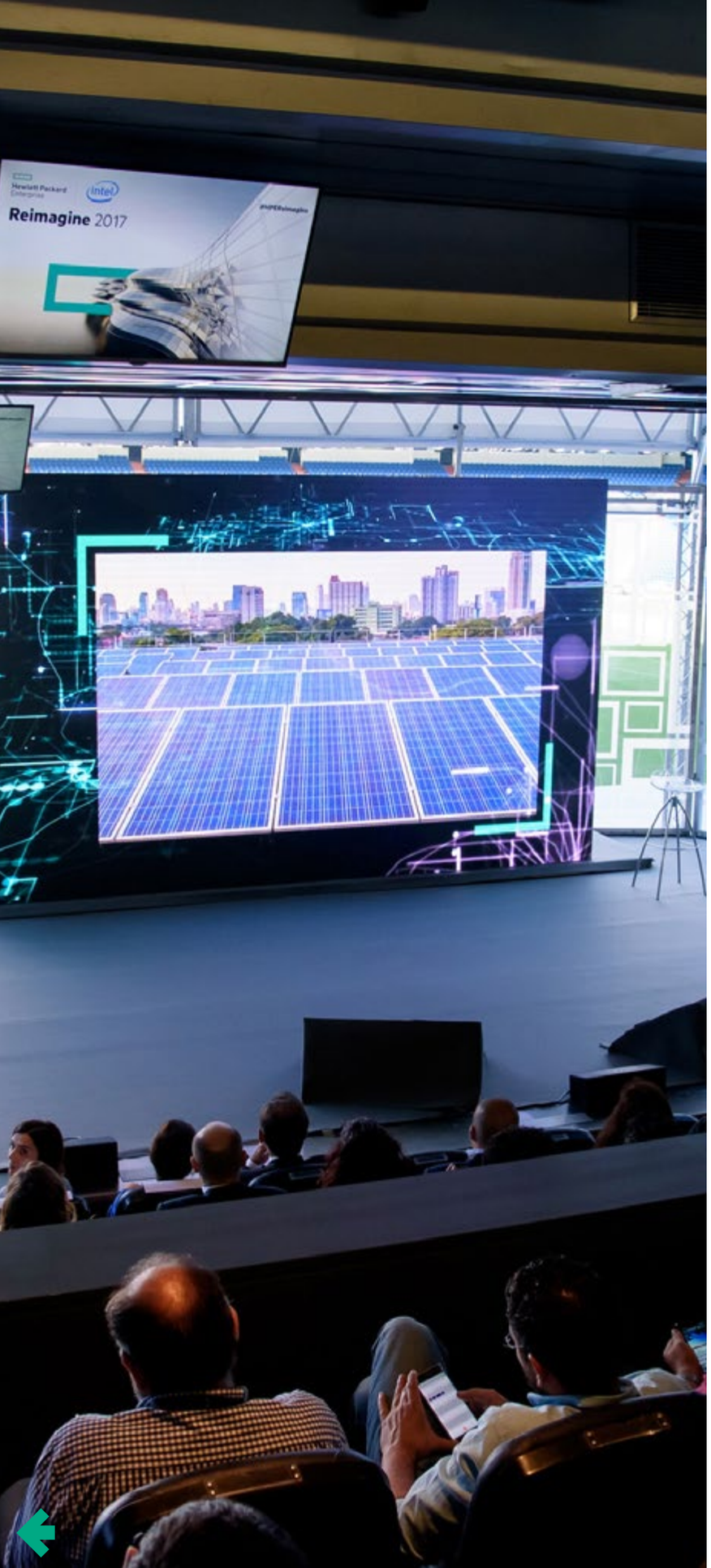
Reimaginando la infraestructura

Para poder aprovechar todas las posibilidades de las que estamos hablando, es necesario redefinir, reimaginar la infraestructura, y, partiendo de estas arquitecturas definidas por software, establecer una nueva generación de plataformas para datos y su análisis, optar por nuevos modelos de consumo flexible y abrir el ecosistema a los partners.

Eso sí, sobre esta infraestructura es necesario simplificar y automatizar muchas de las labores rutinarias, dejando tiempo y recursos liberados para poder innovar. En el caso de HPE, la base de esta automatización es OneView, la herramienta que gestiona el centro de datos definido por software. ¿Qué aporta OneView? Tres son los elementos principales: simplicidad de las operaciones, despliegue rápido y fiable de elementos sobre toda la infraestructura, e incremento de la productividad.

Infraestructura Componible

En la estrategia de Hewlett Packard Enterprise, la base de las nuevas TIC es Synergy, el primer ejemplo de su nueva Infraes-



Inteligencia Artificial: liberando la nueva ola

Carlos Clerencia, director general de Intel Iberia, explicó, durante su intervención en Reimagine, el presente y futuro de uno de los mercados en crecimiento: la inteligencia artificial. El directivo destacó que "nos encontramos invirtiendo en comunicaciones, almacenamiento y computación y explicó las bondades de algunos de sus buques insignia como la última generación de procesadores Xeon o Intel Optane".

"Estamos trabajando en un ecosistema que nos permita tener una estrategia sólida", aseguró Clerencia, quien también explicó cómo Internet de las Cosas y 5G están fomentando "la explosión del dato".

Hablando de la última novedad en la familia Xeon, se trata, en palabras de los responsables de Intel, del mayor conjunto de avances en una plataforma en una década, porque afectan tanto a la computación, la red y el almacenamiento. Los nuevos Intel Xeon ofrecen rendimiento, seguridad, agilidad y eficiencia, con elementos tales como Intel AVX-512, Intel RDT, Intel OPA, Intel QAT, e Intel VMD.

Por su parte, la Tecnología Intel Optane ofrece mejoras en la optimización del almacenamiento, reduciendo la latencia e incrementando el ancho de banda (IOPS) y la Calidad de Servicio.

Y ambas novedades son importantes porque cada día estamos inmersos en una explosión de datos, que ejemplificaba Clerencia al señalar que, si cada usuario consume 1,5 GB de información en Internet, un hospital inteligente genera 3.000 GB, un coche autónomo 4.000 GB, el vuelo de un avión 40.000 GB, o una fábrica inteligente 1.000.000 de GB.

En definitiva, una realidad que necesita un paso más allá a la hora de interpretar y analizar toda esta información. Y ahí es donde entra la Inteligencia Artificial, para cuyo aprovechamiento Intel dispone de un completo ecosistema formado por el hardware, librerías, frameworks, herramientas y experiencias de uso. Con ello, Intel espera que la Inteligencia Artificial transforme todas las industrias, desde el consumo hasta la energía, pasando por las finanzas o la salud, entre otras.

tructura Componible. Definido desde cero sobre la idea de esta infraestructura, Synergy ofrece una clara reducción del CapEx y del sobre-aprovisionamiento, simplifica las actualizaciones para facilitar el trabajo al departamento de TI, despliega en local con la rapidez y la sencillez del despliegue sobre la nube, y se adecúa perfectamente a la nueva forma de desarrollo de apps de la que hemos hablando anteriormente.

Un paso anterior, para clientes más pequeños o con necesidades más específicas, los sistemas hiperconvergentes les ofrecen un sistema pre-configurado que reduce las complicaciones, facilita el despliegue y proporciona una gestión integrada y un soporte unificado.

Pero, ¿qué ocurre cuando necesitamos sistemas críticos en nuestra infraestructura? Para esta necesidad, la propuesta de Hewlett Packard Enterprise pasa por la familia Integrity i6, con Kittson y HP-UX, o los sistemas Superdome X, sobre x86 y sistemas operativos Linux y Windows.

Almacenamiento para la nueva economía

Un elemento importante en la infraestructura tecnológica de cualquier empresa es el almacenamiento. En la estrategia de Hewlett Packard Enterprise, hablamos de dos niveles para este almacenamiento. Por un lado, el almacenamiento all-flash con los sistemas HPE 3PAR, y, por otro, el almacenamiento definido por software, con StoreVirtual y Simplivity.

HPE 3PAR ofrece los mayores niveles de rendimiento y los más altos ratios de disponibilidad, si bien ya se ha anunciado el siguiente paso en su desarrollo, con Storage Class Memory y NVMe, lo que

En la nueva economía, los usuarios reclaman nuevos modelos de consumo de tecnología que se ajusten mucho mejor a sus necesidades en cada momento

supondrá una reducción de la latencia de 16x, dejando la latencia media en la mitad, mientras que se ofrece un 80% más de IOPS.

La red del centro de datos del futuro

Básica para el funcionamiento del centro de datos es la red que lo recorre y, en el caso de Hewlett Packard Enterprise, segmenta este elemento en tres niveles o escenarios diferentes. El primero de ellos, apoyándose en la tecnología de la propia HPE y de Arista, y pensada para implementaciones cloud o SDN, cuenta con diferentes gamas de dispositivos de red, desde las series 7050 y 7060 hasta las series 7500, que ofrecen automatización, estabilidad, estandarización, visibilidad y DeepBuffer. El segundo nivel, pensado para entornos de networking abierto, lo ofrece HPE Altoline, un servidor que presenta crecimientos anuales del 20%, según Dell'Oro Group. Y, en tercer lugar, la familia HPE FlexFabric, para entornos de mediana empresa, que sigue concentrando el 85% del mercado (por unidades).

Nuevos modelos de consumo

Por último, y como capa final de toda esta tecnología para la Nueva Economía, los usuarios reclaman nuevos modelos de consumo de TI, en los que buscan la mayor calidad de servicio posible, la adecuación predictiva de la capacidad de computación a los picos y valles de demanda, la mínima o incluso nula inversión inicial, el pago según el uso que se haga de la tecnología, o una TI que se consuma como si se tratase de un servicio. ■

Enlaces de interés...

- Todas las presentaciones de Reimagine 2017
- Toda la información sobre Reimagine 2017 y la Transformación Digital

Hybrid IT:
La base tecnológica para la **Transformación Digital**

La Transformación Digital, ese camino de transformación vital que algunas empresas han iniciado y otras están a punto de iniciar, busca alcanzar un nivel de integración tal que tecnología y negocio sean uno, con lo que esto supone de cambio, tanto tecnológico como cultural para las empresas.

Y para poder avanzar hacia este horizonte, las empresas necesitan una base tecnológica que se lo permita y que, de paso, no les obligue a deshacerse de su legacy ni les fuerce a optar por determinadas opciones como únicas. La TI híbrida permite a las empresas responder a los requisitos y retos que les impone la Transformación Digital, sin por ello tener que renunciar a nada.

La TI híbrida parte de la base de confeccionar la mezcla más adecuada de recursos tecnológicos para adaptarse de la forma más eficiente posible a las necesidades particulares de una carga de trabajo, un negocio o un proyecto. Esta infraestructura debe ser, además, capaz de adaptarse en función de cómo evolucione el mercado, el contexto o la propia empresa.

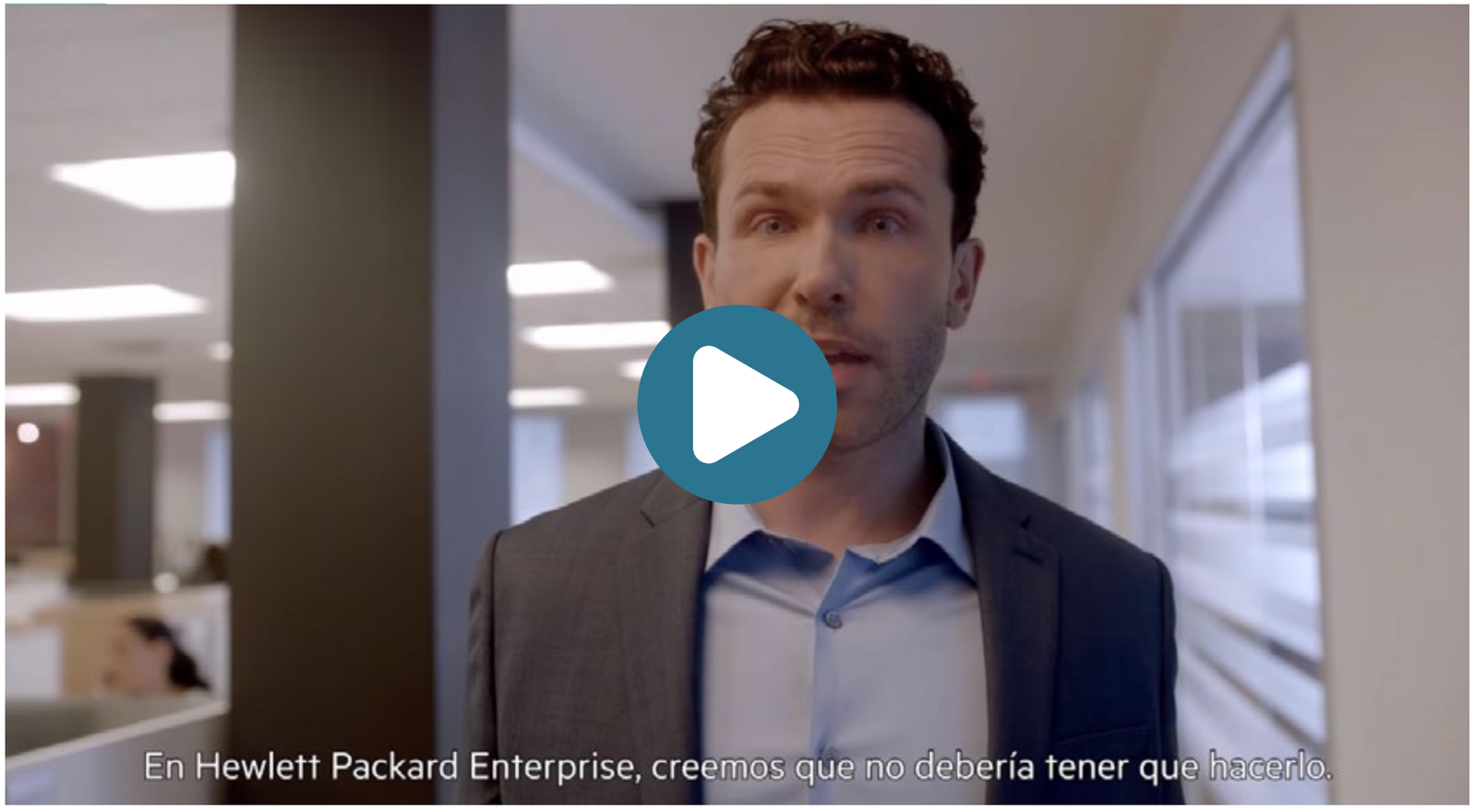
En la vida de una empresa, las cargas y los picos de trabajo son variables, tanto al alza como a la baja, y la infraestructura debe ser capaz de transformarse dinámicamente, tanto para seguir respondiendo a los retos del negocio como para no obligar a la compañía a sobredimensionar su propia infraestructura, ya sea local o en la nube.

Además, no podemos olvidar que una misma infraestructura debe ser capaz de responder a las cargas de trabajo tradicionales, basadas en operaciones y con foco en la robustez, y a las nuevas cargas de trabajo con desarrollos ágiles y basados en nuevos motores de ejecución. El concepto de Software Defined Infrastructure es crítico y una de las bases de esta adaptabilidad, pero no es suficiente, ya que se ejecuta sobre una infraestructura tradicional. Para tener una visión completa es necesario apoyarse en infraestructuras de nueva generación, como la Infraestructura Componible, que completa la fluidez de una visión SDI amoldando los recursos más esenciales a las necesidades de las aplicaciones, en tiempo real.

La nueva economía digital requiere de agilidad, nuevos modelos de consumo flexibles y una visión de plataforma única y completa. Este concepto, habitual en el cloud computing, debe trasladarse a la tecnología on-site, que es donde van a correr algunas de las cargas de trabajo.

Camino por recorrer

Desgraciadamente, la mayoría de las empresas todavía están encorsetadas en modelos tradicionales de TI, que son rígidos y complejos,



La TI híbrida parte de la base de confeccionar la mezcla más adecuada de recursos tecnológicos para adaptarse de la forma más eficiente posible a las necesidades particulares de una carga de trabajo, un negocio o un proyecto

que conllevan unos recursos sustanciales y la necesidad de gastar mucho dinero para ofrecer nuevos servicios. La complejidad de estos centros de datos inhibe la innovación y aumenta los costes, sobre todo cuando se incrementa la presión sobre el departamento IT.

Los entornos tradicionales presionan a las TI para reducir los costes operativos a la vez que simultáneamente se ajustan al nuevo entorno de aplicación para aumentar la velocidad de las operaciones. Este funcionamiento "bimodal" es insostenible para la estructura tradicional de IT, debido a su incapacidad para adaptarse instantáneamente. Para satisfacer las necesidades de ambas facetas del negocio, algunas empresas están instalando una infraestructura de IT adicional e independiente. Sin embargo, esta estrategia incurre en costes, y en la complejidad de gestionar las dos infraestructuras, ambas estáticas y propensas al sobreaprovisionamiento.

Una nueva infraestructura IT

Para competir en la economía digital es necesario una infraestructura que tenga agilidad para conseguir simultáneamente potenciar la innovación y la creación de valor para toda una nueva generación de aplicaciones, y que a la vez ejecute las cargas de trabajo tradicionales con mayor eficiencia.

Esta infraestructura puede optimizar cualquier aplicación, reducir los gastos de capital y liberar recursos, disponiendo de grupos fluidos de recursos físicos y virtuales de computación, almacenamiento y estructura; puede acelerar la entrega de aplicaciones y servicios a través de una sola interfaz que construye con precisión infraestructuras lógicas de forma prácticamente instantánea; puede reducir el esfuerzo y el coste operativo gracias a la inteligencia interna definida por software, con operaciones sin fricciones basadas en plantillas; y puede aumentar la productividad y el control en todo

Enlaces de interés...

- Todas las presentaciones de Reimagine 2017
- Toda la información sobre Hybrid IT

La nueva economía digital requiere de agilidad, nuevos modelos de consumo flexibles y una visión completa de plataforma única y completa

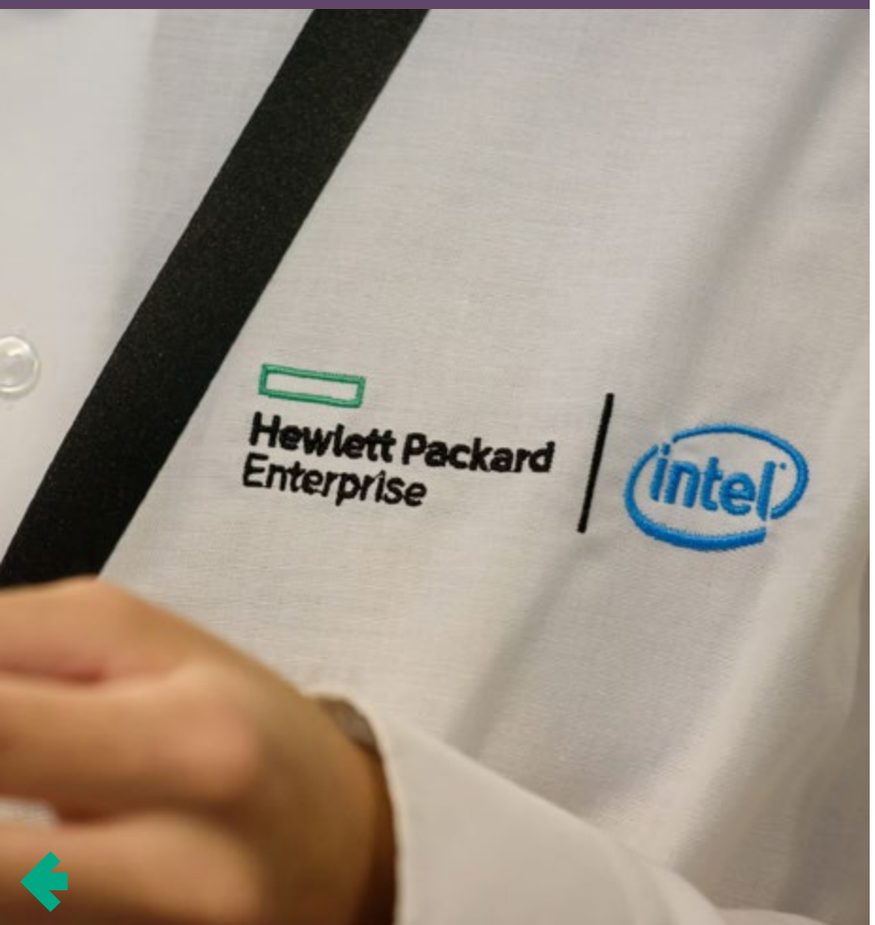
el centro de datos integrando y automatizando las operaciones y aplicaciones de infraestructura.

En definitiva, el mercado cambia muy rápidamente, creando la necesidad de nuevos productos y modelos de servicio, y cualquier cambio del negocio provoca un aumento o disminución de la complejidad de los sistemas IT que lo soportan. Un aumento en la complejidad de IT se manifiesta a través de un incremento de costes tecnológicos asociados, pero en la era de la transformación digital, además de estos costes, el verdadero impacto lo encontraremos en la flexibilidad, velocidad, escalabilidad y experiencia del usuario.

Dentro de la transformación digital, las aplicaciones tienen un papel fundamental. Los clientes y usuarios esperan un acceso fácil y rápido a sus productos, servicios e información. Las empresas deben desarrollar y brindar experiencias de usuario superiores, de las que formen parte sus clientes y su personal, y que requieran transformar lo qué se piensa respecto a la función de IT en la empresa y su funcionamiento.

El departamento IT tiene un impacto directo sobre la estrategia empresarial y sobre la entrega de productos y servicios. Si las empresas quieren la transición con éxito a la próxima era IT, no pueden permanecer inactivas en su entorno IT. Tecnologías que añaden cálculo, almacenamiento y tejido en pools compartidos, como infraestructura componible, pueden permitir al departamento de TI implementar una plataforma única adaptable a distintos tipos de aplicaciones. Esta área será capaz de maximizar la eficiencia con aplicaciones principales y ofrecer el rendimiento necesario para cargas de trabajo de última generación. ■

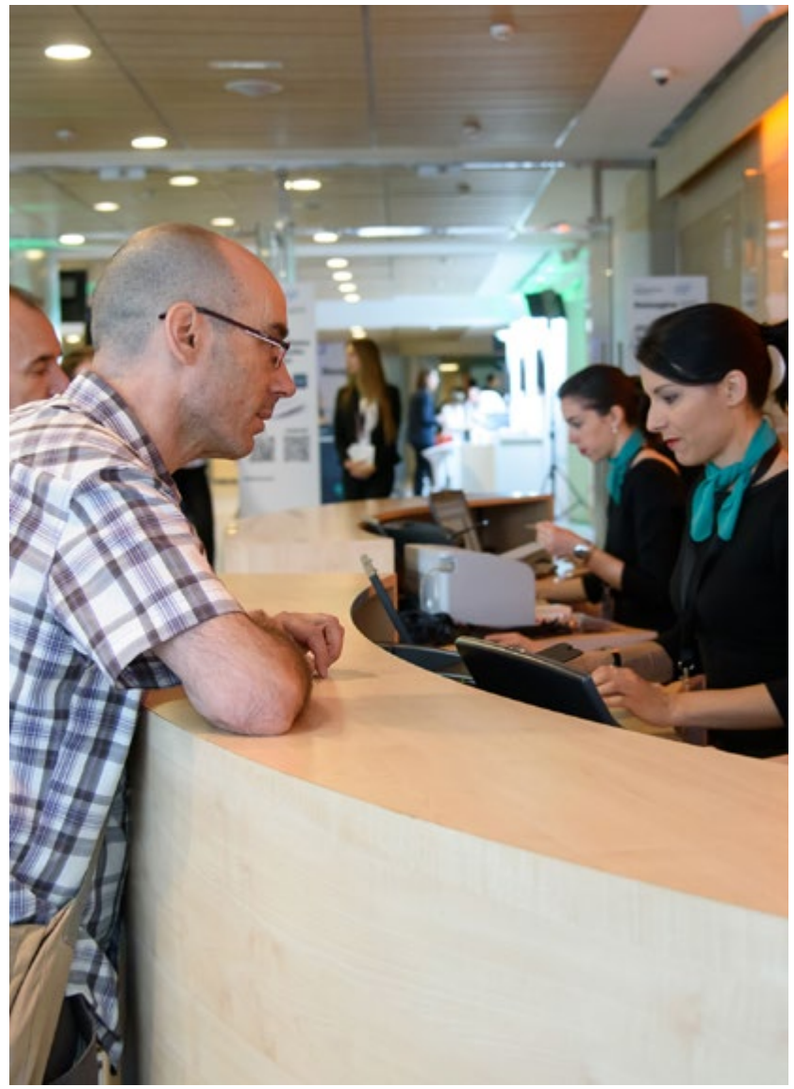
De los tres pilares en los que Hewlett Packard Enterprise ha segmentado el contenido de Reimagine 2017, el de Internet de las Cosas, IoT, es de largo el que presenta un mayor potencial de desarrollo de cara a los próximos años. De hecho, con la posición actual, nos es casi imposible vislumbrar cómo será el potencial real de despliegue de IoT.



