Octubre 2017 - nº 27
it User
TECH & BUSINESS

Bitcoin,
las criptomonedas al asalto del sistema financiero digital

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

VMware acelera en su propuesta de transformación de las empresas

Santander sienta las bases de la nueva economía digital en España

La UE endurece su política contra los delitos informáticos

Inteligencia artificial, clave de la seguridad del futuro

it Digital MEDIA GROUP

Juan Ramón Melara
juanramon.melara@itdmgroup.es

Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdmgroup.es

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

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

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

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

Bitcoin, ¿el futuro de las monedas y las transacciones comerciales?

Llevamos tiempo hablando de Bitcoin y la verdad es que no muchos saben lo que es. Es más, muchos de los que sí saben que es una criptomoneda no saben exactamente cómo funciona, qué seguridad jurídica tiene, con qué respaldo cuenta, y qué posibilidades hay alrededor de ella.

Por este motivo, hemos querido en este número de octubre centrar nuestro En Portada en Bitcoin y, por extensión, en las criptomonedas y la tecnología que las sustenta, Blockchain, de la que muchos más seguro que han oído hablar, pero no solo por su aplicación en este aspecto, sino porque día a día surgen nuevas opciones y funcionalidades alrededor de esta tecnología. Podría parecer que, al tratarse de monedas y de tecnología "de intercambio" solo deberían interesarse por ello personas relacionadas con las finanzas y el sector de la Banca, pero lo cierto es que ya en este momento el radio de efecto es mayor que ése, y lo normal es que siga ampliándose de cara a futuro.

En definitiva, conviene estar informado y preparado por lo que pueda llegar a pasar, porque, como no podía ser de otra forma, es imprescindible conocer las bases, las ventajas y los riesgos de cualquier moneda o elemento financiero antes de empezar a operar con él.

A esto es a lo que podríamos llamar ir sobre seguro. Y precisamente la seguridad es la base de la nueva revista que IT Digital Media Group pone a tu disposición. Se trata de IT Digital Security, una revista digital interactiva centrada en el mundo de la seguridad, y con toda la información que necesita el CISO, el CSO y el nuevo CDO para poder asumir sus funciones.

Para facilitar que puedas leer el primer número, IT Digital Security se integra como suplemento en este número de IT User que estás leyendo. Esperamos que encuentres los contenidos interesantes y que descargues todos los meses también el nuevo miembro de nuestra oferta informativa.

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

Por cortesía de HPE e Intel®. Intel Inside®. Para una productividad extraordinaria.

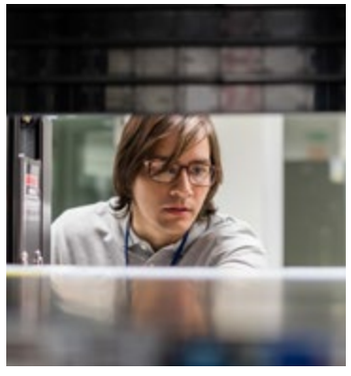
Intel y el logotipo de Intel son marcas comerciales de Intel Corporation en Estados Unidos y en otros países. © 2016 HPED LP.

Sumario

En Portada

Criptomonedas, el primer resultado de la tecnología Blockchain

Especial IT



Hiperconvergencia, la respuesta inteligente a las necesidades de las TI

Hewlett Packard Enterprise

RSC

La educación como vía para promover la salud y erradicar la pobreza

IT Digital Security — Número 1

Todo lo que necesita saber sobre la seguridad TI

Índice de anunciantes

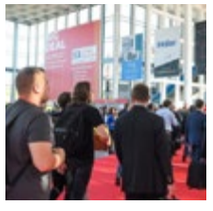
Hewlett Packard Enterprise JRIT	Tecnología para tu empresa
Toshiba Portégé X20W	IT Whitepapers
DXC Technology	IT Digital Security
Micro Focus Discover the New	Ninja Twitter
Kaspersky for Business	Yes Management
HP Probook Serie 400 G4	Discover the New
GMV Transformación Digital	IT Televisión
Hewlett Packard Enterprise Flexible Capacity	IT Reseller

Actualidad

VMware pisa el acelerador en la transformación de las empresas

Santander muestra el futuro de la economía digital

La Unión Europea endurece su estrategia contra ciberataques y delitos informáticos



IFA se ofrece como escaparate de la tecnología de consumo que está por llegar

Inteligencia artificial, ¿base de la efectividad en la lucha contra los mensajes extremistas en las redes?

Diseño elegante

Portégé X20W: Diseñando la perfección

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

Toshiba Portégé X20W. Diseño elegante.

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

Intel Inside®.
Para una productividad extraordinaria.

VMware pisa el acelerador en la transformación de las empresas

Pat Gelsinger, CEO de VMware, fue el principal protagonista del primer día del VMworld Europe que la compañía ha celebrado en Barcelona, ciudad que volverá a acoger nuevamente la cita en 2018, en una edición que ha servido para mostrar cómo se está enriqueciendo con anuncios y alianzas la estrategia de la compañía, que el propio Gelsinger resumía en "cualquier dispositivo, cualquier aplicación, cualquier nube".

Miguel Ángel Gómez (Barcelona)

Y es que, en esta cita en la Ciudad Condal, a pocas semanas de la celebración de la edición estadounidense del evento, tan significativos como los anuncios de productos y soluciones, lo han sido las demostraciones de que el ecosistema con el que trabaja VMware sigue creciendo, desarrollándose y enriqueciéndose, y cuenta con compañías tan significativas como IBM o AWS.

Partiendo de la visión estratégica de la firma, Gelsinger ha querido mostrar cómo se está potenciando y desarrollando cada uno de los tres pilares, si bien dejaba claro que lo que lo transforma todo es la innovación tecnológica, dejando un reto encima de la mesa: "hoy es el día con menos innovación tecnológica del resto de vuestra vida".

Esta innovación, señalaba Gelsinger, remoldea las expectativas, y transforma los negocios y las fuerzas de trabajo, a partir, todo ello, del software y las aplicaciones.

Pero, como decíamos, la base de la propuesta de VMware está en cualquier dispositivo, porque lo importante, comentaba el propio CEO de la compañía, "es conectar a las personas con los servicios y las aplicaciones". De ahí la importancia del desarrollo de VMware WorkSpace One.

En la parte Cloud, se anuncia VMware Cloud Certified, un nuevo programa para proveedores de cloud, además de avances para su plataforma de gestión de la nube que ayudarán a los clientes a desarrollar, operar y gestionar la infraestructura de TI y los servicios de aplicaciones en entornos multinube. VMware vRealize Suite 2017 integra los últimos lanzamientos vRealize Operations, vRealize Automation, vRealize Business for Cloud y vRealize Log Insight.

Y no podía VMware dejar pasar la oportunidad de hablar de seguridad, y de la nueva visión que quiere ofrecer a las empresas para incrementar los niveles de protección. La premisa de la nueva estrategia parte de situar el control junto al hipervisor, lo que conlleva una

María José Talavera, directora general de VMware Iberia

"La mejor forma que tiene la Banca de ir a la cloud pública es con nosotros"

Este 2017 está siendo un buen año para VMware en España, tal y como señala María José Talavera, dado que la compañía "crece más" que el dato, de doble dígito, que ha ofrecido la firma a nivel mundial, un ritmo de crecimiento que quieren mantener hasta 2020 con el objetivo de llegar a ser una compañía de 10.000 millones de dólares de facturación anuales, poco más de los casi 8.000 actuales.

Y es que tras una "gran primera mitad del año", la firma mantiene "buenas previsiones" para la segunda, en un ejercicio en el que VMware ha cerrado en España dos de las operaciones más grandes alrededor de Workspace ONE, una con el Gobierno Vasco, para la gestión de dispositivos en los hospitales de Euskadi, y otra con una gran empresa española. Y, de igual forma, María José Talavera recordaba que La Caixa ha montado su cloud pública de la mano de VMware, porque "la mejor forma que tiene la Banca de ir a la cloud pública es con nosotros".

De hecho, la propia Talavera confirmaba que el desarrollo de la cloud pública está siendo algo más lento de lo previsto por la preocupación de los CIO por dos cuestiones básicas, seguridad y regulación, que les están haciendo mirar hacia una cloud híbrida.

Hablando de cloud, y ante las noticias sobre los acuerdos de VMware con grandes proveedores de nube pública, como AWS, los responsables de la firma en España señalaban que "el número de proveedores que trabajan con nosotros se incrementa", pero es que quiere decir que releguen a nadie, "porque hay mercado tanto para proveedores locales como multinacionales".

Por último, María José Talavera quiso dejar claro el papel que VMware quiere tener en el negocio de la seguridad, porque "con NSX y Workspace ONE tenemos mucho que decir en seguridad".

Hablando de seguridad, Bask Iyer, CIO y vicepresidente ejecutivo, Dell y VMware, señaló en su comparecencia ante los medios de comunicación españoles que "hay un gran interés por parte de los CIO y las compañías alrededor de GDPR, porque existe una gran preocupación por la privacidad de los datos". Sin embargo, algunos informes recientes muestran cierta despreocupación por parte de algunos responsables europeos, si bien Iyer responde que "creo que todas las compañías están interesadas y todavía hay tiempo para prepararse".

reorganización del resto de piezas buscando un entorno más protegido, porque, como mostraba el propio Gelsinger en el escenario, la respuesta de la industria en seguridad ha consistido en una gran oferta de soluciones y productos de múltiples fabricantes y con múltiples funciones específicas, algo que ahora VMware quiere afrontar de otra forma.

DÍA 1, SESIÓN PLENARIA, PAT GELSINGER

CLICAR PARA VER EL VÍDEO

Un evento con múltiples anuncios

A lo largo de los días de celebración de VMworld 2017 Europe en Barcelona se han ido dando a conocer algunos anuncios que vienen a complementar los que la compañía realizó en la edición estadounidense del evento. Así, VMware anunció que Vodafone la ha elegido para respaldar su ampliación mundial de NFV y acelerar así la entrega de nuevas soluciones a clientes

Alejandro Solana, Senior SE Manager, EMEA NSX Práctica, VMware

"Es el usuario el que ha cambiado, no la empresa, y de ahí parte la necesidad de transformarse"

"Estamos viendo en los últimos años una tendencia para situar al cliente en el centro y, como compañía, nos estamos centrando en proporcionarle una experiencia excelente, tanto como cliente como en su faceta de empleado. Intentamos garantizar, en el contexto de transición TI que se está viviendo, es la modernización y la simplificación de los centros de datos; poder extender, para facilitar el crecimiento, hacia la cloud pública; ir a un contexto de espacio de trabajo digital; e integrar en todo ello el mayor nivel de seguridad".

"Quizá lo mejor de este año", continúa, "es que se está viendo la ejecución de los cuatro pilares, con acuerdos como los de IBM, AWS, Microsoft, Google… o lanzamientos como VMware App Defense o NSX. Ver esta visión convertida en realidad es, quizá, la gran diferencia de este VMworld".

En definitiva, tras varios años hablando de la Transformación Digital, parece que los clientes han iniciado su viaje por este camino. "La realidad", asegura Solana, "es que han emprendido el viaje, pero quizá no saben su destino. Han empezado la transformación sin un objetivo claro. Un proceso de Transformación Digital precisa conocerse internamente muy bien, saber cómo sacar el mejor partido de cada uno de los silos de tu organización para poder simplificarlo en beneficio del producto o servicio digital que quieres ofrecer. No se trata solo de un cambio de tecnología, sino de personas, procesos, estructuras… para que el proceso sea un éxito. Lanzar un proyecto de contenedores no hace que tu empresa sea digital".

Puesta la tecnología sobre la mesa, para ayudar en los procesos de Transformación Digital, "uno de los proyectos que estamos lanzando son los procesos de asesoría, porque, aunque cuentes con la tecnología, si tu forma de trabajar y pensar no apunta en la línea adecuada, va a ser difícil que llegues al objetivo. En el mundo TI tradicional, los departamentos de las compañías rara vez hablan entre sí y, si lo hacen, usan diferentes idiomas. Por eso en los grupos de trabajo tratamos de elevar el nivel para que vean qué se necesita y cómo conseguirlo. Es el cliente, al final, el que diseña su propia arquitectura y eso implica a todos los departamentos".

En todo caso, la transformación no es una opción. "Miremos cualquier negocio", apunta Solana, "las expectativas de los clientes son muy diferentes a las que tenían hace diez años, y, si no eres digital, va a ser muy complicado responderles. Los conceptos, como el de tienda, han cambiado. Es el usuario el que ha cambiado, no la empresa. De ahí parte la necesidad de transformarse, no de la empresa. Y éste es el gran cambio".

it whitepapers

ESTRATEGIAS PARA LA IMPLEMENTACIÓN DE INFRAESTRUCTURA HIPERCONVERGENTE

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

Una nueva aproximación a la seguridad

La apuesta de VMware en la seguridad es similar a su propuesta con la virtualización: hacer las cosas de otra forma. Tal y como nos explica Alejandro Solana, con App Defense "establecemos un patrón de comportamiento que entendemos como el adecuado y monitorizarlo para, si se produce alguna alteración, tenerla en cuenta. Con este primer paso, e independientemente de lo que hagamos después, el problema queda aislado. Hasta la fecha, la seguridad se ponía encima de las soluciones y nosotros proponemos hacerlo desde el hipervisor, controlando todo lo que entra y se ejecuta en la máquina virtual".

"Es un cambio de arquitectura en el modelo de seguridad", continúa Solana, quien añade que, "estamos trabajando con el ecosistema de socios tecnológicos para obtener los mejores resultados con esta forma de ver la seguridad. Ellos cuentan con grandes productos para una forma de ver la seguridad y nosotros queremos ver cómo adaptarlos o evolucionar hacia otra manera de entender la seguridad. Las piezas son las mismas, cambia el tablero".

de una forma más eficiente en términos de costes. Así, Vodafone implementará VMware vCloud NFV para dar soporte las funciones de red virtuales de diferentes proveedores en una plataforma común definida por software.

Por otra parte, Dell EMC y VMware han comunicado que han integrado y validado el hardware de infraestructura de nube Dell EMC y la plataforma VMware vCloud NFV para OpenStack con el objetivo de reducir el tiempo de desarrollo necesario y ayudar a abaratar los costes generales de la virtualización de funciones de red (NFV) para proveedores de servicios de comunicación.

Además, VMware dio a conocer la expansión de su Alianza de Seguridad Móvil (MSA, Mobile Security Alliance), un ecosistema de proveedores de seguridad integrado con VMware Workspace ONE. Esta solución proporciona interfaces de programación de aplicaciones (API) diseñadas específicamente para que el ecosistema de seguridad se integre con la plataforma. Con soluciones de seguridad de partners MSA y Workspace ONE, los clientes "se benefician de una moderna plataforma de seguridad que protege contra amenazas específicas a dispositivos, usuarios, aplicaciones y datos; tanto en la nube como en las instalaciones".

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Por último, otro de los anuncios del evento, la nueva plataforma VMware vCloud NFV-OpenStack, que incluye VMware Integrated OpenStack-Carrier Edition, basada en OpenStack Ocata de VMware, lo que permitirá desarrollar, mejorar y operar con facilidad una nube OpenStack en la parte superior de la plataforma NFVI de VMware, una vez que esté disponible en el tercer trimestre de 2018.

Enlaces relacionados

- VMworld 2017 Europe
- VMware vRealize Suite
- VMware App Defense
- VMware Cloud Foundation
- Ranking Global de Cloud Computing de la BSA
- Hábitos sobre una TI híbrida
- Barómetro de emprendimiento de éxito en España

NUEVO.
PERO NO NACIDO AYER.

CSC Y HPE ENTERPRISE SERVICES AHORA SON DXC TECHNOLOGY.

DXC.technology/GetItDone

DXC.technology | THRIVE ON CHANGE.

La ciudad cántabra acoge el 31 Encuentro de la Economía Digital y las Telecomunicaciones

Santander muestra el futuro de la economía digital

A principios del mes de septiembre, Santander volvió a acoger el Encuentro de la Economía Digital y las Telecomunicaciones, organizado por AMETIC, el cual contó con la participación de numerosas personalidades que explicaron la importancia de la conocida como nueva economía, así como explicaron cuál es el futuro del mismo.

Santander volvió a acoger la celebración del 31 Encuentro de la Economía Digital y las Telecomunicaciones, un evento organizado por AMETIC, y que bajo el lema "La realidad digital en España" explicó cuál es su visión sobre el futuro de las TIC en nuestro país.

Mayor foco sobre la revolución digital

En esta ocasión, Álvaro Nadal, Ministro de Energía, Turismo y Agenda Digital, fue el encargado de inaugurar el congreso. Durante su intervención reclamó una mayor atención política, mediática, social, empresarial y académica para que España y Europa se sitúen en la "punta" de la revolución tecnológica y digital actualmente en marcha, un objetivo para el que juzgó igualmente fundamental apostar por la formación.

Para Álvaro Nadal, "la actual revolución digital" se diferencia de las otras dos revoluciones en que ésta "nos ayuda a pensar y a hacer más fácil el esfuerzo mental", debe ser un tema de discusión permanente, si bien reconoció que "raramente es así".

Europa "no es el continente más avanzado en materia digital", algo que, en su opinión, tiene que cambiar apostando por "promover una agenda digital más amplia y ambiciosa" tanto a nivel nacional como continental.

Esta agenda digital "debe descansar sobre unas adecuadas infraestructuras". En este ámbito "España se encuentra mejor posicionado. Somos el tercer país del mundo en redes fijas". No obstante, la industria digital española no es lo que debería de ser. "Este problema, "el mayor al que nos enfrentamos" se debe a varios factores de oferta y demanda. "La financiación debe adaptarse a las necesidades tecnológicas y hacen faltan muchos más hombres de ciencia".

En cuanto a la demanda, el ministro de Agenda Digital destacó que hay nichos de mercados, como la digitalización de la sanidad, la tarjeta social o el lenguaje natural en castellano, en el que España "tiene y debe seguir teniendo un papel protagonista" en el desarrollo de la tecnología en nuestro país y pedir a los sectores

tradicionales una "mayor concienciación" para participar en esta revolución en marcha, Nadal aludió a cómo la digitalización está cambiando la forma de gestionar los derechos y libertades. "Tenemos una muy buena Constitución, pero es analógica y muy poco digital", lo mismo que ocurre, resaltó, con el sistema tributario, al que calificó de "eminentemente analógico".

"España tiene y debe seguir teniendo un papel protagonista en la digitalización"

Álvaro Nadal, Ministro de Energía, Turismo y Agenda Digital

Finalmente, y tras solicitar un esfuerzo y mayores recursos en ciberseguridad para defender mejor nuestros derechos, Álvaro Nadal invitó a toda la sociedad a participar en las profundas transformaciones tecnológicas que se avecinan. "Lo que debemos hacer da para bastante más que para una legislatura".

La transformación digital en fase inicial

Pedro Mier, presidente de AMETIC, afirmó que "la transformación digital no ha hecho más que empezar" y defendió que "todos contamos" en este proceso de Transformación Digital, un fenómeno transversal que, precisó, afecta al conjunto de los sectores productivos, a las administraciones públicas y, por ende, a la sociedad en su conjunto.

"El reto, las oportunidades y los riesgos para toda la sociedad que se abren con esta transformación son de dimensiones enormes", afirmó Pedro Mier. "La innovación se ha convertido en la única estrategia competitiva eficaz. Es imperativo impulsar y potenciar las innovaciones disruptivas".

Para potenciar la industria exportadora, Pedro Mier ha puesto como ejemplo de lo que necesita España, el modelo alemán con su mittelstand (compañías medianas potentes, líderes globales de su especialidad) haciendo una llamada al crecimiento y especialización de nuestras empresas, así como a que se creen las circunstancias propicias para la reindustrialización.

Finalmente, Pedro Mier abogó por "un país digital de primera división donde todas las empresas cuenten". También aludió a la generación de empleo que la industria digital puede y debe crear y a la formación necesaria para cubrir los distintos perfiles que la revolución digital demanda.

Europa tiene que estar a la cabeza

El papel que juega Europa en el desarrollo de la Sociedad de la Información centró la charla de Cecilia Bonefeld-Dahl, directora general de Digitaleurope, quien explicó que el objetivo es "digitalizar Europa de una forma sostenible".

"Como europeos no podemos dejar a la sociedad atrás y tenemos que utilizar la digitalización para beneficiar a la población". Para Bonefeld-Dahl, la clave es buscar una infraestructura común en el continente y potenciar la Red 5G.

A su juicio, los países europeos deben solucionar varios problemas que impiden ese desarrollo digital, entre los remarcó "la escasa formación digital de la población y la falta de capital riesgo".

Bonefeld-Dahl apuntó asimismo algunos datos: menos del 50% de la población europea tiene las competencias adecuadas para el mundo digital, o que en 2020 se estima que desaparecerán siete millones de trabajos debido a la inteligencia artificial.

Retos empresariales

Durante su intervención, Juan Pedro Moreno, presidente de Accenture, reconoció que "estamos viviendo

tres revoluciones "que no se habían dado antes: el cambio tecnológico, social y el demográfico y cultural".

Para explicar estos cambios Moreno indicó en primer lugar que el abaratamiento de la tecnología lleva a su vez a una democratización en su uso a través del dispositivo móvil o el ordenador. En segundo término, destacó que el acceso más fácil al mundo digital y la demanda del usuario hace que surja un cambio social. "El concepto de las rebajas, por ejemplo, queda diluido con conceptos como el black friday o el ciber Monday".

En su opinión, otra gran transformación se desarrolla en el ámbito demográfico y cultural. Juan Pedro Moreno recordó que en 2025 el 75% de los profesionales serán millenials. "Este entorno llevará a que casi cuatro generaciones trabajemos juntas en las empresas". Todos estos cambios hacen, según resaltó, que la sociedad viva un proceso de disrupción en el que hay que reflexionar sobre la excesiva "regulación" de las nuevas tecnologías.

"Hoy lo que los consumidores quieren son productos personalizados para ellos", aclaró. Una característica que, insistió, era inalcanzable para muchos bolsillos, pero que ahora es una de las mayores demandas y obliga a las empresas a una "batalla" por ganar la carrera de la innovación. "La conversión del producto en servicio es una de las claves de esa evolución en la cadena de valor", remarcó Moreno.

Cómo superar los retos en I+D+i

Carmen Vela, secretaria de Estado de Investigación, Desarrollo e Innovación, hizo un llamamiento a "todos los actores responsables de la innovación en España para colaborar, sumar y trabaja juntos", con el fin de sacar al país del retraso estructural que arrastra en este ámbito en Europa, donde ocupa una modesta posición.

> "La inversión destinada a I+D en relación al PIB es solo del 1,22% muy lejos de la media europea"
>
> Carmen Vela, secretaria de Estado de Investigación, Desarrollo e Innovación

Vela insistió en que, a diferencia de lo que ocurre en investigación, donde España ocupa una relevante décima posición en el ranking mundial, a pesar de contar con un sistema "pequeño y limitado", en innovación "lo hacemos regular tirando a mal, por lo que nos queda mucho por hacer".

"No estoy regañando", avisó la secretaria de Estado, "pero la inversión destinada a I+D en relación al PIB es

it whitepapers

PLAN DIGITAL 2020:
LA DIGITALIZACIÓN DE LA SOCIEDAD ESPAÑOLA

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

solo del 1,22% muy lejos de la media europea, que es del 2%, y más aún del objetivo del 3% fijado para el 2020".

Por ello, invitó al sector privado a mejorar su peso en este porcentaje inversor, que ahora ronda el 53% del total cuando en Corea es del 80% o en Alemania supera el 63%, para alcanzar el objetivo deseable de que el sector empresarial asuma las dos terceras partes del total.

Tras resaltar que la Estrategia Española de Ciencia y Tecnología y de Innovación 2013-2020 supone "toda una declaración de intenciones de sumar investigación e innovación", Vela reconoció que el sector empresarial lleva muchos años trabajando en la economía y la sociedad digital, el "reto transversal sobre el que tienen que crecer el resto de desafíos que la sociedad tiene planteados en el Plan estatal de I+D+i".

"La transformación digital no ha hecho más que empezar"

Pedro Mier, presidente de AMETIC

"La industria será digital o no será"

Begoña Cristeto, secretaria general de Industria y de la Pyme del Ministerio de Economía

En este sentido, la secretaria de Estado destacó que España "está bien y mejorando en el ranking europeo de transformación digital, en el que ocupa la posición 14, como así lo refleja el programa europeo Horizon 2020, una estrategia en la que nuestro país es el primero en iniciativas de pymes, medio ambiente y materias primas y en el que, enfatizó, "por primera vez tenemos más retorno, el 9,8%, alrededor de 2.000 millones de euros, de lo que ponemos en Europa".

Industria 4.0

Por su parte, Begoña Cristeto, secretaria general de Industria y de la Pyme del Ministerio de Economía, aseguró que "la industria será digital o no será", afirmó durante su intervención institucional en el 31 Encuentro de la Economía Digital y las Telecomunicaciones que se celebra hasta mañana en Santander, organizado por AMETIC y el Banco Santander.

Cristeto defendió la necesidad de alcanzar una industria "inteligente y conectada" que permita al sector aumentar su contribución al PIB nacional, que actualmente es del 16,1%. Para ello, la secretaria general de Industria reiteró el compromiso del Gobierno de situar a la digitalización en el "centro" de su agenda política.

La responsable pública, que recordó que España es el quinto país más industrializado de la UE y el decimosexto del mundo, admitió que estas posiciones pueden cambiar "si no sabemos manejar los retos a los que nos enfrentamos", entre los que enumeró la "amenaza" de las reglas de la globalización y el libre comercio, la "profunda" transformación del sistema hacía una economía descarbonizada, o el "acelerado" progreso tecnológico en curso.

En su discurso, Cristeto detalló los contenidos y los retos y oportunidades que plantea la iniciativa Industria Conectada 4.0, la estrategia pública diseñada para encarar la cuarta revolución industrial que, según reconoció, "ha venido para quedarse", y reveló algunos datos sobre los potenciales beneficios de esta transformación digi-

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

sarrollo de este sector asegurando que "si nos centramos en el usuario, todo fluirá", aunque puntualizó que la innovación ha sido siempre, y continuará siendo "la palabra clave".

Eugenio Fontán, decano-presidente del Colegio Oficial de Ingenieros de Telecomunicación advirtió que "no necesariamente" los operadores son los más interesados en el desarrollo del 5G, así como destacó que "la madurez tecnológica" en España "empieza a ser una realidad".

El decano de la Deusto Business School, Guillermo Dorronsoro, afirmó, por su parte, que la industria "necesita entender los cambios que se avecinan para poder estar conectada". El sector industrial "vive un buen momento", destacó Dorronsoro, quien emplazó a ésta a "conectar con el resto de la sociedad".

La innovación fue uno de los ejes de este encuentro. Ramón Ruiz, director de operaciones de Ennomotive, aseguró que "la innovación abierta nos garantiza tener más éxito" y defendió una producción industrial "sin barreras ni de talento, ni de personas, ni de orígenes".

"El objetivo es digitalizar Europa de una forma sostenible"

Cecilia Bonefeld-Dahl, directora general de Digitaleurope

tal. En base a diferentes estudios, avanzó que las industrias inteligentes pueden sumar hasta cinco billones de dólares al valor añadido de la economía mundial en los próximos cinco años, periodo en el que España podría generar hasta 1,25 millones de empleos cualificados e incrementar su PIB en 35.000 millones de euros.

Otros ponentes

Durante los tres días de duración del 31 Encuentro de la Economía Digital y las Telecomunicaciones también hubo otros ponentes que dieron su visión sobre cuál es el futuro del sector de las telecomunicaciones. Así, Mike Blanche, jefe de relaciones estratégicas de Google destacó la importancia que tiene el usuario en el de-

Enlaces relacionados

- Cómo la Transformación Digital impacta en los OEM
- Cómo ser flexible y apto para la Transformación Digital
- Las operadoras de telecomunicaciones en la era digital
- GMV: Transformación Digital
- La Transformación Digital como eje estratégico
- Como transformar cuatro sectores clave
- Perspectivas de la pequeña empresa en España

MICRO FOCUS®

Discover

the New

Creará una Agencia de Ciberseguridad

La UE endurece su estrategia contra ciberataques y delitos informáticos

Sólo el año pasado, el 80% de las empresas europeas se vio afectada por al menos un incidente de ciberseguridad. Consciente de la importancia de incrementar el nivel de seguridad, la Comisión Europea ha propuesto crear una Agencia de Ciberseguridad que, a través de la colaboración, ayudará a los países miembros a luchar contra los ciberataques y los delitos informáticos.

La ciberseguridad preocupa a la Unión Europea. Ésta es una de las principales conclusiones del discurso sobre el estado de la Unión que pronunció Jean-Claude Juncker, presidente de la Comisión Europea, el pasado 13 de septiembre, en el que, aunque reconoció que "en los últimos tres años hemos realizado progresos en lo que respecta a la seguridad online de los europeos", todavía queda mucho camino por andar. "Europa sigue sin estar adecuadamente equipada para defenderse de los ciberataques". Esta máxima ha llevado a la Unión a proponer nuevas herramientas "que nos ayuden a repeler estos ataques".

Algunas cifras

Según datos que maneja la Unión Europea, a pesar de la gran confianza de los ciudadanos europeos en las

nuevas tecnologías y de las oportunidades que brinda la nueva economía digital para empresas y para el desarrollo económico de los países, también han propiciado el crecimiento de las amenazas.

"Las tecnologías digitales han traído consigo nuevos riesgos a medida que ciertos agentes, tanto estatales como no estatales, han multiplicado sus tentativas de robar datos, cometer fraudes e incluso desestabilizar gobiernos".

Según cifras que maneja la Comisión Europea, sólo el año pasado se produjeron más de 4.000 ataques con programas de secuestro de archivos al día y el 80% de las empresas europeas se vio afectado por al menos un incidente de ciberseguridad. El impacto económico de la ciberdelincuencia se ha multiplicado por cinco en los últimos cuatro años.

Nueva Agencia de Ciberseguridad de la UE

Con el objetivo de frenar estos ataques, la Comisión Europea ha propuesto una serie de medidas que buscan fortalecer la ciberseguridad de la UE. Entre ellas figura la propuesta de una nueva Agencia Europea de Ciberseguridad, la cual tratará de ayudar a los estados miembros a luchar contra los ciberataques, así como un nuevo régimen europeo de certificación que garantice un uso seguro de los productos y servicios en el mundo digital.

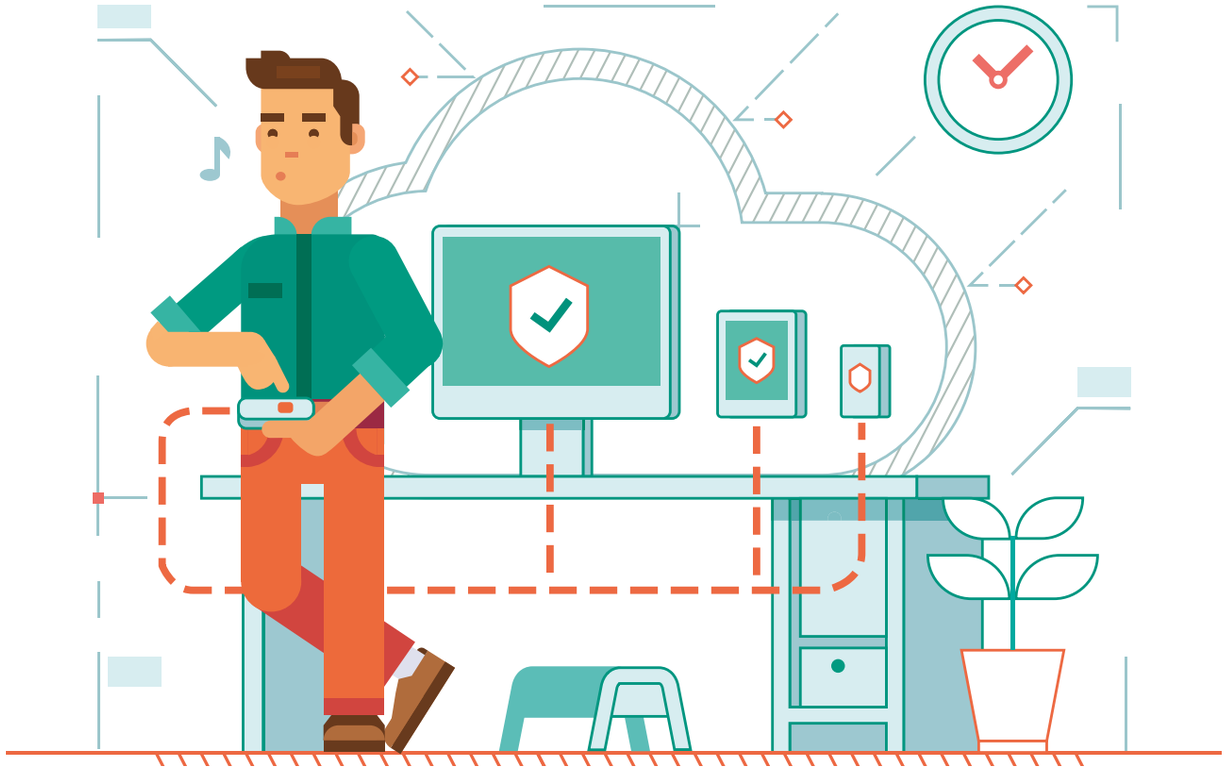
A grandes rasgos, la Agencia Europea de Ciberseguridad, que está basada en la actual Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), recibirá un mandato permanente para ayudar a los estados miembros a prevenir y responder con eficacia a los ciberataques; mejorará la capacidad de reacción de la UE mediante la organización anual de ejercicios paneuropeos de ciberseguridad y "la mejor puesta en común de la información y la inteligencia sobre las amenazas" a través de la creación de centros de intercambio de información y análisis.

Sólo el año pasado se produjeron más de 4.000 ataques con programas de secuestro de archivos al día

whitepapers

LAS LAGUNAS DE CONOCIMIENTO EN CIBERSEGURIDAD

Los jóvenes ciber-inteligentes pueden poner fin al desconocimiento actual existente en las empresas para combatir las crecientes ciberamenazas y evitar la irrupción masiva en sus datos públicos y privados. La industria está fallando a la hora de proporcionar un camino a los jóvenes para que encuentren trabajo, perfeccionen sus habilidades y sirvan a la sociedad. En su lugar, pueden estar fomentando la ciberdelincuencia, en vez de evitarla.



Deje que fluya su creatividad. Y aleje las ciberamenazas

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

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

cloud.kaspersky.com

© 2017 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.

Además, también contribuirá a la aplicación de la Directiva sobre la seguridad de las redes y sistemas de información, que contiene obligaciones de notificación a las autoridades nacionales en caso de incidentes graves.

Asimismo, la Agencia de Ciberseguridad ayudaría a establecer y aplicar el marco de certificación a escala de la UE que propone la Comisión para garantizar que los productos y servicios sean "ciberseguros".

"Del mismo modo que los consumidores pueden confiar en lo que comen gracias al etiquetado de alimentos de la UE, los nuevos certificados europeos de ciberseguridad asegurarán la fiabilidad de miles de millones de dispositivos con los que se manejan infraestructuras fundamentales de nuestro tiempo, como las redes de energía y transporte, pero también de nuevos dispositivos destinados a los consumidores, como los automóviles conectados".

Los certificados de ciberseguridad serán reconocidos en todos los estados miembros, con lo que se reducirán los trámites administrativos y los costes para las empresas.

Trabajar en pos de la ciberseguridad

"La UE seguirá trabajando en pos de una ciberpolítica internacional que fomente el espacio abierto, libre y seguro y apoyará los esfuerzos para elaborar normas de conducta responsables por parte de los estados y aplicar el Derecho Internacional y medidas de fomento de la confianza en materia de ciberseguridad", asegura Federica Mogherini, alta representante y vicepresidenta de la Comisión.

La nueva Agencia de Ciberseguridad fomentará la colaboración. No en vano, y según palabras de Andrus Ansip, vicepresidente responsable del Mercado Único Digital, "ningún país puede hacer frente, por sí solo, a los retos de la ciberseguridad. Nuestras iniciativas refuerzan la cooperación de forma que los estados miembros de la UE puedan acometer juntos estos desafíos. Proponemos también nuevas medidas que potencien la innovación y fomenten la ciberhigiene".

Pero para que la nueva Agencia tenga éxito, "hemos de trabajar codo con codo para desarrollar resilencia, impulsar la innovación tecnológica, potenciar la disuasión, reforzar la rastreabilidad y la obligación de rendir cuentas y encauzar la cooperación internacional hacia el fomento de nuestra ciberseguridad colectiva".

La Agencia Europea de Ciberseguridad recibirá un mandato permanente para ayudar a los estados miembros a prevenir y responder con eficacia a los ciberataques

Mariya Gabriel, comisaria de Economía y Sociedad Digitales, considera, por su parte, que "tenemos que afianzar la confianza de los ciudadanos y las empresas en el mundo digital, especialmente en estos tiempos en los que los ciberataques a gran escala son cada vez más

comunes. Es mi deseo que la existencia de estándares elevados de ciberseguridad se convierta en la nueva ventaja competitiva de nuestras empresas".

Medidas propuestas

Para aumentar el nivel de seguridad, la Comisión Europea ha propuesto una serie de medidas entre las que se encuentran:

- **Un Centro europeo de investigación y competencias en materia de ciberseguridad.** Éste se pondrá en marcha el año que viene en colaboración con los estados miembros y ayudará a desarrollar y desplegar las herramientas y tecnologías necesarias para hacer frente a una amenaza en constante cambio y a velar por que nuestras defensas sean tan punteras como las armas que

El impacto económico de la ciberdelincuencia se ha multiplicado por cinco en los últimos cuatro años

utilizan los ciberdelincuentes. También complementará los esfuerzos de desarrollo de capacidades en este ámbito a escala nacional y de la UE.

- **Un Plan rector para que Europa y los estados miembros puedan responder rápidamente, con operatividad y al unísono cuando se produzca un ciberataque a gran escala.** El procedimiento propuesto se establece en una Recomendación adoptada la semana pasada.
- **Mayor solidaridad.** Más adelante, se podría estudiar la posibilidad de crear un Fondo de Respuesta en casos de Emergencia de Ciberseguridad para aquellos estados miembros que hubiesen puesto en marcha de forma diligente todas las medidas de ciberseguridad exigidas por el Derecho de la UE. El Fondo podría facilitar ayuda de emergencia a los estados miembros, del mismo modo que el Mecanismo de Protección Civil de la UE se moviliza para ofrecer apoyo en los casos de incendios forestales o catástrofes naturales.
- **Capacidades de ciberdefensa más sólidas.** Se anima a los estados miembros a incluir la ciberdefensa en el marco de la cooperación estructurada permanente y el Fondo Europeo de Defensa, con el fin de apoyar los proyectos en materia de ciberdefensa. En el diseño del Centro europeo de investigación y competencias en materia de ciberseguridad, podría contemplarse añadir una dimensión de ciberdefensa. Para resolver el déficit de competencias en la materia, la UE creará en 2018 una plataforma de formación y educación

en ciberdefensa. La UE y la OTAN fomentarán de forma conjunta la cooperación en materia de investigación e innovación sobre ciberdefensa. Se reforzará la cooperación con la OTAN, especialmente la participación en ejercicios paralelos y coordinados.

- **Aumento de la cooperación internacional.** La UE endurecerá su respuesta a los ciberataques mediante la aplicación del Marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas, marco estratégico de prevención de conflictos y aumento de la estabilidad en el ciberespacio. Esta iniciativa irá acompañada de nuevos esfuerzos de ampliación de la cibercapacidad para ayudar a los terceros países a hacer frente a las ciberamenazas.

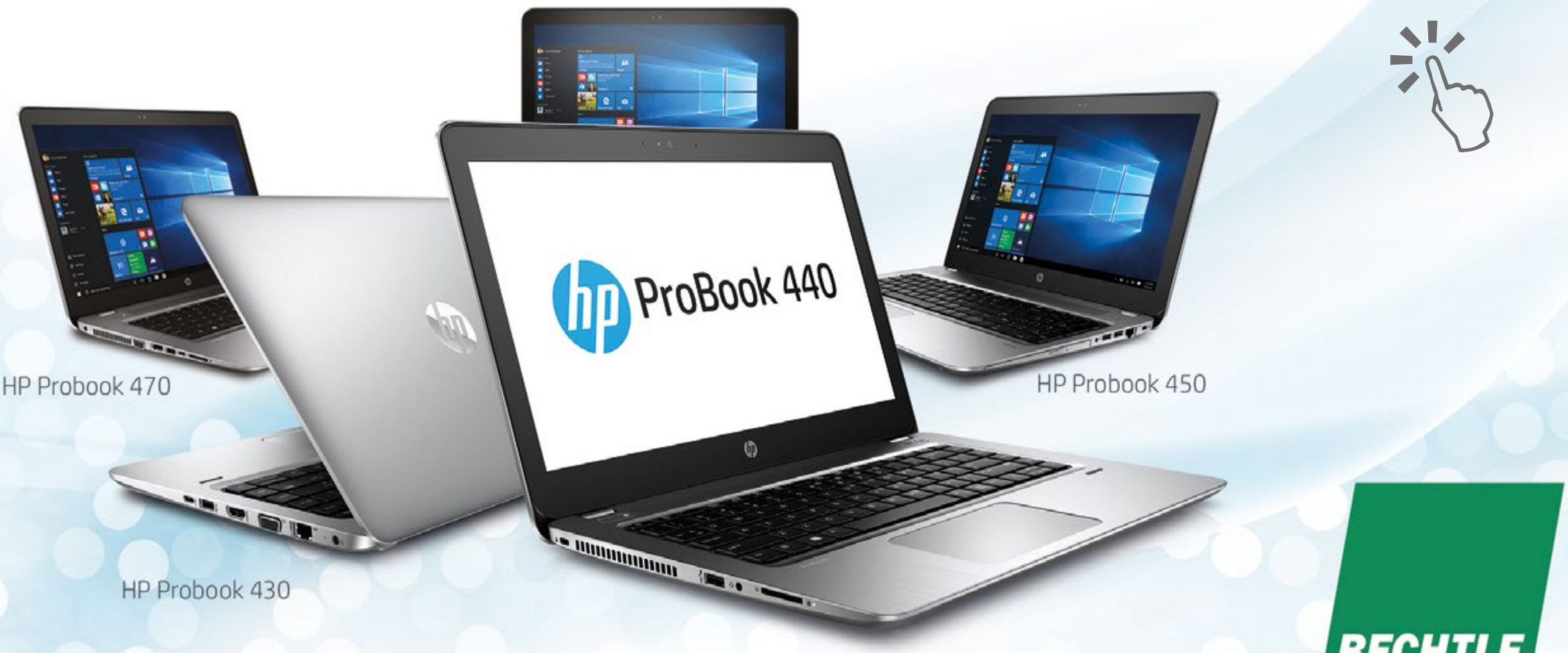
¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Enlaces relacionados

- Ataques con exploits, de las amenazas diarias a las campañas dirigidas
- Informe Symantec sobre la seguridad en 2017
- Informe sobre la responsabilidad de las entidades financieras en el fraude
- La paradoja tras la experiencia del usuario con el criptoransomware
- 7 beneficios de un enfoque holístico de la protección de datos
- 4 formas de protegerse y recuperarse de ataques de ransomware
- Ciberrriesgos y reputación en las pequeñas empresas

HP Probook serie 400 G4

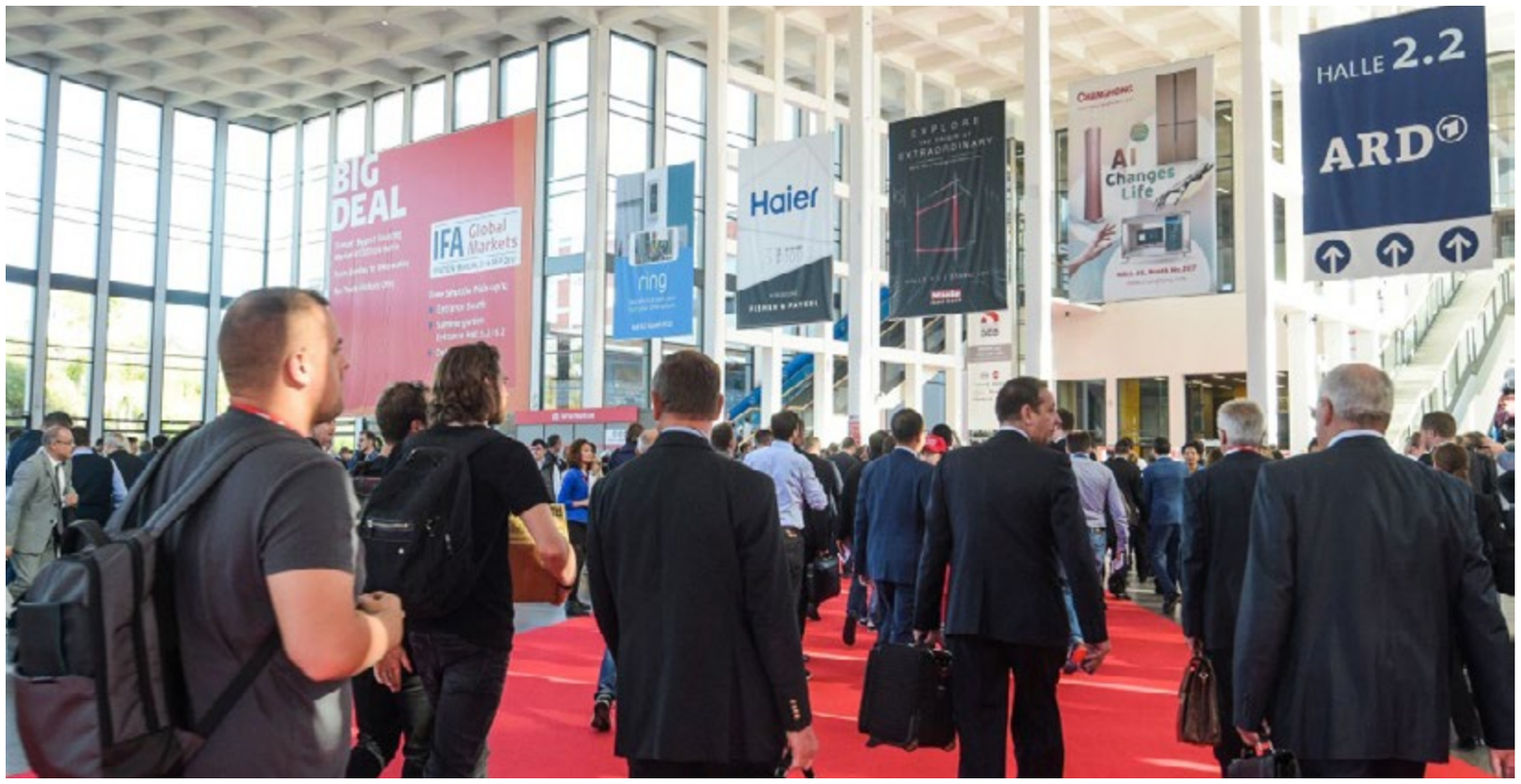
Satisfaga las diversas necesidades de su empresa.



Berlín volvió a acoger una nueva edición de la popular feria

IFA 2017 muestra el futuro de la tecnología de consumo

Con más de 1.800 expositores y 159.000 metros cuadrados de espacio ocupado, IFA confirma su posición como una de las mayores ferias de tecnología de consumo, un espacio en el que las pantallas de TV HD ultra-delgadas, las cámaras que filman vídeos de 360 grados y los dispositivos de control de voz, fueron algunos de los protagonistas.



A principios del mes de septiembre arrancó una nueva edición de la feria IFA, que no sólo acogió aún más innovaciones y lanzamientos de productos que en años anteriores, sino que además reunió un número récord de productos digitales bajo un mismo techo.

Durante seis días, IFA fue el hogar de los últimos productos de las principales marcas mundiales, que mostraron sus productos, accesorios y servicios en el área de exposición. Las pantallas de TV HD ultra-delgadas, las cámaras que filman videos de 360 grados, los wearables con capacidades de control de la salud y los dispositivos de control de voz, fueron algunos de los protagonistas de esta edición. El salón también dió cabida a los electrodomésticos, que se exhibieron en el espacio Home Appliances@IFA. La feria también ofreció una plataforma para investigadores, desarrolladores y start-ups, que mostraron sus ideas de vanguardia

Con más de 1.800 expositores y 159.000 metros cuadrados de espacio ocupado, IFA confirma su posición como una de las mayores ferias de tecnología de consumo

en IFA NEXT, un centro de innovación que ofreció la oportunidad para probar cómo vamos a trabajar y vivir en el futuro, reuniendo conocimientos globales e ideas visionarias que moldearán nuestro futuro digital.

Palabras de la organización

Según Christian Göke, CEO de Messe Berlin, "la innovación está en el ADN de IFA. Durante casi 100 años, la innovación ha estado en el corazón de esta feria, que ha crecido año a año. Ningún otro evento reúne a tantos retailers, compradores, visitantes profesionales y miembros de los medios de comunicación en una época tan ideal del año".

Por su parte, Jens Heithecker, director ejecutivo de IFA, señalaba que el objetivo de la feria es "acelerar el crecimiento y la innovación, y, por eso, IFA se ha vuelto cada vez más atractivo para los visitantes profesionales de todo el mundo. IFA es ahora la feria comercial más importante para la industria de electrónica de consumo, con el mayor número de visitantes profesionales y la mayor asistencia internacional".

Prueba de la importancia del mercado de electrónica de consumo es que, para este año, está previsto que el mercado ingrese 887 billones de euros, lo que indicaría una tasa de crecimiento de alrededor del 4%. Los avances en el mercado mundial de electrodomésticos también son optimistas. Los investigadores de mercado predicen que las ventas de pequeños electrodomésticos alcanzarán a aproximadamente 46,5 billones de euros, un aumento de alrededor del 7%, mientras que las ventas de grandes electrodomésticos alcanzarán los 180 billones de euros, un 5% más.