IoT: Convirtiendo el desafío en oportunidades

Como ya hemos señalado anteriormente, las cifras de IoT son mareantes. La consultora McKinsey estimaba recientemente que el impacto económico potencial se elevará a 11,1 billones de dólares en el año 2025, mientras que Gartner eleva el número de dispositivos conectados en 2020 a 26.000 millones de unidades, muy por debajo de los 75.000 millones de unidades que predice Morgan Stanley.

Pero, más allá de estos números, hay que tener una estrategia al respecto y, en el caso de Hewlett Packard Enterprise se apoya en tres principios clave: conectar, proteger y procesar. Es decir, conectar los dispositivos que constituyan el despliegue de esta red de cosas que, en opinión de IDC serán 20.000 millones en 2020, algo menos de esos 26.000 que veíamos que pronosticaba Gartner. El segundo de los elementos, proteger, tiene mucho que ver con uno de los riesgos de IoT, dado que muchos dispositivos no han tenido en cuenta, en su diseño, la seguridad, con lo que independientemente de cuál sea su función en la cadena, esta falta de seguridad puede constituir una puerta de entrada a nuestro sistema; razón de más para estar preparados. En tercer lugar, procesar, ya que se estima que más del 40% de los datos generados por los diferentes sensores y dispositivos de IoT serán pre-procesados en el extremo para reducir los requisitos de telecomunicaciones, pero incrementando el nivel de inteligencia exigido. Además, no podemos olvidar que las ingentes cantidades de información generadas en todos estos dispositivos y sensores, supondrán un reto y un desafío para los actuales centros de datos.



Elementos de una solución global

Son varios los elementos a tener en cuenta en una solución de IoT, tal y como puede verse en la imagen. En primer lugar, la conectividad, que debe ser ubicua, instantánea y multiprotocolo.

La propuesta IoT de HPE está basada en la experiencia y, a partir de ella, la compañía pone la mirada en tres diferentes escenarios para el despliegue de IoT: en los edificios, en la industria y en abierto

En segundo lugar, inteligencia en el extremo. Para ello, Hewlett Packard Enterprise dispone de sensores y beacons Aruba, redes (cableadas e inalámbricas) de Aruba y cartuchos PXI.

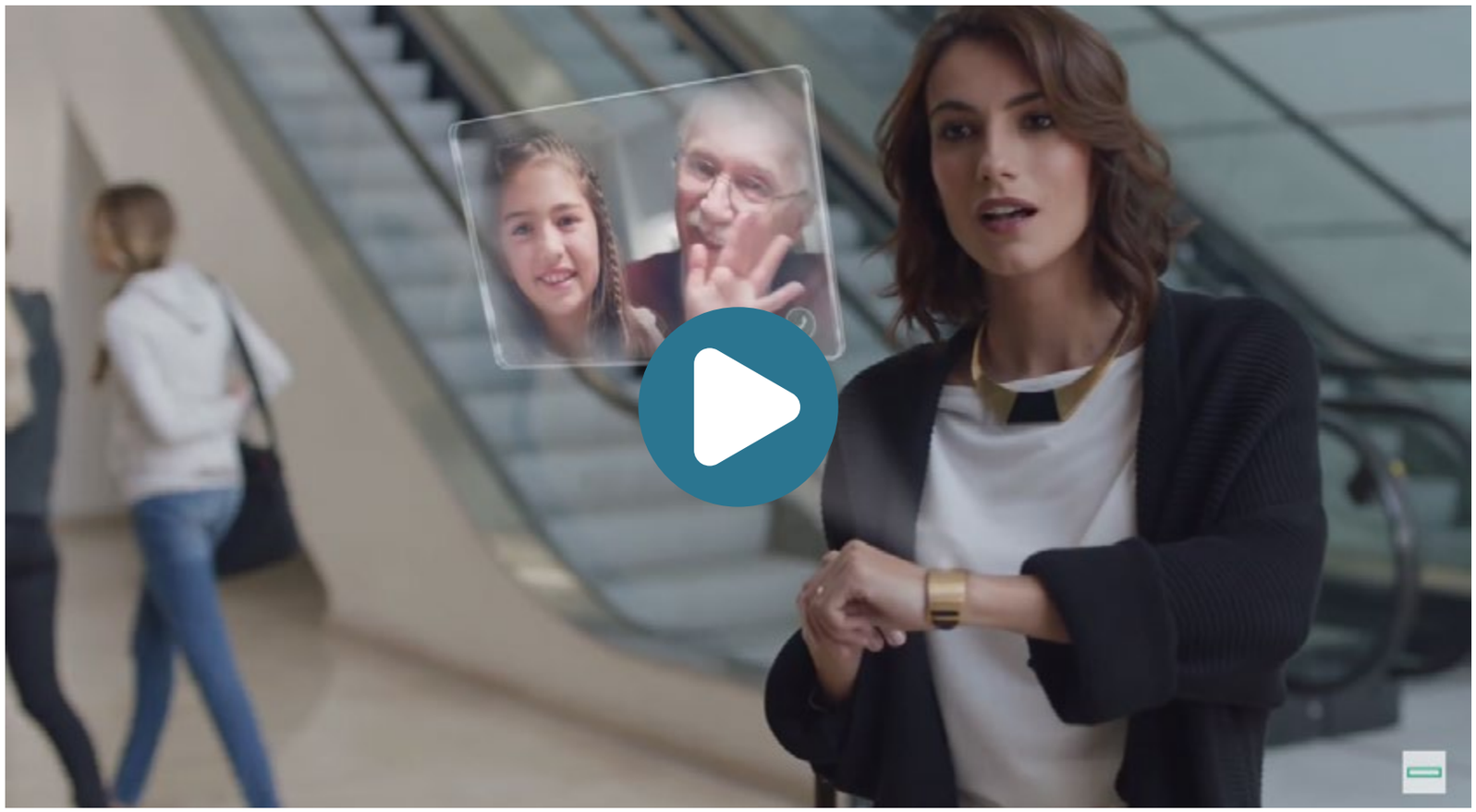
Con el fin de no ocupar la red con comunicaciones prescindibles, debemos dotar de cierta inteligencia al extremo para que sea capaz de procesar eventos, el contexto y la localización. Hablamos, en este caso, de soluciones Aruba Mobile First, sistemas y gateways Edgeline y opciones de computación en el extremo.

Todo esto se ubica sobre una plataforma IoT, que habilita y simplifica la cadena de valor de Internet de las Cosas, con elementos tales como Mobile First-Connectivity, seguridad Ioc, y la Universal IoT Platform con NIP.

Sobre esto, una infraestructura de IT híbrida, distribuida y con cobertura del extremo al cloud y basada en soluciones tecnológicas tales como Apollo, ProLiant, sistemas hiperconvergentes, y productos de Aruba, 3PAR, Nimble y StoreOnce.

Y todo esto sin olvidar el ecosistema desarrollado a partir de IoT, porque HPE ve esta red como una realidad abierta, extensible y orientada a partners, independientemente de que se traten de socios de consultoría, proveedores de servicio, partners de soluciones o partners de tecnología.

Por último, dos elementos que, si bien no forman parte en sí de una solución de IoT, son imprescindibles en cualquiera. Estamos hablando de los servicios y de la seguridad. En el caso de Hewlett Packard Enterprise, los servicios corresponden a Pointnext, la nueva estructura internacional de servicios de la firma, que ofrece tanto workshops IoT como soluciones de Internet de las Cosas como servicio, mientras que, en el caso de la seguridad, esta se basa en las soluciones ClearPass y Niara.



Cómo Internet de las Cosas conecta el mundo

Escenarios IoT

La propuesta IoT de HPE está basada en la experiencia y, a partir de ella, la compañía pone la mirada en tres diferentes escenarios para el despliegue de IoT: en los edificios, en la industria y en abierto.

Cuando hablamos de edificios, pensamos en elementos tales como soluciones de auto-login, ofertas relevantes de servicios,

Enlaces de interés...

- Todas las presentaciones de Reimagine 2017
- Toda la información sobre IoT

Si no queremos que Internet of Things se convierta en Internet of Threats, la seguridad es fundamental

securización, diseño y optimización de espacio, contenidos y anuncios basados en posición o direcciones y guías. Se trata de soluciones para espacios como aeropuertos, puertos, estaciones de autobús, hospitales, hoteles, centros de convenciones y conferencias, tiendas, centros comerciales, museos, galerías de arte, estadios, universidades o salas de conciertos, por poner solo algunos ejemplos.

En el escenario industrial, pensamos en elementos como analíticas en tiempo real (con realidad aumentada), infraestructuras de plantas convergentes, control de luz y condiciones ambientales, manuales de reparación y localización de activos o geo-fencing de equipamiento peligroso. En este caso, hablamos de plantas químicas, yacimientos de petróleo, plantas de fabricación, plantas de energía, granjas eólicas, centros de distribución o centros de mantenimiento y reparación, por ejemplo.

Por último, las soluciones en abierto, con optimización de rutas y servicios; control de humedad, temperatura o luz; localización de bienes o plazas de parking; agua y nutrientes por planta, no por espacio, datos sobre tráfico o seguridad, o vehículos que comparten inteligencia. Y pensamos en ubicaciones tales como ciudades, coches conectados, flotas de reparto, puertos o proveedores de telecomunicaciones.

Seguridad

Pero, evidentemente, si no queremos que Internet of Things se convierta en Internet of Threats, la seguridad es fundamental, porque los nuevos dispositivos no siempre están pensados con el elemento de seguridad integrado, y porque hablamos de millones de potenciales puertas de entrada de amenazas.

ClearPass ofrece visibilidad de todos los elementos conectados a la red, identificación de los mismos, políticas de seguridad contextuales, y firewall de aplicación en la capa de acceso, con lo que podremos contar con un entorno IoT mucho más seguro. ■

Si hay un elemento aglutinador de las posibilidades de la tecnología y, a la vez, facilitador para que éstas se conviertan en una realidad tangible para las empresas, estos son los servicios. En el caso de Hewlett Packard Enterprise, los servicios se concentran en una división recientemente creada, Pointnext, que aprovechó la cita madrileña para su puesta de largo en España, y para explicar cómo trabajan, como “hacen que suceda”, tal y como mostró Carlos Sánchez-Largo en su presentación.

Servicios IT:
Simplificando la transformación

¿Cómo se incrementa la productividad laboral?

El éxito de los servicios no se basa en un acercamiento puntual, sino en establecer una relación a largo plazo con el cliente, que te lleve a entender lo que necesita y cómo es posible proporcionárselo. En el caso de Hewlett Packard Enterprise, y tal y como pudo verse en Reimagine 2017, se establecen tres niveles de servicios para cubrir todo el ciclo de vida de la venta de tecnología y de la Transformación Digital que está llevando a cabo el cliente.

HPE Pointnext ha organizado su oferta de servicios alrededor de tres áreas: Servicios de Asesoría y Transformación, Servicios Profesionales y Servicios de Soporte y Operaciones

El primer paso en este camino son los servicios de consultoría y transformación, encargadosentre otras cosas de entender los retos y resultados potenciales, diseñar un plan de transformación, inclusión de las tecnologías relevantes en la solución, y puesta en marcha de la prueba de concepto y el piloto.

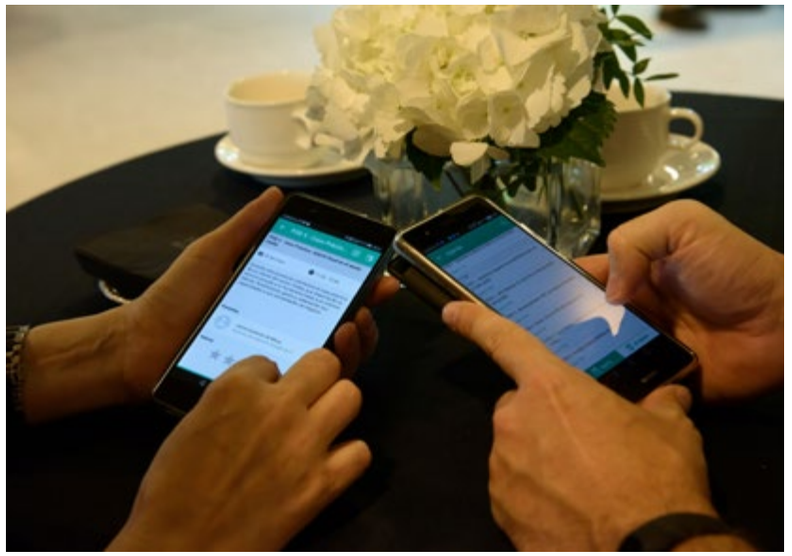
El segundo paso serían los servicios profesionales, encargados de ejecutar el plan de transformación diseñado en la fase anterior y la integración de un entorno multi-fabricante y multi-tecnología, algo imprescindible en el espacio tecnológico actual, marcado por la heterogeneidad y los estándares.

Por último, los servicios operacionales, encargados de la ejecución continuada de la solución integrada y multi-fabricante.

Los servicios en HPE tienen un nombre: PointNext

Pero como decíamos, la estructura de servicios de HPE se concentra en una división de reciente creación: Pointnext. Resumiendo, HPE Pointnext es la nueva organización de servicios tecnológicos de Hewlett Packard Enterprise que ha visto la luz con más de 25.000 especialistas en una amplia gama de disciplinas que dan servicio en 30 idiomas y 80 países diferentes.

La nueva organización se apoya en una serie de pilares en los que basan sus capacidades: la tecnología de la propia HPE, el completo ecosistema de partners y la amplia experiencia de la compañía en servicios tecnológicos



¿El motivo? Empresas de todos los tamaños y de todas las industrias están abordando la Transformación Digital, y necesitan ayuda para averiguar en qué tecnologías deben invertir y la mejor manera de implementarlas para resolver complejos problemas empresariales. Y eso es lo que pretende hacer la nueva organización: estar al lado de los clientes en su proceso de Transformación Digital y hacer que la teoría se convierta en realidad, solucionando los problemas que puedan surgir por el camino.

Así, desde HPE Pointnext colaborarán con empresas de todo el mundo para acelerar la adopción de tecnologías emergentes, incluyendo tecnologías Cloud, IT híbridas, Big Data & Analytics, Intelligent Edge e IoT, porque en la compañía son conscientes de que los servicios son una pieza fundamental para convertirse en el partner estratégico que necesitan los clientes.

La nueva organización se apoya en una serie de pilares en los que basan sus capacidades: la tecnología de la propia HPE, el completo ecosistema de partners y la amplia experiencia de la compañía en servicios tecnológicos de consultoría, integración, soporte y operación.

Su principal objetivo es mejorar la experiencia de los clientes, la creación y suministro de nuevos productos y servicios digitales y la mejora de sus operaciones con gran velocidad y con elevada eficiencia.

Como decíamos, HPE Pointnext ha organizado su oferta de servicios alrededor de tres áreas: Servicios de Asesoría y Transformación, en los que HPE Pointnext colaborará con sus clientes en el diseño de sus estrategias de transformación y en la creación de una hoja de ruta ajustada a sus necesidades; Servicios Profesionales, centrados en la implementación puntual, el cumplimiento del presupuesto y el despliegue de configuraciones de software y hardware personalizadas; y Servicios de Soporte y Operaciones, encargados de la gestión y optimización de cargas de trabajo, recursos y capacidad on-premise y en la nube. ■

Enlaces de interés...

w Todas las presentaciones de Reimagine 2017

i Toda la información sobre Servicios IT

Hewlett Packard Enterprise | intel

Powered by Intel®

Reimagine 2017

Madrid 30 de mayo

¡El primer evento de la nueva Hewlett Packard Enterprise en España!

¿Quiere crear en su organización la Plataforma Digital del Futuro?

Con HPE e Intel podrá experimentar como combinar las infraestructuras y los servicios para afrontar los retos que traerá el Futuro de la Economía Digital.

- Propuestas para un mundo **híbrido**
- Soluciones para exprimir la tecnología de **IoT**
- **Servicios** para construir la plataforma digital

Descargue las presentaciones

Intel Inside®. Para una productividad extraordinaria.

Automatización de procesos, primer paso para la Transformación Digital

serem

Automatización de procesos,
primer paso para la Transformación Digital

Hablar a estas alturas de las ventajas para las empresas de la Transformación Digital no puede hacerse sin hablar de Automatización de Procesos. Una de las ventajas más claras que ofrece la Transformación Digital es el incremento de eficiencia, productividad y eficacia, algo totalmente imposible sin la automatización de determinadas tareas. Muchas tareas y procesos habituales en las empresas consumen un alto grado de recursos tanto tecnológicos como humanos y, lo que es peor, se trata de tareas repetitivas que hacen que este consumo sea reincidente. De ahí que la automatización de estas tareas sea la puerta para alcanzar la eficiencia y productividad prometida por la Transformación Digital.

Pero, qué entendemos por automatización. Se entiende por automatización la sustitución de tareas en las que hay un alto porcentaje de intervención humana por otras tareas que pueden ser desempeñadas de forma automática por plataformas software adaptadas a tal efecto. Las ventajas inmediatas que la automatización proporciona son muchas y evidentes desde el primer momento del proceso: simplificación de tareas; reducción del riesgo de error humano; aumento de la calidad, precisión, exactitud y velocidad; y reducción significativa de la variabilidad y de los costes.

Utilizando ServiceNow, Serem puede gestionar la automatización de los procesos y servicios en los departamentos de IT, Recursos Humanos, Servicios Generales, Personas en Movilidad, Legal, Marketing y cualquier otra organización dentro de una empresa, y con LivingActor, puede favorecer y automatizar las relaciones con el usuario final. Ampliemos los detalles.

Centro de Automatización de Procesos

Gracias al Centro de Automatización de Procesos SEREM, las empresas conseguirán mejorar la calidad en sus servicios, anticipándose a los problemas, reducien-

do costes y garantizando que sus servicios permanezcan siempre activos.

Pero empecemos por el principio, ¿por qué es necesario y conveniente automatizar?

Las empresas tienen que adaptar sus productos y servicios a las nuevas expectativas del mercado: digitalización, movilidad, time to Market... Este escenario obliga las empresas a mejorar y automatizar sus procesos. La automatización permite cumplir con esos objetivos y más, como reducir costes, mejorar la calidad y cambiar la cultura de empresa.

La automatización aporta eficiencia en la gestión de los recursos (evitando realizar tareas repetitivas y con poco valor añadido), evita errores de operación, facilita el mantenimiento correctivo y preventivo, estandariza el conocimiento, y normaliza el proceso.

Serem puede ayudar a las empresas a automatizar sus procesos y servicios, dado que su foco está puesto en las metodologías de transformación y en productos de automatización; su equipo está formado y certificado en metologías Devops, Agile, ITIL; y son partners y distribuidores de herramientas como ServiceNow o Automatic.

Herramientas para la automatización de procesos

Desde Serem nos explican que trabajan con diferentes herramientas, pero quizá la primera de la lista es ServiceNow, una herramienta de automatización de procesos considerado por Gartner como uno de los líderes de la transformación. La firma dispone de diferentes modos de implementación de ServiceNow, según sean

Una de las ventajas más claras que ofrece la Transformación Digital es el incremento de eficiencia, productividad y eficacia, algo totalmente imposible sin la automatización de determinadas tareas

las necesidades de la empresa: ServiceNow Enterprise, ServiceNow Express, ServiceNow MSP. serem también ha desarrollado DevOps con ServiceNow, una aplicación que facilita la aplicación de la metodología DevOps en cualquier empresa y en un tiempo récord.

Pero, además, desde Serem refuerzan sus capacidades conectando con herramientas de automatizaciones de tests, de automatización de despliegues, o herramientas de asistencia virtual, por ejemplo.

La mejor guía para llevar a cabo una automatización de procesos es la que proporciona la metodología DevOps. DevOps es hoy la metodología más eficaz ya que permite una implementación gradual, basado en quick wins y con feedback continuo del cliente.

Una propuesta para cada empresa

Como hemos indicado, existen diferentes versiones de ServiceNow, en función de lo que necesite cada empresa.

Empezando por ServiceNow Enterprise, esta herramienta puede gestionar los servicios de todos los departamentos de la empresa, no solo para los propios de TI, sino también aquellos típicos de los departamentos de Recursos Humanos, Servicios Generales, Personas en Movilidad, Legal, o Marketing, entre otros.

ServiceNow Enterprise ofrece una experiencia de usuario a través de su nube corporativa, y está diseñada para gestionar y ofrecerlo todo como un servicio.

La plataforma de ServiceNow ha sido diseñada para proporcionar un motor de flujo de trabajo bajo rigurosos criterios empresariales que hace posible desplegar servicios de gestión automatizados no solo TI, sino todas las relaciones orientadas a servicio de los diferentes departamentos y unidades de negocio tanto internas como externas a la empresa.

Gracias a un único sistema de registro, una única arquitectura, un único modelo de datos y una única interfaz de usuario, pueden acceder tanto miembros del

Tres ejemplos de automatización

Como el movimiento se demuestra andando, y la teoría con ejemplos, hemos querido recoger en este punto tres ejemplos de automatización de procesos: helpdesk, RRHH, y gestión de salas y plazas de parking.

El nivel 1 de helpdesk de un centro de soporte realiza tareas bastantes repetitivas y con poco valor añadido. Muchas tareas dependen de la documentación compartida. Es posible automatizar el soporte de nivel 1 integrando las capacidades de ServiceNow con herramientas de Inteligencia artificial. Así, un cliente de la empresa pueda chatear con un robot para que le resuelvan su incidencia, lo que acaba proporcionando solicitudes resueltas con más rapidez, reducción del coste del equipo de soporte, y menos problemas de rotación.

En el caso de los Recursos Humanos, se propone un sistema que permita facilitar la información hacia el empleado, y mejorar la gestión por parte del equipo de RRHH de las diferentes tareas diarias, tales como preguntas de nóminas, bajas laborales o incorporación de empleados. Esta ayuda también puede incluir un proceso automatizado de onboarding, donde la herramienta gestiona todas las tareas, que van desde que se da el ok a la incorporación de un empleado, hasta la compra y la configuración de todo el material que se vaya a necesitar, la creación de todos los accesos a las aplicaciones de la empresa, o los cursos de elearning, por ejemplo.

En el tercero de los ejemplos, on ServiceNow se puede gestionar la reserva y liberación de plazas de salas de reuniones o de parking desde el móvil. Eso incluye todo tipo de reporting, y notificaciones, como recordar al usuario un día antes y una hora antes que ha reservado la sala y que pueda cancelarla si no piensa usarla.

departamento TI como otros usuarios de negocio o de gestión, para consultar, interactuar o realizar informes.

Asimismo, ofrece una plataforma para el desarrollo de aplicaciones, no solo una herramienta para desarrolladores especializados, sino también para los mismos usuarios de negocio, que pueden modificar rápida e intuitivamente las aplicaciones de ServiceNow, crear nuevas aplicaciones y añadir servicios al catálogo de servicios empresariales sin necesidad de conocimientos de programación.

Las empresas tienen que adaptar sus productos y servicios a las nuevas expectativas del mercado: digitalización, movilidad, time to Market, y este escenario obliga las empresas a mejorar y automatizar sus procesos

Además, ha sido diseñada para satisfacer la demanda de grandes empresas en cuanto a escalabilidad, flexibilidad y fiabilidad, así como los requisitos más rigurosos de los clientes.

Se incrementa la eficiencia para una amplia variedad de disciplinas TIC, incluyendo la gestión del ciclo de vida de virtualización y de la nube, la organización de cambios, la detección de infraestructura y gobernanza, todo ello habilitado mediante un único motor de flujo de trabajo. Además, se proporciona una visibilidad total del rendimiento de los servicios TI, incluyendo informes ejecutivos, comparativas de mercado e indicadores clave de rendimiento (KPI) de colaboración abierta.

Por último, no podemos dejar de mencionar los programas de soporte especializados, como conferencias de usuarios anuales, grupos de usuarios locales, grupos de intereses afines, foros en línea y blogs, y una biblioteca de KPI “crowd-sourced”, que facilitan la colaboración y compartición de conocimiento entre usuarios finales y creadores de aplicaciones.

Serem puede ayudar a las empresas a automatizar sus procesos y servicios, dado que su foco está puesto en las metodologías de transformación y en productos de automatización

Las fases para la implantación de ServiceNow en cualquier empresa son las siguientes

- **Consultoría.** El primer paso antes de la implantación es averiguar cuáles son los objetivos que se pretenden alcanzar con ServiceNow y ofrecer la mejor solución para alcanzarlos. Esto se resumen en:
  - Identificar cuáles son los procesos que van a ser optimizados.
  - Planificar qué modificaciones se van a realizar.
  - Reducir los costos al implementar las nuevas estrategias.
- **Implantación.** En Serem disponen de una amplia variedad de servicios de implantación de ServiceNow. Con la experiencia adquirida, pueden tener instalado el sistema en cuatro semanas, habiendo estableciendo previamente los objetivos de tu empresa.
- **Formación** – En Serem disponen de un departamento de formación cualificado con experiencia real en la utilización e implantación de ServiceNow, que podrá solventar todas las necesidades formativas de tu empresa.
- **Soporte** – Una vez implementada la solución ServiceNow, la empresa dispondrá de un servicio de soporte específico gracias al cual tendrá un equipo disponible para resolver cualquier tipo de duda o problema que se pueda plantear.

WEBINAR: CLAVES PARA LA AUTOMATIZACIÓN DE PROCESOS Y SERVICIOS IT CON SERVICENOW

CLICAR PARA VER EL VÍDEO

ServiceNow Express es la opción indicada para departamentos de TI de tamaño medio. En este caso, cuenta con una serie de ventajas, tales como que precisamente fue diseñado pensando en los departamentos de TI de tamaño medio, aprovechando el poder de la plataforma empresarial ServiceNow para automatizar incidencias, problemas, cambios, configuración y gestión

Servicios TI

Serem cuenta con especialistas en Outsourcing / BPO, OutTasking, IT Consulting, Contact Center y HR IT Recruitment. Apoyándose en esto, la firma ofrece servicios y orientación sectorial, si bien, con la utilización del outsourcing o del outtasking, el cliente mantiene el control de sus procesos y tareas en todo momento, teniendo acceso a una herramienta para alcanzar sus objetivos.

Desde Serem se identifican los objetivos empresariales que el cliente quiere cubrir (personas, tecnología, procesos), así como los procesos principales de la empresa. Tras ello, se define un plan para el outsourcing o el outtasking, así como los acuerdos de nivel de servicio (disponibilidad, tiempos de respuesta, capacidad de crecimiento). Finalmente, se revisa, de forma periódica, el cumplimiento de los objetivos.

de solicitudes. ServiceNow Express es web-responsive ofreciendo accesibilidad en cualquier momento y lugar con facilidad de uso. Las principales funciones que se pueden configurar son:

- Notificaciones y Alertas
- Modulo Gestión de Incidentes, Problemas y del Cambio
- Gestión y Configuración de Activos
- Visualización de Tablero de Actividades
- Flujos de trabajo preconfigurados
- Escalamiento
- Reportes básicos
- Gestión de Niveles de Servicio
- Automatización muy básica de servidores, basada en factores desencadenantes

Cuando hablamos de la optimización del control de procesos de TI, hablamos de una rápida puesta en marcha, utilizando procesos pre-configurados de ITIL, incluyendo incidencias, problemas y gestión de cambios que se apoyan en una poderosa herramienta de gestión de base de datos (CMDB); un sistema único de registro, mejorando la precisión y acelerando la resolución de problemas; y un flujo de trabajo personalizado, porque los procesos de flujo de trabajo son únicos, incluidas las aprobaciones y las notificaciones automatizadas de correo electrónico, que se configuran fácilmente.

Con esto, se mejora la experiencia del cliente, con un portal amigable, el catálogo de autoservicio, y la base de conocimientos, que son una "puerta de entrada a TI"; con un proceso de aprobación transparente, los usuarios pueden seguir el progreso de sus propias solicitudes; y los empleados pueden acceder a todas las funcionalidades desde móviles (iOS y Android).

Asimismo, se ofrece mayor visibilidad tanto al departamento de TI como a la dirección, con funciones integradas que controlan los servicios TI y ayudan a demostrar el impacto de tu negocio; dirigiendo a los usuarios y a los equipos a través de las consultas, informes y paneles de información; y encontrando fácilmente datos a través de las aplicaciones ITIL para detectar tendencias y resolver problemas.

Otra opción es ServiceNow MSP, diseñada para proyectos de tamaño mediano con un número de licencias concretas para grupos de trabajo limitados, pero que quieren tener toda la funcionalidad de Enterprise.

¿Quieres implantar DevOps en tu empresa?

Ahora es más sencillo y rápido reducir costes aumentando la eficiencia en el desarrollo de aplicaciones. DevOps 120 horas es una aplicación creada por Serem que permite controlar y medir todos los pasos de gestión de proyecto en modo DevOps, del desarrollo al despliegue. Automatizacion, Continous delivery, Continous integration… es posible con ServiceNow y las interfaces desarrolladas. Esta aplicación incluye desarrollos de nuevos roles, de nuevas funcionalidades (creación automática de tests plans, de documentación…), de interfaces con herramientas de automatización de operaciones de producciones como Jenkins, Puppet, Chief, XLDeploy, Automatic…

Enlaces relacionados

- Serem
- Automatización de procesos
- ServiceNow
- Impacto económico del desarrollo de aplicaciones de negocio con ServiceNow
- Automatizar procesos y servicios IT con ServiceNow

Una visión a la ciberseguridad del futuro

Check Point
SOFTWARE TECHNOLOGIES LTD.

Una visión a la ciberseguridad del futuro

Check Point Software Technologies organizó el pasado mes de junio una nueva edición de su cita anual, CyberDay 2017, un evento dirigido a profesionales de TI y de ciberseguridad con el objetivo de mostrarles cuál es la situación real del malware y el mundo de la prevención y la ciberseguridad. El ransomware, la ciberseguridad de la nube, los móviles, IoT y las infraestructuras de riesgo, han sido los grandes protagonistas de la reunión.

INFINITY, LA ARQUITECTURA DE CIBERSEGURIDAD DEL FUTURO

CLICAR PARA VER EL VÍDEO

Los departamentos de TI deben balancear, en una mano, los deseos de los usuarios y los departamentos de negocio en cuanto a acceso a información, libertad de movimiento, velocidad de adaptación, y un largo etcétera de peticiones; en la otra, las necesidades de la empresa de mantener su información, dispositivos y usuarios dentro de un entorno seguro que garantice, por una parte, la supervivencia de la compañía, y, por otra, las adecuadas condiciones para que el negocio pueda desarrollarse sin sobresaltos ni cortes.

A este difícil equilibrio tenemos que añadirle , por una parte, un incremento de las amenazas -no solo en vectores conocidos- sino también en nuevos vectores de ataque (movilidad, IoT…) con nuevas formas evolucionadas que buscan puertas ocultas para entrar en nuestra red (ransomware) y otras amenazas desconoci-

SOBREVIVIR A LA PLAGA DE RANSOMWARE

CLICAR PARA VER EL VÍDEO

das que van surgiendo y para las que la seguridad tradicional no da respuesta. Por otro lado, tenemos los presupuestos que manejan los departamentos de TI que no crecen a la velocidad necesaria para estar siempre a la última en todo momento. Es decir, que los departamentos de TI se hallan en medio de lo que podríamos denominar una tormenta perfecta y son una embarcación que, si han hecho bien su trabajo, podría permitirles seguir navegando, pero que, si no, ya porque tenga grietas o ya porque el diseño sea demasiado anticuado para responder a las exigencias actuales, empezará a hacer aguas y podría llevar a la empresa a acabar hundida en el fondo del mar.

Pero dejemos las metáforas marineras y hablemos de tecnología, y de cómo las nuevas tendencias en la ciberseguridad buscan más la prevención como forma de atajar cualquier posible ataque antes de que se produzca. Porque no podemos olvidar que el departamento de TI debe atender demandas de usuarios y negocio que parecen no tener límites, y esto convive con la a explosión de nuevas tecnologías que prometen simplificación, eficiencias incalculables y ahorro de costes, pero mientras, crean incertidumbre, complejidad y riesgo. Es necesario que haya una estrategia global que asuma el compromiso de permitir aprovechar la promesa de estas nuevas tecnologías para el beneficio de las operaciones comerciales y los clientes, sin que esto suponga un problema para la ciberseguridad de la empresa, los datos y el propio negocio.

En el caso de Check Point Software Technologies hablamos de Check Point Infinity, una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas.

Un cambio de estrategia en la ciberseguridad

La tradicional concepción de la ciberseguridad como una muralla alrededor de un castillo (el centro de datos) ha saltado por los aires porque, para empezar, los límites que marcaban la red hace unos años ahora han desaparecido. La proliferación de dispositivos móviles inteligentes, instancias virtuales, nube pública, nube privada, todo como servicio (EaaS), Internet de las cosas (IoT)… han hecho que los límites de la red sean difusos, los puntos de acceso se hayan multiplicado, y

El ransomware, la ciberseguridad de la nube, los móviles, IoT y las infraestructuras de riesgo, han sido los grandes protagonistas de CyberDay 2017

el reto de los responsables de la ciberseguridad se hayan incrementado exponencialmente. Para adecuarse a esta realidad, las empresas deben transformarse digitalmente. La transformación digital consiste en cambiar la forma en que el negocio opera, y esto, necesariamente, también afecta a la ciberseguridad de TI. Se trata de aprovechar la interconexión y satisfacer el flujo y el reflujo natural de los negocios con una infraestructura elástica que entrega automáticamente todos los servicios de la manera más eficiente y rentable. Se trata de una completa transformación a un nuevo paradigma mediante el aprovechamiento de las redes virtuales, móviles, cloud, EaaS y más para ofrecer operaciones de negocios rápidas y confiables de una manera más conectada, dinámica, eficiente y rentable.

Desafortunadamente, con demasiada frecuencia, las estrategias y diseños de ciberseguridad para estos nuevos entornos se remontan a los primeros años del 2000, donde se desplegó un sinfín de productos no integrados y dispares. Así que, en lugar de una arquitectura de ciberseguridad unificada, las empresas están de nuevo atascadas con las ineficiencias de la gestión de múltiples

WANNACRY 3.0, PRÓXIMAMENTE EN SUS PANTALLAS... DEL MÓVIL

CLICAR PARA VER EL VÍDEO

2016 fue un año de récord para el ransomware y 2017 será peor todavía, según Check Point Software

Aprovechando la celebración del CyberDay 2017, Check Point Software Technologies ha hecho un repaso de la actualidad en el mundo de la ciberseguridad, una actualidad marcada por la notoriedad del ransomware, que en 2016 vivió un año de récord en volumen de malware, en número de afectados, en innovación y en beneficios. Pero lo más preocupante es que desde la firma esperan que en 2017 vamos a ver cómo se incrementan estos datos.

Y es que en este 2016 se ha producido un cambio de estrategia de los ciberdelincuentes. Hasta la fecha, trataban de conseguir información personal de los usuarios y las empresas para venderla y convertirla en dinero. Sin embargo, ahora buscan vender sus datos al propio usuario, una práctica menos arriesgada y más beneficiosa, sobre todo por la anonimidad y la imposibilidad de rastrear el pago en Bitcoins. Con todo, los datos del ransomware se resumen afirmando que el 40% de la base atacada es infectada, y, de ellos, el 70% acaba pagando, lo que, solo en Estados Unidos, según datos del FBI, ha reportado más de mil millones de dólares. Y es que en este año se ha mejorado el mecanismo de entrega del malware, se atacan datos importantes para el usuario, y, somo hemos comentado, se ha mejorado el sistema de pagos.

De cara a 2017, se espera la expansión del ransomware as a service, los programas de filiación y nuevos modelos de pago, además de mejorar el malware, con capacidades para encriptar los backups, por ejemplo, y el despliegue por nuevos dispositivos, principalmente el smartphone, pero también todos los conectados a IoT.

productos de ciberseguridad separados que, al final, no protegen eficazmente la nueva operación de TI o el negocio.

En resumen, ¿qué necesita una empresa? Necesita una plataforma unificada de ciberseguridad que le permita gestionar entornos móviles, de nube y de red; que se adelante a los problemas con la prevención integrada de amenazas; con una política de ciberseguridad que integra las necesidades de la empresa; y que puede adaptarse al ritmo que necesite adaptarse el negocio.

Check Point Infinity

El pasado mes de abril, Check Point Software Technologies presentó Check Point Infinity, una arquitectura de ciberseguridad diseñada para satisfacer las necesidades de ciberseguridad de las empresas. Check Point Infinity incorpora protección consolidada a través de las redes, la nube y los dispositivos móviles, y proporciona prevención de amenazas para mantener a los clientes a salvo frente al creciente número de ciberataques.

Tal y como señaló en su presentación Gabi Reish, vicepresidente de gestión de productos de Check Point, "Check Point Infinity es la culminación de nuestra visión global de construir una arquitectura de ciberseguridad que unifique la mejor protección, la mejor inteligencia y la mejor gestión que podemos ofrecer a través de las redes, la nube y los dispositivos móviles".

Asimismo, este responsable añadía que Check Point Infinity "está diseñada para asegurar que las organizaciones estén preparadas para manejar la dinámica tan cambiante de la TI del futuro. El principio es muy simple: una arquitectura de ciberseguridad unificada mantendrá a las empresas a salvo en todos los entornos, con operaciones de TI más eficientes y efectivas".

Check Point Infinity se apoya en tres elementos clave:

- Una única plataforma de ciberseguridad: aprovecha las plataformas comunes, la inteligencia

UN VIAJE SEGURO A LA NUBE

CLICAR PARA VER EL VÍDEO

El 20% de operadores de infraestructuras críticas no han hecho ninguna evaluación de riesgo

Durante la celebración del CyberDay 2017, Check Point Software Technologies ha presentado en informe Estado de la Ciberseguridad en los operadores de infraestructuras críticas en España.

De los datos del informe se desprende que el 20 por ciento de los operadores de infraestructuras críticas no han realizado ninguna evaluación de riesgo, dato que se duplica cuando hablamos de los sectores de agua y transporte.

Otro de los datos que llaman la atención es que el 22% de las empresas encuestadas no tienen proceso de gestión de incidentes o solo funcionan de forma reactiva. Además, solo el 27 por ciento de ellos mantienen sus redes industriales separadas del resto con múltiples niveles de segmentación.

En cuanto a los responsables de negocio, el 40% dice tener una sensibilidad alta, si bien en el 25% es escasa o nula (un 67% en el sector del agua). De ahí que solo el 35% de los encuestados planifican acciones de ciberseguridad en el tiempo. Es más, solo el 12% dice mejorar por exigencias provenientes de la dirección.

La nota positiva llega de la mano de la previsión de presupuestos para el año próximo, dado que tres de cada cuatro esperan incrementar esta partida. Eso sí, no es igual en todos los sectores, dado que, si bien es el 100% en el sector eléctrico, nuclear, agua y financiero, apenas alcanza el 37% en el sector del transporte.

Por último, cabe destacar que, pese a la pérdida de predominio en otros segmentos por el desarrollo y la expansión de la Transformación Digital, esta preocupación y contratación de proyectos de ciberseguridad sigue en manos del área de TI.

La tradicional concepción de la ciberseguridad como una muralla alrededor de un castillo (el centro de datos) ha saltado por los aires porque, para empezar, los límites que marcaban la red hace unos años ahora han desaparecido

de amenazas y la infraestructura abierta. Ofrece protección sin precedentes en todas las plataformas, independientemente de la red o del tamaño.

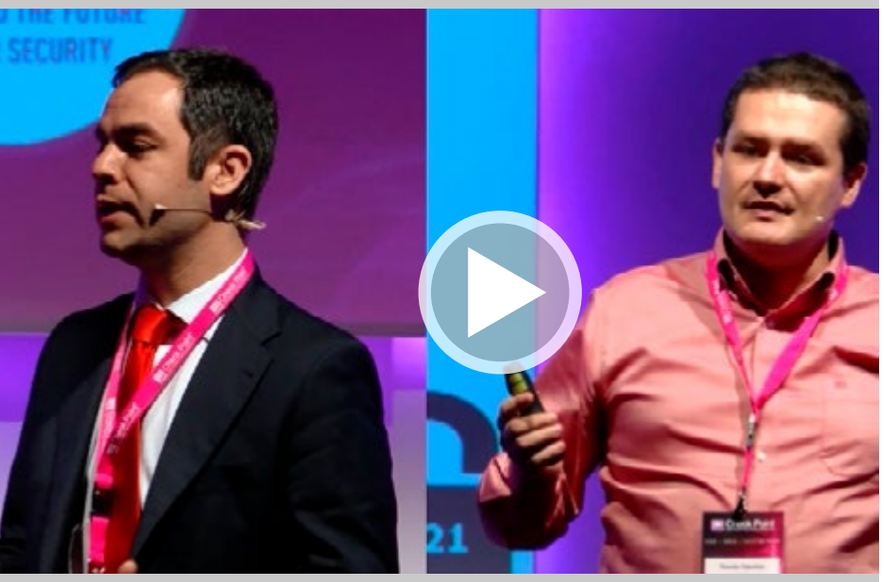
- Prevención de amenazas anticipada: se centra en la prevención para bloquear los más sofisticados ataques conocidos y desconocidos antes de que sucedan.
- Sistema consolidado: una gestión única, gestión de políticas modular y visibilidad integrada de las amenazas para centralizar eficientemente la ciberseguridad a través de un cuadro de mando único

Check Point Infinity permite a las empresas tomar el control de su ciberseguridad y proteger y administrar toda su operación de TI como una arquitectura única cohesiva para el beneficio de sus operaciones comerciales y sus clientes.

Innovación en ciberseguridad

Los avances en tecnología han impulsado innumerables mejoras en la forma de trabajar de las empresas, pero también han alterado la forma en que deben abordar la ciberseguridad. Check Point Infinity responde a esta necesidad e introduce nuevas capacidades:

CYBERTALKS: MAPFRE Y FERROVIAL



CLICAR PARA VER EL VÍDEO

- Gestión de la ciberseguridad: El lanzamiento de la versión R80.10 de Security Management cuenta con docenas de nuevas mejoras, incluidas capas de políticas, múltiples zonas de ciberseguridad y rendimiento potenciado para mantener a las organizaciones a salvo de cualquier amenaza, en cualquier momento y en cualquier lugar.
- Cloud: La cartera integral actualizada de vSEC Cloud Security de Check Point se integra con las plataformas de nube privadas y públicas, lo que garantiza la ciberseguridad de los entornos cloud.
- Móvil: El nuevo SandBlast Mobile es la única solución unificada y multiplataforma del sector, que protege a las empresas de las brechas móviles. SandBlast Mobile detecta y bloquea malware conocido y desconocido, protección contra redes Wi-Fi envenenadas y ataques man-in-the-middle, así como esquemas de phishing SMS.
- Prevención de amenazas: La nueva tecnología Check-Point Anti-Ransomware permite a las empresas mantenerse protegidas contra la ciberextorsión e incluso los programas de ransomware más sofisticados.

Gestión de ciberseguridad

Las redes crecientes, las tecnologías disruptivas y la proliferación de dispositivos interconectados exigen un nuevo enfoque para gestionar la ciberseguridad. La arquitectura de Check Point Infinity consolida la gestión de múltiples capas de ciberseguridad, proporcionando una eficacia superior y permitiendo gestionar la ciberseguridad a través de un único panel.

Con R80.10 una única plataforma gestiona toda la infraestructura de TI, desde el centro de datos hasta las implementaciones de nube privadas / públicas, para garantizar la eficacia y la coherencia de la ciberseguridad. La gestión de políticas está unificada para que pueda crearse y supervisarse de forma única. Una sola política gestiona sus usuarios, dispositivos, aplicaciones, datos y redes. Con esta política unificada, también obtiene un control granular más amplio.

Las empresas necesitan una plataforma unificada de ciberseguridad que le permita gestionar entornos móviles, de nube y de red y que se adelante a los problemas con la prevención integrada de amenazas

La API R80.10 facilita la integración segura con sistemas de orquestación, gestión de cambios y ticketing. Con la capacidad de controlar exactamente lo que la integración puede y no puede hacer, las organizaciones tienen la confianza necesaria para integrar la ciberseguridad en su ecosistema de TI. Las tareas rutinarias pueden ser automatizadas y delegadas, liberando equipos de ciberseguridad de tareas repetitivas para centrarse en tareas estratégicas de ciberseguridad como la respuesta a las incidencias.

ESTADO DE LA CIBERSEGURIDAD EN OPERADORES DE INFRAESTRUCTURAS CRÍTICAS ESPAÑOLAS

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON GABI REISH, VP MUNDIAL DE MARKETING Y GESTIÓN DE PRODUCTO EN CHECK POINT

CLICAR PARA VER EL VÍDEO

Check Point Infinity es una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas

Las organizaciones necesitan una ventana de control única para el análisis de eventos, el monitoreo de amenazas y la mitigación para asegurar una visibilidad completa de las amenazas a través de la red. Los datos deben ser recolectados de todas las pasarelas desplegadas y pasados por fuentes externas de inteligencia de amenazas para proporcionar información contextual.