Equipos con procesadores Intel

IFA Berlin 2017 es un gran escaparate en el que se exhiben muchas tecnologías y dispositivos nuevos e innovadores creados para el mundo del futuro, y en el que no podía faltar Intel.

Desde los procesadores a plataformas completas, Intel está impulsando todo lo que el ecosistema puede ofrecer a los consumidores, proporcionando unas experiencias inmersivas, portabilidad, conectividad y más potencia informática en unos formatos más finos,

whitepapers

EL NUEVO PUESTO DE TRABAJO PRODUCTIVO:

ESTRATEGIAS PARA LA MOVILIDAD EMPRESARIAL

Las soluciones de movilidad juegan un papel importante para las medianas empresas en la mejora de la productividad del lugar de trabajo. Nuevos recursos y herramientas permiten a los empleados móviles y remotos colaborar de forma tan eficiente como los que se encuentran en la misma oficina. El desafío es cómo reforzar la seguridad y la gestión de la red para obtener conexiones más seguras. Este informe de IDC aporta algunas ideas para llegar a ese objetivo.

IDC
El nuevo lugar de trabajo productivo: estrategia de recursos móviles en medianas empresas

ligeros e innovadores que van a establecer nuevos estándares.

Uno de los mecanismos para conseguir estos objetivos es el establecimiento de una sólida colaboración con partners en todo el mundo, especialmente con fabricantes de PC. Pues bien, desde que el 21 de agosto la compañía presentase la 8ª generación de procesadores Intel Core y lanzase el primer conjunto de productos –unos procesadores móviles que facilitan el diseño de portátiles finos y ligeros y diseños 2 en 1 para los consumidores, con hasta un 40% más de potencia en comparación con la generación anterior–, son muchos los partners OEM que han anunciado dispositivos equipados con los nuevos procesadores, muchos de los cuales se han podido ver en primicia en IFA. Entre los productos presentados destacan:

- **El Dell XPS 13,** que ofrece una batería de larga duración y una potencia superior, y los últimos 2-en-1 y portátiles Inspiron 7000, que proporcionan una experiencia visual sin igual y un gran rendimiento en unos equipos elegantes.
- **El ASUS ZenBook Flip S,** que combina sofisticación con la comodidad y versatilidad de una pantalla de 360º y tan solo 10.9 mm de grosor, y el ZenBook Flip 14, un equipo potente y refinado, con prestaciones para dar rienda suelta a tu creatividad.
- **El Lenovo Yoga 920,** que incluye unos mecanismos intuitivos e inmersivos para trabajar y jugar, y que se puede personalizar aún más con los diseños de carcasas Gorilla Glass, y el Miix 520, que ofrece a los usuarios prestaciones para crear contenidos o para disfrutar de un entretenimiento inmersivo en cualquier lugar en el que se encuentren.
- **Los equipos HP ProBook 400 Series,** que permiten a los profesionales realizar sus tareas tanto en la oficina como cuando se encuentran en desplazamiento, y el HP Spectre x360, diseñado para los más creativos, que ha sido actualizado para proporcionar aún más potencia.
- **El Acer Nitro 5 Spin,** diseñado para ofrecer la máxima versatilidad para los juegos ocasionales, y el Swift 5, que ofrece la máxima portabilidad, un ágil uso y un diseño elegante en un portátil ultra fino y ligero.

Todos estos diseños tienen algo en común: el elevado rendimiento que proporciona la 8ª generación de procesadores Intel Core. Más de 145 diseños móviles en todos los formatos y tamaños se van a encontrar disponibles para los consumidores de todo el mundo a lo largo de los próximos meses, y esto es solo el comienzo, pues se prevé que las unidades para equipos de sobremesa estén disponibles este otoño y se anuncien más modelos a lo largo del año que viene.

NOVEDADES DE IFA BERLÍN 2017

CLICAR PARA VER EL VÍDEO

Durante seis días, IFA fue el hogar de los últimos productos de las principales marcas mundiales, que mostraron sus productos, accesorios y servicios en el área de exposición

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

Pantallas de TV HD ultra-delgadas, las cámaras que filman vídeos de 360 grados, los wearables con capacidades de control de la salud y los dispositivos de control de voz, fueron algunos de los protagonistas

Otros anuncios

Pero no sólo se presentaron equipos portátiles. D-Link, por ejemplo, acudió a IFA con los productos que lanzará a lo largo de los próximos meses para mejorar la experiencia de los usuarios con las redes WiFi y la videovigilancia.

Por un lado, se ha presentado D-Link COVr Hybrid Powerline Wi-Fi Mesh System, la primera solución en usar la tecnología PLC Powerline, en lugar de los extensores Wi-Fi en los que se basan la mayoría de soluciones Wi-Fi Mesh. Por otro lado, D-Link ha ampliado su gama de Cámaras IP mydlink con la DCS-8000LH Mini HD Wi-Fi Camera, un modelo ultracompacto pensado para no llamar la atención y realizar una monitorización discreta, y la DCS-8100LH HD, que dispone de visión de 180º sin distorsión, ideal para para monitorizar grandes estancias.

En el apartado de smartphones, Lenovo, propietaria de Motorola, acudió a la cita para presentar su Moto X4, un teléfono que incorpora un sistema de doble cámara como una de sus principales características. LG, por su parte, presentó el LG V30, que cuenta con doble cámara y dispone de Google Assistant, el cual ya está disponible en castellano. Sony mostró sus nuevos Xperia. Conocidos como XZ1 y XZ1 Compact, disponen de una cámara de 19 megapíxeles que permite el escaneo 3D de objetos y personas.

Las gafas Mirage AR de Lenovo mostraron todo el potencial de la realidad aumentada. No en vano, éstas fueron anunciadas junto al juego Star Wars: Jedi Challenges, mientras que una de las novedades de Samsung fueron sus relojes inteligentes Gear Sport y Gear Fit 2.

La importancia de las Smart TV

Más y más consumidores quieren acceder a contenido de video on-line en su televisión, por lo que están optando por comprar una Smart TV. En el primer semestre de 2017, estas compras ya constituyen más de la mitad de todas las ventas de televisores realizadas en todo el mundo, mientras que las ventas de dispositivos Ultra HD / 4K y televisores con tecnología OLED también continuaron aumentando. Estas son las conclusiones

sobre el mercado mundial de televisores dados a conocer por GfK con motivo de la feria IFA 2017 de Berlín.

Alrededor del 59% de todos los televisores vendidos en los primeros seis meses del año a nivel mundial fueron Smart TV, lo que significa que pueden conectarse

Está previsto que el mercado de electrónica de consumo ingrese 887 billones de euros, lo que indicaría una tasa de crecimiento de alrededor del 4%

a Internet y permitir el acceso a aplicaciones y navegadores. El año pasado el porcentaje estaba en el 51%. La impulsora de esta tendencia es China, donde el 89% de todos los televisores vendidos entre enero y junio eran Smart TV. En Europa el porcentaje es del 56%, 10 puntos más que en el mismo período del año anterior.

En el último año también se ha registrado un aumento en el volumen de ingresos. En el primer semestre de este año, la subida ha alcanzado más del 1%. GfK también predice que esta tasa de crecimiento se mantendrá el resto del año, y que las ventas globales de televisores superarán probablemente los 100 billones de euros.

El gasto medio en un televisor ha aumentado globalmente a 448 euros, frente a los 431 euros del año pasado. La razón de esta subida es el deseo de los consumidores de televisores más grandes y mejor equipados que puedan satisfacer sus necesidades individuales.

Las tecnologías nuevas y mejoradas también están impulsando el mercado de la televisión. Especialmente en términos de calidad de imagen, ha habido importantes avances en los últimos doce meses. HDR (High Dynamic Range) que ofrece un contraste mejorado y WCG (Wider Color Gamut) para un espectro de colores mejorado, han aumentado la calidad de imagen en los televisores Ultra HD / 4K. No es de extrañar pues que el 29% de todos los televisores vendidos en la primera mitad del año fueran Ultra HD. Se prevé un aumento adicional en la segunda mitad del año, por lo que es de esperar que en 2017 uno de cada tres televisores vendidos sea Ultra HD. Debido a que los televisores Ultra HD son significativamente más caros, estos constituyen el 48% del mercado de televisión en volumen de ingresos.

La tecnología OLED también continúa teniendo éxito y está siendo ofrecida cada vez por más fabricantes desde este año. 478.000 de estos televisores se vendieron en todo el mundo en los primeros seis meses del año, lo que representa un aumento del 94%.

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Enlaces relacionados

- Toda la información de IFA Berlín 2017
- Clima de consumo en Europa de GfK
- Barómetro del sector de los drones en España
- Perspectivas de la pequeña empresa en España
- Estado del negocio digital 2015-2020

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

Los gobiernos exigen a las tecnológicas que actúen con mayor rapidez

La Inteligencia Artificial, ¿arma contra la propagación de mensajes extremistas?

Durante su discurso ante la Asamblea General de Naciones Unidas, Theresa May exigió a las tecnológicas mayor rapidez a la hora de eliminar contenido extremista. La Inteligencia Artificial es, para la Primera Ministra Británica, una de las claves. No obstante, las compañías se defienden explicando que hacen todo lo que pueden, pero que no es tan sencillo.

Los gobiernos siguen instando a las compañías tecnológicas a acelerar la eliminación de contenido extremista de las redes sociales. La última en hacer este llamamiento ha sido Theresa May, Primera Ministra del Reino Unido, quien, durante su discurso ante la Asamblea General de Naciones Unidas, ha exigido a las tecnológicas a ir "más rápido" a la hora de eliminar este tipo de contenido.

De hecho, en una reunión que mantendrá con otros líderes mundiales y con las principales compañías TIC, entre las que se encuentran Facebook, Microsoft o Twitter, exigirá a éstas a eliminar el contenido extremista, tanto de las redes sociales como de los motores de búsqueda, en menos de dos horas, tal y como publica la BBC.

Ésta no es la primera vez que Theresa May responsabiliza a este tipo de firmas de la propagación de este tipo de contenido y de la labor de captación que se realiza por parte de grupos terroristas, como Daesh. Tras el atentado de London Bridge, May instó a poner fin a "los espacios seguros" que disfrutan los terroristas en Internet.

Dentro de las exigencias gubernamentales se encuentran poner límite a la encriptación de extremo a extremo, lo que impide que, de ser interceptados, los mensajes sean leídos por terceros, o adoptar medidas para frenar la difusión en las redes sociales.

No obstante, durante el discurso, Theresa May ha destacado los esfuerzos que las tecnológicas han reali-

zado en la lucha contra este contenido desde la creación de un foro de la industria para luchar contra el terrorismo el pasado mes de junio.

Theresa May considera que el desarrollo de tecnologías como la Inteligencia Artificial puede reducir considerablemente el tiempo necesario para eliminar el contenido extremista.

Theresa May exigirá a las tecnológicas eliminar el contenido extremista, tanto de las redes sociales como de los motores de búsqueda, en dos horas

Reino Unido no va a ser el único país que va a exigir a las compañías eliminar el contenido en dos horas. A los británicos también se les une Francia e Italia.

"No sólo tenemos que derrotar a los terroristas, sino que las ideologías extremistas que los alimentan son ideologías que predican el odio, dividen a la sociedad y socavan la convivencia", ha asegurado Theresa May.

Respuesta de Google

Tras el discurso de Theresa May, Primera Ministra del Reino Unido, ante la Asamblea General de Naciones Unidas, en el que reclamaba a las tecnológicas a eliminar el contenido extremista de redes sociales y buscadores, llegan las respuestas de las TIC.

Para Ken Walker, consejero general de Google, eliminar el contenido extremista en unas pocas horas supone un "enorme reto tecnológico y científico".

Walker, quien hablará en nombre no sólo de Google, sino tmbién de otras compañías como Microsoft, Twitter, Facebook y YouTube, en la reunión que va a mantener con los principales líderes mundiales en la sede de las Naciones Unidas el próximo 20 de octubre,

Twitter "saca pecho" de su lucha contra los mensajes extremistas

Twitter "saca pecho" de sus controles internos para eliminar contenido que promueva el terrorismo. Así lo ha asegurado la red social quien ha destacado que estos permiten eliminar este tipo de mensajes antes de que reciban las solicitudes gubernamentales.

Estas declaraciones llegan en medio de la polémica surgida tras los ataques terroristas que han sufrido diversas ciudades europeas y que han llevado a las autoridades tanto de la UE como de Estados Unidos a solicitar a las redes sociales mayor contundencia con este tipo de mensajes. No en vano, las redes sociales han sido utilizadas por yihadistas como herramientas de captación y difusión de sus mensajes.

Concretamente, Twitter ha eliminado casi 300.000 cuentas (299.649) en el primer semestre de este año, un 20% menos que hace seis meses, por enaltecimiento del terrorismo. Un 75% de éstas fueron eliminadas antes de que publicasen su primer tuit.

Menos del 1% se eliminaron por solicitudes gubernamentales, mientras que el 95% se eliminaron gracias "a los esfuerzos internos de Twitter por combatir el contenido extremista con herramientas propietarias".

Entre el 1 de agosto de 2015 y el 30 de junio de 2017, Twitter ha eliminado cerca de un millón de cuentas por enaltecimiento del terrorismo (concretamente, 935.897).

considera que estas empresas están haciendo "progresos significativos para eliminar todo ese contenido en pocas horas o que dejen de aparecer en primer lugar en las búsquedas". No obstante, y según las declaraciones de Walker, "no hay una barita mágica cuando se trata de encontrar y eliminar este contenido, aunque estamos mejorando mucho".

Walker recuerda que descubrir "material problemático" requiere "no sólo miles de horas de trabajo de personas", sino una inversión importante en avances de ingeniería y de I+D. "Los pajares son inimaginablemente grandes y las agujas muy pequeñas y cambian constantemente".

A pesar de que la Inteligencia Artificial supondrá un avance enorme a la hora de eliminar este tipo de contenido, Walker explica que las compañías necesitarán personal humano que ayude a "distinguir material legítimo, como la cobertura de noticias, con material problemático". Con lo que "enseñar" a las máquinas a distinguir este tipo de contenido no será sencillo.

"El aprendizaje de las máquinas ha mejorado, pero todavía hay mucho camino que recorrer". En este sentido, Walker reconoce que "necesitamos personas y necesitamos información de fuentes fiables de los gobiernos y de nuestros usuarios para identificar y eliminar algunos de los contenidos más problemáticos".

Además, asegura que, aunque una vez que se identifica este contenido es eliminado, "el gran reto es luchar contra aquellas personas que lo vuelven a publicar o identificar todas las copias que hay del mismo en Internet".

Dentro de las exigencias gubernamentales se encuentran poner límite a la encriptación de extremo a extremo o adoptar medidas para frenar la difusión en las redes sociales

whitepapers

Probando los límites de seguridad de los robots industriales

En 2018, las fábricas a nivel mundial emplearán aproximadamente 1,3 millones de robots industriales, y el valor del mercado internacional para los sistemas robóticos alcanzará aproximadamente 32.000 millones de dólares. Inevitablemente, estas previsiones de crecimiento producirán más intentos de atacar y comprometer a los robots industriales para obtener ganancias.

Trabajo ¿insuficiente?

Estos argumentos son insuficientes para los gobiernos. No en vano, según fuentes cercanas a Theresa May, citadas por la BBC, "estas compañías están formadas por algunas de las mejores mentes del planeta", con lo que cumplir con los requerimientos tendría que ser más sencillo. "Deberían centrarse realmente en lo que importa, que es detener la propagación del terrorismo y la violencia".

Y mientras, las tecnológicas continúan defendiéndose. De hecho, éstas aseguran que el atentado de London Bridge el pasado mes de junio ha supuesto un antes y un después. Tras el ataque, muchos Gobiernos señalaron a estas firmas y, según ellas, han intensificado su lucha contra este tipo de contenido.

DISCURSO DE THERESA MAY ANTE LA ONU

CLICAR PARA VER EL VÍDEO

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Para Google, eliminar el contenido extremista en unas pocas horas supone un "enorme reto tecnológico y científico"

Facebook y Twitter han repetido en numerosas ocasiones que están trabajando "duro" para eliminar de sus redes cualquier viso de actividad terrorista, como la exaltación, la apología o la captación, y todo lo que apoye estos mensajes extremistas.

YouTube, por su parte, asegura que recibe más de 200.000 alertas de contenido inapropiado al día, y que revisa el 98% de éstas en menos de 24 horas.

Coalición internacional

En este punto, tanto las tecnológicas como los Gobiernos reclaman una mayor colaboración internacional. Un portavoz del foro internacional de Internet para combatir el terrorismo afirma que combatir contra la propagación del discurso extremista en la Red requiere una respuesta de Gobiernos, la sociedad civil y el sector privado. "Unidos, estaremos comprometidos a hacer todo lo que esté a nuestro alcance para asegurar que nuestras plataformas no son utilizadas para distribuir contenido terrorista".

En este punto, desde el Reino Unido se cree que Naciones Unidas "es probablemente el mejor lugar" para debatir de qué manera se puede luchar contra el extremismo salvaguardando la libertad de expresión. Y es que, en su opinión, "necesitamos colaboración internacional".

Las compañías tecnológicas, que han estado, y están, sometidas a una enorme presión para hacer más en lo que a eliminación de contenido, cuentas y prevención de ataques terroristas se refiere, aunaron esfuerzos el año pasado para lograr este objetivo. Así, decidieron crear una base de datos conjunta para compartir información e impresiones digitales únicas que se asignan de manera automática a videos y fotos de contenido extremista. Con esta acción, la intención es detectar y eliminar contenido similar.

Enlaces relacionados

- Declaraciones de Ken Walker, de Google, en la BBC
- Asamblea General de Naciones Unidas
- La nueva generación de ransomware ha llegado
- ¿Eres parte de una botnet?
- Tres pasos para proteger tu negocio

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

>> La reinvención digital: una oportunidad para España >>

>> Inspiración para pymes: cómo transformar cuatro sectores clave >>

>> Internacionalización de Startups Españolas de Base Tecnológica >>

>> TI híbridas para pymes, en busca del equilibrio >>

>> tecnologiaparatuempresa.ituser.es <<

Hiperconvergencia:

La respuesta inteligente a las necesidades de las TI

Hewlett Packard Enterprise

Octubre 2017

Hiperconvergencia:

La respuesta inteligente a las necesidades de las TI

La infraestructura hiperconvergente son soluciones innovadoras de virtualización todo en uno que integran computación y almacenamiento definido por software en una única plataforma, también definida por software, y fácil de gestionar.

La TI se encuentra bajo una imparable presión para moverse más rápido y ser más ágil. Los procesos manuales complejos y la infraestructura no integrada no pueden proporcionar la potencia, la simplicidad y la velocidad necesarias para cubrir las necesidades de la empresa. Las aplicaciones están creciendo 5 veces más rápido de lo que la TI puede ofrecer, la gestión de las pilas de TI consume el 80 % del tiempo y de los presupuestos, y los gastos de la nube están aumentando rápidamente.

Introducción

La empresa está pidiendo a la organización de TI que cambie. En todo el mundo, los profesionales de TI están empezando a comprender que las arquitecturas heredadas no son capaces de responder a las demandas empresariales de hoy en día, como, por ejemplo,

los nuevos modelos de entrega de nube, el crecimiento drástico de los datos y la necesidad de desplegar servicios nuevos en cuestión de días.

En esta nueva era, el statu quo ha dejado de ser una opción. En respuesta a estos requisitos empresariales, numerosas organizaciones de TI han puesto en marcha proyectos de virtualización de servidores y computación en la nube para mejorar la prestación de servicios y multiplicar la agilidad de las TI. No obstante, para algunas organizaciones, las iniciativas ambiciosas de virtualización, nube e infraestructura han llevado a proyectos interminables, un aumento de la complejidad de la gestión y la multiplicación de los costes operativos. Los métodos antiguos ya no sirven, pero los nuevos no son necesariamente fáciles. Lo que se requiere en realidad es un nuevo tipo de solución donde todos los elementos trabajen juntos.

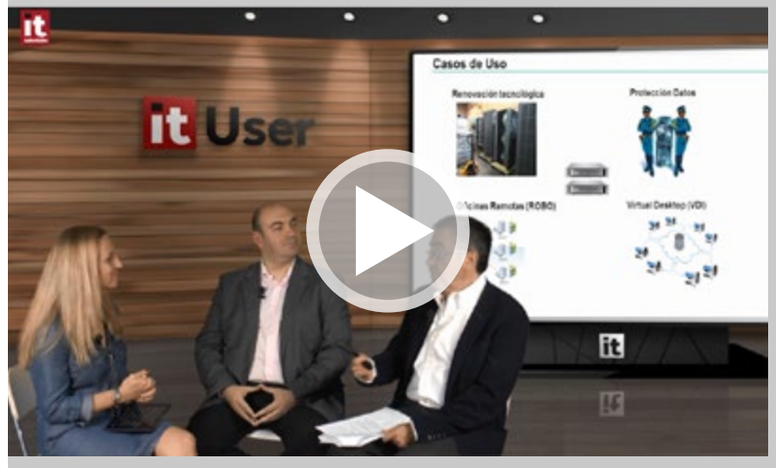
Aquí es donde entra en juego la hiperconvergencia, que proporciona muchas de las ventajas de un centro de datos virtualizado en un sistema compacto y rentable, caracterizado además por su facilidad de implementación, gestión y soporte.

En qué ayuda la hiperconvergencia

Con la hiperconvergencia, todo viene preconfigurado, preinstalado, listo para operar en minutos con tan sólo pulsar un botón, y diseñado a escala, sin necesidad de una SAN independiente.

Con los sistemas hiperconvergentes llave en mano, cualquiera, desde los generalistas de TI hasta los administradores más experimentados, puede implementar rápidamente entornos de TI completos en tan sólo 15 minutos desde el encendido al aprovisionamiento. Y pueden hacerlo sin la ayuda de integradores de sistemas externos.

WEBINAR HPE SIMPLIVITY: HIPERSIMPLE, HIPERESCALABLE, HIPERCONVERGENTE



CLICAR PARA VER EL VÍDEO

¿Se enfrenta a un crecimiento imprevisible? Con los sistemas hiperconvergentes, puede estar tranquilo. Los sistemas se amplían de forma lineal. Basta con añadir un sistema y nuevos nodos, sin interrupciones, a un clúster común. La arquitectura hiperconvergente integra software de red que descubre y añade automática-

La hiperconvergencia proporciona muchas de las ventajas de un centro de datos virtualizado en un sistema compacto y rentable, caracterizado además por su facilidad de implementación, gestión y soporte

mente nuevos nodos al clúster con el objetivo de multiplicar los recursos de computación y almacenamiento con cada módulo nuevo adicional.

La gestión es sencilla. Gracias a la integración de todos los componentes en un sencillo chasis con gestión común, no hay necesidad de contar con un equipo de especialistas con experiencia en virtualización, almacenamiento, servidores y redes. Frente a los sistemas que requieren multitud de componentes diferentes, incluida una SAN asociada con sus propios conmutadores, la naturaleza simplificada de los sistemas hiperconvergentes puede ayudarle a reducir los gastos de capital y operativos. Ahora tendrá todo en una pequeña caja de fácil gestión y mantenimiento que permite contar con mayor capacidad de computación y almacenamiento en el mismo espacio del centro de datos.

Y por si fuera poco, un solo proveedor puede dar soporte a todo el sistema, incluidos el hardware y software.

Ventajas para la empresa

Desde una perspectiva empresarial, las ventajas de los sistemas hiperconvergentes incluyen la reducción de los gastos iniciales de capital y operativos, gracias a que requiere menos componentes que los sistemas convencionales, a su reducido tamaño, a la gestión simplificada y a la eficiencia energética y de refrigeración.

Además, no necesitará varios especialistas para mantener un sistema hiperconvergente en funcionamiento. En la mayoría de los casos, bastará con un generalista de TI para ponerlo en marcha y realizar las tareas de gestión diarias.

Ventajas para la organización de TI

En el aspecto tecnológico, los sistemas hiperconvergentes facilitan el día a día de sus profesionales de TI. Ya no tendrán que gestionar sistemas de servidores, almacenamiento y redes dispares, cada uno con sus propias herramientas distintas. La infraestructura incluye capacidad de recuperación integrada y es fácil de configurar, aprender, mantener y escalar. Y sólo porque el sistema sea pequeño no significa que no sea potente.

Cuatro potentes servidores, servicios de datos completos con categoría empresarial, y una protección de datos inherente proporcionan el mismo nivel de servicio que las soluciones de TI tradicionales. La gestión diaria resulta muy simple con VMware vCenter: no requiere el aprendizaje de una nueva consola.

Otras ventajas

Toda la organización, tanto en la vertiente empresarial como en el área de TI, puede beneficiarse de la mayor agilidad que ofrecen unos sistemas de TI fáciles de poner en funcionamiento y capaces de escalar linealmente para apoyar las necesidades de una empresa dinámica. Cuando surge la necesidad de multiplicar los recursos, puede ponerse en funcionamiento un sistema hiperconvergente en 15 minutos, desde el encendido al aprovisionamiento.