VSEC para la ciberseguridad de la nube pública y privada

La eficiencia de los procesos y la mayor agilidad de la red están impulsando la adopción de la tecnología IaaS y SDN a un ritmo rápido. Pero esta nueva infraestructura también está presentando a las empresas un conjunto único de desafíos de ciberseguridad. Check Point vSEC protege los activos en la nube de las amenazas más sofisticadas con escalabilidad dinámica, provisión inteligente y control constante a través de redes físicas y virtuales.

La virtualización de la red ha creado un cambio en el comportamiento del tráfico. Ahora, más y más tráfico se mueve en el centro de datos creando nuevos desafíos de ciberseguridad. Con pocos controles para asegurar este tráfico, las amenazas pueden viajar sin obstáculos una vez dentro del centro de datos. Check Point vSEC ofrece protección avanzada contra amenazas para evitar su propagación lateral dentro de los centros de datos definidos por software, así como la visibilidad y el control para gestionar eficazmente la ciberseguridad tanto en entornos físicos como virtuales, desde una única solución de gestión unificada.

Mover recursos y datos de computación a nubes públicas significa que las responsabilidades de ciberseguridad se comparten entre la empresa y su proveedor de la nube. Mientras que la protección de la infraestructura es trabajo del proveedor, las empresas quieren la capacidad de controlar sus propios datos y mantenerlos en privado, así como proteger los activos de la nube, todo mientras cumple los mandamientos regulatorios. Check Point vSEC permite una conectividad confiable a los activos de la nube pública mientras protege las aplicaciones y los datos con la prevención avanzada de amenazas en entornos de nube públicos e híbridos.

Check Point vSEC ofrece también ciberseguridad avanzada de múltiples capas para entornos virtuales de centro de datos y virtualización de la función de red (NFV) y está diseñado para equipar a los proveedores de servicios con ciberseguridad integral contra amenazas, protección de día cero, entrega ágil, administración y automatización a través de la red básica.

SandBlast Móvil

El uso de teléfonos inteligentes y tabletas para acceder a información crítica en cualquier momento tiene muchos beneficios, pero puede exponer sus datos confidenciales a riesgos. SandBlast Mobile de Check Point protege sus dispositivos de amenazas móviles avanzadas, asegurando que puede desplegar y defender dispositivos con confianza.

ENTREVISTA CON MARIO GARCÍA, DIRECTOR GENERAL DE CHECK POINT PARA ESPAÑA Y PORTUGAL

CLICAR PARA VER EL VÍDEO

Los principales beneficios de esta solución son la posibilidad de detectar, evaluar y mitigar amenazas avanzadas de ciberseguridad para móviles; proteger los datos empresariales confidenciales en reposo, en uso y en tránsito en dispositivos móviles iOS y Android de ataques cibernéticos; mejorar la visibilidad y la protección mediante la integración con los sistemas existentes de movilidad y ciberseguridad (MDM, MAM, NAC, SIEM...); habilitar la respuesta rápida a ataques de amenazas persistentes avanzadas (APT) entre plataformas; preservar la experiencia del usuario y la privacidad, a la vez que añade la protección requerida por los mandatos organizacionales o regulatorios.

SandBlast Mobile es una solución de ciberseguridad móvil completa que protege los dispositivos de las amenazas en el dispositivo, en las aplicaciones y en la red y ofrece la mayor tasa de captura de amenazas de la industria para iOS y Android. SandBlast Mobile utiliza la detección de aplicaciones malintencionadas para detectar amenazas conocidas y desconocidas aplicando emulación de amenazas, análisis de código estático avanzado, reputación de aplicaciones y aprendizaje automático.

SandBlast Mobile está diseñado para ayudar a proteger los dispositivos móviles de forma rápida y segura a través de la integración con todas las soluciones EMM. Esto ayuda a que la solución sea altamente escalable y ofrece eficiencias operativas sólidas para administrar la ciberseguridad móvil dentro de una infraestructura de ciberseguridad más amplia.

Prevención de amenazas

El Ransomware se ha convertido en una gran amenaza para las empresas y los individuos de todo el mundo. La incapacidad de hacer frente eficazmente a los ataques de ransomware puede causar pérdidas significativas y grandes interrupciones a las organizaciones. La implementación de mejores prácticas convencionales y protecciones anti-malware puede defenderse contra algunas variantes conocidas y antiguas de ransomware, pero dada la sofisticación y la evolución continua de los ransomware modernos, no son suficientes por sí solos para identificar y bloquear nuevos ataques de día cero.

La tecnología Anti-Ransomware de Check Point utiliza un motor de propósito específico que se defiende contra las variantes de día cero más sofisticadas y evasivas de ransomware y recupera con ciberseguridad los datos cifrados, garantizando la continuidad del negocio y la productividad.

SandBlast Agent incluye la tecnología Anti-Ransomware y proporciona protección a los navegadores web y puntos finales, aprovechando las protecciones Check Point. SandBlast Agent ofrece una prevención completa de amenazas y remediación en tiempo real a través de todos los vectores de amenazas de malware, permitiendo a los empleados trabajar con ciberseguridad sin importar dónde se encuentren y sin comprometer la productividad.

Enlaces relacionados

- El futuro de la ciberseguridad
- Sobrevivir a la plaga de ransomware
- WannaCry 3.0... en sus móviles
- Check Point Mobile Threat Penvention
- SandBlast
- vSec
- Security CheckUP

Seguridad móvil:

No hay amenaza pequeña, sino una nueva oportunidad

En el mundo en el que vivimos, en el que se impone un ritmo rápido para todo, los teléfonos móviles son ya considerados por muchos como unas herramientas de trabajo de valor incalculable. La flexibilidad que facilita a los empleados y las ventajas para el negocio de estar siempre conectado, independientemente del lugar, son algunas de las características que lo convierten en indispensables.

Pero como casi cualquier beneficio, su uso conlleva algunos riesgos. La mayoría de los dispositivos móviles no están conectados a la red empresarial tradicional (aunque acedan a ella con frecuencia). Los empleados usan estos dispositivos móviles para acceder a datos empresariales sensibles, como correos electrónicos, hojas Excel repletas de números o presentaciones corporativas. En muchas ocasiones lo hacen, además, a través de equipos personales, no facilitados por la corporación. Y todo ello hace que, en muchos casos, estos equipos no tengan las protecciones adecuadas instaladas.

Algo se escapa del control del departamento de TI

Las empresas, por tanto, tienen que prepararse para estos riesgos, siendo conscientes, además, de que este escenario supone un gran cambio, especialmente para el departamento de TI, acostumbrado a tener la última palabra sobre cómo los compañeros de trabajo debían usar ordenadores y redes corporativas. Algo que ahora no responde al mismo patrón.

Uno de los mayores retos que enfrentan los equipos de seguridad corporativos es administrar dispositivos como smartphones y tabletas que son utilizados por los empleados tanto para el trabajo como para el uso personal. El fenómeno de llevar su propio dispositivo (BYOD) ha conllevado un cambio radical en la forma en que las empresas se ocupan de la movilidad empresarial. En muchas empresas, esta tendencia se ha acelerado desde arriba, con ejecutivos de nivel C-suite exigiendo utilizar dispositivos que ofrecen una experiencia mucho más rica.

"Debemos identificar dónde están almacenados los datos, determinar los flujos de trabajo y los sistemas que se utilizan para manejarlos, evaluar los riesgos, aplicar controles de seguridad y planificar ante posibles amenazas"

David Sanz, EMEA Solutions principal de Commvault

Al mismo tiempo, los delincuentes y piratas informáticos están encontrando nuevas maneras de dirigirse específicamente a los móviles de la empresa, porque saben que las enormes cantidades de datos que podrían desbloquear y obtener importantes ganancias económicas. De hecho, Hervé Lambert, Retail Global Consumer Operations Manager de Panda Security, asegura que los dispositivos móviles están en el punto de

CHEMA ALONSO: SEGURIDAD EN DISPOSITIVOS MÓVILES

CLICAR PARA VER EL VÍDEO

mira de los ciberdelincuentes por una razón de peso: son muy populares. "Tan populares que hoy en día Android es el sistema operativo más usado en el mundo. Android alcanza la cifra de un 37,93% de usuarios frente Al 37,91 de Microsoft, según datos de StatCounter". A ello habría que sumar que con los smartphones hacemos transferencias bancarias, guardamos fotografías, direcciones… "información muy personal y valiosa para los hackers que usan con fines malintencionados. Y la información es dinero porque muchos son los que la quieren comprar".

Pero tampoco debemos alarmarnos. Como cualquier otro riesgo, el móvil puede ser mitigado.

En el software está la clave

Aplicaciones y sistemas operativos obsoletos son algunos de los riesgos más evidentes que nos vienen a la cabeza, pero tampoco hay que irse tan lejos. Incluso un uso incorrecto de aplicaciones que corporativas pueden tener graves consecuencias como fuga de datos empresariales.

Un reciente estudio de la empresa Lookout también denunciaba que muchas aplicaciones piden permiso para el acceso a datos que podrían ser utilizados de manera fraudulenta. Así por ejemplo, y tomando solo a iOS como referencia, este informe detalla que el 30% de las aplicaciones acceden a los contactos, el 30% de las aplicaciones acceden al GPS, 31% al calendario y el 39% al micrófono.

Además, la mayoría de las empresas no gestionan dispositivos móviles, sino que simplemente realizan un seguimiento de las actualizaciones de software o establecen políticas en torno a las aplicaciones problemáticas.

El problema para los equipos de TI corporativos es cómo mantener seguros los datos corporativos con-

> ***"El dispositivo móvil tiene que estar gestionado por el mismo administrador de sistemas que ya controla la seguridad de ordenadores, servidores y portátiles"***
>
> *Angel Victoria, country manager de G DATA Software Iberia*

Impulsa tu cuenta en twitter

Pruébalo gratis

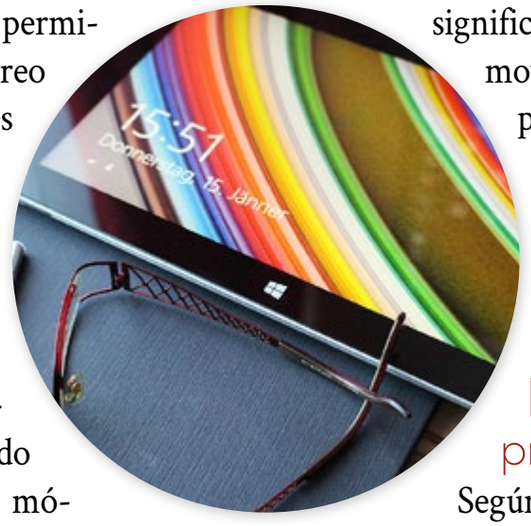
ninja CM

TU MEJOR COMMUNITY MANAGER

"Las organizaciones necesitan transformar sus defensas de seguridad en un sistema inmune integrado, donde el puesto de trabajo es una parte más a proteger"

Eduardo Argüeso, director de IBM Security para España, Portugal, Grecia e Israel

fidenciales, al mismo tiempo que permite a los empleados acceder a su correo electrónico, mensajes y aplicaciones personales. "La proliferación de dispositivos móviles puede socavar la seguridad de las redes empresariales en ausencia de políticas y disposiciones de seguridad eficaces", advierte un informe de Juniper Networks. "El mayor desafío relacionado con la proliferación de dispositivos móviles es cómo acomodar a todos los diferentes usuarios, muchos de los cuales tienen varios dispositivos ejecutando una variedad de aplicaciones diferentes, ya que se conectan a la red de la empresa de diferentes maneras en diferentes momentos y desde diferentes ubicaciones".



A medida que los trabajadores migran de una ubicación de escritorio fijo donde todo su trabajo está hecho, aquellos que buscan atacar a las redes corporativas están cambiando su enfoque de los sistemas operativos de escritorio a los sistemas operativos móviles. Esto significa que los planes de seguridad para la movilidad empresarial deben estar preparados para una gran variedad de ataques, incluyendo malware móvil, ataques de phishing, fugas de datos y vulnerabilidades en versiones anteriores de sistemas operativos.

Las principales preocupaciones

Según la encuesta de NetEnrich, el 45 por ciento de los encuestados dijo que el malware móvil era la mayor causa de ataques de movilidad de la empresa. Otra preocupación importante es la vulnerabilidad que plantea el acceso a los servicios públicos en la nube desde los teléfonos, ya que la nube pública aún no es lo suficientemente segura.

Utilizar el mismo dispositivo para el trabajo y el uso personal conlleva, para el 42 por ciento de los encuestados, que se produzcan fugas de datos debido a que se copian y pegan datos seguros a lugares no garantizados o públicos. Uno de los métodos más difundidos para contrarrestar esta amenaza específica es a través de la contenedorización o sandboxing. Un contenedor de datos seguro es una aplicación móvil utilizada para separar y asegurar una parte del almacenamiento de un dispositivo del resto del dispositivo. En esencia, permite crear un enclave seguro dentro del dispositivo donde puedes almacenar la información más sensible y que no pueda tener acceso a las aplicaciones o servicios que no tienen permiso.

Mientras que la contenedorización es una parte importante del plan de gestión de seguridad móvil de una empresa, su estrategia también debe incorporar medidas de seguridad adicionales, como el uso de la autenti-

CONFERENCIA DE CHEMA ALONSO EN CHILE: BIG DATA Y SEGURIDAD DE DISPOSITIVOS MÓVILES

CLICAR PARA VER EL VÍDEO

cación de dos factores y una lista blanca para aplicaciones aprobadas que los usuarios pueden descargar a sus dispositivos.

Según el informe de Juniper Networks, "es necesario tratar diferentes dispositivos de manera diferente, incluso para el mismo usuario, mientras se proporciona a todos los usuarios una experiencia de conectividad coherente y sin problemas, independientemente del dispositivo y el método de acceso utilizado".

Preocupados por la seguridad, olvidados en el móvil

Todo ello hace que David Sanz, EMEA Solutions Principal de Commvault, entienda que, en cierto modo, los dispositivos móviles los grandes olvidados de la seguridad corporativa "aunque hay diferentes grados de madurez en las empresas y, en general, se están dando algunos pasos hacia su protección, aún queda mucho recorrido". Y apunta algunos datos: según los analistas, el 50% de las organizaciones no tiene una estrategia de protección de datos de puestos de trabajo, pese a que la mayor parte de la información de las empresas hoy en

día reside en dispositivos de usuario – contando como tales ordenadores portátiles, móviles y tablets.

Pero si para alguien la seguridad móvil es una gran prioridad es para los CISO. Así al menos lo entiende Eduardo Argüeso, Director de IBM Security para España, Portugal, Grecia e Israel. "El problema es que todavía son muchas las empresas que no son conscientes de que una puerta abierta en el móvil de un empleado puede dejarla desvalida ante un ataque cibernético", asegura.

Argüeso también advierte de que los ciberdelincuentes han evolucionado y "son capaces de controlar el dispositivo móvil sin hacerse notar, con ataques cada vez más sofisticados. La falta de precaución es su principal aliada para adentrarse rápidamente en la red corporativa mediante un troyano, por ejemplo". Por eso, en su opinión lo principal es que la empresa "tenga capacidad de anticiparse y desarrollar una política de seguridad interna que deberá complementarse con una campaña de información y formación al usuario. El eslabón débil en la cadena de seguridad es siempre el ser humano. La compañía puede optar por crear restricciones en el uso y acceso de dispositivos o bien implementar una solución de gestión y seguridad robusta. Otra opción consiste en instalar un software en el dispositivo del usuario y gestionarlo de forma remota".

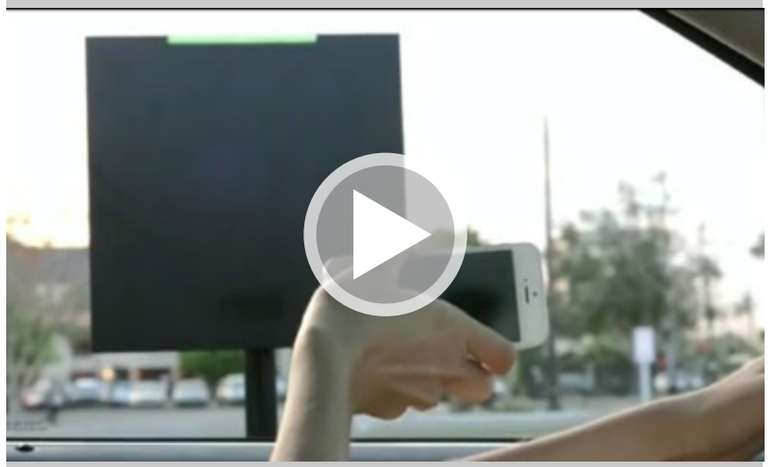
Pero, ¿por qué se ha tardado tanto en integrar la seguridad de los dispositivos móviles en la política corporativo? Los expertos de la unidad "Advanced Cybersecurity Services" de S21sec consideran que se debe a que las compañías no los han considerado una amenaza real, o no tan real como otras a las que se enfrentaban a

diario y, de hecho, aún sigue existiendo una gran falta de concienciación al respecto. "Muchas empresas creen que con tener sus redes y equipos protegidos es suficiente, cuando la realidad es que los últimos informes de seguridad, como el que publicó S21sec hace pocos meses dejan patente el extraordinario incremento del malware dirigido contra dispositivos móviles, sobre todo el del tipo ransomware y contra dispositivos Android", añaden.

Ni siquiera un antivirus

Resulta paradójico comprobar cómo, incluso a título personal, la seguridad en el móvil brilla por su ausencia. Puede hacer una pequeña prueba a su alrededor y preguntar cuántos tienen instalados un antivirus en su móvil. Prácticamente nadie tendría un ordenador sin,

SECURE ACCESS CONTROL WITH BLUETOOTH CELL PHONE MANAGED BY YOUR CORPORATE SECURITY SYSTEM



CLICAR PARA VER EL VÍDEO

"Efectivamente. Existe la falsa creencia de que en el móvil todo vale", aseguran los expertos de la unidad "Advanced Cybersecurity Services" de S21sec. "No concebimos navegar en nuestros equipos de sobremesa o portátiles sin una protección mínima, pero navegamos a diario con nuestro Smartphone, descargamos información, correos electrónicos, etc., sin ser conscientes del tremendo riesgo que estamos corriendo".

Y esto no solo sucede a nivel empresarial, también ocurre en nuestra vida cotidiana como usuarios. Según el Instituto Nacional de Estadística, los españoles ya nos conectamos a Internet con el móvil más que con cualquier otro dispositivo. "La respuesta ante esta realidad es solamente una: falta mucha concienciación sobre este tema en toda la sociedad", aseguran.

En términos parecidos se muestra Ángel Victoria, country manager de G DATA Software Iberia, quien lamenta que parece como si la seguridad no fuera un asunto de los dispositivos móviles. "Quizá porque inconscientemente seguimos pensando que la función primordial de nuestros actuales smartphones es realizar llamadas y no reparamos en que eso es ya secundario, que en realidad estamos ante ordenadores de bolsillo cuyas capacidades de almacenaje de información, procesamiento y comunicación son tan potentes como las de los ordenadores más sofisticados. Y, en consecuencia, son un objetivo claro del cibercrimen, como lo demuestran las cifras: más de 8.400 nuevas apps maliciosas para Android según el último informe de G DATA Security Labs".

A ello habría que añadir el hecho de que, a nivel personal, tenemos la falsa idea de que "nadie va a querer nuestras fotos o nuestra información, cuando hoy en día se utiliza esta información como moneda de cambio. No nos damos cuenta de que en la actualidad nuestros dispositivos móviles son una extensión de nosotros mismos y que tenemos tanta o más información en ellos que en nuestros propios ordenadores. Y además parte de esa información es muy sensible: desde el móvil accedemos a nuestras cuentas bancarias, correo electrónico o hacemos compras", explica David Sanz.

Mientras, en el terreno empresarial, "el problema suele estar en que se tiene la percepción de que la seguridad de la información corporativa y la privacidad del usuario están reñidas, cuando esto no tiene por qué

"La descarga de aplicaciones, ya sea de origen desconocido o desde tiendas oficiales, puede llevar oculto un malware o virus u otro tipo de código que nos puede salir muy caro"

Hervé Lambert, Retail Global Consumer Operations manager de Panda Security

Desarrollo Directivo

Equipos de Alto Rendimiento con

psicobusiness

ser así. En realidad, las empresas no tienen que invadir la privacidad de sus empleados si, además de plantearse instalar soluciones MDM (Mobile Device Management) en el dispositivo, que no son factibles en todos los casos, se definieran estrategias basadas en la información. De esta forma se podrían proporcionar los controles necesarios para mejorar la seguridad y la productividad, mientras disminuye el riesgo, con una buena aceptación de los usuarios".

La explicación a esta falta de conciencia es que aún no existe madurez en seguridad móvil y el empleado no es consciente de la importancia que tiene proteger adecuadamente su dispositivo. Éste es, precisamente para el responsable de IBM, el riesgo número uno. "Pero hoy en día, los usuarios se pueden conectar fácilmente desde fuera de la empresa y además, desde dentro, a través de múltiples canales de colaboración. Esto significa que las identidades están más expuestas que nunca y deben ser la primera línea de defensa frente a las amenazas", añade.

El responsable de Panda también asegura que la descarga de aplicaciones, "ya sea de origen desconocido o desde tiendas oficiales, puede llevar oculto un malware o virus u otro tipo de código que nos puede salir muy caro (alta a suscripción a SMS Premium, por ejemplo). Con un antivirus, este archivo malicioso será detectado y desinfectado al instante. Es cierto que la Play Store de Google está chequeando las apps que se suben aun así pillamos apps con código malicioso en ella".

Por eso recomienda la instalación de un antivirus, porque, además de en seguridad, puede ayudar a comprobar, en tiempo real, el consumo de las aplicaciones que estás usando en tu dispositivo; analiza y muestra los derechos de acceso de las aplicaciones instaladas (contactos, cuenta bancaria, fotos, etc.); facilita en caso de robo o extravío, saber dónde está tu teléfono móvil al instante; bloquearlo remotamente, evitar que alguien acceda a datos confidenciales del dispositivo o de la tarjeta de memoria SD; o bloquear el acceso a tus apps (Facebook, Whatsapp, Instagram,..) por medio de un PIN.

"La concienciación de los empleados juega un papel importantísimo, deben sentirse involucrados y responsables de aplicar un uso correcto en sus dispositivos"

Expertos de la unidad "Advanced Cybersecurity Services" de S21sec

Poner el parche antes de la herida

En opinión de David Alonso, director de B2B de Samsung España, "muchos de nuestros comportamientos de uso con el móvil son ciertamente arriesgados, como descargar apps de las que desconocemos su procedencia (algo que ha hecho la mayoría de usuarios en alguna ocasión) o entrar en enlaces maliciosos. Existe la creencia generalizada de que este tipo de prácticas nos puede acarrear simplemente una avalancha de spam o de publicidad no deseada. Sin embargo, los peligros van mucho más allá y pueden comprometer completamente la seguridad de nuestros datos y del dispositivo".

Además, recuerda que, según una investigación sobre seguridad en empresas europeas recientemente, "solo el 35 % de los trabajadores reconocía que acceder a la información de trabajo desde un dispositivo móvil puede no ser seguro, lo que da una idea del grado de desconocimiento generalizado".

Desafortunadamente, "a veces es necesario que un ataque masivo nos ayude a tomar conciencia de verdad. Como ha sucedido con WannaCry, que nos ha recordado a todos la importancia de mantener los equipos

"Los dispositivos móviles deben estar protegidos con tecnología de encriptación avanzada y permitir configurar perfiles personales y de trabajo separados para garantizar la seguridad y la privacidad de los empleados"

David Alonso, director de B2B de Samsung España

actualizados… una de las recomendaciones de seguridad en la que los fabricantes llevamos años insistiendo", recuerda Ángel Victoria.

Porque, pese a que en opinión de IBM la mayoría de las empresas sí son conscientes de las amenazas y riesgos a los que se enfrentan, "pero, sorprendentemente, hasta ahora no han abordado el tema con determinación", se hace más necesario "concienciar y formar a los empleados y también utilizar la tecnología para reducir el riesgo de comprometer la seguridad de la empresa. De hecho, más de la mitad de los usuarios creen que la seguridad en ellos es igual o superior a la de sus PCs o portátiles, lo cual es peligroso pues puede provocar incluso que bajen la guardia".

El EMEA Solutions Principal de Commvault considera que el problema es que muchas empresas piensan que no les va tocar, "pero la cuestión no es si les tocará o no, sino cuándo ocurrirá. Por eso es imprescindible estar preparados". ¿Y cómo podemos prepararnos? "Desarrollando un programa basado en los datos, no en el dispositivo. Debemos identificar dónde están almacenados los datos, determinar los flujos de trabajo y los sistemas que se utilizan para manejarlos, evaluar los riesgos, aplicar controles de seguridad y planificar ante posibles amenazas. Si algo no está protegido, no se puede recuperar. Además, se deben emplear procesos de backup y de recuperación ante desastres que incluyan protección contra amenazas tipo ransomware. Por último, hay que utilizar tecnologías de protección contrastadas, que detecten y notifiquen ataques potenciales, y que conserven una imagen de referencia de los sistemas y configuraciones con una estrategia de backup completa".

Estos son los principales riesgos

¿Cuáles son las principales amenazas o riesgos que se corren con los dispositivos móviles a la hora de plantear la seguridad corporativa? Eduardo Argüeso cree que las principales amenazas son el phishing, los ataques mediante ingeniería social y el malware, los cuales pueden venir por diferentes medios como el correo electrónico, un SMS engañoso, un acceso WIFI en un lugar público o, incluso, a través de una petición de contacto por Bluetooth. "Las amenazas a las que se enfrentan están evolucionando y cada vez son más sofisticadas. El cambio ya está aquí. Más dispositivos, más puntos de acceso y más datos valiosos en la nube que nunca antes".

Por todo ello, considera fundamental que "las organizaciones pongan en marcha un enfoque mucho más proactivo e integrado, alineado con las exigencias de cumplimiento normativo. Las organizaciones necesitan transformar sus defensas de seguridad en un sistema inmune integrado, donde el puesto de trabajo es una parte más a proteger. Este sistema hará posible las analíticas de seguridad y defensa en tiempo real".

¿POR QUÉ ME VIGILAN, SI NO SOY NADIE? MARTA PEIRANO. TEDXMADRID

CLICAR PARA VER EL VÍDEO

Estas amenazas descritas no son muy diferentes a los riesgos que los que afectan a un equipo de sobremesa. "Al final, el dispositivo móvil es un terminal que puede tener acceso a la red corporativa, nos sirve para navegar, descargar correos electrónicos, nos descargamos apps, guardamos información confidencial... Además, tiene el riesgo añadido el de ser un dispositivo que fá-

cilmente se puede extraviar, perder o ser sustraído. Esto hace que sea más sensible si cabe y que por tanto haya que aplicar unas políticas muy concretar para paliar estas amenazas", especifican desde S21Sec.

Y es que virus, robo de información, fuga de datos corporativos, servir de puerta de entrada a la red corporativa... Todos estos riesgos son peligros reales. "Desde un punto de vista empresarial, los dispositivos móviles almacenan agendas, correos electrónicos y un largo etcétera de información sensible de cada organización. Y, además, pueden ser usados como puerta de entrada a la red corporativa", explica el responsable de G Data.

Y, como recuerdan desde Commvault, la entrada en vigor del GDPR añade aún más presión, "ya que las organizaciones tienen la responsabilidad de proteger los datos personales de sus empleados y clientes".

David Alonso considera que todos estos peligros son igualmente graves, aunque el acceso por parte de los hackers a la red corporativa "puede tener consecuencias nefastas e impredecibles. Si los atacantes toman el control de la red corporativa, no solo pueden robar gran cantidad de información confidencial y sensible, sino que también se puede poner en peligro el propio suministro de servicios y ejecución de operaciones de la empresa afectada. Este tipo de ataques tiene además un efecto dominó (del proveedor al cliente, del cliente al colaborador…) muy peligroso".

IDENTIDAD, ADMINISTRACIÓN MÓVIL Y SEGURIDAD TRABAJANDO EN CONJUNTO PARA TU EMPRESA

CLICAR PARA VER EL VÍDEO

Más que un botiquín, un escudo

Hemos querido conocer también cuáles serían las medidas básicas que toda empresa debería tener implantadas en materia de seguridad de dispositivos móviles. Podemos decir que la política de seguridad móvil empresarial "debe extender de la forma más natural posible las políticas de información existentes (normalmente aplicadas a entorno de centro de datos) al mundo móvil. Luego hay particularidades como BYOD o el uso de nubes públicas, pero esto debe abordarse desde un marco común de gestión de información corporativa", determina Sanz.

Por tanto, no basta con instalar una app de seguridad (aunque también es recomendable). "Cuando hablamos de empresas el dispositivo móvil tiene que estar gestionado por el mismo administrador de sistemas que ya controla la seguridad de ordenadores, servidores y portátiles. El smartphone es tan solo un dispositivo más y tiene que formar parte de la infraestruc-

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

"Lo más recomendable sería que no hubiera una política BYOD, pero es tan caro para la empresa como desagradable para los trabajadores"

Lorenzo Martínez, Securízame

Ingeniero Informático de profesión y experto en seguridad informática, Lorenzo Martínez pertenece a ANCITE (Asociación Nacional de Ciberseguridad y Pericia Tecnológica), cuenta con certificaciones CISA y CISSP y es el fundador de la empresa Securízame.

Como asesor en temas de seguridad de grandes empresas, considera que los dispositivos móviles ya no son ("o deberían") los grandes olvidados de la seguridad corporativa, pero sí que "muy posiblemente, junto con los usuarios en sí, sin lo más complicado de securizar, plataformar y controlar, sobre todo en casos en los que impera el BYOD, traducido originalmente como Bring Your Own Device o con acepciones posteriores como Bring Your Own Disaster o Bring Your Own Damage".

Por eso, considera que "lo más recomendable sería que no hubiera una política BYOD, y que el uso del dispositivo profesional estuviese completamente restringido a las aplicaciones corporativas, con limitación de instalación de software de cualquier tipo, así como de navegación por lugares no recomendables, así como cumplir con estrictas medidas de seguridad en cuanto a la existencia passcode de acceso, complejidad y política de cambio del mismo, etc.". Sin embargo, asegura que esta opción, "que a mi criterio es la más segura", es "tan cara para la empresa como desagradable para los trabajadores, puesto que tienen que cargar con dos teléfonos, y el corporativo, en líneas generales suele ser de menos prestaciones que el personal, por lo que el equipo "se cuelga", va lento, le dura poco la batería...".

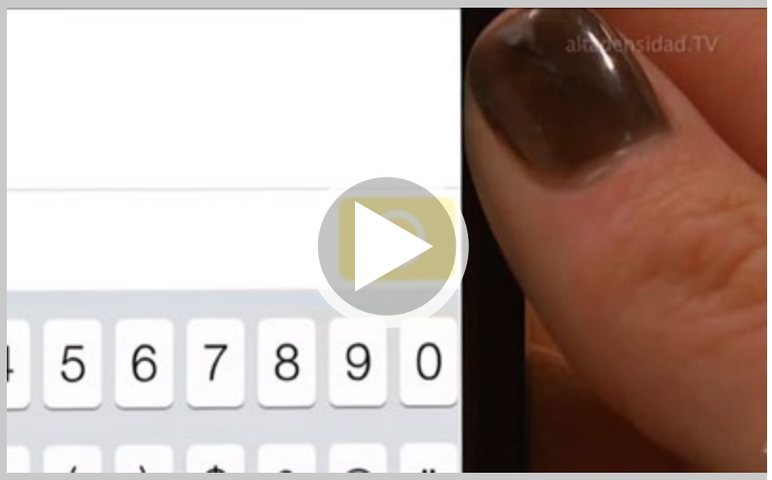
Por eso, en aquellas empresas donde sí impere el BYOD, Martínez ve una buena opción el "ofrecer a los trabajadores la posibilidad de llegar a un win-win, por el que el software antivirus o el de gestión MdM lo paga la compañía, y buscar alternativas que les aporten valor a los dueños de los equipos", con mensajes como "Tu información estará siempre respaldada", "Si pierdes el dispositivo, nos lo notificas y podremos buscarlo", "la empresa te ayuda a proteger tu información", etc. En cualquier caso, y sobre si la empresa puede exigir a sus empleados que instalen determinadas aplicaciones de seguridad, Martínez aclara que no es abogado especialista en temas laborales, pero que, en cualquier caso, "mi experiencia como trabajador durante 17 años y con gente a mi cargo desde hace menos, es que las imposiciones y exigencias nunca son buenas. Es mejor intentar llegar a un entendimiento o un acuerdo con tu gente, y que trabajen a gusto, estando concienciados de la importancia de lo que llevan en el bolsillo".

¿Recomendaría al menos tener un antivirus en cada móvil? "Depende fundamentalmente del sistema operativo del dispositivo, puesto que para mundo iOS no hay antivirus que valga puesto que, a no ser que tengas jailbreak hecho al smartphone, si no está en iTunes -el market de Apple-, simplemente no está. En el caso de Android, sí que hay una oferta variada de antimalware. Cierto es que se ha demostrado en varias ocasiones que no demuestran un grado de eficiencia del 100%, pero aunque sólo fuese del 20%, si yo usase Android, te aseguro que tendría un software antimalware instalado", asegura.

Y en este punto remarca que aunque podamos creer que las amenazas móviles son un bulo, "existen. Están ahí y en general yo diría que lo más peligroso es la instalación de software por parte del usuario. La diversidad de aplicaciones con múltiples utilidades, a veces incluso que rozan el frikismo o lo rocambolesco, es lo que hacen que confiemos en darle acceso a un montón de secciones del móvil".

Respecto a los mayores peligros, este experto en seguridad cree que, a nivel particular, el "malware que inutilice el teléfono, que consuma los datos, que exponga nuestra información (fotos, conversaciones, correos, cuentas que conforman nuestra identidad digital...). Sin embargo, a nivel empresarial, me centraría en la fuga de datos corporativos (desde comunicaciones hasta la propia agenda de contactos o reuniones), así como la propiedad industrial que todo ello encierra. Y en general, todo suele ser por una app con demasiados permisos, o por no disponer de un mecanismo de acceso al dispositivo protegido correctamente, que pueda hacer que alguien generalmente con acceso físico al equipo, lo envenene en un momento de descuido".

8 CONSEJOS DE SEGURIDAD PARA TU DISPOSITIVO MÓVIL



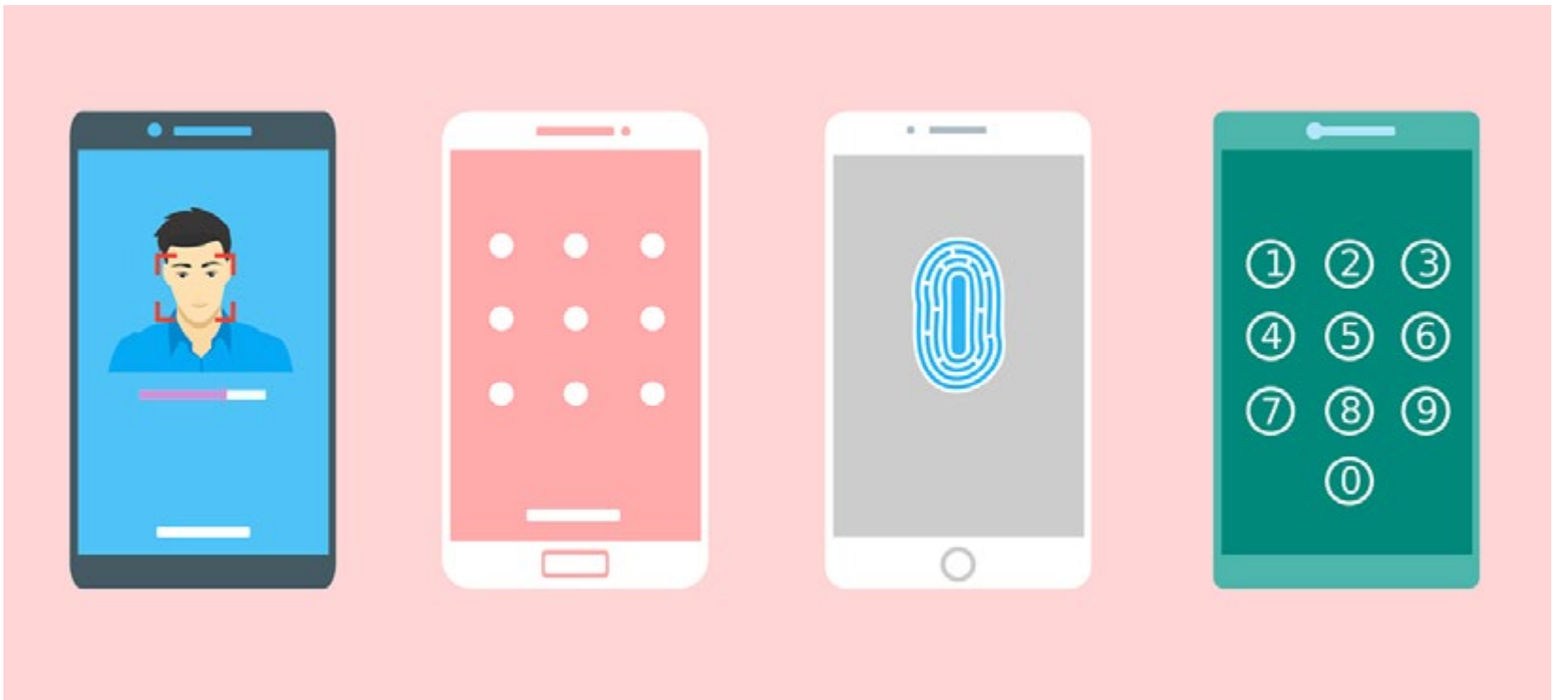
CLICAR PARA VER EL VÍDEO

en caso de pérdida o robo. No podemos dejar la responsabilidad en manos del empleado, porque lo que no se puede administrar no se puede proteger con eficacia. Y para ello, no basta una app de seguridad, es necesario recurrir a soluciones de seguridad empresarial que incluyan un módulo MDM (Mobile Device Management)", explica el country manager de G DATA Software Iberia.

Desde S21Sec creen que la clave está en establecer políticas y mecanismos apropiados de seguridad para dichos dispositivos que permitan gestionarlos y controlarlos en todo momento (herramientas MDM) y garantizar que en estos dispositivos se sigue una misma línea de cumplimiento y seguimiento de las políticas establecidas. "Los equipos de TI deberán controlar, por ejemplo, el acceso a las aplicaciones y recursos de la red con las garantías de seguridad, detectar manipulaciones indebidas en los terminales, poder bloquear remotamente un dispositivo si este ha sido robado o extraviado, detectar malware, actualizar contraseñas, etc. También es imprescindible tener en cuenta que la concienciación de los empleados juega un papel importantísimo, y que éstos deben sentirse involucrados y responsables de aplicar un uso correcto en sus dispositivos".

Por su parte, el director de IBM Security para España, Portugal, Grecia e Israel, declara que la protección del dispositivo, la revisión de la seguridad de los aplicativos, una adecuada gestión de identidades, y la concienciación de los empleados para que apliquen el sentido común y unas mínimas medidas de seguridad son las áreas básicas en las que las empresas tienen que poner foco si hablamos de seguridad móvil.

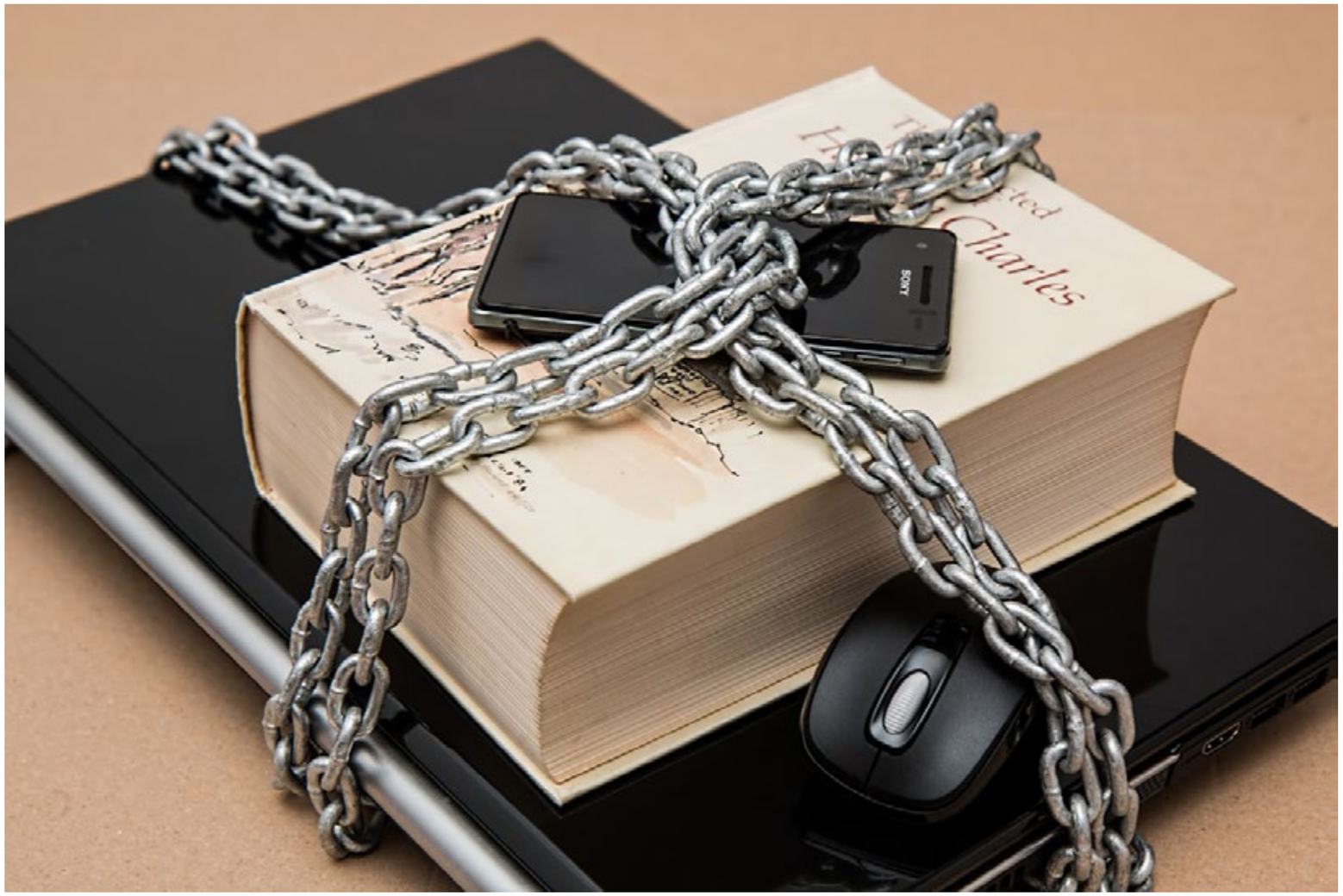
Respecto al primer punto, entiende que es frecuente la utilización de soluciones de MDM (Mobile Device Management) para la protección y el control remoto de los dispositivos. "En este sentido y como punto de partida, las políticas de seguridad deberán aplicarse de igual forma y con independencia a si se permite el uso de dispositivos personales para tener acceso a las aplicaciones empresariales, o se utilizan únicamente móviles de empresa. La revisión de la seguridad de los aplicativos idealmente debería integrarse desde su conceptualización y durante todo su ciclo de vida mediante el paradigma de "security-by-design" o "security-by-default", si bien al menos es imprescindible un análisis exhaustivo antes de su paso a producción y revisiones



periódicas posteriores según el riesgo para el negocio", añade.

Además, y en lo que a la gestión de identidades se refiere, este responsable considera que las empresas están dotándose de mecanismos para controlar el acceso a la información de la organización mediante una aproximación integral, incorporando a sus clientes y a sus proveedores digitales a la hora de pensar e implementar sus controles de identidad y de gestión de acceso. "A partir de aquí y en función del riesgo y los medios de la organización, se deberían complementar las medidas preventivas descritas antes con el despliegue de sistemas de monitorización, y capacidades cognitivas de inteligencia y detección de fraude en las transacciones móviles".

Como enumera Heré Lambert, los principios básicos de seguridad en dispositivos móviles pasan por cuatro puntos: 1- un antivirus "de última generación que permita auditar todos los dispositivos que se conecten en las empresas"; 2- una política de seguridad móvil "de calidad y muy robusta, que cuente con controles y auditorías"; 3- políticas claras y controles del software que se usa; y 4- un sistema de comunicación encriptado.

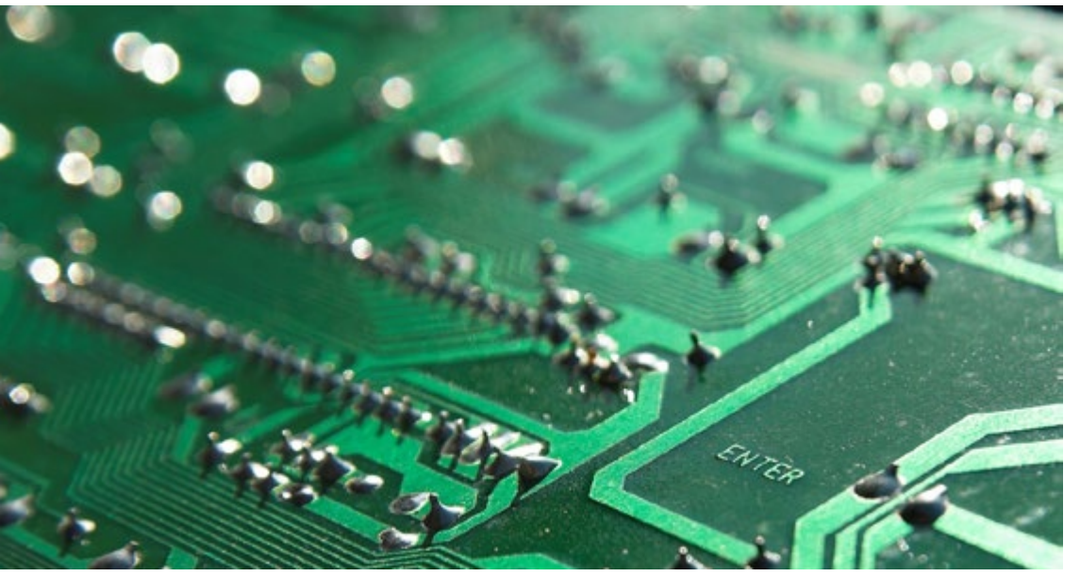


Las obligaciones del BYOD

Sin embargo, desde hace tiempo se constata que cada vez más empresas tienen en marcha políticas BYOD (Bring Your Own Device). En este escenario, ¿se puede obligar a instalar una determinada herramienta de seguridad por parte de la empresa?