Las empresas con emplazamientos remotos se benefician de sistemas estandarizados fáciles de implementar, gestionar y escalar por generalistas de TI. Para mantener el ritmo de las cargas de trabajo crecientes y en ocasiones imprevisibles, los emplazamientos remotos necesitan sistemas que puedan escalarse rápidamente y sin interrupciones.

Y para mantener la continuidad empresarial, necesitan sistemas que permitan la copia de seguridad, la recuperación y la replicación de datos centralizada, siguiendo configuraciones estándares y procesos corporativos. Los sistemas hiperconvergentes satisfacen todos estos requisitos.

Tomemos como ejemplo una empresa cuyos equipos de desarrollo y pruebas se encuentren repartidos por oficinas de todo el mundo. Una solución común que pueda obtenerse a nivel global permite a la empresa estandarizar los procesos de implementación, gestión y soporte de sus sistemas en emplazamientos remotos.

La empresa también puede estandarizar sus procesos de copia de seguridad y recuperación, además de aprovechar los recursos existentes en el centro de datos corporativo. Los desarrolladores de distintos lugares pueden beneficiarse también de las funcionalidades del sistema hiperconvergente, puesto que cada equipo de desarrollo puede disponer de su propia máquina virtual dedicada para sus proyectos. Y a medida que sus proyectos crecen, los desarrolladores pueden añadir rápidamente recursos de infraestructura para mantener unos tiempos de respuesta excelentes.

Además, la sencillez de los sistemas hiperconvergentes permite dejar en manos de generalistas de TI los trabajos de mantenimiento y gestión en los emplazamientos remotos. Ello ayuda a la empresa a reducir costes al tiempo que satisface el abanico completo de requisitos de computación y almacenamiento en sus emplazamientos remotos.

Ventajas para líneas de negocio

En muchas organizaciones de gran tamaño, las líneas de negocio o los departamentos internos necesitan una forma sencilla de gestionar los servicios de aplicaciones sin demasiada carga adicional para las TI y sin reducir las expectativas de rendimiento. Veamos, por ejemplo, un departamento financiero que se ocupe habitualmente de la elaboración de informes al final de cada trimestre. A medida que crecen los datos, se tarda cada

vez más en procesar los informes. Este departamento financiero también tiene nuevos proyectos en fase de planificación, incluido un sistema de contabilidad avanzado que podría tener que implementarse durante el trimestre en curso.

Un sistema hiperconvergente constituye una solución perfecta para apoyar nuevas aplicaciones o servicios, ya que puede encargarse y ponerse en marcha rápidamente con herramientas de configuración basadas en secuencias de comandos listas para utilizar. La capacidad de desplegar rápidamente un entorno de TI totalmente funcional podría permitir a la empresa implementar su nuevo sistema de contabilidad antes de finalizar el trimestre, generar informes puntualmente y evitar el caos habitual de fin de trimestre.

Ventajas para medianas empresas

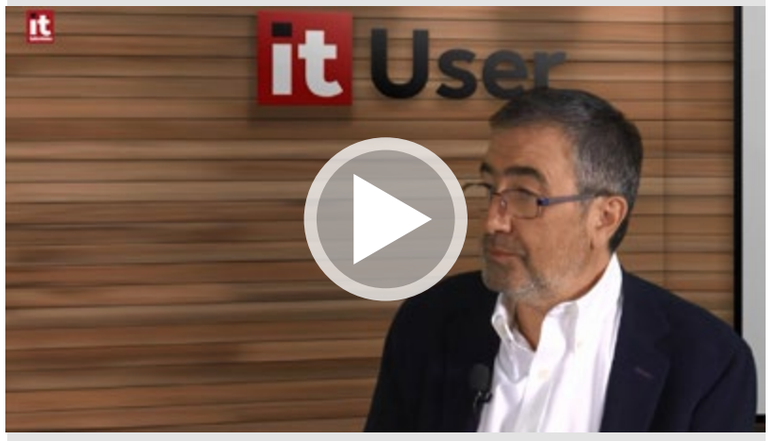
Tomemos ahora como ejemplo una mediana empresa que necesita expandir su capacidad de servidores y almacenamiento y desea evitar hacerlo con un proyecto de TI costoso e interminable.

Los sistemas hiperconvergentes son esencialmente un centro de datos llave en mano listo para usar que puede obtenerse e implementarse en cuestión de minutos. Pensemos también en un hospital que desea que su personal médico pueda acceder a aplicaciones y datos de forma segura, ya sea en las propias instalaciones o trabajando desde una ubicación remota.

El hospital puede implementar sistemas hiperconvergentes para ejecutar un entorno de infraestructura de escritorios virtuales (VDI). La solución de VDI otorga al personal del hospital acceso a aplicaciones y datos que residen en un sistema centralizado. De este modo, el hospital consigue satisfacer los requisitos de acceso y rendimiento del personal médico de forma eficiente al tiempo que mantiene la confidencialidad de los pacientes.

A medida que el volumen de datos almacenados aumenta con el tiempo, el hospital puede ampliar con facilidad su entorno de infraestructura de escritorios virtuales (VDI) añadiendo sistemas hiperconvergentes adicionales o ampliar hacia otro almacenamiento basado en VSA en el centro de datos, que expande a su vez sin interrupciones un grupo de recursos común dentro de un entorno virtualizado y definido por software. El hospital también se beneficia de las reducidas dimensiones de los sistemas, una ventaja que facilita la ampliación de la infraestructura en un centro de datos con restricciones de espacio.

WEBINAR HPE SIMPLIVITY: CASOS DE USO



CLICAR PARA VER EL VÍDEO

Otra serie de ventajas para las empresas

Las soluciones de hiperconvergencia potencian la TI proporcionando una plataforma simple, eficiente y definida por software que combina todo por debajo del hipervisor y ofrece la agilidad y la rentabilidad de la nube con las capacidades empresariales de la infraestructura local.

Pero, en realidad, ¿qué ventajas ofrecen este tipo de plataformas? En primer lugar, permiten la consolidación del centro de datos. Colocar toda su infraestructura de TI por debajo del hipervisor en una plataforma x86 escalable reduce sus dispositivos de centro de datos

en 10:1, lo que supone una reducción de los costes iniciales, una mayor eficiencia operativa y una mejora del rendimiento.

Además, se incrementa el nivel de seguridad, porque se pueden proteger los datos en una fracción del tiempo requerido por las soluciones anteriores, al no estar tan integradas. Con protección de datos global, integrada y recuperación ante desastres automatizada, en el caso de Hewlett Packard Enterprise con HPE SimpliVity, se reduce los requisitos de almacenamiento y ancho de banda, dando lugar a más puntos de recuperación y protección de máquinas virtuales mejorada.

En tercer lugar, se pueden reducir los costes sin sacrificar el rendimiento o la resiliencia. Es posible conseguir más escritorios virtuales en menos hardware, añadir nodos fácilmente cuando se implementen nuevos escritorios, y realizar copias de seguridad, restaurar o clonar una máquina virtual globalmente en tres clics o menos.

Otra ventaja es la de unificar y proteger sucursales y oficinas remotas. En el caso de la plataforma de HPE, SimpliVity introduce escalabilidad rentable para oficinas sucursales y remotas, proporciona eficiencia y protección de datos integrada para ROBO, y centraliza la gestión en una única solución unificada.

HPE SimpliVity

HPE Simplivity es una plataforma hiperconvergente, de nivel empresarial y potente que unifica los mejores servicios de datos de su categoría con el servidor más vendido del mundo.

La rápida proliferación de aplicaciones y el creciente coste de mantenimiento de la infraestructura anterior ocasiona importantes desafíos de TI para muchas organizaciones. Con HPE SimpliVity, puede simplificar y habilitar las operaciones de TI a una fracción del coste de las soluciones de nube tradicional y pública combinando su infraestructura de TI y servicios de datos avanzados en una única solución integrada. HPE SimpliVity es una plataforma hiperconvergente, potente, sencilla y eficiente que une los mejores servicios de datos de su categoría con el servidor más vendido del mundo y ofrece la garantía más completa del sector.

Los sistemas hiperconvergentes son esencialmente un centro de datos llave en mano listo para usar que puede obtenerse e implementarse en cuestión de minutos

Una infraestructura más moderna

El verdadero poder de la hiperconvergencia proviene de la consolidación total de su software y dispositivos de hardware. HPE SimpliVity combina toda su infraestructura en un módulo simple y flexible para que pueda reducir el coste y la complejidad de su entorno de TI y proporcionar la tecnología que su organiza-

WEBINAR HPE SIMPLIVITY: ¿POR QUÉ LA HIPERCONVERGENCIA DE HPE ES DIFERENTE?

CLICAR PARA VER EL VÍDEO

ción necesita. Éstas son algunas de las ventajas que se obtienen con la infraestructura hiperconvergente de HPE Simplivity:

- **La compresión y la deduplicación** siempre en funcionamiento permite un potente rendimiento de las aplicaciones y ahorros de coste de la capacidad en el almacenamiento y la copia de seguridad.
- **La gestión global centralizada y sencilla** permite que administre todas las operaciones a través de su consola de gestión de hipervisor y actualice rápidamente políticas a lo largo de todo su entorno.
- **Mejore drásticamente la eficiencia general** en toda su empresa con ahorros significativos de TCO (según algunos cálculos el ahorro puede alcanzar un 73%) en comparación con la infraestructura tradicional y la nube pública.
- **Consiga mejoras importantes** en eficiencia de datos, disponibilidad, complejidad y costes con capacidades de almacenamiento y gestión de datos con diseño específico.
- **La eficiencia de datos** ofrecida por HPE SimpliVity mejora el rendimiento de las aplicaciones, libera el almacenamiento y acelera las funciones de restauración y copia de seguridad remotas, ofreciendo un promedio de mejora de eficiencia de datos de 40:1 en las implementaciones.

- **La gestión centrada en máquinas virtuales** y basada en políticas extraída del hardware subyacente simplifica las operaciones diarias y permite una movilidad de datos sin interrupciones, haciendo que los equipos de desarrollo y los usuarios finales sean más productivos.
- **Elimine la necesidad de protección de datos de otros fabricantes.** HPE SimpliVity proporciona la resiliencia, la copia de seguridad integrada y la replicación con eficiencia de ancho de banda que necesita para garantizar los mayores niveles de integridad de datos y disponibilidad.

Enlaces relacionados

- V HPE Simplivity: Hiperconvergente, hiperescalable e hipersimple
- W Qué puede hacer la hiperconvergencia para ayudar a la organización de TI
- W Diez cosas a tener en cuenta antes de comprar infraestructura hiperconvergente
- W Estrategias para la implementación de infraestructura hiperconvergente
- W Infraestructura hiperconvergente para la protección de datos
- W Simplivity 380
- W Credit Union
- W Totes
- W NewPage

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

La educación como vía para promover la salud y erradicar la pobreza

Habitualmente, en esta sección hablamos de atención médica, porque la Fundación Adelias pone una gran parte de sus esfuerzos en el cuidado de la salud de los más pequeños. Sin embargo, en esta ocasión vamos a tocar otro de las áreas en las que la Fundación está trabajando. En este caso, tal y como nos cuenta Samira Brigüech, presidenta de la Fundación Adelias, vamos a hablar de la relación entre educación y salud, así como en el trabajo desarrollado por la Fundación en esta área.

Hablemos de educación y del impacto que tiene cuando hablamos de niños en situación de pobreza. Está comprobado que cuanto menor es el nivel de formación, mayor es la probabilidad de que la pobreza se consolide.

También está demostrado por múltiples estudios en todo el mundo que hay una conexión entre la salud y la educación. Leí recientemente en un artículo en internet que un catedrático comentaba que "una mejor educación se asocia a una vida más larga, porque aquellos que tienen mayor nivel educativo son más propensos a tener los recursos y el conocimiento para seguir comportamientos más saludables, ganar más dinero y vivir con menos estrés crónico".

También comentaba que "el nivel educativo que una persona alcanza se relaciona con su nivel de alfabetización y su nivel de conocimiento de la salud, y esto está vinculado con sus conductas: a mayor nivel educativo, mejor nutrición, se hace más ejercicio y se consumen menos drogas".

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

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.

Nuestra ambición, como ONG comprometida con la salud y la educación, es promover durante el año 2018 diferentes programas de apoyo en diferentes colegios de la Comunidad de Madrid

Mejorar el nivel educativo contribuye eficazmente a no perpetuar la pobreza. Según datos de UNICEF, si todos los niños del mundo aprendieran a leer, 171 millones de personas abandonarían su situación de pobreza absoluta.

Proyectos educativos

Desde la Fundación Adelias promovemos proyectos educativos tanto en lo relativo a la construcción de escuelas como fomentando el uso de la tecnología.

Actualmente, contamos con 2 proyectos, uno en Madrid y otro en Marruecos. En Madrid, ayudamos a niños con problemas de aprendizaje, donándoles equipos informáticos para motivarles a realizar sus tareas educativas. Hemos informatizado desde hace años, con ayuda del BBVA, el Colegio Público Alhambra, y hemos contribuido, en colaboración con nuestros colegas de Save the children, en este mismo colegio, en su proyecto contra el fracaso escolar.

En Marruecos, construimos un colegio para 50 niños, patrocinado por la Caixa, en su proyecto contra la pobreza infantil, y promovemos espacios de conocimiento y entretenimiento para fomentar una vida sana.

Nuestra ambición, como ONG comprometida con la salud y la educación, es promover durante el año 2018 diferentes programas de apoyo en diferentes colegios de la Comunidad de Madrid. Proporcionando ordenadores, impresoras, tablets y otros dispositivos que estimulen el aprendizaje. También contaremos con programas para que los voluntarios que lo deseen, puedan dar apoyo extraescolar a niños con dificultades de aprendizaje o que muestran desinterés por estudiar y/o hacer sus deberes. Contaremos igualmente con un proyecto de innovación tecnológica en el que los voluntarios, con habilidades en el uso de herramientas informáticas, puedan donar tiempo y conocimiento a niños que presentan dificultades para entender la informática y todo lo que puede aportar como instrumento educativo.

Si estás interesado en participar en alguno de estas iniciativas, contacta con nosotros en info@fundacionadelias.org, tanto para donar equipos en desuso como para participar como voluntario en nuestros proyectos educativos.

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Enlaces relacionados

Fundación Adelias

GDPR: cómo lograr una gestión integral de la información

La normativa GDPR está ejerciendo una fuerte presión sobre los CIO, que luchan por encontrar el equilibrio entre su deseo de consolidación y gestión centralizada, y la necesidad de cumplir con la fecha límite de 2018 y resolver los retos operativos relacionados con el GDPR. El mayor reto al que se enfrentan es conseguir el control de los datos sin estructurar. ¿Cómo lograrlo? Lee este informe.

Barreras para alcanzar el éxito en el negocio digital

La transformación digital impacta en todos los departamentos y funciones de un negocio, hasta el punto de que ha dejado de ser un dominio del CIO y de los departamentos de TI. Los líderes de negocio se ven constantemente retados a llevar a sus empresas al siguiente nivel, innovando y creando nuevos modos de operar para lograr el crecimiento. Este informe repasa algunas de las mayores barreras para alcanzar el éxito de los negocios digitales y cómo estos retos están frenando la consecución de los objetivos empresariales.

Cómo acelerar la Transformación Digital gracias a la analítica

Para mejorar su balance económico, las medianas empresas deben adoptar una estrategia basada en datos y analítica. Necesitan construir un marco de trabajo para reunir, conservar y analizar datos que les hagan ganar inteligencia de negocio y garantizar que todos los empleados acceden al nivel de información adecuado. Este informe de IDC explica por qué la inversión en soluciones de infraestructura de TI avanzada no es más una opción para acelerar la transformación digital, sino una obligación para progresar en la economía digital.

4 formas de protegerse y recuperarse de ataques de ransomware

El número de incidentes de ransomware sigue creciendo porque se han convertido en una sencilla fuente de ingresos para los ciberdelincuentes. Cuando uno de esos ataques ocurre, las organizaciones pierden acceso a archivos críticos y, para recuperarlos, se enfrentan a la decisión de pagar por su rescate, con la esperanza de que le sean devueltos, o someterse a un proceso de recuperación que no les garantiza que los datos se restablezcan de una forma totalmente fiable. Para mantener el acceso necesario a estos datos críticos, sigue las cuatro mejores prácticas que te propone este documento.

La Documentación TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

Criptomonedas: el primer resultado de la tecnología blockchain

Todos hemos oído hablar de blockchain pero son pocos los que se atreven a explicar en profundidad las implicaciones que esta tecnología tiene. El sector financiero es uno de los más señalados como afectados, algo lógico si se tiene en cuenta los cambios que conllevan las criptomonedas como Bitcoin. Pero son muchas las industrias que no pueden mirar para otro lado ante la llegada de una tecnología llamada a cambiar la forma en que trabajan y se relacionan con partners, clientes y socios.

¿Te avisamos del próximo IT User?

Así que vayamos por partes. Blockchain es una idea de una persona o grupo de personas (conocidas por el seudónimo Satoshi Nakamoto) que se ha convertido en algo que está llamado a cambiar el mundo. Pero ¿qué es Blockchain? Además, las criptomonedas se han convertido en un fenómeno mundial conocido por la mayoría de la gente. Aunque algunos consideran que aún es una cosa muy geeky y no entendido por la mayoría de la gente, los bancos, los gobiernos y muchas empresas son conscientes de su importancia.

Vamos pues, paso a paso.

Blockchain, la cadena de bloques revolucionaria

La tecnología blockchain está llamada a revolucionar muchas industrias, entre ellas la financiera. De hecho, blockchain fue pensada originalmente para la moneda digital Bitcoin, aunque la comunidad tecnológica está encontrando otros usos potenciales para la tecnología.

CRITOMONEDAS, EL DINERO DEL FUTURO

CLICAR PARA VER EL VÍDEO

Al permitir que la información digital se distribuya pero no se copie, la tecnología blockchain está creando lo que para muchos es la columna vertebral de un nuevo tipo de Internet. Y al igual que la red o que otros productos y servicios (como un coche), no hace falta saber cómo funciona blockchain para usarlo. Básicamente, podríamos imaginarnos una hoja de cálculo que se duplica miles de veces en una red de ordenadores, que está diseñada para actualizar regularmente esta hoja de cálculo y que se configura como una cadena de bloques.

La información almacenada en la cadena existe como una base de datos compartida y continuamente reconocida por todas las partes. Algo que tiene beneficios obvios. La base de datos no se almacena en una sola ubicación, lo que significa que los registros que guarda son verdaderamente públicos y fácilmente verificables. No existe una versión centralizada de esta información, por lo que un hacker no lo puede corromper. En realidad, los datos están alojados en millones de ordenadores simultáneamente, lo que también permite que sean accesibles por cualquier persona en Internet. La tecnología Blockchain no puede ser controlado por una sola entidad.

Bitcoin fue inventado en 2008. Desde entonces, la cadena de bloque Bitcoin ha operado sin interrupciones significativas, ya que los fallos que ha habido se deben a la piratería informática o a la mala administración por errores humanos.

Si Internet lleva funcionando casi 30 años y la tecnología blockchain está configurando una nueva red, cabe esperar que la tecnología blockchain siga desarrollándose.

La red de cadenas de bloques se nutre del consenso de todas las partes que la forman, por lo que se controla cada diez minutos. Una especie de ecosistema que se auto-audita y que concilia cada transacción que ocurre en intervalos de diez minutos. Cada grupo de estas transacciones se denomina “bloque”.

it whitepapers

BITCOIN:
EL ORIGEN

Satoshi Nakamoto, supuesto creador de la criptomoneda bitcoin, describe en este documento este sistema de pago electrónico entre iguales. Según él describe en el documento, una versión puramente peer-to-peer de los pagos electrónicos permitiría que los pagos online se envíen directamente desde una parte a otra sin la intervención de una institución financiera.

¿Te avisamos del próximo IT User?

it Digital Security

Todo lo que necesitas saber de Ciberseguridad está a un click

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

Bloques transparentes e iguales

Por eso, se dice que las cadenas de bloques se caracterizan por su transparencia y por el hecho de que los datos se integran en la red como un todo. Además, no se puede corromper y la alteración de cualquier unidad de información sobre la cadena de bloque significaría el uso de una enorme cantidad de poder de computación para anular toda la red.

Sin embargo, es poco probable que esto suceda en una cadena de bloques porque si alguien tomara el control del sistema para capturar Bitcoins, por ejemplo, esto provocaría destruir su valor.

Cada nodo es un "administrador" de la cadena de bloques, y se une voluntariamente a la red (en este sentido, la red está descentralizada). Sin embargo, cada uno tiene un incentivo para participar en la red. Originalmente, es la posibilidad de ganar Bitcoins.

Los nodos es lo que se conoce como "minería" Bitcoin, aunque en realidad cada uno de ellos está compitiendo para ganar Bitcoins resolviendo puzzles informáticos. Se calcula que puede haber unas 700 criptomonedas ya disponibles. Pero, además, hay una serie de otras adaptaciones potenciales del concepto de blockchain original que están actualmente activas o en desarrollo.

Por diseño, la cadena de bloques es una tecnología descentralizada. Cualquier cosa que suceda en ella es una función de la red como un todo. Esto tiene algunas implicaciones importantes. Al crear una nueva forma de verificar las transacciones, los aspectos del comercio tradicional podrían resultar innecesarios. Las operaciones bursátiles llegan a ser casi simultáneas en la cadena de bloques, por ejemplo, o pueden hacer que los tipos de registros sean totalmente públicos. Y la descentralización ya es una realidad. Por eso se dice que esta tecnología tiene el potencial de eliminar a todos los intermediarios en muchas de las industrias actuales.

Así, existe una red global de ordenadores que utiliza la tecnología blockchain para gestionar conjuntamente la base de datos que registra las transacciones de Bitcoin. Es decir, Bitcoin es administrado por su red, y no por una autoridad central. La descentralización significa que la red funciona de una forma de usuario a usuario (o peer-to-peer). Las formas de colaboración masiva que esto hace posible apenas están comenzando a ser investigadas.

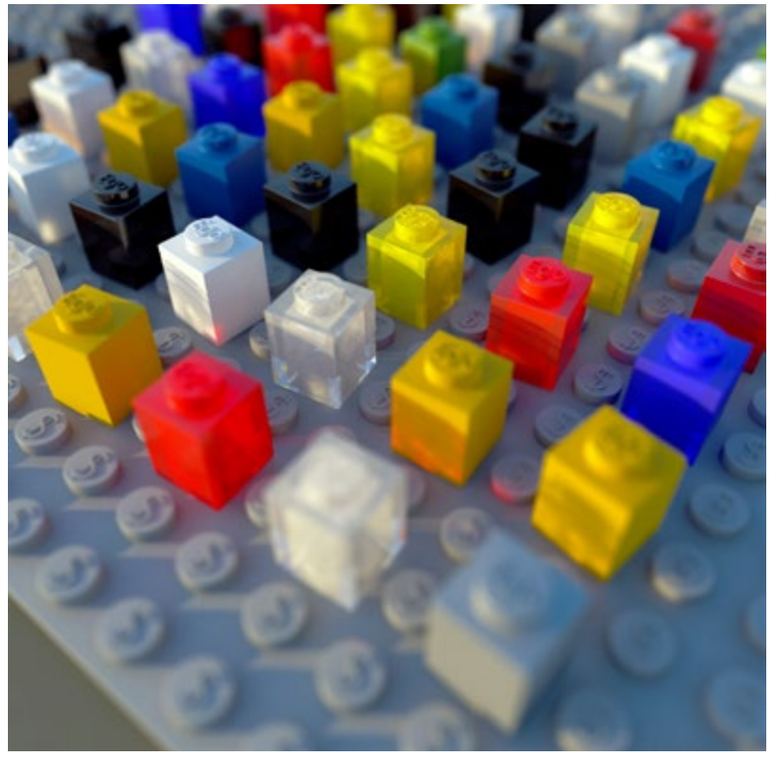
BLOCKCHAIN, MÁS ALLÁ DE BITCOIN

CLICAR PARA VER EL VÍDEO

¿Quién usará la cadena de bloques?

Actualmente, las finanzas ofrecen los casos de uso más fuertes para la tecnología y algunas remesas internacionales ya se están gestionando con esta tecnología. El Banco Mundial calcula que se enviaron más de 430.000 millones de dólares en transferencias de dinero en 2015. Y por el momento existe una gran demanda de desarrolladores de cadenas de bloque.

Por diseño, la cadena de bloques es una tecnología descentralizada. Cualquier cosa que suceda en ella es una función de la red como un todo



Coches inteligentes basados en Blockchain

Como hemos visto, la tecnología blockchain es una de las que más proyección tiene en el mercado tecnológico y sus implicaciones y repercusiones están aún por conocer, aunque muchos creen que puede transformar completamente muchos de los negocios tal y como los conocemos hoy en día.

Uno de esos mercados en los que se está experimentando con el uso de la tecnología de bloques es en los coches. Así, ZF, UBS e IBM se han aliado para desarrollar conjuntamente una plataforma abierta de transacciones automotrices para servicios de movilidad basados en la tecnología blockchain.

Car eWallet, que es como se llama la iniciativa, tiene el potencial de cambiar radicalmente la forma en que los fabricantes, proveedores y proveedores de servicios procesan las transacciones digitales y simplifican considerablemente el uso de los servicios del vehículo.

Car eWallet es un asistente digital en el coche que permite pagos seguros y convenientes incluso en cualquier lugar. Además, también puede realizar otras tareas, como abrir el maletero o las puertas. El Car eWallet se basa en la tecnología IBM Blockchain, que permite sincronizar la información de cada participante en la red en un registro de datos confiable e inalterable. Al mismo tiempo, garantiza que los usuarios sólo tienen acceso a la información que se les permite ver y utilizar.

Esto hace que las transacciones seguras casi en tiempo real sea posible sin necesidad de una instancia central o un tercero confiable. La plataforma abierta de transacciones automotrices para servicios relacionados con la movilidad tiene el potencial de cambiar radicalmente el comercio electrónico entre fabricantes, proveedores, proveedores de servicios y clientes.

"Nos aproximamos a un tiempo de grandes cambios que requieren soluciones transformacionales. Este acuerdo sobre Car eWallet se enmarca en esta nueva realidad", comenta Olga Blanco, directora de Blockchain en IBM España.

Las criptomonedas han dado a luz a un mercado increíblemente dinámico, de rápido crecimiento para los inversores y especuladores

La cadena de bloques elimina al intermediario para este tipo de transacciones. Si la informática se hizo accesible al público en general con la invención de la interfaz gráfica de usuario (GUI), conocida como "escritorio", la GUI más común diseñada para la cadena de bloques son las denominadas aplicaciones "wallet", que la gente usa para comprar cosas con Bitcoin, y almacenarlas junto con otras criptomonedas.

En opinión de Alexey Malanov, experto en malware de Kaspersky Lab, las Bitcoin y otras criptomonedas "pueden compararse con el oro virtual: su emisión es limitada, tiene cierto valor en la vida real (pagando anónimamente a través de Internet, transferencias transfronterizas rápidas con tarifas muy bajas...). Así que la gente está tratando de asegurarse de que su dinero no se deprecie".

Las transacciones en línea están estrechamente conectadas con los procesos de verificación de identidad. Es fácil imaginar que las aplicaciones de cartera se transformarán en los próximos años para incluir otros tipos de gestión de identidad.

Almacenando datos a través de su red, la cadena de bloques elimina algunos riesgos actuales, sobre todo con aquellos que se almacenan centralmente. Si la red carece de puntos centralizados de vulnerabilidad, los piratas informáticos tienen más dificultades para acceder a la información. Si el Internet de hoy en día tiene problemas de seguridad que son familiares para todos (con el sistema de "nombre de usuario / contraseña" como forma de proteger nuestra identidad y nuestros activos en línea), los métodos de seguridad Blockchain utilizan tecnología de cifrado.

La base para esto son las llamadas "claves" públicas y privadas. Una "clave pública" (una larga cadena de números generada aleatoriamente) es la dirección de un usuario en la cadena de bloqueo. Los Bitcoins enviados a través de la red se registran como pertenecientes a esa dirección. La "clave privada" es como una contraseña que le da acceso a su Bitcoin u otros activos digitales. Si guardamos los datos en la cadena de bloques, serán incorruptibles. Aunque esto es cierto, también lo es que la protección de sus activos digitales también requerirá la salvaguardia de su clave privada mediante la impresión, creando lo que se conoce como una cartera de papel.

Criptomonedas, el primer producto blockchain

Las criptomonedas nacen como un producto secundario de otra invención. Satoshi Nakamoto, el desconocido inventor de Bitcoin, nunca tuvo la intención de inventar una moneda. Pero cuando nació a finales de 2008, Satoshi dijo que había desarrollado "un sistema de dinero electrónico de igual a igual".

Después de ver cómo habían fracasado todos los intentos centralizados, Satoshi trató de construir un sistema de efectivo digital sin una entidad central. Como una red Peer-to-Peer para compartir archivos. Esta decisión se convirtió en el nacimiento de la criptomoneda.

Para realizar efectivo digital necesita una red de pago con cuentas, saldos y transacciones. Un problema importante que toda red de pago tiene que resolver es evitar el denominado doble gasto: evitar que una entidad gaste la misma cantidad dos veces. Por lo general, esto es hecho por un servidor central que mantiene un registro sobre los saldos.

En una red descentralizada, no tiene este servidor. Así que se necesita que cada entidad de la red haga este trabajo. Cada par en la red necesita tener una lista con todas las transacciones para comprobar si las transacciones futuras son válidas o un intento de duplicar la inversión.

Pero ¿cómo pueden estas entidades mantener un consenso sobre estos registros? Si los que comparten esta red no están de acuerdo con un solo balance menor, todo se rompe. Necesitan un consenso absoluto. hasta ahora, había una autoridad central para declarar el estado correcto de los saldos. Pero, ¿cómo se logra el consenso sin una autoridad central?

Ésta es una de las grandes innovaciones de Bitcoin y Satoshi: demostrar que era posible lograr el consenso sin una autoridad central. Las criptomonedas forman parte de esta solución.

BLOCKCHAIN, LA VERDAD MATEMÁTICA

CLICAR PARA VER EL VÍDEO

Enterprise Ethereum Alliance (EEA), en la que está el Santander, tiene como objetivo desarrollar e impulsar el uso de los registros contables compartidos (blockchain) entre empresas con la tecnología de código abierto Ethereum

¿Qué son las criptomonedas realmente?

Básica y técnicamente, son sólo entradas limitadas en una base de datos que nadie puede cambiar sin cumplir las condiciones específicas. En realidad, toda cuenta bancaria no deja de ser entradas en una base de datos que sólo se puede cambiar en condiciones específicas. Al fin y al cabo, el dinero es una entrada verificada en algún tipo de base de datos de cuentas, saldos y transacciones.

En las criptomonedas como Bitcoin, hay una red de pares. Cada par tiene un registro de la historia completa de todas las transacciones y por lo tanto del saldo de cada cuenta.

Una transacción es un archivo en el que se dice que un sujeto a dado un número dado de Bitcoin a otro usuario. Este archivo está firmado por la clave privada del primer usuario. Es criptografía básica de clave pública. Después de firmado, una transacción se transmite en la red, enviada de un par a otro. Ésta es la tecnología p2p básica. La transacción es conocida casi de inme-

it whitepapers

BLOCKCHAIN:

LA ÚLTIMA DISRUPCIÓN EN EL SISTEMA FINANCIERO

Lee este documento de BBVA Research, que detalla en qué consiste la tecnología de cadena de bloques, o blockchain, por qué supone una disrupción y cuáles son sus riesgos y desafíos.

diato por toda la red. Pero sólo después de un tiempo determinado se confirma.

La confirmación es un concepto crítico en las criptomonedas. Se podría decir que las criptomonedas son sobre todo confirmaciones. Mientras una transacción no sea confirmada, está pendiente y puede ser falsificada. Cuando se confirma una transacción, se establece en firme. Ya no es forjable, no puede ser revertida, es parte de un registro inmutable de transacciones históricas: la llamada cadena de bloques.

Soy minero (de bitcoin)

Sólo los mineros pueden confirmar las transacciones. Éste es su trabajo en una red de criptomonedas. Toman transacciones, las marcan como legítimas y las difunden en la red. Después de que una transacción es confirmada por un minero, cada nodo tiene que incluirlo en su base de datos. Se ha convertido en parte de la cadena de bloques.

Para este trabajo, los mineros reciben una recompensa con un símbolo de la criptomoneda (por ejemplo, Bitcoins). La actividad del minero es la parte más importante del sistema de criptomonedas.

Sobre todo debido a sus propiedades revolucionarias, las criptomonedas se han convertido en un éxito que ni siquiera su inventor se atrevió a soñar. Mientras que cualquier otro intento de crear un sistema de dinero digital no atrajo a una masa crítica de usuarios, Bitcoin tuvo algo que provocó entusiasmo y fascinación.

Las criptomonedas son también llamadas como el oro digital, que está a salvo de la influencia política y que promete preservar y aumentar su valor con el tiempo. Las criptoconversiones son también un medio de pago rápido y cómodo con alcance mundial, y son lo suficientemente privadas y anónimas como para ser temidas también como medio de pago en los mercados negros y en cualquier otra actividad económica ilegal. Además, las criptomonedas son utilizadas como un medio de especulación y una reserva de valor, lo que empequeñece los aspectos de pago.

En cualquier caso, las criptomonedas han dado a luz a un mercado increíblemente dinámico, de rápido crecimiento para los inversores y especuladores. Intercambios como Okcoin, poloniex o shapeshift permite el comercio de cientos de criptocurrencies. Su volumen diario de comercio supera el de las principales bolsas europeas.

De hecho el mercado de criptomoneda “se comporta actualmente como una burbuja. El precio de mercado subirá cuanta más gente quiera comprarlo. Cada dos años vemos el colapso de los precios. Pero lo que es importante nunca cae a cero, ya que las criptomonedass dan valor real para una parte de los usuarios”, asegura el experto en malware de Kaspersky Lab.

¿Cuál será el impacto de Ethereum en el sector fintech?

Ethereum es la primera plataforma genérica de blockchain que permite a los usuarios crear y desplegar fácilmente sus aplicaciones descentralizadas e ilimitadas. Ha creado increíbles oportunidades en el espacio fintech. Su creación y adopción ha permitido una nueva forma de innovación que impulsará una mayor eficiencia en el sector.

Como ejemplo, se puede construir una aplicación para facilitar la remesa de dinero transfronteriza que cuesta una parte mínima de los costes actuales, lo que en última instancia beneficia a los remitentes con menor coste de transacción y al receptor con más cantidad recibida. Los micropagos también son algo exclusivamente permitido por Ethereum y Blockchains, en general, y permiten a la gente pagar pequeñas cantidades (por ejemplo, una fracción de un céntimo) con frecuencia. Por ejemplo, los usuarios pueden pagar un céntimo por cada hora que vean Netflix o algunos videos premium de YouTube.

Impulsa tu cuenta en twitter

Pruébalo gratis

ninja CM

TU MEJOR COMMUNITY MANAGER

Al mismo tiempo, la praxis de la Distribución Inicial de Monedas (OIC), en su mayoría facilitada por los contratos inteligentes de Ethereum, dio vida a proyectos de crowdfunding increíblemente exitosos, en los que a menudo una idea es suficiente para recaudar millones de dólares.

En este rico ecosistema de monedas y fichas experimenta una extrema volatilidad. Es común que una moneda gane un 10 por ciento al día para perder lo mismo al día siguiente. Aunque Bitcoin sigue siendo, de lejos, la criptomoneda más famosa, el resto tienen un bajo impacto especulativo, aunque los inversionistas y los usuarios deben mantener un ojo en varias criptomonedas.

En cualquier caso, las ventajas de estas monedas virtuales son, a ojos de Alexey Malanov, evidentes. "Puedes pagar a través de Internet rápidamente, de forma anónima, con tarifa baja. Gracias al uso de los smart-contratos también puedes programar las operaciones con estas monedas y todo el mundo va a confiar sin conocerte personalmente".

Mientras, las desventajas siguen los mismos principios. "No puedes retirar el pago, no puedes confiar en la regulación de terceros. El precio de la criptomonedas es muy volátil. Todavía es un inconveniente para los comerciantes offline el obtener pagos en criptomonedas en comparación frente al dinero tradicional. Es muy difícil para ellos, pero hay que tener en cuenta que no pagan una comisión enorme".

¿Cuál es el futuro de las criptomonedas?

El mercado de las criptomonedas es rápido y salvaje. Casi todos los días aparecen nuevas criptomonedas emergen, algunas mueren, los primeros adoptantes se hacen ricos y los inversores pierden dinero. Cada criptomoneda viene con una promesa, pero pocas sobreviven los primeros meses.

Además, las criptomonedas plantean nuevos riesgos para los usuarios. Por ejemplo, Kaspersky considera que un par de escenarios comunes son el ransomware que cifra los datos sensibles del usuario y pide rescate para el descifrado. "En 100% los casos de rescate se pagan en criptomoneda. Esto no es un riesgo que traiga la criptomoneda pero este problema ha crecido al tener esta forma de pago". Por otro lado, el usuario infectado "puede perder todas sus carteras de cripto-dinero y es imposible recuperarlo. En cuanto a los usuarios tradicionales de banca por Internet es mucho más seguro en este momento", explica Malanov, quien asegura que la minería maliciosa de criptomoneda es cada vez más popular. "Para los malhechores es una forma buena y estable de monetizar la infección: los ordenadores comienzan a minar a sus billeteras".

Además, alerta de las estadas financieras y proyectos falsos. "Si el usuario va a tomar parte en ICO (oferta inicial de monedas) y enviar su dinero, debe ser cauteloso y comprobar la autenticidad del proyecto dos veces".

Se calcula que en estos momentos hay más de 1.500 criptomonedas, aunque este número varía casi día a día. Sin duda, la de mayor capitalización es Bitcoin, pero existen muchas otras. La segunda en importancia es Ethereum, tanto por el dinero que mueve en el mercado como, sobre todo, por las entidades que las respaldan, dado que muchas entidades bancarias están dando soporte a esta moneda virtual.

it whitepapers

MONEDAS DIGITALES:
DIVISAS MÓVILES Y DIGITALIZADAS

Este documento de BBVA proporciona las claves para introducirnos en el mundo de las monedas digitales. ¿Qué es la tecnología blockchain? ¿En qué áreas puede desarrollarse esta revolucionaria tecnología? ¿Cuál es su futuro en los próximos cinco años? Moneda, medio de pago y seguridad son tres ejes clave que resumen uno de los grandes asuntos económicos de ahora y de siempre.

¿Te avisamos del próximo IT User?

De hecho, el Santander es el cofundador de una alianza para fomentar el uso de blockchain. Según la entidad bancaria, esta alianza sin ánimo de lucro en la que participan otras entidades internacionales se denomina Enterprise Ethereum Alliance (EEA). Su objetivo es desarrollar e impulsar el uso de los registros contables compartidos (blockchain) entre empresas con la tecnología de código abierto Ethereum, una plataforma descentralizada que permite crear contratos inteligentes entre pares.

Julio Faura, director de Investigación y Desarrollo en iniciativas de innovación de Santander, asegura que el "Santander y otras entidades han estudiado el potencial de registros contables compartidos y contratos inteligentes para su uso en aplicaciones empresariales. Ethereum ha resultado ser una de las mejores tecnologías. Ahora es el momento de colaborar para crear estándares que permitan con el tiempo una adopción generalizada en la industria".

Enterprise Ethereum Alliance tiene como objetivo investigar y desarrollar estándares y arquitecturas de referencia poniendo especial atención a aspectos como la privacidad, la confidencialidad, la adaptabilidad y la seguridad.

Santander ha estado trabajando durante meses con otros miembros fundadores para hacer realidad esta alianza. Entre los miembros fundadores, se encuentran Santander, Accenture, BlockApps, Bank of New York Mellon, CME Group, ConsenSys, IC3, Intel, JPMorgan, Microsoft y Nuco. También se han unido BBVA, BP, Credit Suisse, ING, Thomson Reuters, UBS, entre otros.

Como ya hemos dicho, el sector financiero siempre ha sido señalado como uno de los más afectados por las criptomonedas y la tecnolgoía blockchain ."Los reguladores financieros ven un montón de riesgos en las criptomonedas: no pueden controlar el flujo de caja y temen las actividades ilegales y otras actividades ilegales. También es fácil no pagar impuestos si tiene ingresos en criptomoneda", relata el experto en malware de Kaspersky Lab. Sin embargo, también considera que para algunos organismos financieros hay nuevas posibilidades. "Los bancos pueden hacer transferencias transfronterizas más rápido y más barato que antes. Otros utilizan la tecnología blockchain como una inspiración y están tratando de mover la comunicación bancaria a un nuevo nivel", explica.

Ethereum es la primera plataforma genérica de blockchain que permite a los usuarios crear y desplegar fácilmente sus aplicaciones descentralizadas e ilimitadas

"Y por supuesto hay un montón de especuladores que sólo ganan dinero debido a los rápidos cambios de precio", apostilla.

Y recuerda que alrededor de 70 de los principales bancos se han aliado en un consorcio R3 para desarrollar las tecnologías inspiradas en bblockchain para cambiar significativamente sus operaciones. "El tiempo dirá cómo esas tecnologías cambiarán el sector bancario".

Otros proyectos de dinero digital

Pero, además, el Banco Santander también se ha unido con otros bancos a un proyecto que tiene como fin investigar y promover el uso del dinero digital entre instituciones financieras y con los bancos centrales. Además de Santander, los bancos UBS, BNY Mellon y Deutsche Bank, el operador de mercado ICAP y la startup Clearmatics desarrollarán el proyecto "Utility Settlement Coin" (USC), un sistema que tiene por objetivo el facilitar pagos y liquidaciones de forma eficiente, rápida y segura.

Lo verdaderamente innovador de este proyecto, según sus responsables, está en el hecho de que utiliza la tecnología blockchain, sobre la que se basan criptomonedas como bitcoin, para representar y permitir la transaccionalidad de activos reales como euros o dóla-

res. Así, un USC sería una "moneda" que existe en un registro contable distribuido, es decir, en un blockchain (literalmente significa "cadena de bloques"). Este registro contable lo comparte un gran número de entidades financieras, razón por la que es tan seguro, y representa digitalmente dinero respaldado por un activo real. De esta manera, un USC es convertible en paridad con un depósito en su correspondiente divisa, es decir, que se puede intercambiar entre entidades, y gastar un USC es como si gastáramos el dinero equivalente en el mundo real.

Julio Faura señala, en este sentido, que las "conversaciones recientes de los bancos centrales y los reguladores sobre divisas digitales confirman el enorme potencial que tienen. El USC es un paso clave hacia el mercado financiero futuro con tecnologías de registro contable distribuido".

Los responsables del proyecto y las entidades están ya en contacto con los bancos centrales y los reguladores para asegurar que USC se lanza en una estructura que cumple todos los requisitos regulatorios, y es sólida y eficiente. El dinero digital será clave en el futuro de los mercados financieros y estará basado en blockchain, una tecnología que podría revolucionar la banca en los próximos años. USC tiene ya planes para hacer pruebas en el mercado.

Sin embargo, en opinión de Alexey Malanov, experto en malware de Kaspersky Lab, es muy poco probable que las criptomonedas se vuelvan lo suficientemente popular como para desbancar a las monedas reales. "La razón está en las tecnologías. Blockchain tiene como objetivo crear un sistema de pago sin confianza entre los usuarios, es por eso que todos los "nodos" tienen toda la historia de la transacción y validan todas las transacciones. Como resultado las criptomonedas actuales son muy lentas (alrededor de 10 transacciones por segundo para el mundo entero) y, lo que es más importante, no son escalables en absoluto. Esto significa que es necesario duplicar el hardware para cambiará el rendimiento del sistema. Ese principio es inasequible en el mundo moderno".

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Enlaces relacionados

- Bitcoin: el origen
- Blockchain: la última disrupción en el sistema financiero
- Monedas digitales: divisas móviles y digitalizadas
- Haciendo banca con Blockchain
- Observatorio 2017 de la Banca a nivel mundial
- Criptodivisas, Bitcoin y Seguridad
- Tecnología Blockchain, más allá del bitcoin
- ¿Qué es el blockchain?
- Blockchain: el avance de bitcoin y los pagos virtuales
- Bitcoin, el internet del dinero
- Evolución del mercado de las criptomonedas
- El futuro de las criptomonedas: Bitcoin vs. Ethereum

Desarrollo Directivo

Equipos de Alto Rendimiento con

psicobusiness

Socio Comercial de **ENSIZE** para España

Líder en Análisis DISC, 360º...

www.yesmanagement.es
Tlf. 94 652 61 29

yes.
¡hagámoslo realidad!

it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Octubre 2017 - nº 1

¿Por qué IoT no es seguro?

Hacia la autenticación biométrica

Las brechas de seguridad más sonadas de la historia

Data Protection Officer, el nuevo superhéroe

El actual contexto europeo de ciberseguridad

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

ITDS, una apuesta segura

¿Será ITDS una apuesta segura? Pues no lo sé, vosotros como lectores y el mercado lo dirá. Nosotros hemos puesto de nuestra parte todo lo posible, la experiencia de IT Digital Media Group con propuesta como IT User o IT Reseller sirven de referencia, y la confianza en una profesional como Rosalía Arroyo porque no creo que haya muchos periodistas en España que sepan de Seguridad más que ella, así que por nuestra parte la apuesta es segura. Veremos qué os parece a vosotros. Todos los detalles en este enlace.

Y yendo al grano. Nos ponemos en marcha hablando de IoT. ¿Es segura? Pues como decía el otro, ojo al dato. Demasiados dispositivos y conectados demasiado rápido. Los dispositivos que conforman ese Internet of Things del que llevamos hablando desde hace un tiempo, suman miles de millones e invaden el mercado cada día y de una manera acelerada. Llegar el primero tiene un coste, y ése es el que estamos a punto de pagar todos, sobre todo cuando si para llegar el primero se han obviado las medidas de seguridad más básicas.

Son, además, muy diferentes entre sí, y controlar miles de millones de dispositivos a los que a veces ni siquiera se puede cambiar la contraseña por defecto, es un reto. También es un reto proteger el IoT con un modelo de seguridad que apenas ha empezado a contemplar la movilidad y el BYOD. ¿Una referencia? Nada como echarle un ojo al nacimiento de Mirai hace unos meses, una botnet utilizada para lanzar ataques de denegación de servicios distribuido (DDoS), como el que dejó sin conexión a medio internet tras el ataque a Dyn. El hecho de que empiecen a diferenciarse entre botnets y thingbots no hace sino demostrar el interés que los ciberdelincuentes tienen en la capacidad que ofrecen de miles de millones de dispositivos conectados.

Pero no todo está perdido. Echa un ojo a nuestro tema de portada y mantengamos la esperanza.

IT Digital Media Group

Juan Ramón Melara
juanramon.melara@itdmgroup.es

Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdmgroup.es

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

Colaboradores
Hilda Gómez, Arantxa Herranz, Reyes Alonso

Diseño revistas digitales
Contracorriente

Diseño proyectos especiales
Eva Herrero

Producción audiovisual
Antonio Herrero, Ismael González

Fotografía
Ania Lewandowska

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

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

En Portada

Por qué IoT no es seguro

Actualidad

Data Protection Officer, el nuevo superhéroe

Las brechas de seguridad más sonadas de la historia

Hacia la Autenticación Biométrica

Entrevista a Sanjay Beri, CEO y fundador Netskope

No solo IT

El actual contexto europeo de ciberseguridad

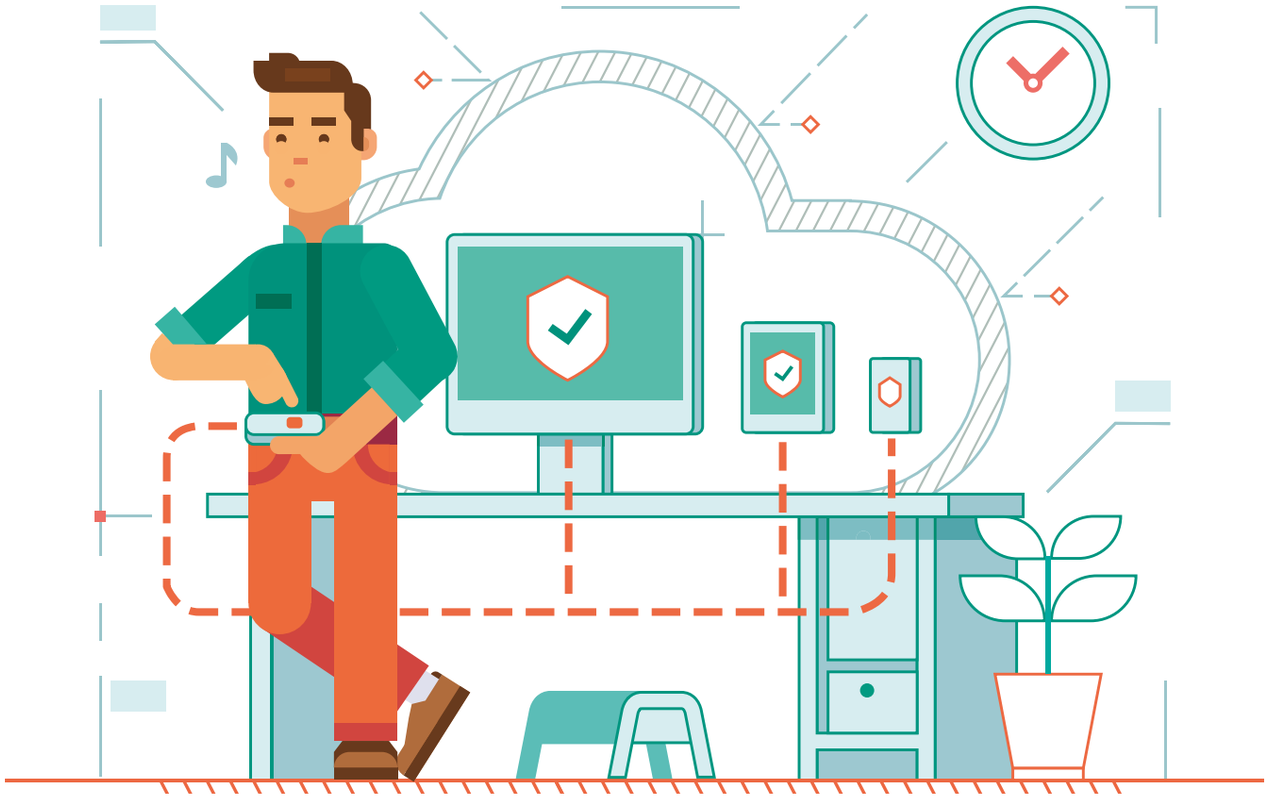
El estado de la ciberseguridad en España

Seguridad Informática y previsiones de futuro para el sector financiero

Índice de anunciantes

Kaspersky Lab	Micro Focus	Check Point
DXC	Trend Micro	Eset
Netskope	IT Whitepapers	IT Webinars

¿Te avisamos del próximo IT Digital Security?