"La protección del dispositivo y de los aplicativos es fundamental y los empleados deben saber que la empresa ha de aplicar las mismas políticas de seguridad a estos dispositivos", incide el responsable de IBM. "Hoy en día, los usuarios se pueden conectar fácilmente desde fuera de la empresa utilizando sus terminales móviles, y además realizar prácticamente las mismas operaciones que habitualmente realizan cuando están usando el PC en su puesto de trabajo, lo que significa que el potencial impacto de un ataque y de que datos confidenciales (información sensible, propiedad intelectual, planes estratégicos...) caigan en otras manos será muy similar en ambos casos". No obstante, considera que tambié es importante "garantizar una protección diferenciada del entorno ocupado por las aplicaciones empresariales del entorno de uso particular del dispositivo".

En este punto el máximo responsable de G Data se muestra tajante. "Por supuesto que la empresa puede exigir al empleado la instalación de una solución de seguridad en su smartphone. La empresa es dueña de su



red empresarial y puede exigir a sus empleados que se conecten a dicha red desde equipos seguros. Es legítimo que los empleados prefieran usar sus dispositivos particulares a los ofrecidos por la propia empresa, pero eso no significa que se deban obviar unos requisitos de seguridad mínimos".

El problema, según Sanz, es que el enfoque más tradicional a la hora de proteger dispositivos móviles en las empresas son las soluciones MDM (Mobile Device Management) centradas en el dispositivo. "Estas soluciones aportan su valor, pero su aproximación centrada en el dispositivo hace que en algunos casos no sean suficientes. En el caso de Bring Your Own Device, al entrar en juego la privacidad del usuario, los MDM no siempre son bien acogidos. Por eso hay que pensar en soluciones que protegen lo que realmente queremos salvaguardar desde el punto de vista empresarial: la información corporativa creada y accedida desde dispositivos móviles, sin tocar la parte personal".

Desde S21Sec se apuesta por el hecho de que la compañía garantice una política de seguridad centralizada, "con las soluciones de seguridad que se decidan estratégicamente, tanto en la red como en los dispositivos, y que controle en todo momento los usos y aplicaciones que los empleados hacen de los recursos móviles".

En este punto, el responsable de Samsung señala que los dispositivos móviles "deben estar protegidos con tecnología de encriptación avanzada y, además, permitir configurar perfiles personales y de trabajo separados no solo para garantizar la seguridad sino también la privacidad de los empleados", mientras que los usuarios "deben respetar normas básicas como no entrar en sitios no verificados o no descargar ficheros de remitentes desconocidos".

Enlaces relacionados

Si quieres leer íntegramente las entrevistas realizadas para elaborar este reportaje, puedes hacerlo en este enlace

- W BYOD: Consideraciones de seguridad y riesgos para tu programa de dispositivos móviles
- I 2016, año de récord para el ransonware
- W El impacto de los dispositivos móviles en la seguridad de la información
- I La mitad de los incidentes de seguridad en 2016 los sufrieron dispositivos móviles
- W Ciberamenazas contra los teléfonos móviles
- I España quiere ser un referente en ciberseguridad
- W Gestión de la seguridad en un mundo móvil
- I El malware para dispositivos inteligentes se duplicará en 2017
- W Dispositivos móviles: ¿son seguros o un riesgo para la seguridad?
- I Las pymes, las más perjudicadas por el cibercrimen
- W Guía para gestionar la seguridad de los dispositivos móviles en la empresa
- W Políticas de seguridad para el uso de dispositivos portátiles en entornos corporativos

Movilidad y seguridad: ¿una quimera?

Difícil nos sería hoy encontrar una empresa, independientemente de su tamaño, sector o nivel de transformación digital, que no se enfrente al problema de securizar dispositivos móviles. El avance imparable de la movilidad ofreció una serie de beneficios a los que ninguna empresa quería renunciar. Sin embargo, no en todos los casos se prestó la debida atención a la seguridad a la hora de integrar la movilidad en las empresas, lo que ha supuesto y supone, un problema para muchos responsables de TI.

¿Es equiparable el nivel de concienciación con la seguridad que tienen los responsables de TI y los usuarios empresariales? ¿Se ha convertido la movilidad en un grave problema de seguridad para las empresas? ¿Es esta movilidad la que obliga a una empresa con límites difusos y, por tanto, más difíciles de proteger? ¿Existen vías para proteger los dispositivos móviles de igual forma y con similares resultados que si se protegen el resto de elementos de una empresa?

Éstas y otras preguntas son las que queríamos responder en esta Mesa Redonda IT, y, para ello, hemos querido contar con Mario García, director general España y Portugal de Check Point Software Technologies; Raúl Flores, system engineer de F5 Networks; y Juan Miguel Haddad, responsable de la Unidad de Negocio de Puesto de Trabajo de VMware.

Pero antes de adentrarnos en el área específica de la seguridad de la movilidad, quisimos preguntar a los miembros de la mesa por la situación en que queda el mundo de la seguridad después de los ataques y la repercusión de WannaCry y Petya, y sobre la realidad de unas empresas cuyos responsables siempre colocan la seguridad como una de las grandes preocupaciones y objetivos de mejora en las encuestas año tras año. En este sentido, Mario García, director general España y Portugal de Check Point Software Technologies, indica que "el entorno cada vez es más inseguro, y la cantidad de amenazas existentes se multiplican de forma exponencial mes a mes y casi día a día. La diferencia principal es que ahora ha llegado a los medios de comunicación. Porque las empresas no llevan años preocupadas por la seguridad, sino que se empiezan a preocupar ahora. Y, en el caso específico de los dispositivos móviles, estamos muy lejos, casi no hemos empezado el camino y lo que nos queda por recorrer es enorme. Sin embargo, lo bueno de estos dos últimos ataques es

que sirven para que las empresas se conciencien y se preparen".

Raúl Flores, system engineer de F5 Networks, coincide con él, y señala que "siempre ha habido ataques, pero el hecho de que lleguen a los medios de comunicación nos va a ayudar a concienciar bastante. Los ataques cada vez son más avanzados, mezclando diferentes amenazas. Y, encima, en España, cada vez que ha habido un ataque se ha preferido ocultar y que nadie se entere. La parte positiva es que existen herramientas para paliar o evitar estos ataques, pero todavía no han llegado a los clientes, que tienen que invertir más en seguridad".

Juan Miguel Haddad, responsable de la Unidad de Negocio de Puesto de Trabajo de VMware, también se muestra en una línea similar al indicar que, sin duda, "falta mucha seguridad en las empresas. Pero si lo ligamos a la movilidad, al menos podemos decir que los ataques de esta semana no han sido específicos para dispositivos móviles. Han sido ataques más cercanos a los sistemas más convencionales, pero con otros fines que los de años atrás. Pero, por supuesto, hay mucho que mejorar en el ámbito de la seguridad informática".

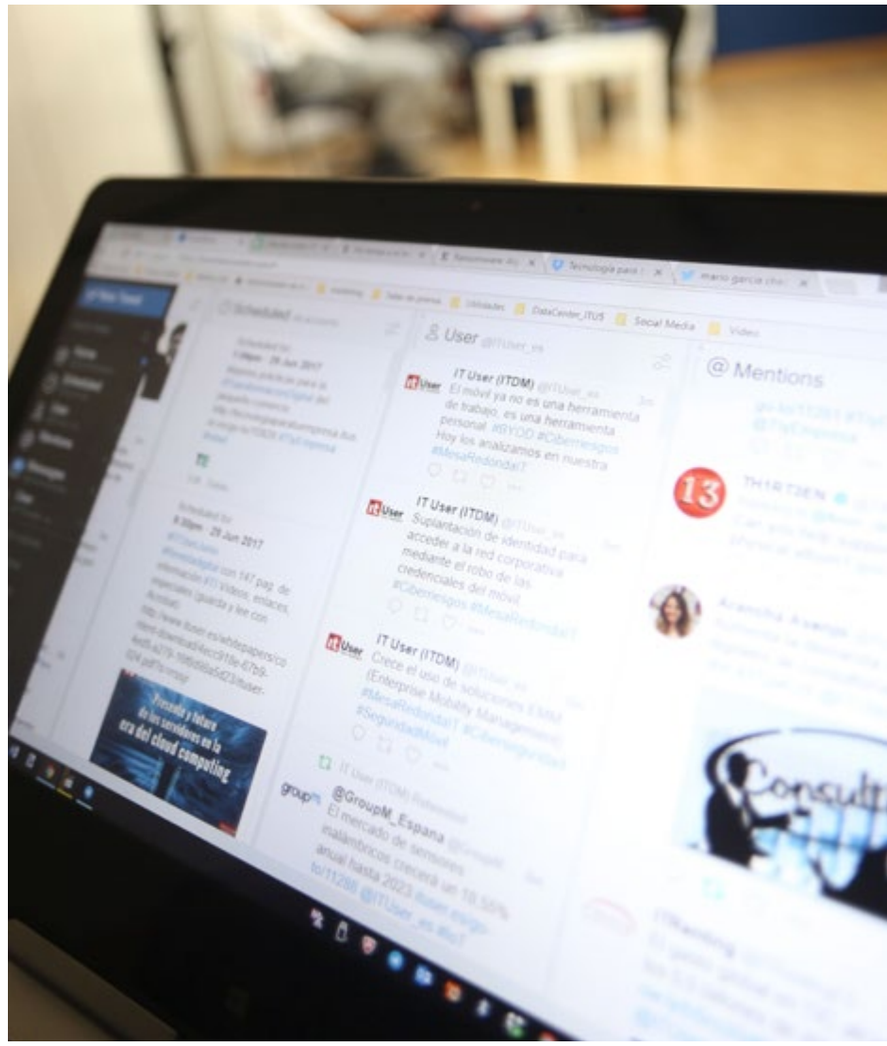
La seguridad, una preocupación para las empresas, ¿en qué se traduce?

Sin embargo, como comentábamos, la seguridad lleva años en el top 3 de las preocupaciones de las empresas, sin que esto parezca que se note en la realidad de las inversiones. Para Mario García, "hay muchas personas preocupadas por el calentamiento global o por el hambre en el mundo, pero eso no quiere decir que enfoques tus esfuerzos directamente en solucionar el problema. Han podido tomar algunas medidas, pero no se ha convertido esa preocupación en una intervención real sobre el problema".

"Lo que han demostrado estos ataques", añade, "es que han podido dejar a las empresas fuera de línea. Antes no podían parar ni un minuto para implementar una herramienta de seguridad, pero ahora se han dado cuenta de que si no tienen la empresa preparada el tiempo de parada es mucho mayor. En esa evaluación del riesgo, ya no solo tienen en cuenta la pérdida de datos, sino también el tiempo sin poder trabajar. El coste en horas, en muchas empresas de España, ha sido elevado. Así que esperemos que esa preocupación se convierta, por fin, en poner los medios para que no ocurra".

MESA REDONDA IT. SEGURIDAD Y MOVILIDAD, ¿UNA QUIMERA?

CLICAR PARA VER EL VÍDEO



Dispositivos móviles, ¿uno de los principales vectores de ataque?

En opinión de Raúl Flores, "no es la principal puerta de entrada de malware, pero hay que empezar a tomar conciencia de que hay un riesgo creciente. Eso sí, hay que analizar cada caso, porque no es lo mismo que los usua-

"Es difícil para un director de TI, porque trabajaban de una forma y en los últimos años toda su experiencia de décadas ha saltado por los aires"

Mario García, director general España y Portugal de Check Point Software Technologies

rios traigan su propio dispositivo a la empresa (BYOD) a que estos mismos usuarios accedan a dispositivos que ya están integrados en la propia plataforma de la compañía. Tampoco es lo mismo que el que acceda a los datos o una aplicación sea un trabajador o un cliente".

Pero la realidad es innegable y, según añade Flores, "en 2016 se descubrieron 23.000 ejemplos de aplicaciones falsificadas para introducir malware, con lo que sí es cierto que está creciendo el malware para dispositivos móviles".

¿Se piensa en la movilidad cuando se securiza una empresa?

Cuando parece que puede empezar a haber un mayor número de empresas concienciadas con la seguridad, ¿se tendrán en cuenta la movilidad y los dispositivos móviles en estas políticas de protección? En palabras de Juan Miguel Haddad, "yo creo que sí, y, de hecho, lo están teniendo en cuenta. Lo primero es la concienciación de las empresas. Éstas deben ser conscientes de que los dispositivos móviles pueden ser una fuente de malware, pero, también, una fuente de fuga de información. Se trata, por tanto, de instalar soluciones que gestionen el dispositivo móvil y lo securicen correctamente, tanto para que no entre malware como para que no se instalen aplicaciones nocivas en esos dispositivos. Y, por otro lado, proteger los elementos del dispositivo desde los cuales se acceder a información específica de la empresa, ya sea el correo electrónico, ya sean repositorios de datos… Las empresas lo están viendo, y están implantando, en mayor o menor medida, soluciones de Enterprise Mobility Management (EMM) que permitan gestionar esto".

Movilidad: libertad frente a seguridad

El uso de la movilidad en la empresa aporta, entre otros aspectos, más libertad a la hora de trabajar. Sin embargo, esto choca de forma casi frontal con la necesidad de mantener la empresa y los datos en un entorno seguro y protegido. Es algo que implica a TI, a la dirección y a los empleados. Y la pregunta es obvia, ¿son conscientes todos de la necesidad de este equilibrio?

Mario García nos responde con un rotundo no, y añade que "la movilidad y la capacidad que ofrecen ha pillado en total fuera de juego a los departamentos de TI y de seguridad. Ahora hay empresas pensando en esto, cuando la revolución de la movilidad ya llegó hace varios años, y cuentan con cientos de empleados accediendo al correo y otros recursos de la empresa desde el móvil. Ahora empiezan a darse cuenta de que hay datos importantes en los móviles y, además, hay otro claro vector de ataque no para robar datos, ni para alterar aplicaciones o para acceder a mensajes y llamadas, que es posible, sino para robar las credenciales corporativas. Con eso, pueden suplantar la identidad del usuario para introducir malware en la red corporativa".

Además, añade un ejemplo muy esclarecedor. "Podemos poner una reja en la ventana, pero si dejamos al lado las llaves de la puerta, no necesitarán entrar por la ventana, sino que accederán por la puerta".

El problema, prosigue García, "es que el móvil no es solo una herramienta de trabajo, sino que es una parte de la vida personal del usuario, y éste suele ser poco receptivo a las limitaciones por seguridad".

Porque BYOD, apunta Haddad, "es una realidad, y es responsabilidad de la empresa, ser consciente de los mecanismos que existen para separar la identidad personal de la profesional. Es absolutamente obligatorio que las empresas cuenten con herramientas para separar ambos mundos en el dispositivo del usuario, porque, al final, se trata de una herramienta con la que el usuario no quiere complicarse. IT tiene que facilitarle la vida al empleado y, a la vez, llevar el nivel de seguridad al nivel necesario".

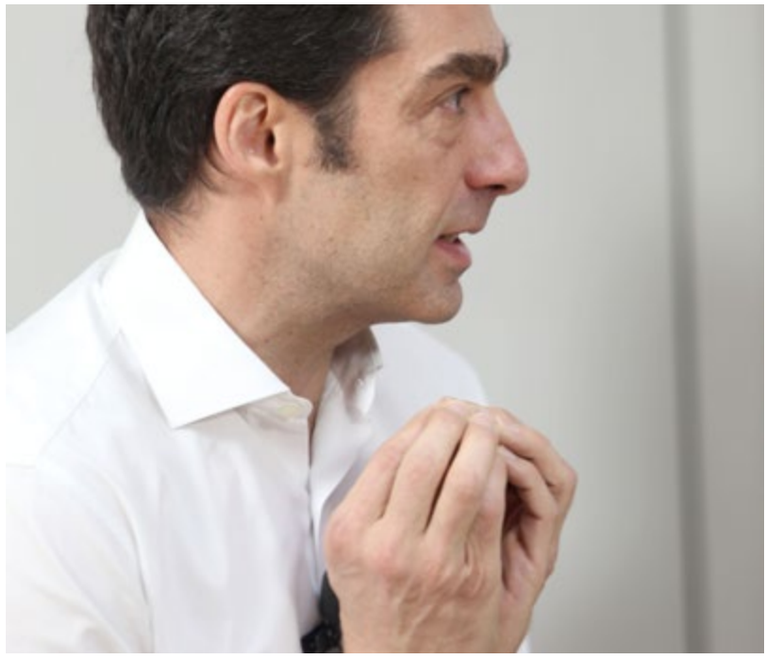
Pero, ¿y el usuario? "Es necesaria mucha evangelización para concienciar al usuario", apunta Raúl Flores, que añade que cuando éste se enfrenta a las aplicaciones corporativas "es más consciente, sabe que tiene que poner su usuario y contraseña, pero si cuenta con malware en el dispositivo, le estarían robando las credenciales de acceso, incluso al Directorio Activo. Lo que hay es que securizar el acceso desde dispositivos móviles a la aplicación dependiendo de lo que denominamos el contexto, con más o menos medidas para asegurarlo. Eso sí, ese mismo usuario emplea el dispositivo para su vida personal y ahí no es consciente para nada del riesgo, aunque sea un problema para su faceta profesional posteriormente".

"En 2016 se descubrieron 23.000 ejemplos de aplicaciones falsificadas para introducir malware, con lo que sí es cierto que está creciendo el malware para dispositivos móviles"

Raúl Flores, system engineer de F5 Networks

Usuarios y políticas de seguridad

Muchos usuarios tienden a ser menos cumplidores con políticas de seguridad corporativas si éstas son complejas. Pero ¿esto es peor cuando hablamos de dispositivos móviles? En opinión del director general de Check Point en España y Portugal, "a veces sí, pero es injustificado, porque todo el mundo hace transferencias bancarias con el móvil, y no hay nada más complicado. Los usuarios están preparados para hacerlo si es su dinero, así que deberían implantarse políticas de seguridad razonables, aunque sean complejas para el usuario. Dependiendo del tipo de usuario, el nivel de seguridad puede ser uno u otro, pero hay rebeldías de los usuarios que no pueden ser permitidas por el bien de la seguri-



dad de la empresa. Las normas no pueden ser opcionales ni permitir atajos".

¿Qué pasos debe dar un responsable de TI para poder tener cierto nivel de tranquilidad con los dispositivos móviles de la empresa? En opinión de Juan Miguel Haddad, "lo primero que tiene que asumir es que la casa ya no es como la conocíamos. Ya no tienes toda la información en el CPD, sino que hay información en la nube, ya sea privada o pública, y muchos puntos de acceso. Con lo que la casa ya incluye también el campo que la rodea, y hay que tener en cuenta muchos elementos. La clave está en la identidad del usuario y en todos los elementos que atañen a este usuario. Se debe conseguir que todos los accesos desde un dispositivo móvil sean lo más seguros posibles. Por otro lado, hay que evitar que puedan extraer información del propio dispositivo. Evidentemente, es algo complicado, pero tenemos mecanismos para alcanzar cierto grado de seguridad, siempre que se definan y se implanten".

> *"La clave está en la identidad del usuario y en todos los elementos que atañen a este usuario. Se debe conseguir que todos los accesos desde un dispositivo móvil sean lo más seguros posibles"*
>
> *Juan Miguel Haddad, responsable de la Unidad de Negocio de Puesto de Trabajo de VMware*

Se muestra de acuerdo Raúl Flores, que añade que "existen esos mecanismos y hay que ponerlos en funcionamiento. Se puede filtrar también por el contexto o asegurarse de que no existe un malware en ese dispositivo, antes de nada. Son herramientas que existen y se pueden implementar. También hay que tener en cuenta análisis de riesgo, porque hay sistemas que no controlan, por ejemplo, que un usuario se conecte a su red desde Madrid y una hora después lo haga desde Brasil. Hay que tener sistemas que alerten de estos riesgos. Las herramientas están disponibles, pero las empresas deben implementarlas".

En opinión de Mario García, "es difícil para un director de TI, porque trabajaban de una forma y en los últimos años toda su experiencia de décadas ha saltado por los aires. Si no hacen algo en la empresa, alguien lo va a hacer por ellos, ya sea darle un acceso a la nube, una aplicación o un dispositivo. Es la puerta al Shadow IT, que no debería existir en ninguna empresa para ningún concepto. Pero existe, porque la respuesta de TI no ha sido lo suficientemente rápida para el negocio. Pero si le añadimos el componente de seguridad, la situación se complica todavía más. Por tanto, los directores de TI tienen que redefinir totalmente como planteaban su realidad y, a eso, añadirle el componente de seguridad, porque no hacerlo puede dejar a una empresa fuera, no solo de la competición, sino de la existencia".

Enlaces relacionados

- W El impacto de los dispositivos móviles en la seguridad de la información
- I La mitad de los incidentes de seguridad en 2016 los sufrieron dispositivos móviles
- W Ciberamenazas contra los teléfonos móviles
- I España quiere ser un referente en ciberseguridad
- W Gestión de la seguridad en un mundo móvil

NO SOLO it

Psicobusiness

¿Insatisfacción en la innovación? No con PsicoBusiness

Por Asier de Artaza, director de www.yesmanagement.es

En la nube

BlockChain, la innovación en el mundo de las aplicaciones

Por Kevin L. Jackson, experto en Cloud y fundador de Cloud Musings

Tecnología y Negocio

Telefónica, CaixaBank, El Corte Inglés, Inditex y Mercadona, empresas españolas más exitosas

Por Jorge Díaz-Cardiel, socio director general de Advice Strategic Consultants

Social & Business

Cómo usar Gmail como herramienta de marketing

Por Juan Merodio, experto en Marketing 2.0, redes sociales y Web 2.0

Internet de las Cosas

IoT y Transformación Digital, retos y oportunidades

Por Dario Ferraté, consultor TIC

Asier de Artaza Azumendi
Director de
www.yesmanagement.es

¿INSATISFACCIÓN EN LA INNOVACIÓN? NO CON PSICOBUSINESS

El 72% de los nuevos productos se estrellan cuando tocan el mercado *(fuente: Simon Kucher)*, mientras que el 6% de los ejecutivos están satisfechos de gestión de la innovación en sus compañías *(fuente: McKensey)*.

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

En fin, con estas cifras tan terribles no estamos diciendo que seamos tontos a la hora de lanzar o innovar en un producto o servicio, sino que no seguimos la orientación y el recorrido adecuado, desde un punto de vista metodológico, ni utilizamos las herramientas adecuadas y, por tanto, las decisiones que tomamos nos conducen al fracaso.

Sin embargo, veamos otro caso más alentador: nuestro tan sobado Apple. La compañía de la fruta mordida ganó el 94% de todos los beneficios del mercado de smartphones con tan solo una cuota de mercado de 14,5%. Impresionante, pero ¿dónde está la cuestión de fondo?

Pues una vez más en la comprensión de la mente y el comportamiento humano aplicado al negocio; digamos que hablamos de Psicobusiness. Y es que no nos cansamos de relacionar la Psicología y el negocio, porque las empresas están formadas por personas y ellas son las que fabrican, gestionan y consumen. Con lo cual, por favor, desterremos de una vez algunos conceptos, como que las empresas fabrican productos y servicios que venden al comprador que usa sus productos. ¡Mal, mal y mal! Las personas actúan exclusivamente por inputs emocionales y se conducen bajo diferentes estilos de comportamiento, y para eso ya tenemos las herramientas de Ensize, comentadas en otros artículos y que nos dan una importante información. Así que, por favor, utilizadlas

Lo primero que tenemos entender es qué actividades, tareas, tiene que hacer el cliente para realizar su trabajo que tiene relación con nuestro ámbito

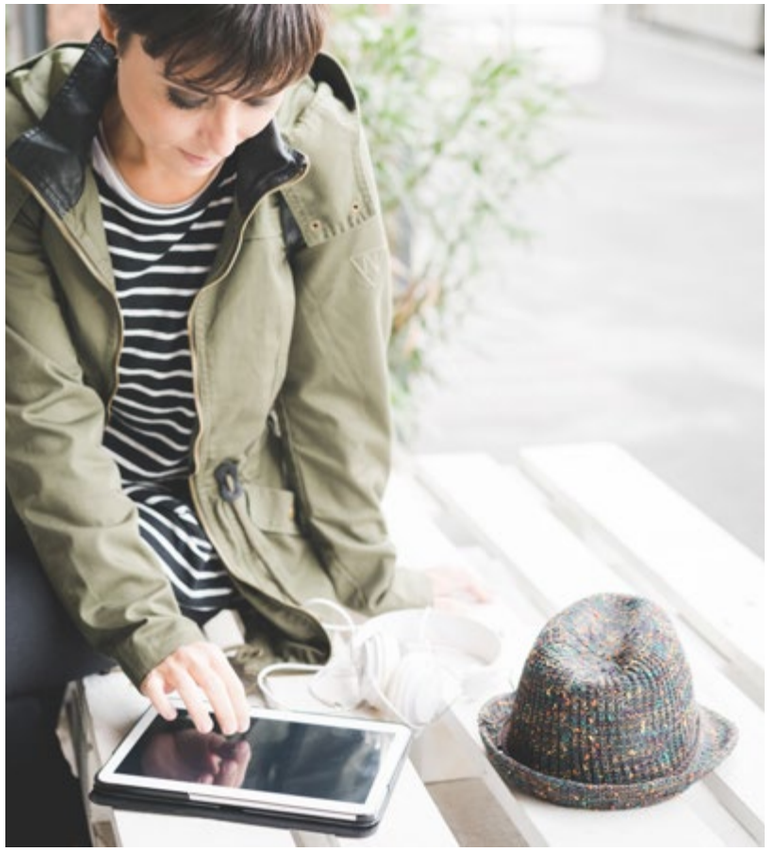
y algo ya habremos avanzado, pero no nos descarrilemos, nos habíamos quedado en inputs emocionales.

Así que, si fabricamos taladros y nos volvemos locos con que la precisión de entrada en la pared de la broca sea pluscuamperfecta, posiblemente esto no aporte ningún valor al cliente, es decir, no emocione para nada al cliente, y, por tanto, será una pérdida de tiempo y dinero. Bueno ya tenemos dos palabrotas, emoción y valor para el cliente; como vemos, de momento, de producto nada de nada. Y, ¿por qué? Porque el producto no es el fin, sino el medio. ¿El medio para qué? Pues para emocionar al cliente.

Vale, entonces, el tema va de emocionar al cliente, perdón, que los tecnólogos y marketinianos lo llaman Customer Experience in the business night, bueno, sí, vale, yo tengo mi corazoncito marketiniano, 12 años de director de marketing no se olvidan… pero también tengo un corazón ¡pragmático y honesto! Y es que este concepto se conoce en Psicología desde hace más de 100 años, eso sí, aplicado a otros contextos.

Pero no sólo la psicología lo conoce, hace ya 30 años surgió en libro específico llamado Experiential Maketing que, si bien no trataba con toda su dimensión estas cuestiones, sí hacía unas interesantes aportaciones; y, bueno, hace al menos 40 años que nuestro amigo Philip Kotler lo llevó a las aulas y despachos a través del concepto de necesidad del cliente o de evitar la "óptica de producto". Así que el tema no va de lanzar productos, sino de atender emociones o satisfacer necesidades.

Dicho esto, las empresas que fallan lo hacen porque lanzan productos o iniciativas de innovación, sin tener



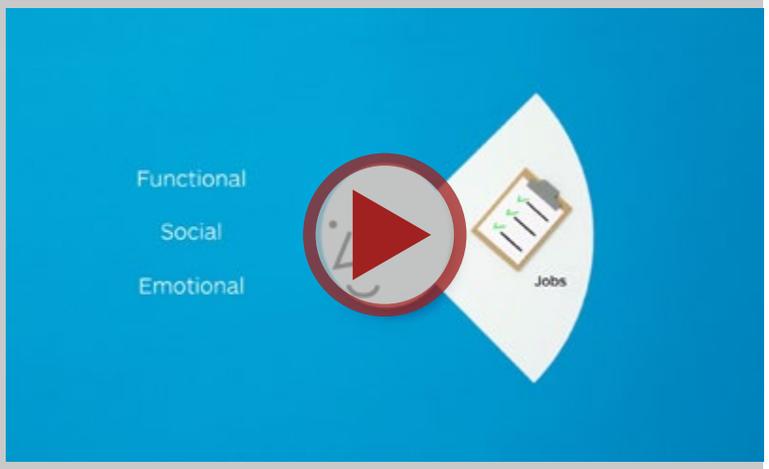
en cuenta con la profundidad suficiente las emociones y necesidades de los clientes. Eso sí, se preocupan por hacer un Business Megaplan en un Excel que lo aguanta todo y un TeraPowerpoint que les permite sentirse publicistas creativos, y que encima se encariñan cada vez más con un producto que antes de nacer ya tiene una enfermedad terminal.

Y ahora lo mejor, luego lo lanzan al mercado y viene el siguiente disparate, se matan en la ejecución, en "business development and performance", perdón que me estaba quedando poco "cool". Es decir, por hacerlo viable, se dejan la piel en la escalada de una montaña que nunca coronarán y caerán en picado cuando hayan agotado hasta la última de sus fuerzas; bueno, que termina con un tremendo os… osado disparate.

Con lo cual, si hablamos de valor, de emoción, como algo que mueve al individuo (e – motion = e- motor) y le lleva a cubrir esa necesidad, nos encontramos con que donde está el juego, el terrible, difícil, abstracto y difícil juego, es precisamente no en el lado del producto, sino al otro lado de la barra, en la mente del decisor de compra. Ahí es donde tenemos que dejarnos todos los esfuerzos, en entender eso. Vale, muy bien y cómo nos vamos acercando a ese conocimiento, pues muy bien y muy poco sencillo, haciendo unas hipótesis y preguntándole.

Vayamos entonces a por las hipótesis. Lo primero que tenemos entender es qué actividades, tareas, tiene que hacer el cliente para realizar su trabajo que tiene relación con nuestro ámbito. A estas cosas que hace, darles intencionalidad, porque no olvidemos que siempre estará presente una parte de actividades orientadas a la tarea, otra dirigidas a sus necesidades sociales, (el qué piensan de mí), y finalmente, la más importante de todas, sus necesidades personales de cómo me siento… yo muy, pero que muy, bien.

THE VALUE PROPOSITION CANVAS



CLICAR PARA VER EL VÍDEO

Vale pues esto es sólo el medio, no el fin, es decir esas tareas que él emprende porque es lo que considera que tiene que hacer, tendrán que ser exitosas, y aquí empieza el juego, ¿cuándo percibe él que ha hecho las cosas con fundamento? Perdón, que sigo nada cool, ¿cuándo percibe él un "well-done job"?

Pues nada a pensar en los indicadores de éxito que él maneja, cuáles son los resultados mínimos, los esperados, los deseados y los que le sorprenderían al realizar esas actividades del trabajo. Porque ahora sí que tenemos la diana para construir un producto que le genere valor y lo desee. En tanto en cuanto él tenga esas ganancias, esas alegrías o esas satisfacciones gracias a nuestra propuesta de valor, estará encantado de entregarnos a cambio su dinero. Así que tendrá que haber una relación lógica entre lo que le llene nuestra propuesta y lo que esté dispuesto a pagar por esa aportación.

¡Qué bonito es todo! Pero no, nos falta un elemento. A nuestro amigo también hay un espectro oscuro de cuestiones, que le molesta, le frustra, le ralentiza o le impide conseguir sus objetivos. Estas cuestiones también debemos de localizarlas, porque todos esos aspectos en el caso de ser aliviados con nuestra propuesta de valor, entonces le generarán más satisfacción acumulada y seremos todavía más deseados.

Conclusión, me entero de lo que tiene que hacer, porque desde aquí obtendré las dos claves, que son; ¿cómo mide el hacerlo bien? ¿Que le impide o empeora

El 72% de los nuevos productos se estrellan cuando tocan el mercado; mientras que el 6% de los ejecutivos están satisfechos de gestión de la innovación en sus compañías

hacerlo bien? Y ya tengo el caldo de cultivo a trabajar, respecto al aportar de mis productos y servicios para conseguir una Mega User Experience looking for the bright side of life.

Obtenido esto nos deberíamos fijar cómo es el encaje de sus necesidades-motivaciones y la propuesta de valor que le entrego en mi modelo de negocio. Pero bueno, para esto ya mejor me mandáis un mensaje por Linkedin que tiene también su miga.

Pero claro, tampoco desde el despacho con cuatro reuniones en las que hacemos nuestras hipótesis vamos

Todo este proceso podríamos denominarlo como la navegación en marejada que tiene de puerto de salida la idea de la innovación y como puerto de destino un negocio rentable, sostenible y escalable

a dar en el clavo, vamos, que ni de coña, así que clasifiquemos nuestras hipótesis por orden de menos peso a más, la que menos nuestras opiniones, la siguiente nuestras experiencias en la materia, la tercera y más importante, la información del mercado. Así que nada, para el mercado a preguntar, explorar, comprender, validar, modular, ampliar, reducir, añadir, quitar… y todo lo que se os ocurra, también.

¿Y qué vamos a obtener en nuestra incursión en el mercado? Pues un bamboleo "quepaqué". Por eso lo recomendable es inicialmente no desarrollar con muchos detalles nuestras hipótesis, sino ir profundizando gradualmente según el mercado nos va dejando las cosas más claras. Llegar a mucho detalle, que luego nos van a desmontar, sólo nos da trabajo y complejidad en la gestión.

Todo este proceso podríamos denominarlo como la navegación en marejada que tiene de puerto de salida la idea de la innovación y como puerto de destino un negocio rentable, sostenible y escalable.

Con lo cual en una rueda de reiterados intercambios de información con el mercado, bueno llamémosle "una guapa interación (con una c solo) plena en la dimensión Lean Startup", obtendremos un matrimonio casi perfecto entre lo que necesita y emociona a nuestro cliente, y las aportaciones de nuestra propuesta de valor, a través de nuestro producto, servicio, producto ampliado y relación con el cliente.

Y, para terminar, visualizaremos el caso de Hilti. Esta empresa líder, tras volverse loca en la búsqueda de crecimiento empresarial, no había tenido otra fijación que crear las mejores herramientas de mano (taladros industriales...), hasta que se dio cuenta de que las especificaciones como la precisión de la entrada de la broca en la pared era irrelevante para que les comprase su cliente, las empresas constructoras.

Y lo que sí que era decisivo tenía que ver con cumplir los plazos de ejecución de sus contratos, el no tener que hacer inversiones adelantadas en recursos, tener siempre el conjunto de herramientas más moderno y en mejor estado, y poder hacer un cálculo exacto de costes en sus presupuestos al cliente, para no estar al amparo, entre otras cosas, de si tendría que comprar más herramientas de las esperadas, lo que le mermaría su margen; o que los posibles fallos en las herramientas le harían retrasarse y tener que pagar tremendas penalizaciones en sus contratos.

Como vemos, todo esto nada tiene que ver con las especificaciones del producto, y finalmente el crecimiento del negocio le vino de la mano del lanzamiento de un servicio de suscripción mensual de cuota fija donde Hilti garantiza que el cliente the right tools, right place, right time. El cliente emocionado y el proveedor bien rentabilizado. ¡Hasta el mes que viene!

Enlaces relacionados

- The value proposition Canvas
- Psicobusiness
- Ataques con exploits. De las amenazas diarias a las campañas dirigidas
- La paradoja tras la experiencia del usuario con el Criptornsomware

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

La Cadena de Bloques:

la innovación en el mundo de las aplicaciones

¿Hay algo más que bitcoin dentro de blockchain? Definitivamente sí, ya que la blockchain actual está abriendo un nuevo camino para la provisión de servicios online de confianza.

Entender esta afirmación implica ver la cadena de bloques como algo más que su caso de uso más famoso (bitcoin). Blockchain, como herramienta digital fundamental, es un libro mayor inmutable para registrar historiales de transacciones. Usado de esta forma, permite habilitar aplicaciones transaccionales con atributos integrados de confianza, rendición de cuentas y transparencia. A diferencia de una blockchain Bitcoin que dependa

Consenso: códigos de enrutamiento compartidos

Problema: Los competidores y los colaboradores necesitan compartir datos de referencia, pero cada parte mantiene su propio libro mayor, y debe redirigir a una autoridad central para su cobro y reconciliación.

Solución: Blockchain proporciona un registro seguro y compartido del estado del contrato, que se actualiza automáticamente a medida que progresan la compra y la entrega, algo que está disponible para todas las partes, incluyendo entidades financieras y partners.

Ventajas

- Datos consolidados y uniformes, con una menor tasa de errores
- Mayor transparencia para los participantes en la red

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.

BLOCKCHAIN EN 3 MINUTOS

CLICAR PARA VER EL VÍDEO

Los responsables de innovación en prácticamente cualquier sector podrán de esta forma construir, ejecutar y gestionar su propia red blockchain corporativa

del intercambio de criptodivisas con usuarios anónimos en una red pública, una blockchain Corporativa permite establecer una red permissioned (privada) con identidades conocidas y verificadas, con una visibilidad transaccional que hace posible que todas las actividades dentro de dicha red sean observables y auditables por cualquier usuario. Esta visibilidad end-to-end, conocida también como ledgering (apuntes contables) compartido, puede también vincularse con reglas y lógica de negocio que permitan asegurar la confianza, transparencia e integridad en toda la red corporativa. Las aplicaciones construidas, gestionadas y permitidas en este entorno adquieren así un historial verificable, con una seguridad integrada que hace posible:

- Evitar que ningún usuario -incluso los usuarios root y los administradores- tomen el control de un sistema
- Rechazar intentos ilícitos de modificación de datos o aplicaciones dentro de la red
- Bloquear accesos a datos no autorizados asegurándose de que las claves de encriptación no puedan utilizarse de manera ilegítima

Procedencia: mantenimiento de vehículos

Problema: el seguimiento del origen y movimiento de piezas en una cadena de suministro compleja es una tarea complicada y susceptible a errores

Solución: Blockchain permite a todos los usuarios de la cadena de suministro monitorizar los movimientos mediante un registro común, transparente y accesible, con un análisis forense mucho más rápido en caso de retirada de producto

Ventajas

- Mayor confianza, con registros inviolables
- Las retiradas son aisladas, en lugar de afectar a toda la flota

Inmutabilidad: contabilidad financiera

Problema: Tanto auditoría como compliance requieren un registro de todas las transacciones durante el período correspondiente a cada informe, a pesar de la dispersión habitual de los datos de carácter financiero en la estructura de las grandes organizaciones (divisiones, países ...)

Solución: Blockchain registra transacciones de una gran variedad de sistemas y fuentes de datos de carácter financiero, con atributos inviolables, para crear una pista de auditoría de confianza, que se convierte en la única fuente fiable, proporcionando funcionalidades de privacidad que garantizan el acceso para los usuarios autorizados.

Ventajas

• Reducción de costes de auditoría y compliance regulatorio

• Simplificación de procesos y mejoras en la cronología de auditores y/o reguladores

Desde el punto de vista de los distintos sectores verticales de la economía, este enfoque permite:

- Reducir el tiempo necesario en las entidades financieras para la liquidación de valores de días a minutos
- Reducir el número de retiradas de producto de los fabricantes, dado que los registros de producción estarían compartidos con los OEM (fabricantes de equipos originales) y los reguladores
- Gestionar de manera más precisa el flujo de bienes y sus correspondientes pagos con mayor celeridad y menor riesgo en empresas de todo tipo

Los responsables de innovación en prácticamente cualquier sector podrán de esta forma construir, ejecutar y gestionar su propia red blockchain corporativa. Incluso si la empresa no está lista para asumir el grueso de la carga de trabajo, siempre podrá contratar servicios blockchain a través de distintos proveedores.

Proyectos como el Hyperledger ofrecen además la opción de Ready-made frameworks a través de las iniciativas de colaboración open source para el desarrollo de tecnologías blockchain transversales, de aplicación a distintos sectores. Las opciones hyperledger business frameworks disponibles incluyen:

- **Sawtooth** - una plataforma modular para la construcción, despliegue y ejecución de distributed ledgers que incluye un algoritmo de consenso dirigido a grandes grupos distribuidos de validadores con un consumo mínimo de recursos
- **Iroha** - un framework de blockchain corporativo diseñado para su incorporación en proyectos de

CÓMO BLOCKCHAIN CAMBIARÁ RADICALMENTE LA ECONOMÍA

CLICAR PARA VER EL VÍDEO

Las aplicaciones construidas, gestionadas y permitidas en este entorno adquieren un historial verificable con una seguridad integrada

infraestructura que precisen tecnologías distributed ledger

- **Fabric** - una estructura base para el desarrollo de aplicaciones o soluciones con una arquitectura modular que permita disponer de componentes -como servicios de consenso y membership- tipo plug-and-play
- **Burrow** - una máquina inteligente de contratos inteligentes que proporciona un cliente blockchain modular con un intérprete permissioned de contratos inteligentes integrado de acuerdo con las especificaciones de la Máquina Virtual Ethereum (EVM)

(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)

En un equipo interesado en la innovación, y con vocación por liderar su sector, las blockchains corporativas pueden ser la opción perfecta para el desarrollo de nuestras aplicaciones de negocio.

Enlaces relacionados

- Blockchain
- Atributos integrados
- Punto de vista de los distintos sectores verticales
- Servicios blockchain
- Hyperledger
- Barómetro de emprendimiento de éxito en España
- Bankia Índicex. La digitalización de las empresas en España
- Plan Digital 2020. La digitalización de la sociedad española

Jorge Díaz-Cardiel
Socio director general de Advice Strategic Consultants

Telefónica, CaixaBank, El Corte Inglés, Inditex y Mercadona, empresas españolas más exitosas

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.

El Estudio "Advice de éxito empresarial" analiza –por séptimo año consecutivo y trece oleadas semestrales- quiénes son las grandes empresas españolas más exitosas en el mercado nacional, de entre los principales sectores de actividad económicos que componen nuestro Producto Interior Bruto, como Telecomunicaciones, Banca, Gran Distribución, Infraestructuras, Energía, Turismo/Cadenas Hoteleras... Este año, dada la cantidad de operaciones corporativas en marcha, las muestras del estudio se han incrementado con 2.400 personas en población general y 800 líderes de opinión, con un índice de confianza del 95,5% y margen de error del +-1,8%.

Telefónica, La Caixa-CaixaBank y El Corte Inglés, son las tres grandes empresas españolas mejor gestionadas empresarialmente y, en consecuencia, con más prestigio y mejor reputación: son los rasgos que más las definen. Les siguen compañías como Inditex, Mercadona, Banco Santander y Gas Natural Fenosa. Inditex preside el ámbito textil (seguida por Mango, H&M Primark y Cortefiel), Mercadona está asociada a "una política de precios muy barata" en Alimentación, Banco Santander sobresale por su exitosa trayectoria internacional y Gas Natural Fenosa es referente mundial en energías limpias y eficiencia empresarial.

El Estudio muestra que, "en el mercado español, Telefónica lidera telecomunicaciones; CaixaBank el sector financiero, El Corte Inglés la gran distribución, Inditex el sector Textil y venta Retail; Mercadona, la Alimentación; Gas Natural Fenosa, el sector energético; Abertis la gestión de infraestructuras; Meliá el sector turístico y Cellnex Telecom la gestión de infraestructuras de Telecomunicaciones en Europa. Mapfre lidera en seguros, SEAT en Automóviles y e Iberia en aerolíneas. En 2017 suben Gas Natural Fenosa, Vodafone, Bankinter y Gestamp, descendiendo Grifols, Orange, Banco Popular y Ferrovial, El Estudio analiza las primeras 200 empresas de España por facturación en los sectores clave de la actividad económica de España".

Los principales cambios con respecto a 2016 se producen en Telecomunicaciones, donde Vodafone se despega fuertemente de Orange y se sitúa segunda tras Telefónica; Turismo, en que Meliá sustituye a Barceló y en Gestión de Infraestructuras de Telecomunicaciones, en que aparece una empresa catalana líder europea, Cellnex Telecom. En Banca, Banco Popular pasa al último lugar con una evolución negativa a lo largo de doce meses, versus Bankinter, que avanza posiciones y lidera la banca mediana, por encima de Banc Sabadell. En construcción ACS arrebata a Ferrovial la primera posición del sector

La ficha técnica del estudio es la siguiente: con un índice de confianza del 95,5% y un margen de error del +-1,8% para el total de la muestra, se han llevado a cabo 800 entrevistas entre líderes de opinión (empresarios, analistas, periodistas, académicos, políticos, representantes del tercer sector) y 2.400 entrevistas entre población general, reflejando estadísticamente la sociedad española por criterios sociodemográficos. El estudio es cuantitativo y se ha realizado mediante entrevista telefónica. El trabajo de campo se realizó entre los meses de enero a mayo de 2017 y ésta es la séptima edición anual del estudio Advice de éxito empresarial y su oleada semestral número trece. El reforzamiento y de las muestras (en 2016 fueron 1.800 personas en población general y 600 entre líderes de opinión) se debe a los cambios corporativos producidos en el último año en la gran empresa en nuestro país, que se refleja, por ejemplo, en la entrada de Vodafone, Bankinter y Gestamp entre las grandes empresas y la salida de Grifols o la OPA de Atlantia por Abertis, aún en sus inicios cuando se produjo el trabajo de campo o encuestación.

En cada uno de sus sectores las tres primeras empresas han obtenido las mejores calificaciones en los parámetros del éxito empresarial, situándose como líderes de su sector Telefónica, La Caixa y El Corte Inglés

Partiendo del nivel de conocimiento informado que tienen los españoles acerca de nuestras grandes empresas, destaca que Telefónica, La Caixa-CaixaBank, El Corte Inglés, Inditex, Mercadona, Banco Santander y Gas Natural Fenosa son las empresas más conocidas por los españoles, por encima del 80%. Sólo las tres primeras superan el 90% en conocimiento, alcanzando, Telefónica, La Caixa y El Corte Inglés una familiaridad cercana al 99%. Esto las convierte en las más cercanas y son conocidas mediante diversas formas de comunicación.

Canales de comunicación de las empresas para darse a conocer

Sobre los canales a través de los cuales se dan a conocer las grandes empresas españolas, por este orden sobresalen "las noticias que sobre ellas aparecen en los

Los principales cambios con respecto a 2016 se producen en Telecomunicaciones, donde Vodafone se despega fuertemente de Orange y se sitúa segunda tras Telefónica

medios de comunicación" (prensa, radio, TV), "los patrocinios", "el tipo de actividad a que se dedican", "las campañas de publicidad" y "las noticias que sobre ellas se pueden leer en Internet" (redes sociales, blogs…), todos estos canales tienen una valoración superior al 7 en una escala de 1 a 10.