Deje que fluya su creatividad. Y aleje las ciberamenazas

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

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

cloud.kaspersky.com

© 2017 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.

Data Protection Officer, el nuevo superhéroe

Entre las novedades que propone la GDPR, de obligado cumplimiento a partir del próximo 25 de mayo de 2018, está la figura de un Data Protection Officer (DPO), la figura responsable de la privacidad que, con una función preventiva y proactiva, se encarga de supervisar, coordinar y trasmitir la política de protección de datos tanto dentro como fuera de la empresa. Además, se le considera como el punto de encuentro entre el responsable del fichero y/o tratamiento, el afectado y la autoridad de control, que en España será la AEPD (Agencia Española de Protección de Datos).

El 25 de mayo de 2018 el Reglamento General de Protección de Datos (GDPR), la normativa sobre protección de datos firmada hace año y medio, será de obligado cumplimiento. Pocas dudas hay sobre el impacto que tendrá en las empresas, en todas las que, independientemente de su tamaño, gestionen datos personales, de empleados o de terceros. Su objetivo es el de superar la fragmentación normativa existente y modernizar los principios de privacidad en la Unión Europea. Pero quizá la mayor novedad de la GDPR es que ha elevado la privacidad y la protección del dato a la máxima potencia. Si el big Data convirtió al dato en el petróleo del nuevo siglo, la GDPR hace que "por primera vez, la responsabilidad en cuanto al dato sí que se incorpora como una variable de decisión en cómo voy a trabajar", decía Roland Ruiz, consultor de software de Information Builder, durante la tercera edición del Chief Data Officer Day (CDO 2017) celebrado en Madrid y en el que, por primera vez se ha desarrollado un summit dedicado al DPO (Data Protection Officer) y ciberseguridad.

Compartir en RRSS

La GDPR impacta sobre las empresas en distintos niveles: técnico, legal y organizativo. Sus elementos más relevantes son el derecho de los ciudadanos a la portabilidad de sus datos; la necesidad de obtener un consentimiento activo a la hora de recabar los datos; el deber de las empresas a notificar a la Agencia de Protección de Datos y a los clientes potencialmente afectados si han sufrido una intrusión; y el nuevo cargo de DPO, o Data Protection Officer, el responsable de supervisar la estrategia de protección de datos y su implementación para cumplir con la normativa.

Durante su participación en una ponencia, David Moreno, CISO de Grupo Cortefiel, aseguraba que "los retos del DPO van más allá de lo técnico, hacia lo legal. Tienen que enfrentarse a la estructura y mentalidad de la organización, a la regulación, a los departamentos de marketing –que tiene que saber cómo tratar cierta información. Es un superhéroe". Y añadía el directivo que "nadie sabe hacer eso porque hasta ayer esa figura no existía", y requiere un proceso de aprendizaje continuo.

GDPR – THE DATA PROTECTION OFFICER **CLICAR PARA VER EL VÍDEO**

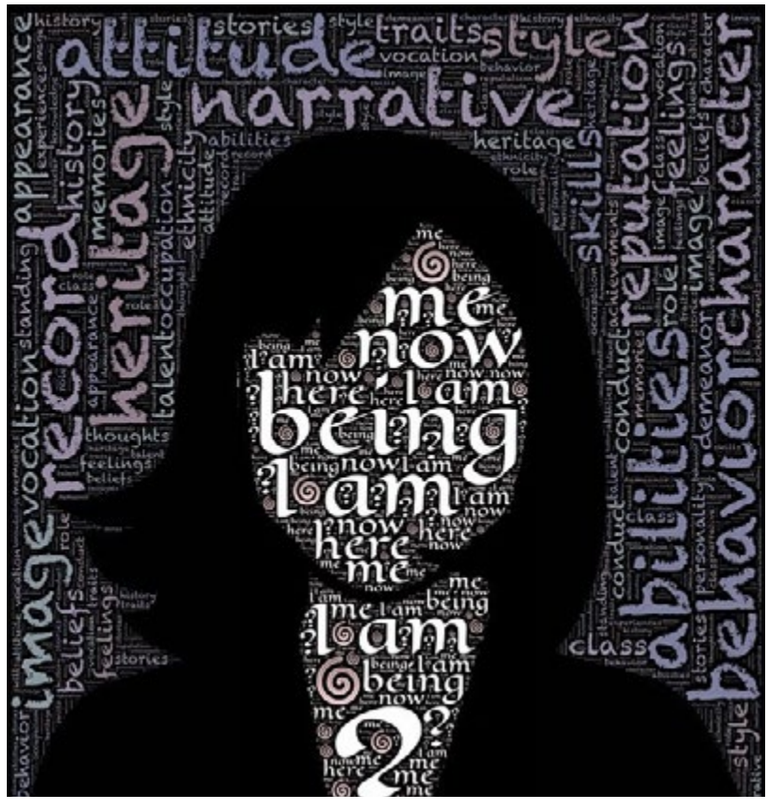
Se Busca

Responsable de protección de datos, DPO, para cumplir con la normativa GDPR, que será de obligado cumplimiento el próximo 25 de mayo de 2018, y cubrir 40.000 puestos vacantes en Europa.

Su papel será el supervisar, coordinar y transmitir la política de protección de datos tanto en el interior de la institución como desde dentro hacia el exterior.

Se requiere:

- Conocimientos legales y de TI
- Gran capacidad de negociación
- Ser pragmática y realista
- Capacidad de visión holística del negocio
- Capacidad de hacer de puente entre las diferentes áreas del negocio y las áreas técnicas



Compañera de escenario, Montserrat Valentí Vall, responsable de Asesoría Jurídica y Cumplimiento Normativo de Seguros Catalana Occidente, aseguraba que el DPO es "una figura que debe tener mucha capacidad de negociación, de poder convertir en ventaja lo que estaba en contra. Una persona pragmática y realista capaz de responder a cómo llevar a cabo una portabilidad o cómo establecer la base legal asociada a ese tratamiento". Elena Mora González, Subdirectora Marco Regulatorio de Seguridad de Mapfre, por su parte, no quiso olvidarse del papel del Data Protection Officer en cuanto a concienciar y divulgar, "porque cuando hablamos de un proyecto de adecuación hablamos de un proyecto de toda la organización. La GDPR es una obligación de toda la compañía", y advertía que el día a día de un DPO "puede ser muy diferente de una organización a otra, porque una puede ser muy tecnológica y otra más legal. Un centro médico difiere de un centro asegurador".

Los expertos hablan

Sobre el perfil del DPO y el impacto que la GDPR va a tener en las empresas hablamos con algunos de los asistentes al Chief Data Officer Day.

El DPO es una figura que cuesta encontrar y en Europa hay 40.000 puestos vacantes sin cubrir

María José Pérez Guillén, Senior DSG Consultant de Informatica, dice que la GDPR impacta de una forma muy global a todas las compañías y por eso se hace necesaria la figura de un DPO que centralice todos los cambios que supone esta regulación. ¿Y cuál sería el perfil de un DPO? “Debe ser una persona que conozca muy bien la legislación, por lo tanto, tendrá que venir del departamento de legal, y a su vez tendrá que ser tecnólogo porque tendrá que ser capaz de traducir todos los cambios que trae la legislación al departamento de TI. Por tanto, es un perfil bastante complejo y bastante completo”, dice Pérez Guillén.

Dice también la ejecutiva que la del DPO es una figura que cuesta encontrar y recuerda que en Europa hay 40.000 puestos vacantes de DPO sin cubrir.

Pablo Boixeda, Sales Ingineer de Cloudera, dice que el primer impacto de la GDPR en las empresas es que “van a tener que proteger la información y van a tener que segmentar esa protección”. El control y visión de los datos será total, porque hay que tener claro cuándo han sido manipulados los datos y por quién; “en definitiva, va a tener que dar una protección de 360 grados a esos datos desde el punto de vista de acceso, que esos accesos puedan ser auditados, aplicar cifrado a esos datos para que no puedan ser extraídos y se puedan explotar desde fuera”.

Respecto al perfil que debe tener un DPO, la visión personal de Boixeda es “una persona que haga de puente entre las áreas de negocio y las áreas técnicas. Ha de entender cómo los datos han de servir al negocio, cómo pueden genera más volumen de negocio, cómo pueden ayudar al departamento de operaciones, cómo puede ayudar a recortar costes, cómo puede ayudar las tecnologías orientadas al dato a sistemas de compliance y de seguridad. Y después tiene que tener una parte más orientada a la tecnología”, ya que tiene que integrarse y tiene que conversar con los departamentos de IT tradicionales.

Ventaja de la GDPR

“Que por primera vez un porcentaje de tu ingreso pueda ser una multa anual está haciendo que todo el mundo, de verdad, vaya a tener una responsabilidad sobre la gobernanza del dato”, asegura Roland Ruiz, de Information Builder, para quién la GDPR ha hecho que “la responsabilidad sobre el dato haya pasado a ser prioritario”.

Entre las tareas del DPO, el supervisar el cumplimiento de lo dispuesto en el Reglamento, así como en otras disposiciones de protección de datos de la Unión o de los estados miembros

Ante la insinuación de que el DPO proceda del departamento legal, Ruiz asegura “si es un perfil puramente legal puede perder contacto con la realidad del negocio. Yo pondría más a una persona que tuviese visión IT y también visión de negocio. Que realmente venga de operaciones o venga de IT es una decisión de la empresa, pero que tenga una visión holística del negocio. Creo que la parte legal se la pueden aconsejar y por tanto no creo que haga falta que sea un experto en esa área”.

Julia Urío Rodríguez, responsable del portfolio de soluciones y gobierno de IBM, explica que la regulación de protección de datos que será de obligado cumplimiento el próximo 25 de mayo tiene varias dimensiones: una más organizativa, otra más de procedimientos y procesos, otra de cómo impacta a las personas de la organización, una dimensión más cercana a los datos, a cómo impacta en la información que esas empresas manejan y usan, y la última es una dimensión relacionada con los niveles de seguridad con respecto al tratamiento de esa información. “A nivel organizativo el impacto va a requerir que se cree una figura de DPO en aquellas organizaciones importantes con volumen de datos a tratar importantes”, dice la directiva.

Sobre ese DPO dice Urío que “tradicionalmente estaba el security data officer que dependía mucho del área de IT pro el hecho de que era un componente de seguridad del dato, pero el DPO está adquiriendo más un componente del negocio, muy cercano a sus departamentos legales, y sus departamentos de gestión de riesgos. Y por tanto sale del área de IT; esa figura del DPO está próxima al negocio, próxima a legal y con ciertos conocimientos tecnológicos”.

Para David Cristóbal Campanario, Pre-Sales Consultant de Talend, la GDPT trae algunos cambios importantes. El primero con respecto a la calidad, puesto que la información debe ser veraz, debe ser cierta y debe ser actualizada; el segundo está relacionado con la trazabilidad del dato, un aspecto al que hasta ahora no se le había prestado mucha atención y que ahora es de vital importancia por lo que implica la portabilidad de la información. “Más allá del borrado de la información, que es algo que se puede considerar relativamente sencillo, el tema de portabilidad de la información es algo que puede convertirse en un quebradero de cabeza para la mayor parte de las empresas”, asegura David Cristóbal.

Sobre el perfil de un Data Protection Officer, dice el ejecutiv de Talend que “en general debe ser eminentemente IT pero conocimientos legales y de las implicaciones que las regulaciones tienen”. Dice también David Cristóbal que el DPO en un perfil “muy difícil de encontrar”.

Aspectos de la regulación como el derecho al olvido o la portabilidad del dato van a tener un gran impacto en las empresas, dice Juan Julián Moreno Piedra, IM&G Pre-Sales Manager de Micro Focus. Añade el ejecutivo que “prácticamente todas las empresas grandes han nombrado un DPO y están empezando a hacer un estudio de los datos, un estudio que tiene que comenzar por hacer un inventario de tus datos, entender qué usuarios usan los datos de tu empresa y para qué los usan, y a partir de aquí establecer la estrategia”.

Respecto al perfil que debería tener un DPO, el ejecutivo de Micro Focus lo tiene claro: “Una persona completamente centrada en los datos, independiente de la parte de TI de las empresas. Un perfil absolutamente cross, presente en todos los departamentos”.

Figura legal o figura de TI, lo que parece cierto es que el DPO se está formando ahora, que es una de las piedras angulares de todo este proceso de adaptación. Que hacen falta 40.000 profesionales y que no es consistente esperar al 24 de mayo para nombra uno, porque no tendrá conocimiento de todo el proceso.

Enlaces de interés...

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

¿Te avisamos del próximo IT Digital Security?

MICRO FOCUS®

Discover

the New

Compartir en RRSS

Hacia la autenticación **biométrica**

La biometría, la ciencia de analizar características físicas o de conducta que son específicas a cada individuo con el objetivo de ser capaz de autenticar su identidad, se ha vuelto un elemento cada vez más importante en un mundo dominado por los servicios cloud. Para muchos la identidad se ha convertido en el nuevo firewall.

El mundo se ha vuelto digital y cada persona utiliza, o debería utilizar, 27 contraseñas para gestionar el acceso a todos sus servicios, desde el correo electrónico, banca online, redes sociales y todo tipo de recursos.

El momento parece el adecuado. La capacidad que aportan los smartphones junto con los avances tecnológicos, hacen que la biometría sea fácil de utilizar. Al mismo tiempo las grandes empresas, los bancos, compañías se seguros y de salud se han dado cuenta de que necesitan una mejor seguridad. El interés en la adopción de biometría para una autenticación segura está creando una industria con un tamaño de mercado que pasará de los 10.740 millones de dólares en 2015 a más de 32.000 millones para 2022. Además, según en el informe Global State of Information Security Survey 2017 de PwC, el 40% de los encuestados citaron la biometría como una prioridad para proteger a las organizaciones.

¿Te avisamos del próximo IT Digital Security?

¿Y están las empresas españolas preparadas para adoptar soluciones de autenticación biométrica? Para Cristina de Sequera, directora de la unidad de negocio de Transformación Digital de Grupo CMC, está claro que sí, y si no lo están, “han de prepararse rápidamente porque los clientes están demandando soluciones más ágiles, cómodas y seguras”.

De la misma opinión es Jordi Quesada, Key Account Manager Cyber Security de G+D Mobile Security, quien asegura que “dar el salto al acceso lógico es una transición natural si lo que se persigue es mejorar la seguridad en todo tipo de accesos, ya sea a lugares como a información, sistemas, etc.”

Además, y aunque para Héctor Sánchez, director de tecnología de Microsoft Ibérica, “cada vez son más las empresas que están adoptando este tipo de tecnología para su seguridad”, para Rodrigo Chávez Rivas, responsable de IT Security Services & Solutions en Unisys, “son muchas las variables que determinan si una empresa está preparada para adoptar soluciones de autenticación basadas en biometría. Entre las más relevantes destacaría dos: la experiencia de usuario y la madurez de la tecnología”.

Las infraestructuras y recursos TI actuales deben permitir el acceso simultáneo de varios individuos, dispositivos y aplicaciones, y deben hacerlo de forma segura, con garantías. La información y recursos de una red corporativa son cruciales para la continuidad de negocio y una brecha de seguridad no sólo impide esa continuidad, sino que impacta en la reputación de la marca y su futuro crecimiento.

Hay que estudiar no sólo cuándo sino para qué debe una empresa plantearse adoptar soluciones

El paraíso de los hackers

Un buen reto es un regalo para los investigadores. Cuando parece claro que una huella dactilar es más segura que una contraseña, ¿por qué no demostrar lo contrario? Y si se hace a lo grande mejor.

Eso es lo que pensó Starbug, nombre en clave de Jan Krisller, especialista en biometría que en diciembre de 2014 demostró ser capaz de clonar la huella dactilar de la Ministra de Defensa de Alemania, Ursula von der Leyen, utilizando únicamente fotografías en alta definición que había tomado durante una rueda de prensa celebrada en octubre.

La investigación se presentó en el evento anual Chaos Communication Congress, donde Starbur explicó que trató las fotos con el software comercial de huellas digitales de Verifinger con el fin de trazar los contornos de la huella digital de la ministra.

El experto invirtió la imagen del dedo de Von der Leyen y lo imprimió en una hoja transparente con saturación de tóner.

A continuación, vertió una capa de pegamento de madera sobre la parte superior, que, al levantarse, capturó una impresión que Krisller fue capaz de utilizar para desbloquear un iPhone.

Starbug ya es conocido por sus investigaciones en seguridad biométrica. En 2013 fue capaz de falsificar los sensores TouchID de Apple 24 horas después del lanzamiento del iPhone 5S. Usando una mancha en la pantalla de un iPhone imprimió un dedo falso con pegamento de madera y grafeno pulverizable, que desbloqueó con éxito un teléfono registrado en el pulgar de otra persona. En este caso tuvo que tener acceso al terminal de donde robó la huella.

Esta historia, que no deja de ser algo más que curiosa, plantea una cuestión: Cuando una contraseña es robada se puede cambiar, ¿qué ocurre cuando una huella dactilar es copiada?

Windows Hello

Los fabricantes de ordenadores primero, y los de terminales móviles después, han normalizado el uso de la biometría para verificar la identidad del usuario. Los lectores de huellas dactilares empezaron a aparecer las PDA u en ordenadores portátiles profesionales hace bastantes años. Ahora son comunes en smartphones, y no sólo en los de gama alta.

Y en este proceso de normalización de uso de una tecnología también participa el software, en este caso Windows 10, la última versión del sistema operativo de Microsoft que llegó al mercado con Windows Hello, "una forma más personal de iniciar sesión en tus dispositivos Windows 10 con solo un vistazo o un toque", dice la compañía.

Windows Hello usa una combinación de cámaras de infrarrojos (IR) y software especial para proteger contra la suplantación de identidad.

Windows almacena los datos biométricos que se usan para implementar Windows Hello de forma segura sólo en el dispositivo local. Los datos biométricos no pasan de un dispositivo a otro ni se envían nunca a servidores o dispositivos externos. Dado que Windows Hello sólo almacena los datos de identificación biométrica en el dispositivo, no hay ningún punto de colección único que un atacante pueda poner en riesgo para robar los datos biométricos.

De cara a las empresas, las credenciales de Windows Hello se pueden enlazar con el dispositivo y el token. Además, el proveedor de identidad (por ejemplo, la cuenta Active Directory, Azure AD o Microsoft) valida la identidad del usuario y asigna la clave pública de Windows Hello a la cuenta del usuario durante el paso de registro. En función de la directiva, las claves se pueden generar en el hardware o en el software, aunque el gesto de Windows Hello no vale en otros dispositivos, ni se comparte con el servidor, sino que se almacena localmente en un dispositivo concreto.

Añadir que las cuentas personales (cuenta Microsoft) y las corporativas (Active Directory o Azure AD) usan un solo contenedor para las claves. Todas las claves están separadas por dominios de proveedores de identidad para garantizar la privacidad del usuario.

de autenticación biométrica, dice Cristina de Sequera, asegurando al mismo tiempo que "se están desarrollado muchas iniciativas de transformación digital que integran tecnologías de autenticación biométrica en el ámbito de relación con el cliente para mejorar la experiencia de usuario en el proceso de identificación.

Para Héctor Sánchez, director de tecnología de Microsoft Ibérica, "en un mundo en el que las amenazas son cada vez más constantes, las empress

2017 USER RISK REPORT

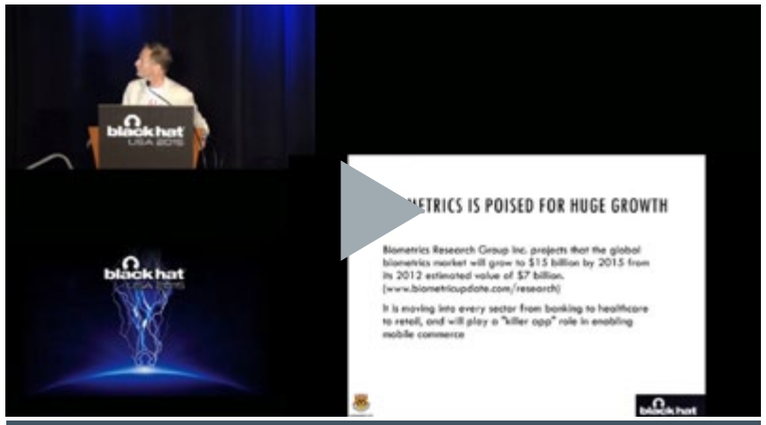
Una encuesta elaborada por Commvault entre grandes responsables de empresas recoge que el 81% se sienten extremadamente preocupados por perderse los avances del cloud. Es lo que se llama el Cloud FOMO (Fear of Missing Out).

La encuesta concluye que el Cloud FOMO está impulsando a los líderes empresariales a avanzar a toda velocidad en las estrategias de nube, con el 93% de los encuestados afirmando que están moviendo al menos algunos de sus procesos a la nube. Además, el 56% declaró que se han movido o tienen la intención de trasladar no sólo algunos, sino todos sus procesos a la nube.

deben ser conscientes de que deben adoptar cuanto antes medidas de seguridad que les permitan proteger su información y la de sus empleados".

"Cualquier empresa que tenga aplicaciones donde se requiera una autenticación basada en usuario y password, puede plantearse el adoptar esta tecnología", dice Jordi Quesada, añadiendo que la seguridad biométrica no debe adaptarse por seguridad que se añade, "también por una mejora de la experiencia de usuario, facilidad de uso y gestión".

Rodrigo Chávez Rivas añade el tema del coste en la ecuación al asegura que una empresa debe plantearse adoptar este tipo de tecnologías "cuando tenga casos de uso en los que el coste de su adopción se justifique, por ejemplo, cuando se necesite tecnologías de autenticación que no sólo proporcionen seguridad confiable, sino que sean además extremadamente difíciles de falsificar". Y es que hay que tener en cuenta que, si bien la relación entre los beneficios y el precio asociados a las soluciones de autenticación biométrica han mejorado significativamente durante la última década, no significa que



CÓMO EVITAR LOS RIESGOS OCULTOS DE LOS IDENTIFICADORES BIOMÉTRICOS **CLICAR PARA VER EL VÍDEO**

se deban adoptar para todos los casos, añade.

"Tradicionalmente la inclusión de soluciones de autenticación biométrica incrementaba significativamente los costes frente a las alternativas convencionales. Sin embargo, el uso masivo de dispositivos móviles por parte de los consumidores y la disponibilidad cada vez mayor de aplicaciones de autenticación biométrica han abierto una puerta a la adopción masiva de la biometría como mecanismo de autenticación para múltiples casos de uso. Por ejemplo, los sistemas de pago con móvil que usan autenticación biométrica hacen que la acción de pago sea cómoda y segura", dice también el directivo de Unisys.

"Si las empresas no están preparadas para la autenticación biométrica han de prepararse rápidamente porque los clientes están demandando soluciones más ágiles, cómodas y seguras"

Cristina de Sequera, Grupo CMC

Elementos de autenticación esenciales

Hay tres factores de autenticación, el primero basado en lo que eres (biometría), el segundo basado

THE RANSOMWARE X.

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

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

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

#WhatsYourX

TREND MICRO™

trendmicro.es/xgen

Apple FaceID

A mediados de septiembre se anunciaba el lanzamiento del iPhone X. Entre sus características más destacadas el haber sustituido el TouchID por el FaceID, o lo que es lo mismo, haber sustituido la huella dactilar por el reconocimiento facial como sistema de verificación, que se utilizará no sólo para desbloquear el terminal, sino para firmar en las aplicaciones y autorizar los pagos realizados a través de Apple Pay o iTunes.

FaceIS funciona con la cámara frontal del terminal y un sistema de infrarrojos conocido como TrueDepth que proyecta una red de 30.000 puntos sobre el rostro del usuario para crear una estructura en tres dimensiones.