Las noticias aparecidas en los medios es un canal de información empresarial relativamente más usado por mujeres, menores de 35 años, personas de clase alta/media-alta, estudios superiores, residentes en Cataluña o Madrid, personas que viven en poblaciones de más de 50.001 habitantes y aquellos que priman en el éxito empresarial la buena reputación.

Factores del éxito empresarial

Los parámetros -cuarenta- que han sido considerados como más importantes en la composición del éxito empresarial de las grandes empresas españolas en la primera mitad de 2017 han sido: "liderazgo en innovación", "buen trato a clientes", "tener productos o servicios de calidad", "presencia internacional", "implicación social", "gestión empresarial efectiva", una "buena reputación" y "una adecuada relación con clientes, accionistas y empleados", de entre cuarenta parámetros de gestión empresarial.

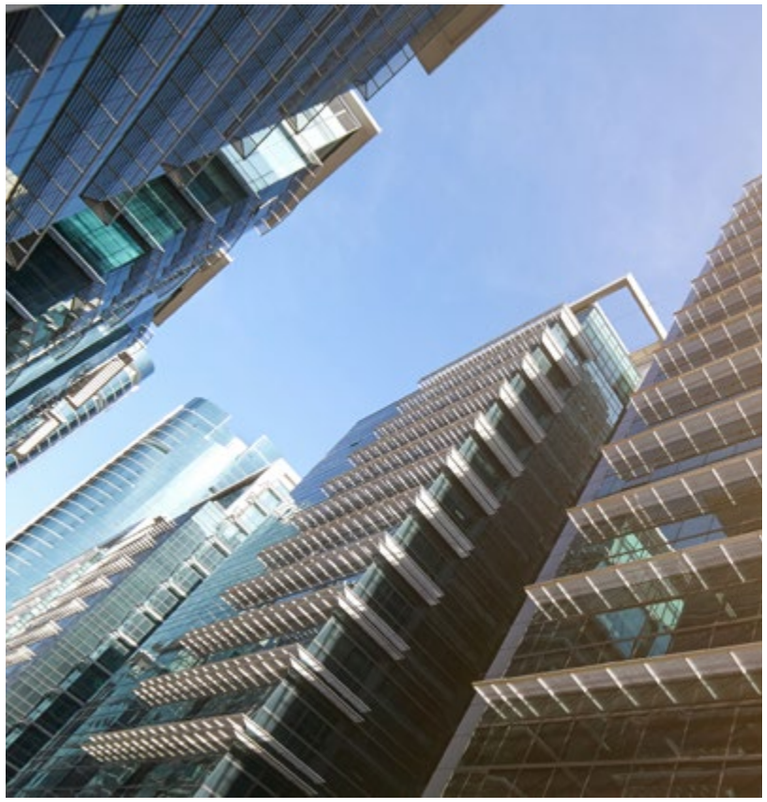
De entre esos factores, los dos que más cumplen las grandes empresas españolas exitosas son "el estar bien gestionadas" y "tener una buena reputación".

Rasgos que más caracterizan a las empresas más exitosas de España

Telefónica destaca por ser la empresa más innovadora de España, La Caixa-CaixaBank por su implicación social (responsabilidad social empresarial) y liderazgo sectorial y El Corte Inglés por tener productos de calidad y su transformación digital hacia el comercio electrónico. Abertis ha sobresalido por su liderazgo mundial en gestión de infraestructuras, factor en el que Foro Económico Mundial da un sobresaliente a España. Durante el período de campo del Estudio Advice de éxito empresarial se anunció la OPA de la italiana Atlantia sobre la española Abertis y las reticencias -según los medios de comunicación- a la operación del gobierno español.

Cada una de estas empresas está haciendo una aportación esencial a la economía: en el caso de Telefónica, porque la innovación es parámetro esencial para desarrollar la Sociedad del Conocimiento y crear un nuevo modelo productivo sostenible. La Caixa tiene una doble faceta: como banco (CaixaBank), encabeza el ranking en el mercado nacional y apoya a las pymes y autónomos, que son el 99,88% del tejido empresarial español; al mismo tiempo, gracias a su Obra Social,

El Corte Inglés, mediante sus centros comerciales y la venta online, es un termómetro del principal aportador actual al crecimiento económico de España: el consumo interno



hace una contribución a la sociedad que se traduce en empleo, innovación, proyectos sociales, cultura, emprendimiento y medioambiente; además es el banco digital y tecnológicamente más innovador del mundo (Forrester, 2017). El Corte Inglés, mediante sus centros comerciales y la venta online es un termómetro del principal aportador actual al crecimiento económico de España: el consumo interno.

En cada uno de sus sectores las tres primeras empresas han obtenido las mejores calificaciones en los parámetros del éxito empresarial, situándose como líderes de su sector Telefónica, La Caixa y El Corte Inglés. Es decir, todas ellas han obtenido las más altas puntuaciones en liderazgo en innovación, buen trato a clientes, tener productos o servicios de calidad, implicación social, gestión empresarial efectiva, una buena reputación en medios de comunicación y una adecuada relación con clientes, accionistas y empleados. De las tres, Telefónica es la que sobresale por su internacionalización.

Por sectores de actividad, el ranking de empresas más exitosas en España es el siguiente:

En Telecomunicaciones, lidera Telefónica, seguida por Vodafone -que sube puestos-, seguida de lejos por Orange.

En Banca, lidera CaixaBank-La Caixa en el mercado español, seguida por Santander y BBVA. La banca mediana para a estar liderada por Bankinter, que sustituye a Banc Sabadell en el ranking; luego van Bankia y Banco Popular, el primero mejorando, el segundo, empeorando.

En Distribución, lidera El Corte Inglés, seguido por Inditex, Mercadona, Carrefour, Alcampo y Eroski.

En Energía, Gas Natural Fenosa lidera el ranking de compañías de gas y electricidad, seguida por Iberdrola y Endesa; Repsol encabeza el ranking de empresas petrolíferas.

En Turismo, destacan, por este orden: Meliá, Barceló, AC Hoteles, NH, Ritz-Carlton y Paradores Nacionales.

El trabajo de campo se realizó entre los meses de enero a mayo de 2017 y ésta es la séptima edición anual del estudio Advice de éxito empresarial y su oleada semestral número trece

Y, en Gestión de Infraestructuras, lidera Abertis seguida por las empresas constructoras, ACS, Ferrovial, Acciona, OHL, Sacyr y FCC.

En Gestión de Infraestructura de Telecomunicaciones destaca Cellnex Telecom, compañía catalana presente en el IBEX-35, líder europeo.

Por lo que se refiere a las relaciones que las empresas más exitosas de España tienen con sus accionistas, por este orden, Telefónica, La Caixa-CaixaBank y El Corte Inglés destacan por sus buenas relaciones con los medios de comunicación, los clientes, los accionistas y los empleados.

En Telefónica se hace un seguimiento muy fuerte de su aparición en las noticias de los medios de comunicación; en La Caixa-CaixaBank, tiene una importancia esencial la notoriedad de la Obra Social y la innovación tecnológica y de El Corte Inglés, hay un gran conocimiento, derivado de la actividad que realiza en su propio sector de gran distribución y la expansión del comercio electrónico y su posible salida a bolsa.

Hay otros sectores donde también sobresalen campeones nacionales: en aerolíneas, Iberia, pues afecta al negocio turístico. En Automoción, SEAT, aunque pertenezca a un grupo multinacional alemán (le sigue Citroen, que es francesa). En Seguros, Mapfre y la Mutua Madrileña. Entra en el ranking Gestamp y baja muchos puestos Grifols.

Enlaces relacionados

- Estudio Advice Éxito Empresarial
- La comunicación al servicio del éxito empresarial
- Evolución y perspectivas del e-commerce 2017
- Spain e-commerce Outlook
- Cómo ser el mejor en Internet
- Mejores prácticas para optimizar la experiencia digital del cliente

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

Cómo usar Gmail como herramienta de publicidad

Los anuncios de Gmail son mensajes que aparecen en formato email en la parte superior de la pestaña "Promociones" dentro de la cuenta de Gmail de los usuarios, y que permite que el usuario entre, lo vea y si le interesa haga clic y generes una conversión.

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.

¿Te avisamos del próximo IT User?

GOOGLE ADWORKS EN MENOS DE 5 MINUTOS

CLICAR PARA VER EL VÍDEO

Es importante que selecciones la segmentación adecuada para que el anuncio llegue a quien debe llegar

Es importante destacar que cuando el usuario lo abre, sólo pagarás por el primer clic para abrir el anuncio.

Para crearlo debes entrar en tu cuenta de adwords, vas a la pestaña de anuncios y en crear anuncios seleccionas "Galería de anuncios" y ya verás la opción de "Anuncios de Gmail", donde una vez dentro podrás seleccionar varias opciones, desde usar plantillas predefinidas a subir tu propio HTML, y conseguir un anuncio personalizado a tus necesidades.

Es importante que selecciones la segmentación adecuada para que el anuncio llegue a quien debe llegar y para ello dispones de 4 tipos diferentes:

- **Públicos personalizados:** puedes crear un público basado en usuarios de los que tengas su email, de tal manera que impactas a usuarios que ya han tenido algún punto de contacto con tu empresa
- **Público similar:** esta orientación se asocia con "públicos personalizados", donde creas públicos que tienen similares características al que creaste previamente.
- **Palabras claves:** puedes seleccionar palabras clave específicas
- **Dominios:** puedes seleccionar dominios para incluir o excluir, con los que le usuario haya tenido relación al recibir algún correo de determinada empresa. Para ello, el sistema hace una revisión del cuerpo y asunto de los 100 últimos emails que el usuario recibió y no se marcaron como SPAM, y se incluyen los eliminados y archivados.

¿Te animas a probar este nuevo formato?

PUBLICIDAD EN GMAIL

CLICAR PARA VER EL VÍDEO

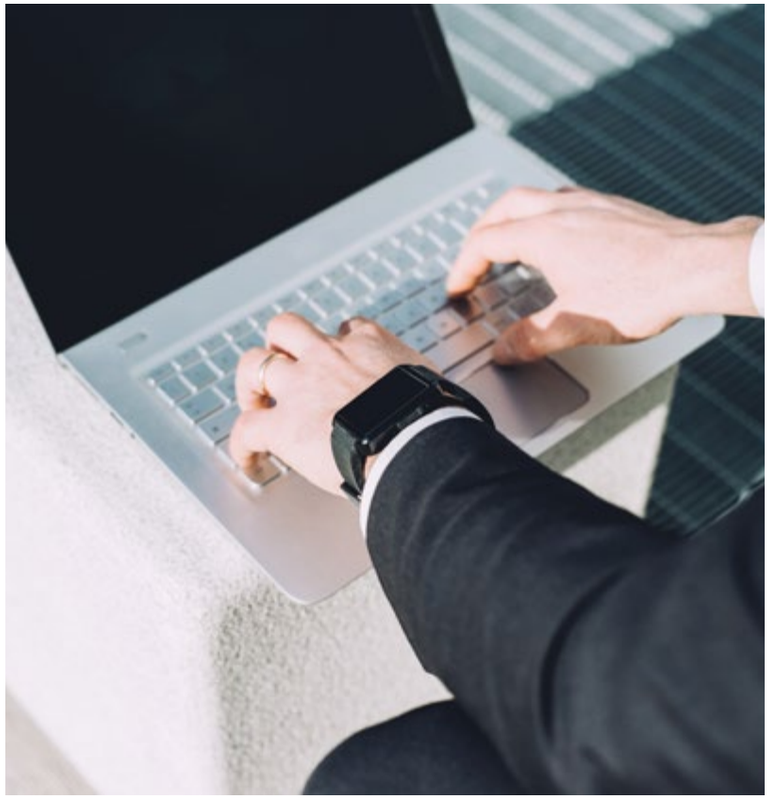
Enlaces relacionados

- Google Adworks en menos de 5 minutos
- Publicidad en Gmail

IoT, Transformación Digital: retos e incertidumbres

Darío Ferraté
Consultor TIC

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



Hace unos días fue mi cumpleaños y tuve la suerte que me regalaran ¡un smartwatch! (¡¡¡se ve que me he sido bueno este último año!!!). Yo era un poco reticente a comprarme uno (vengo leyendo comparativas entre modelos hace tiempo) porque quería tenerlo "todo" y también que la batería "aguantase" lo necesario para no estar pendiente de otro "cacharro" más, al que debo conectar cada día o que cuando realmente lo necesitara estuviera sin batería. Ya con el smartphone tengo suficiente…

Pero, me alegré muchísimo por el gran "detalle" y aunque lo miraba "de reojo" porque era más grande del que suelo usar, y pesaba más, lo cargué al 100% y me dispuse a darle una oportunidad… ¡¡¡Menuda oportunidad!!! La sorpresa fue tal, que no me lo he quitado ni un día, solo las 2 horas que tarda en cargarse al 100% y no paro de "jugar" y descubrir cosas interesantes que puedo hacer con él y gracias a él. No voy a dar detalles de la marca y del modelo (no es cosa de hacer publicidad), pero realmente estoy muy sorprendido. Este wearable (o dispositivos que se usan en nuestra vestimenta o como complemento) monitoriza y almacena cada movimiento que hago y a cada minuto. Desde saber cómo duermo, si descanso bien, si mi sueño es profundo, leve o si me despierto (a qué hora y el tiempo que me quedo despierto antes de volverme a quedar dormido), los pasos que doy, los pisos que subo, si corro, camino, hago elíptica, remo o inclusive sentadillas o fuerza de brazos/plancha, mi ritmo cardíaco, mis tiempos de inactividad (avisándome que me mueva cada 2 horas, apro-

Leyendo sobre la Transformación Digital e Internet de las Cosas (IoT), algunas empresas se plantean soluciones a través de los wearables para potenciar el negocio y acercar más las soluciones de empresas a las necesidades del cliente

ximadamente) y ya puestos, al complementarlo con el smartphone, las calorías que ingiero si indico la comida que he comido durante el día y mucho más…

Además de todo esto, realmente consigue motivarte, ya que te da estadísticas diarias y semanales de las actividades que haces, te indica si vas bien de ritmo según el objetivo que te hayas fijado y hasta puedes "competir" con otras personas para obligarte a no quedarte rezagado; inclusive, te posiciona en un rango, según tu actividad física para tu sexo y edad.

Por otra parte, las opciones disponibles para este wearable en la red son muchísimas para poder personalizar el reloj como tú quieras, tanto en aspecto como en funcionalidades y es, en ese momento, cuando pienso lo que se podría hacer con él empleándolo para mejorar la productividad del personal en la empresa… Llevar este "monitor" contigo constantemente y poder intercambiar información con sistemas centrales de la empresa para conocer qué, quién, cómo, por qué y cuándo necesita mi cliente algo de lo que mi empresa ofrece y, por qué no decirlo (seguro que a más de uno se le ha ocurrido), monitorizar a nuestros propios empleados.

Leyendo sobre la Transformación Digital e Internet de las Cosas (IoT), algunas empresas se plantean soluciones a través de los wearables para potenciar el negocio y acercar más las soluciones de empresas a las necesidades del cliente, conociendo sus necesidades a través del uso de BigData o SmartData, a través de información que volcamos principalmente en redes sociales, por citar un ejemplo. También hay que decir que un alto porcentaje de CIO ve los problemas de seguridad como un freno a la hora de implantar este tipo de soluciones.

Hay que acotar que IoT se sustenta sobre unos pilares básicos: Hardware, Servicios, Software y Conectividad. Existen distintos artículos en la red que hablan que IoT tendrá un impacto importante en las empresas sobre todo en lo que a "Servicios" se refiere.

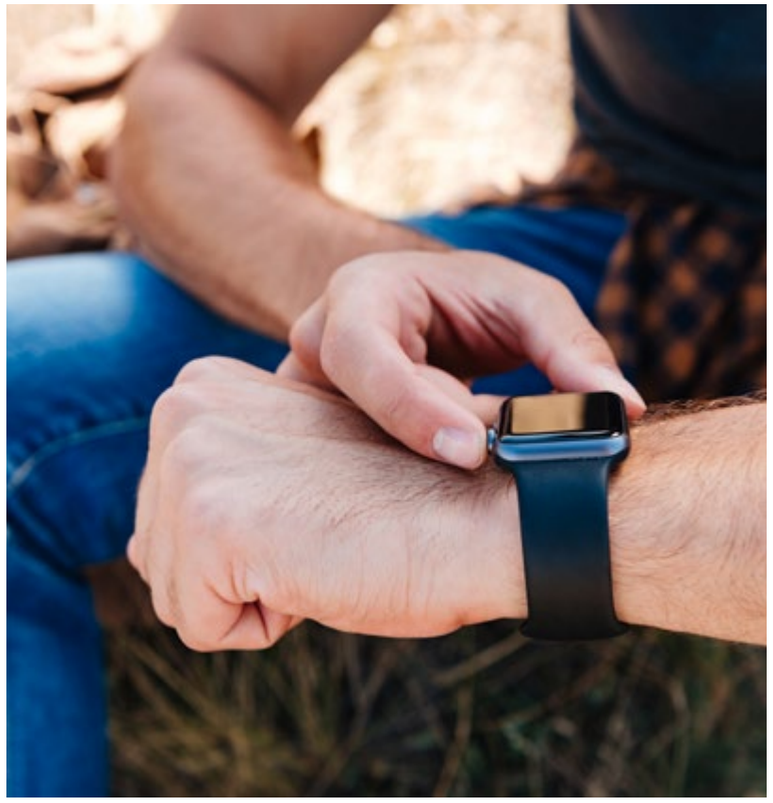
Aquí me choco con un tema que siempre sale en mis artículos y es el tema de la seguridad, al que incluyo ahora la protección de la información privada y de conceptos que, siendo importantes, hoy por hoy, la mayoría de nosotros damos a "aceptar las condiciones de uso" sin leer en detalle que estamos aceptando…

A partir de este punto entramos en un terreno espinoso… ¿saber qué hacen nuestros comerciales en su jornada laboral? ¿Hasta qué punto es legal monitorizarlos? Hace tiempo escuché que las empresas de transportes monitorizan por GPS a sus vehículos para evitar robos y otras fechorías, pero que también utilizan la información para saber si un conductor se desvía de su ruta, pasa demasiado tiempo en un área de servicio, consume más combustible de la cuenta por haberse retrasado en su tiempo de descanso, haber hecho algún trámite personal aprovechando que el desvío es mínimo frente a la ruta establecida o, inclusive, saber si se roba combustible.

En el caso de disponer de wearables como el que tengo, podrían conocer el tiempo que pasan con el cliente, clientes que visitan diariamente, rutas, tiempos muer-

En 20 años, todos los chavales que ahora tienen 12-15 años tendrán sus vidas publicadas en internet y podrás saber de dónde vienen, qué han hecho y hacia dónde van antes inclusive de entrevistarlos para un puesto de trabajo

tos y donde los pasan (la ubicación por GPS es bastante precisa) y un conjunto de información adicional que se podría decir que roza el límite de la legalidad y confidencialidad de las personas (ya sea en lo personal o en lo profesional) sea o no en horario laboral. De más está decir que fuera del horario laboral, lo que hagamos, es cosa nuestra, pero… ¿quién me asegura que esto será así? Es más aún, ¿quién me asegura que las actividades que yo realizo y la información que yo permito almacenar en mi smartwacth o smartphone quedará siempre a buen recaudo?



Con el fin de que mi entrenador "virtual" me asesore lo mejor posible sobre cómo realizar un determinado ejercicio para que no me lesione y en función de los objetivos que me he fijado, dejo que mi dispositivo almacene un montón de información valiosa sobre mi persona y hábitos o costumbres. ¿Y si esa información llega el día de mañana a "manos" de gente o entidades que analizándola conocerá mis hábitos de vida, el estado de mi salud, dónde suelo ir durante la semana, durante los fines de semana, los festivos... Y, mejor aún, ¿quién me garantiza que el día de mañana no me hagan ofertas personalizadas de un seguro médico, un seguro de vida, seguro de coche o agencias de viajes, escapadas, sitios para cenar en pareja en el rango de precio que me suelo manejar y otras cosas que hoy por hoy las conozco yo y mi pareja y, en el mejor de los casos, conoce parcialmente mi entorno cercano (familia, amigos íntimos), pero que a nadie más le interesa? Lo mejor/peor (todo tiene su lado positivo y negativo) de todo, es que esto es imparable, que cada vez nos animamos más a dejar nuestros datos en la red o proporcionarlos a servicios que dicen ser "seguros".

Recuerdo que hace años, muchos años, cuando empecé a comprar cosas por internet, me preguntaban si

no tenía miedo de que aquellos "amigos de lo ajeno" utilizaran la información de mi tarjeta para otros fines y compraran cosas sin mi autorización, con el dolor de cabeza que después acarrea estas situaciones (seguros, bancos…). Hoy por hoy el comercio electrónico es un hecho. También algunas cosas se resuelven gracias a las posibilidades que nos ofrece la tecnología actual. Por ejemplo, si están comprando con tu tarjeta en Barcelona y tu reloj indica que tienes actividades en Madrid y ambos están enlazados, hay mecanismos que podrían bloquear la tarjeta a la espera de confirmación. De todos modos, yo siempre he sostenido que el que quiera hacer algo en contra de alguien (en este mundo digital), seguro que lo hace, porque esa "gente" va 10 pasos por delante de los ciudadanos normales, ajenos al conjunto de cosas malas y delictivas que se pueden realizar. Está claro que el día que me haga "famoso", tendré que tener más cuidado, porque mi histórico está ahí y por más que quisiera (que no es el caso) nunca se podría eliminar todo.

Pero aquí me asalta otra pregunta, porque, al fin y al cabo, yo tengo una edad y no nací en esta generación donde todo es táctil, todo está en la red, ¡todo hay que compartirlo y no en una sola red social, sino en todas las redes sociales dependiendo del momento! El otro día en una reunión comentaba que, en 20 años, todos los chavales que ahora tienen 12-15 años tendrán sus vidas publicadas en internet y podrás saber de dónde vienen, qué han hecho y hacia dónde van antes inclusive de entrevistarlos para un puesto de trabajo. ¿Son conscientes los padres de que sus hijos, niños de 10-17 años, están dejando una huella imborrable en las redes sociales y que el día de mañana podrá ser utilizada, normalmente, en su contra? Todos hemos sido niños y en nuestra etapa adolescente hemos tenido épocas de rebeldía, pero antes, salvo cosas graves o muy graves que quedaran registradas en las autoridades, nadie sabría hasta qué punto de rebeldes hemos sido, ¿pero ahora? Con el afán de ser popular, con los medios que tenemos, lo graban todo y lo suben a las redes sociales para jactarse de la hazaña, sin saber que eso quedará para siempre allí (en las redes) hasta que alguien lo encuentre y lo pueda utilizar en su contra.

Ya estamos viendo consecuencias de nuestros comentarios en redes sociales en políticos, famosos. ¿Se imaginan como será esto dentro de 10-15 años? Aquí os dejo el debate…

Cada vez nos animamos más a dejar nuestros datos en la red o proporcionarlos a servicios que dicen ser "seguros"

Enlaces relacionados

- Los wearables mejoran o explotan nuestros datos
- El gran negocio de wareables basado en apis
- Videovigilancia y wearables
- Informe sobre la responsabilidad de las entidades financieras ante el fraude electrónico
- El perfil del defraudador global
- Perspectivas de la pequeña empresa en España
- II Termómetro del Mercado de mediana empresas en España

it Digital MEDIA GROUP

it Reseller TECH&CONSULTING

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