Esta capacidad no sólo refuerza la seguridad, sino que ayudará al FaceID a procesar todas las imágenes y reconocer el rostro del usuario independientemente del peinado, gafas, vello facial, iluminación y otros posibles cambios.

en lo que sabes (contraseña) y el tercero basado en lo que tienes (un dispositivo móvil por ejemplo), y tres elementos esenciales para asegurar el acceso a la información: Single Sign-On, gestión de contraseñas y control de accesos.

El llamado Single Sing-On, o acceso único, es un servicio que permite al usuario utilizar un conjunto de credenciales (por ejemplo, ID y contraseña) para acceder a varias aplicaciones. Este tipo de acceso mejora la experiencia del usuario porque sólo debe iniciar sesión una vez al tiempo que ayuda con el registro y la actividad del usuario en el backend.

Es una realidad que el número de servicios online a los que accedemos ponen a prueba autenticación de la identidad. Si a este inicio de sesión se le suma la biometría, el tema se simplifica. Por ejemplo, las huellas dactilares, que son bastante fáciles de integrar con la mayoría de los servicios, pueden utilizarse para el inicio de sesión único para un conjunto de aplicaciones. Se une una buena experiencia de usuarios con una mayor seguridad de la cuenta.

Los gestores de contraseñas nacieron para garantizar que los usuarios escogieran contraseñas complejas sin que tuvieran la necesidad de recordarlas. Se trata de programas que son capaces de generar, almacenar y recuperar esas contraseñas para el usuario. Actualmente son extremadamente accesibles –a veces incluso presentes en productos de seguridad de consumo, incluso como un servicio online. Las contraseñas se almacenan de manera cifrada para mantenerlas a salvo de usuarios y aplicaciones maliciosas. En ocasiones estos programas son capaces de rellenar los campos de login/password por el usuario, lo que mejora enormemente la experiencia de los usuarios.

El control de accesos tampoco es nuevo, pero ha ganado protagonismo en los últimos años. Conocida por las siglas IAM (Identity and access control), esta tecnología permite la identificación y autenticación de usuarios. También aquí la biometría puede jugar un papel fundamental a la hora de garantizar

"En materia de seguridad todo suma, y los métodos de seguridad biométrica añaden neuvas formas de asegurar nuestros equipos y la información que almacenan"

Héctor Sánchez, Microsoft Ibérica

"Actualmente pueden encontrarse soluciones de autenticación biométrica de buena calidad a precios razonables y con costes predecibles de instalación, operación y mantenimiento"

Rodrigo Chávez Rivas, Unisys

de una manera más fácil que sólo la persona correcta accede a la información correcta en el momento correcto y por las razones correctas, que es la idea que está detrás de las soluciones de gestión de identidades y accesos

Una huella dactilar no sólo elimina el riesgo asociado a un pin y una contraseña, sino que la persona que accede a los recursos es la que tiene que acceder.

Critina de Sequera va un paso más allá. Explica que la propuesta de Grupo CMC, llamada 02 Digital, se basa "por un lado, en adaptar el tipo de biometría a utilizar al proceso concreto en el que se desea utilizar y, por otro, en utilizar la biometría dentro de una combinación de factores, de forma que conseguimos elevar exponencialmente la seguridad de la autenticación. No hay biometrías buenas o malas, hay procesos que utilizan esas biometrías de forma adecuada y procesos mal diseñados".

La oferta de G+D se centra en dispositivos móviles y permite combinar diferentes opciones biométricas en función del riesgo o nivel de seguridad que queramos aplicar. Además, la solución está preparada para ir incorporando más tecnologías biométricas a medida que sean soportadas por los dispositivos móviles.

Unisys cuenta con una plataforma abierta y orientada a servicios, Stealth Identity, que permite una gestión de la identidad completa a través de la biometría y que integra todos los módulos del ciclo de vida de la identidad.

De la huella dactilar al mapa de las venas

Cuando se trata de aplicar la biometría a la autenticación se tienen en cuenta no sólo aspectos físicos que son inherentes a cada ser humano, sino los patrones. O lo que es lo mismo tecnologías biométricas fisiológicas y tecnologías biométricas de comportamiento. "Entre las fisiológicas están las que permiten el reconocimiento de huella dactilar, reconocimiento facial, de iris, de retina, de la mano, entre otras. Entre las de comportamiento están las que permiten el reconocimiento de firma, de voz, de escritura de teclado, entre otras", dice Rodrigo Chavez Rivas. Por ejemplo, en el caso de la dinámica de firmas, que no sólo tiene en cuenta la imagen de esa firma sino cómo se ha producido teniendo en cuenta diferencias en la presión y velocidad de escritura en varios puntos de la firma.

Eso mismo ocurre con los patrones de tecleo, donde no sólo se reconoce la contraseña sino los

intervalos entre cada pulsación de la tecla y la velocidad total a la que se escribe.

Sin duda una de las biometrías más conocidas es la de la huella dactilar, presente ya en muchos dispositivos de consumo como móviles o portátiles. La huella dactilar recoge dos tercios de todo el mercado de autenticación biométrica. Entre sus grandes ventajas no sólo el ser únicas, sino que el hardware de lector de huella requiere muy poco espacio físico y los datos que genera son pocos.

Pero para Chavez Rivas, es necesario explorar y desarrollar otras opciones por varias razones: “El uso mayoritario de la tecnología de huella dactilar lleva asociado un mayor número de amenazas comparado con otras tecnologías biométricas; y es necesario ofrecer alternativas a los casos de excepción. Por ejemplo, usuarios que no disponen de una huella dactilar reconocible o cuya huella se va deteriorando significativamente con el tiempo”.

Además, dice Jordi Quesada, “se puede dar el caso de que un usuario tenga una lesión en el dedo. También que intentemos usar el sistema justo después de salir de una hora de piscina. En esos casos, la biometría a través de la huella no va a funcionar. Además, por experiencia de usuario podemos querer ofrecer otras opciones o alternativas”.

Por eso, aunque el uso de la huella dactilar se haya extendido, hay que seguir avanzando. El reconocimiento facial es otro tipo de biometría que se lleva utilizando desde hace algún tiempo; se centra en diferentes rasgos, incluyendo los contornos superiores de los ojos, las áreas que hay alrededor de los pómulos, los lados de la boca o la ubicación de la nariz y boca.

El escáner de retina o de iris, el mapa de las venas de la mano, o los latidos del corazón como elementos de autenticación biométrica están siendo objeto de gran estudio. Los investigadores de seguridad consideran el cuerpo humano como la parte del cuerpo más fiable para la autenticación biométrica porque la retina y el iris no sufren cambios durante toda la vida de las personas.

"Dar el salto al acceso lógico es una transición natural si lo que se persigue es mejorar la seguridad en todo tipo de accesos, ya sea a lugares como a información o sistemas"

Jordi Quesada, G+D

Un escáner de retina iluminará los complejos vasos sanguíneos del ojo de una persona usando luz infrarroja, haciéndolos más visibles que el tejido circundante. En el caso del escáner de iris, se basa en fotos o vídeos de alta calidad de uno o ambos iris de una persona, que también son únicos para el individuo. Sin embargo, los escáneres de iris han demostrado ser fáciles de engañar simplemente usando una fotografía de alta calidad de los ojos o la cara del sujeto.

El reconocimiento de voz para asuntos de seguridad busca identifica quién habla y no lo que se dice. Para identificar al usuario un software especializado descompone las palabras en paquetes de frecuencias llamadas formantes. Estos paquetes de formantes también incluyen el tono de un usuario, y juntos forman su impresión de voz.

La disposición de las venas es única para cada persona, ni siquiera compartida en gemelos, lo que ha hecho que algunas empresas opten por este tipo de soluciones de reconocimiento y autenticación. Las venas tienen una ventaja añadida ya que son increíblemente difíciles de copiar y robar porque son visibles bajo circunstancias estrictamente controladas. Un escáner de geometría de vena iluminará las venas con luz infrarroja cercana, lo que hará que sus venas sean visibles en la imagen.

Respecto a la tecnología de autenticación que se vende más, dice Cristina de Sequera que "actualmente está implantándose mucho en el mercado la biometría facial y probablemente en los próximos meses veremos también bastante uso de biometría de voz. Otras biometrías, como la conductual o la de gestual, todavía tendrán que afinarse para que uso se haga más más extensivo".

Para Rodrigo Chavez Rivas, "la tecnología de autenticación más vendida está basada en un doble factor de autenticación que combina la autenticación de usuario/contraseña con la autenticación basada en OTP (One Time Password)".

Enlaces de interés...

- La revolución de la Autenticación
- Escogiendo la mejor Autenticación biométrica
- Autenticación biométrica en la banca móvil
- Mercado de aplicaciones biométricas móviles

Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

› of the hype

LOS HECHOS:

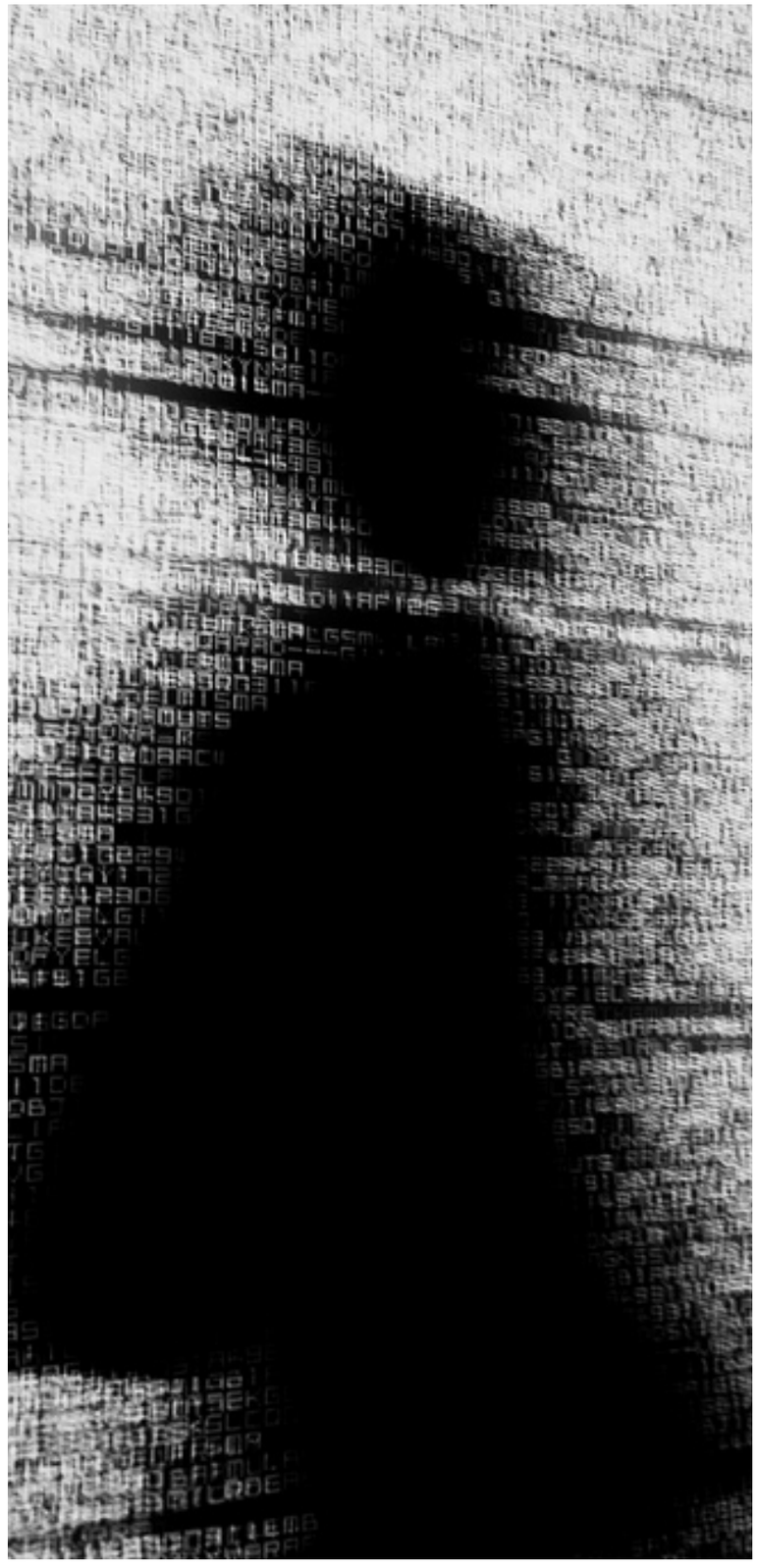
CHECK POINT THREAT PREVENTION OFRECE LA TASA DE DETECCIÓN DE MALWARE. MÁS ALTA DE LA INDUSTRIA

LGUNOS FABRICANTES EXPONEN A SUS CLIENTES AL MALWARE DURANTE 5 MINUTOS. CHECK POINT NO

CHECK POINT PROTEGE A SUS CLIENTES CONTRA EL MALWARE EN ARCHIVOS. OTROS NO

No hay segundos premios en ciberseguridad.
Contacta con nosotros. 91 799 27 14 — info_iberia@checkpoint.com

Las brechas de seguridad **más sonadas** de la historia



Se calcula que en la última década se han producido unas cinco mil brechas de seguridad. Las hay grandes y pequeñas, las más conocidas y las que han pasado desapercibidas, las que han llevado a la desaparición de la empresa que las sufrió y la que acabó, voluntaria o involuntariamente, con el que la lideraba.

Las brechas de seguridad son habituales. No en vano se habla de tres tipos de empresas: las que han sido atacadas y lo saben, las que han sido atacadas y no lo saben y las que van a ser atacadas. Es una chanza conocida en el sector, pero muy cierta. La movilidad, el cloud, el as-a-service no han hecho más que complicar la seguridad, ofrecer más opciones y puntos de entrada a los hacker. Pero las brechas se han producido desde hace más de una década, aunque las primeras fueran más el resultado de un error que de un ciberataque.

Aunque las brechas de seguridad se llevan produciendo desde antes de 2005, empezaron a tener

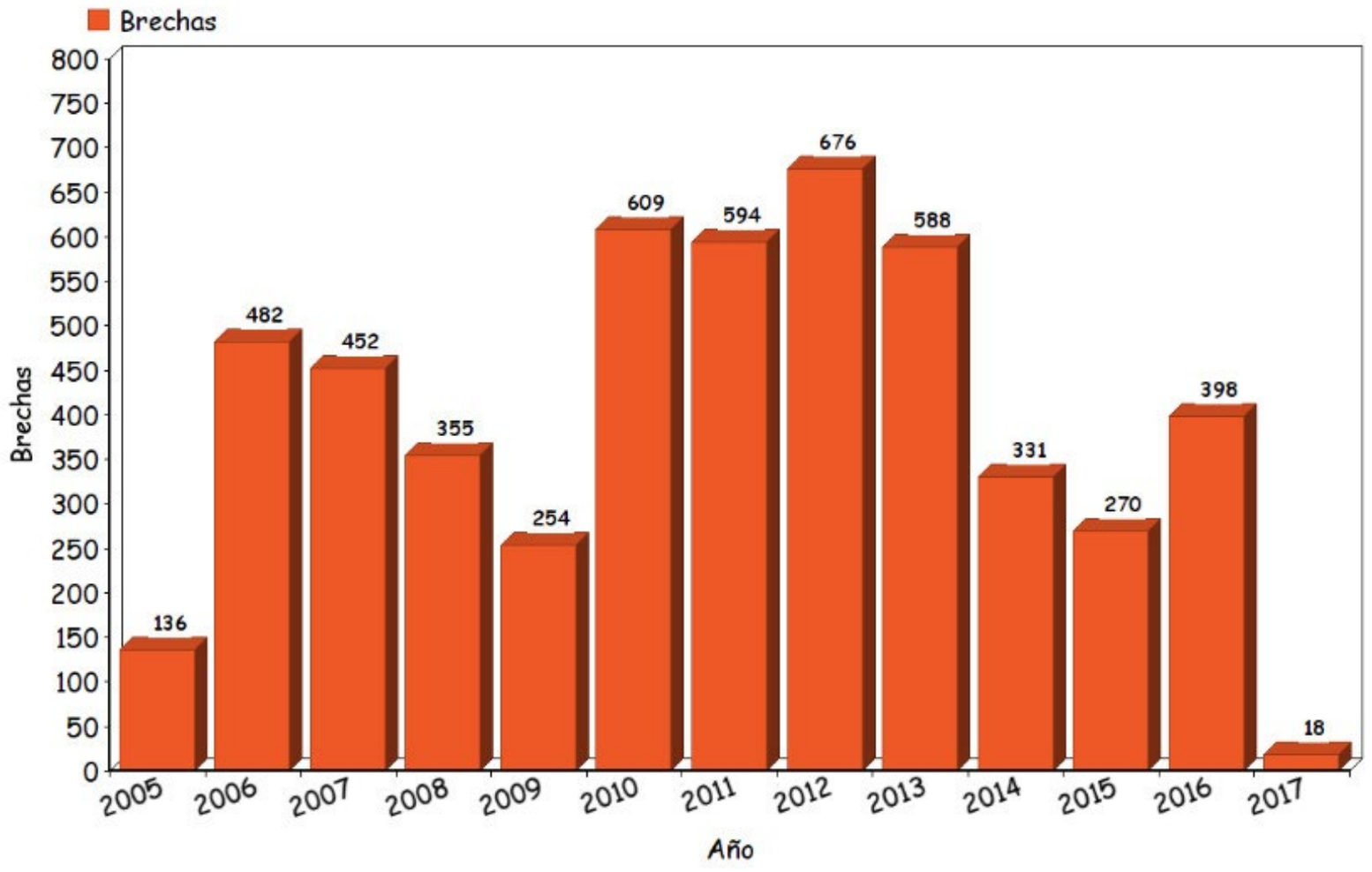
Compartir en RRSS

cierto volumen a partir de ese año, algo que se atribuye al incremento exponencial del volumen de datos, lo que dio a los cibercriminales una mayor oportunidad de exponer gran cantidad de datos en una única brecha

2017

En lo que va de año se han producido decenas de brechas de seguridad. El año se iniciaba con la de Arby's, un gigante de comida rápida que se vio afectado por un software malicioso instalado en terminales de venta de más de mil tiendas. La información robada incluye tarjetas de crédito y débito utilizadas entre el 25 de octubre de 2016 y el 19 de enero de 2017.

También a primeros de año una brecha en Dailymotion, uno de los servicios para compartir vídeos en internet más populares fue hackeado, desvelando algo más de 85,2 millones de direcciones y nombres de usuarios. Además, una quinta parte de los registros robados incluían contraseñas, aunque cifradas.



Dow Jones & Co., propietario entre otros del Wall Street Journal, anunció en julio que registros de unos 2,2 millones de suscriptores con información relacionada con sus nombres, IDs, direcciones de sus casas y trabajos, direcciones de email y los último cuatro dígitos de sus tarjetas de crédito, habían sido robados.

Unicredit, uno de los bancos más importantes de Italia, anunciaba este verano una brecha de datos que afectó a 400.000 de sus clientes cuyos números de cuenta y datos personales habían sido robados. El banco aseguró que las contraseñas no habían sido comprometidas, por lo que los ciberdelincuentes no han podido realizar transacciones no autorizadas.

Una inapropiada configuración de backup en River City Media –uno de los mayores proveedores de spam del mundo, dejó expuestas 1.370 millones de direcciones de email, algunas de las cuales iban acompañadas de direcciones IP y físicas. El fallo de seguridad también desveló la estrategia de la com-

pañía incluyendo detalles como planes de negocios, registros de Hipchat, cuentas y más.

Hasta el cierre de la revista la última gran brecha de seguridad ha sido la de Equifax, una firma crediticia que a primeros de septiembre anunciaba haber sufrido una brecha de seguridad que dejaba expuesta la información de 143 millones de consumidores en Estados Unidos. La compañía admitía que la brecha fue descubierta el 29 de Julio, cuando se detectó un acceso no autorizado al sistema. Las primeras investigaciones muestran que los hackers estuvieron accediendo a los sistemas de la compañía durante un período de más dos meses. Se investiga además la venta de dos millones de dólares en acciones por parte de dos empleados de Equifax el día después de conocerse la brecha.

2016

La brecha de seguridad más sonada de 2016 fue la de Yahoo!, no sólo por la cantidad, 500 millones de usuarios, sino porque fue detectada dos años después de haberse producido. En octubre de 2016 Weenly y Foursquare fueron las últimas compañías en anunciar sendos ciberataques que desvelaron 43,4 millones de registros en el caso de la primera y 22,5 millones de la segunda. Cada registro incluía el nombre de usuario, dirección de email, contraseña y dirección IP.

Con 32 millones de credenciales robadas, Twitter también ocupa un espacio en la lista de brechas de seguridad más importantes de 2016, aunque parece que los dos fueron robados directamente a los usuarios más que de los servidores de la red social. No fue el caso de MySpace, otra red social, que fue hackeada para el robo de 360 millones de datos de cuentas con direcciones de email y contraseñas, que posteriormente se vendieron por 2.800 dólares.

2016 también fue un mal año para la red Friend Finder Networks, compañía que está detrás de

Cómo gestionar una brecha de seguridad según la GDPR

Parece que en lo que respecta a brechas de seguridad, todo pasa en Estados Unidos. Se ven pocas empresas europeas en este listado de las brechas de seguridad más importantes de la historia, pero las cosas podrían empezar a cambiar a partir de mayo de 2018, cuando entre en vigor el nuevo Reglamento Europeo de Protección de Datos, más conocido como GDPR.

Entre las novedades más significativas la obligatoriedad de notificar las brechas de seguridad o fugas de información tanto a las autoridades como a los usuarios afectados, algo que las empresas de Estados Unidos tienen que hacer desde hace bastantes años.

Es decir que se deben notificar las incidencias de seguridad que impliquen una violación de datos personales sin demora injustificada y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella.

La diferencia respecto a la LOPD, Ley Orgánica de Protección de Datos, es que esta sólo afecta a los operadores de telecomunicaciones o proveedores de acceso a Internet. Con la GDPR cualquier empresa, independientemente de su tamaño o actividad, que maneje datos personales tendrán que informar.

Los usuarios afectados, así como la Agencia de Protección de datos, tendrán que recibir información de las posibles consecuencias de la violación de privacidad de sus datos, sobre todo si pudiera generar un problema de fraude o de usurpación de identidad, así como perjuicio a su reputación.

También habrá ocasiones en las que no se exigirá la notificación a los afectados. Si los datos extraídos estén cifrados y por tanto esa brecha de seguridad no afecte a los datos personales la notificación a los afectados no será obligatoria; tampoco la intrusión y la violación de datos no pueda afectar negativamente a los datos personales o a la intimidad del particular.

No adaptarse al nuevo reglamento supone asumir un riesgo que puede salir muy caro, pues las empresas que no lo hagan pueden enfrentarse a sanciones de hasta veinte millones de euros, frente al máximo de 600.000 de la LOPD vigente en estos momentos.

GDPR obligará a toda empresa que maneje datos de usuarios a informar sobre una brecha de seguridad 72 horas después de haberla sufrido

Penthouse, entre otras publicaciones. Un total de 412 millones de cuentas quedaron expuestas en un ciberataque que explotó una vulnerabilidad de inclusión de archivos locales, lo que permitió a los hackers acceder a todos los sitios de la red.

La conducta de VTech, el conocido fabricante de juguetes, en lo que se refiere a la ciberseguridad quedó en entredicho después de que un ciberataque consiguiera extraer información de 11,6 millones de cuentas, de las que 6,4 correspondían a niños. La información extraída incluía direcciones físicas, nombres de los padres y los niños, imágenes de los niños utilizadas como sus avatares online, contraseñas cifradas, direcciones de email e incluso preguntas secretas en texto plano.

2015

Este fue el año de una de las brechas más famosas, la que afectó a Ashley Madison. Los ciberdelincuentes extrajeron casi 100 gigabytes de datos correspondientes a más de 37 millones de clientes. Dos años después, en julio de este año, la compañía ha tenido que pagar 11,2 millones de dólares para indemnizar a las víctimas afectadas.

También sonada fue la brecha que afectó a Sony Pictures, a la que robaron entre 10 y 10,5 millones de registros con nombre, fechas de nacimiento, números de la seguridad social, direcciones de email, números de teléfono, además de información financiera como número de tarjetas de crédito.

2014

En octubre de 2014 JPMorgan desveló el que se ha convertido en del mayor robo de datos de clientes a una institución financiera en la historia de Estados Unidos. Los ciberdelincuentes consiguieron acceder a cerca de 76 millones de cuentas con nombres, direcciones postales, teléfonos y direcciones de email. El ciberataque consiguió acceder a los servidores con derechos de administrador.

RIVER CITY MEDIA HACKEADA — CLICAR PARA VER EL VÍDEO

2014 fue además un año negro para la industria del retail con brechas que afectaron a dos conocidos retailers de Estados Unidos, The Home

¿CUÁNTO CUESTA UNA BRECHA DE SEGURIDAD?

IBM ha patrocinado el 12th annual Cost of Data Breach Study elaborado por Ponemon Institute, un informe que asegura que este año el coste de medio de una brecha de seguridad o fuga de datos ha descendido un 10% respecto al año anterior. También es menor el coste de cada registro perdido o robado. Casi en compensación el tamaño de las brechas ha crecido un 1,8%. ¿Por qué una brecha es más cara cuando impacta en una empresa de Estados Unidos? ¿Qué elementos hacen que una brecha cueste más o menos?

Depot y Target. El primero sufrió dos brechas, la primera por parte de tres empleados que se cree que se llevaron 30.000 registros y la segunda en septiembre, cuando un ciberataque contra las TPV de sus más de dos mil tiendas consiguió extraer información de 56 millones de tarjetas de crédito y débito.

En el caso de Target se conoció en 2014 un ciberataque ocurrido a finales de 2013 que dejó expuesta la información de 70 millones de tarjetas de pago. Una sentencia de este año obliga a la compañía a pagar 18,7 millones de dólares.

eBay fue también protagonista en 2014 después de que un ciberataque permitiera a los hackers tener acceso a una de sus bases de datos y robar información de más de 145 millones de cuentas. Entre los datos robados contraseñas, direcciones de email, fechas de cumpleaños, direcciones de correo electrónico y otros detalles personales. No se tuvo acceso a datos financieros porque esa información se guarda cifrada de manera separada.

2013

El impacto de la brecha de seguridad sufrida por Adobe a finales de 2013 pasó rápidamente de tres millones de registros a más de 38 millones, cifras oficiales de la compañía, mientras algunos investigadores subían hasta los 150 millones. Adobe fue víctima de un ataque que expuso los ID de cliente y las contraseñas cifradas.

Evernote publicaba en marzo de 2013 un aviso informando a sus cerca de 50 millones de usuarios que había sufrido una seria violación de seguridad que permitió a los hackers robar nombres de

Consecuencias financieras de una brecha de seguridad

El incremento de las brechas de seguridad es constante. Sin embargo, su coste varía dependiendo de cada organización. En general, y según un informe de Ponemon Institute patrocinado por IBM, el coste de las brechas está descendiendo, un 10% de manera global y un 2,9% per cápita. Por otra parte, el tamaño medio de la brecha, es decir, el número de registros perdidos o robados se ha incrementado un 1,8%.

El informe también dice que las brechas son más caras en Estados Unidos o Canadá que en Brasil o India, y que varían dependiendo de las industrias. En este sentido, el coste medio de una brecha por registro perdido o robado es de 141 dólares, cifra que se eleva hasta los 245 dólares cuando hablamos del vertical de sanidad, y se reduce a los 71 dólares en el sector público.

Obvio, cuando más rápido se detecta y contiene una brecha de seguridad, menor es su coste. Los datos del 2017 Ponemon Cost of Data Breach Study indican que por tercer año consecutivo se ha detectado una relación entre cuán rápido puede una organización identificar y contener la brecha y las consecuencias financieras.

Los ciberdelicuentes causan la mayoría de las brechas de seguridad, que además tienen un coste superior que cuando es un error o negligencia.

Un equipo de respuesta ante incidentes y utilizar tecnologías de cifrado reduce el coste de registro comprometido hasta los 19 dólares.

Con 1.370 millones de registros expuestos, la sufrida por River City Media este año es la brecha de seguridad más grande de la historia

usuario, direcciones de correo electrónico asociadas y contraseñas cifradas. Los hackers, sin embargo, no fueron capaces de acceder a detalles financieros ni a las notas que los clientes habían almacenado.

2012

En 2012 Dropbox sufrió una brecha de seguridad que afectó a 68 millones de cuentas. La información no se conoció hasta 2016 cuando se descubrió online una gran cantidad de datos de usuarios del servicio de almacenamiento con información sobre nombres de usuarios y contraseñas. Dropbox confirmó años después que las credenciales habían sido robadas con los detalles de acceso robados a un empleado.

También en 2012 quedaban expuestas doce millones de Apple IDs. Un grupo de hackers llamado AntiSec y con relaciones con Anonymous aseguraba haber obtenido los datos personales de los doce millones de usuarios hackeando un ordenador del FBI. El grupo publicaba, como demostración, los datos de un millón de esas cuentas.

Blizzard, responsable de juegos tan populares como Diablo III, Starcraft II o World of Warcraft, anunciaba una brecha de seguridad con impacto en cerca de 14 millones de jugadores y que desvelaba contraseñas cifradas, direcciones de email y las respuestas a las preguntas de seguridad.

2011

Una de las brechas más sonadas de la historia se produjo este año, cuando Sony detectó una intrusión de 24,6 millones de cuentas de usuario de una base de datos de 101,6 millones. La base de datos contenía nombres, direcciones postales y de correo electrónico, fechas de nacimiento, credenciales de inicio de sesión para Playstation Network (PSN) y Qriocity. Se sospecha que los hackers también pueden tener acceso a historiales de compras, direcciones de facturación y preguntas de seguridad.

En abril de 2011 PlayStation Network tuvo que interrumpir su servicio después de detectar una intrusión externa en los servicios PlayStation Network y Qriocity, en la que los datos personales de aproximadamente 77 millones de cuentas se vieron comprometidos. El ataque ocurrió entre el 17 de abril y el 19 de abril de 2011, obligando a Sony a desactivar temporalmente PlayStation Network el 20 de abril.

Wordpress sufrió en 2011 un ataque contra varios de sus servidores que dejó expuesto el código fuente y contraseñas de 18 millones de sus usuarios.

2010

La mayor brecha de datos en 2010 generó el robo de trece millones de registros. Los hackers fueron capaces de penetrar deviantART, una de las mayores redes sociales para artistas a través de la empresa de comercialización Silverpop Systems Inc. La base de datos expuesta consistía en nombres de usuario, direcciones de correo electrónico y fechas de nacimiento de todos los usuarios de deviantART.

2009

RockYou, un fabricante de aplicaciones para redes sociales, pedía a 32,6 millones de usuarios que cambiaran sus contraseñas tras ser atacado. Un fallo de inyección SQL en su base de datos dejaba expuesta la lista entera de nombres de usuario,

Y si no cumplo la GDPR, ¿Qué?

Apenas quedan unos meses para que una de las normativas más exigentes en materia de protección de datos entre en vigor. ¿Estás seguro de cumplir con ella? ¿Qué pasaría en caso de que no fuera así?

Regístrate en este IT Webinar y conoce las principales claves de la Regulación Global de Protección de Datos, la nueva normativa europea que exige una nueva forma de gestionar y proteger la información que manejan las empresas.

direcciones de email y contraseñas, que estaban almacenadas en texto plano.

También en este año 76 millones de registros de veteranos de Estados Unidos fueron expuestos cuando un disco duro defectuoso fue enviado a reparar sin que primero se destruyeran sus datos. La unidad era parte de una matriz RAID de seis unidades que contenían una base de datos de Oracle llena de información de veteranos. La unidad se consideró irreparable y luego fue enviada a otra entidad para el reciclaje, una vez más, sin ser borrada.

Fue en 2009 cuando 130 millones de tarjetas de crédito fueron robadas en un ciberataque contra Heartland Paymant System. El problema de agravó por los retrasos a la hora de revelar la brecha y las informaciones inexactas relacionadas con la misma.

2008

No fue un ciberataque, sino el robo de información por parte de un empleado que robó información de 17 millones de cuentas lo que añadió a Countrywide Financial Corp. a la lista de 2008.

Tampoco fueron los ciberdelincuentes los culpables de que 12,5 millones de registros del Bank of New York Mellon con nombres, números de seguridad social y números de cuentas fueran expuestos. Los datos se perdieron cuando una caja de cintas de respaldo llegó a una instalación de almacenamiento con una cinta desaparecida.

Los datos de 18 millones de miembros de Auction.co.kr, una página de subastas de Corea del Sur, fueron robados por un hacker chino. Entre la información se encontraba una gran cantidad de datos financieros.

También curiosa fue la brecha de GS Caltex en 2008: En una calle de Seúl se encontraron dos CD con una lista de 11,9 millones de clientes de la compañía.

2007

En marzo de 2007 el retailer TJ MAxx sufrió una brecha de seguridad que afectó a cien millones de registros con números de tarjetas de crédito y débito, así como los registros de devolución de mercancías que contienen nombres y números de licencia de conducir, así como números de cuenta de tarjeta de crédito. El ciberdelincuente, que

¿Te avisamos del próximo IT Digital Security?

atacó los sistemas de Heartland un año después, robó los números durante un periodo de 18 meses, con un impacto económico que se calcula en 118 millones de dólares.

HM Revenue and Customs (HMRC) perdía en 2007 discos informáticos que contenían datos confidenciales de 25 millones de beneficiarios de prestaciones para niños. La organización dijo en su momento que no creía que los registros -nombres, direcciones, fechas de nacimiento y cuentas bancarias, hubieran caído en malas manos caído en manos equivocadas.

Mantener la información sensible cifrada es una manera de reducir el impacto de una brecha de seguridad

2006

Un portátil y un dispositivo de almacenamiento con datos confidenciales de 26,5 millones de veteranos de Estados Unidos fueron robados del hogar de un empleado no identificado del Department of Veterans Affairs, recuperándose casi dos meses después. La información almacenada consistía en nombres, números de seguridad social, fechas de nacimiento, números de teléfono y direcciones de todos los veteranos estadounidenses dados de alta desde 1975.

Más de 17 millones de registros de iBill, un servicio de pago online asociado con sitios de pornografía, fueron colgados en Internet con información sobre nombres, números de teléfono, direcciones de email y postales, credenciales de acceso, y cuentas de compra.

Por razones que aún se desconocen AOL publicó 20 millones de registros de 650.000 usuarios. Entre los datos expuestos, el historial de búsquedas de tres meses, así como si pincharon en un enlace. La descarga con los datos estuvo disponible durante varios días.

2005

La mayor brecha de seguridad de este año fue la sufrida por CardSystems. Un individuo no autorizado se infiltró en la red informática de un procesador de pagos de terceros y robó hasta 40 millones de números de tarjetas de crédito. El 2009 se supo que CardSystems almacenaba información sobre tarjetas de crédito sin cifrar en sus servidores.

Enlaces de interés...

- W ¿Cuánto cuesta una brecha de seguridad?
- W Fuga de información en un despacho de abogados: ¿cómo gestionarla?
- W GDPR: todas sus claves
- I Calcula el coste de una Brecha de Seguridad

NUEVO.
PERO NO NACIDO AYER.

CSC Y HPE ENTERPRISE SERVICES AHORA SON DXC TECHNOLOGY.

DXC.technology/GetItDone

DXC.technology | THRIVE ON CHANGE.

“El éxito de Netskope es una plataforma capaz de supervisar todas las aplicaciones cloud y cumplir con directivas como la GDPR”

Sanjay Beri, CEO y fundador de Netskope

En su visita a Madrid el 19 de septiembre, Sanjai Bery, CEO y fundador de Netskope, se acercó a las oficinas de IT Digital Media Group para hablar con IT Digital Security sobre cuál es la mejor manera de ofrecer seguridad y visibilidad de los servicios cloud en tiempo real, garantizando el cumplimiento de normativas y previniendo la pérdida de datos.

“Habilitar el cloud de una manera segura”, ese es el gran reto de la seguridad Cloud, dentro de la cual empieza a despegar CASB (Cloud Access Technology Broker), un mercado en el que Netskope es experto. El reto, continúa Sanjay Beri, CEO y fundador de Netskope, “es cómo decir sí a mis unidades de negocio, pero con garantías”. Y el gran reto técnico es tener el producto de seguridad adecuado para trabajar con la nube de una manera segura.

La clave de todo está en el CASB, una tecnología que responde al incesante uso de aplicaciones basadas en cloud y la necesidad de controlar la pérdida de datos, la monitorización en tiempo real y el cumplimiento normativo.

A su paso por Madrid, Sanjay Beri nos explica que las empresas utilizan centenares de aplicaciones basadas en cloud; “una media de 700, según un informe que hicimos hace un par de años”, especifica el directivo. Para Sanjay Beri

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

NETSKOPE DEMO **CLICAR PARA VER EL VÍDEO**

"Cuando un departamento de TI no tiene bajo control las aplicaciones que se utilizan en sus empresas, también pierde el control sobre los datos"

está claro que “no se puede detener el avance de las aplicaciones cloud”, que “el cloud es bueno para para las empresas”, pero que, al mismo tiempo, “la seguridad cloud es un reto”, porque cuando un departamento de TI no tiene bajo control las aplicaciones que se utilizan en sus empresas, también pierde el control sobre los datos. Se dan cuenta, dice el CEO de Netskope, que sus datos están en una aplicación de la que no saben nada, ni siquiera quién está accediendo a ella.

¿Por qué se necesita una solución de Cloud Access Security Broker? Sencillamente porque el firewall se queda corto, incapaz de proporcionar la visibilidad granular que se necesite para saber qué aplicaciones se están utilizando, quién está accediendo a ellas, desde dónde y, sobre todo, si el uso de los datos en esas aplicaciones está conforme a las regulaciones.

En términos generales CASB ofrece visibilidad sobre el uso de las aplicaciones basadas en la nube, ayudando a proteger los datos corporativos de las ciberamenazas gracias a controles granulares y una mayor detección. Con CASB se acaba el Shadow IT y además se puede detectar actividad anómala y establecer políticas y controles. Por lo pronto el mercado promete: 7.510 millones de dólares para 2020, con un crecimiento medio anual del 17,6% hasta la fecha, según datos de MarketsandMarkets.

Una nueva era

Desde el punto de vista de una empresa, Internet ha cambiado mucho, asegura Sanjay Beri. No sólo se trata de que se accede desde casa, o a través de dispositivos móviles, “es que el lenguaje de Internet ha cambiado. Está basado en APIs (Application Programming Interfaces)”. Y por eso “si el lenguaje sobre el que las aplicaciones está basado cambia, si hablas en un idioma nuevo, alguien no te entenderá”. Explica el directivo que si tratas de saber lo que la gente está haciendo y gestionando la seguridad con unos dispositivos desarrollados hace diez años… “no se van a entender. Por eso nosotros construimos nuestros productos entendiendo la nueva era de Internet”.

Ya no se trata de asustar a la gente, de demostrarles que no tienen control sobre cientos de aplicaciones, sino de habilitarles a que puedan permitir el uso de esas aplicaciones en lugar de hacer esperar a los usuarios y generar el llamado Shadow IT. Esta es, según Sanjay Beri, la clave del éxito de Netskope: haber creado una plataforma capaz de supervisar todas las aplicaciones basadas en la nube que utiliza una empresa y que además “tiene la capacidad de detener el malware, el ransomware, de cumplir con la GDPR, que te habilita para utilizar dispositivos personales y acceder con ellos, de forma que finalmente puedas decir: Si”.

La plataforma de Netskope

Explica Sanjay Beri que la plataforma de seguridad pone en manos de los responsables de TI toda la información sobre el uso de la nube que se está haciendo en su empresa ya sea de manera remota o a través de un dispositivo móvil. De esta forma

"Cuando alguien dice que está adoptando Office 365 no está solo adoptando una aplicación, sino todo un ecosistema"

"se pueden comprender las actividades arriesgadas, proteger los datos confidenciales, detener las amenazas en línea y responder a los incidentes de una manera que se ajusta a la forma actual en que las personas trabajan".

Netskope es capaz de detectar todas las aplicaciones cloud que se están utilizando en una empresa, hayan sido, o no, permitidas por la empresa. La plataforma no sólo muestra qué aplicaciones cloud se utilizan más, sino, sobre cada aplicación, qué usuarios la están utilizando y desde dónde, estableciéndose además una puntuación de riesgo asociado a cada una. Además, al haber inventariado e inspeccionado cientos de archivos, la plataforma es capaz de informar sobre los datos que se están compartiendo o utilizando en cada aplicación, ofreciendo al administrador una visión clara de las posibles violaciones de políticas de seguridad gracias a Netskpope DLP.

Se trata, en definitiva, de poner fin al Shadow IT y de entender el uso que de cada aplicación hacen los empleados, estableciendo una infraestructura segura, independientemente de si se accede desde un dispositivo móvil, repite el CEO De Netskope.

Le preguntamos a Sanjay Beri de manera específica por Office 365, que ha sido una de las aplicaciones que ha impulsado el uso del cloud en las empresas. Para el directivo "es una de las muchas aplicaciones que la gente utiliza", pero lo que añade no deja de ser interesante: "de media, las empresas conectan 25 aplicaciones SaaS a Office". No se trata de aplicaciones de Microsoft, sino de terceros, como DocuSign o Box, pero el hecho es que "cuando alguien dice que está adoptando Office 365 no está sólo adoptando una aplicación, sino todo un ecosistema, y eso es muy importante porque cuando escoges una plataforma desde el punto de vista de seguridad no puede escogerse una plataforma que esté centrada sólo en Microsoft Office 365, porque vas a tener muchas aplicaciones asociadas, y necesitas una manera consistente de gestionarlas".

En todo caso, y a pesar de que Office 365 es parte importante del negocio de Netskope, "nuestro foco es cubrir todas las aplicaciones cloud con una sola plataforma enfocada a hacer fácil su configuración y gestión de las mismas".

Netskcope en España

"Estamos muy enfocados en grandes empresas y contamos con un responsable local de ventas, ingeniería de sistemas, servicios profesionales y soporte de clientes en España", asegura el directivo cuando le preguntamos por la situación de Netskope en España.

Y como España es uno de los países en los que la GDPR será de obligado cumplimiento a partir

Enlaces de interés...

- 15 Casos de uso crítico de CASB
- Tecnologías de seguridad Cloud listas para su adopción
- Market Guide for CASB

"Las mayores compañías del mundo en cada vertical son clientes de Netskope, y ahora apuntamos hacia el midmarket"

del 25 de mayo de 2018, aprovecha Sanjay Beri para decir que la plataforma de Netskope "incorpora todos los diferentes mandamientos reguladores con los que tengan que trabajar las empresas".

En España la compañía tiene un modelo de canal basado en integradores de sistemas como Telefónica o GMV, además de trabajar con Exclusive Networks.

Y las empresas españolas, ¿están adoptando soluciones de CASB? Sí, responde el CEO de Netskope, añadiendo que hace dos o tres años "la historia era muy diferente, pero que las cosas han cambiado". Explica Sanjay Beri que en este tiempo, los clientes han adoptado aplicaciones SaaS, no sólo Office, sino Salesforce, ServiceNow, y otras, y se dan cuenta de que hay miles de aplicaciones, que tienen que enfrentarse al Shadow IT, "y buscan una solución que les ayuda a gestionar todo ese problema"; "sobre todo porque una de las cosas que la GDPR va a exigirte es que sepas dónde están tus datos, los datos de tu negocio, los datos de tus clientes".

Sobre el IoT en relación con su negocio, dice el responsable de Netskope que "es sólo otro caso de uso para la nube", porque en realidad la compañía no va a construir un software para el IoT.

Para terminar Sanjay Beri resume "lo que debes saber de Netskope". En primer lugar, que no están pensando en ser absorbidos por otras empresas, que "cuando creamos la compañía lo hicimos pensando en ser autónomos y ser una 'iconic security company'", y que por tanto "estamos muy centrados en construir nuestra compañía". En segundo lugar, que "las mayores compañías del mundo en cada vertical son clientes de Netskope" y que la compañía apunta ahora hacia el midmarket. Y, en tercer lugar, que "nuestra visión es muy amplia", cubriendo no sólo Office, sino cientos de aplicaciones. "Nadie en el mercado tiene estas tres cosas", finaliza Sanjay Beri, CEO y co-fundador de Netskope.

ENJOY SAFER TECHNOLOGY™

Adapta tu empresa a la nueva normativa de protección de datos

ENDPOINT ENCRYPTION

DESCARGA GUÍA GRATUITA GDPR

http://gdpr.eset.es

Por qué IoT no es seguro

En la variedad está el gusto, aunque cuando se trata de proteger el Internet de las Cosas (IoT), habría que hablar de reto. Demasiada heterogeneidad, en los dispositivos, redes, protocolos métodos de autenticación o plataformas en la nube. El IoT, además, llega como un tsunami, con una implementación masiva que dificulta la seguridad por defecto. El resultado es un entorno donde hay millones de productos conectados en todo el mundo con bajos niveles de seguridad.

Algo importante ocurrió en 2008: el número de cosas conectadas a Internet superó la población mundial. La ratio de adopción del IoT es cinco veces más rápido que la adopción de la electricidad o la telefonía, lo que supone unos seis dispositivos conectados por cada persona que habita la Tierra. Hablamos del Internet de las Cosas, o lo que es lo mismo, decenas de miles de millones de dispositivos con sensores y capacidad de actuación, conectados entre sí y con Internet. En el mismo saco del IoT entra una pulsera de fitnes o un smartwatch, un dispositivo que controle el sistema eléctrico de un hogar o con capacidad para controlar una fábrica, un automóvil o una máquina de salud. En realidad, el mismo sensor se utiliza en todos los entornos y la seguridad no es una gran prioridad para estos dispositivos.

Cientos de miles de dispositivos de IoT se han utilizado recientemente para lanzas una de las

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

DIRECTRICES DE SEGURIDAD PARA EL IOT DE LA GSMA

CLICAR PARA VER EL VÍDEO

campañas de Denegación de Servicio Distribuido (DDoS) más grandes de la historia, con un volumen de tráfico que superara el terabyte por segundo en algunos casos. La realidad es que el número de ciberataques contra dispositivos IoT vulnerables está creciendo rápidamente.

Tanto los sistemas pertenecientes a ese universo de dispositivos conectados como otros sistemas embebidos suelen fabricarse sin los mismos estándares y el mismo nivel de compromiso con la seguridad. A menudo no contemplan una forma segura de conexión remota para su gestión y actualizaciones y en algunos casos ni siquiera existe la posibilidad de ser gestionados y actualizados de forma remota. ¿Por qué? La respuesta más fácil tiene que ver con el propio coste de los dispositivos IoT. Se pueden encontrar enchufes inteligentes por 25 euros corriendo sobre un kernel de Linux, un sistema operativo completo y un sistema de archivos. Con ese precio, el margen de beneficio en un enchufe inteligente es pequeño, a lo que se suma los gastos de desarrollo inicial. Esto genera presión para mantener los costes controlados y dejar el tema de la seguridad en un segundo plano.

Todas las industrias se ven afectadas desde el momento en que, más a menudo de lo que parece, los departamentos de TI no tienen visibilidad sobre estos sistemas no tradicionales que están conectados a la red corporativa. Y de la misma manera en que se habla de Shadow IT, el Shadow IoT es un término que se utiliza cada vez más, y que no dejaremos de escuchar durante los próximos años.

Falta de concienciación

Según Gartner, aunque en 2020 más del 25% de los ataques a empresas estarán relacionados con el IoT, éstas asignarán menos del 10% de sus presupuestos de seguridad al IoT.

Por lo tanto, habría que plantearse si el mercado, las empresas, ¿están concienciadas para aplicar la seguridad al IoT? Para Eutimio Fernández, director de ciberseguridad de Cisco España, “están concienciadas, pero no preparadas”. Añade el directivo que el modelo de seguridad de red actual fue diseñado para conectar ordenadores de propósito general, y no miles de millones de dispositivos de propósito específico, y que la situación se complica aún más si no hay una verdadera integración de la arquitectura de seguridad entre las IT (Information Technologies) y las OT (Operation Technologies).

Para Pedro Pablo Pérez, CEO de ElevenPaths, la falta de seguridad del IoT “debe verse como una barrera, como un inhibidor de la adopción del IoT y, en consecuencia, de la implantación de soluciones

"El apetito que tienen ciertos fabricantes por conseguir un posicionamiento en el mercado, o simplemente por vender, está generando que muchos productos y soluciones de IoT salgan al mercado sin los mínimos controles de seguridad que deberían tener de fábrica"

Rodrigo Chávez, Responsable de IT Security Services & Solutions en Unisys

que se aproevechen de los enormes beneficios que esta tecnología puede traer". Y es por ello, asegura también el directivo, que la seguridad "es ya una preocupación de primer orden para el negocio y debe formar parte de cualquier solución IoT.

"Lamentablemente, aún queda mucho para que esto suceda", para que el mercado esté concienciado para aplicar seguridad al IoT, dice también Josep Albors, responsable de concienciación de ESET España.

Lo cierto es que los dispositivos conectados han sido tradicionalmente ignorados, o incluso no inventariados. Son endpoints que se han extendido por las redes empresariales, a veces sin controles o segmentación adecuados para evitar que se vean comprometidos o evitar que se utilicen en ataques contra otros sistemas corporativos. Se suma el he-

Un Jeep en manos de unos hackers

Es habitual que cuando se habla del Internet de las Cosas pensemos en sensores de tipo industrial o para el hogar, pero lo cierto es que el coche conectado lo es gracias al IoT. La principal característica de estos automóviles es que están conectados a Internet y desde ese momento son accesibles a los ciberdelincuentes.

Han pasado ya dos años desde que Charlie Miller, director de investigación en Twitter, y Chris Valasek, responsable de Vehicle Security Research en IOActive, fueron capaces de hackear el sistema de entretenimiento de un Jeep Cherokee. Aprovechando una vulnerabilidad en Uconnect, el software que permite a los vehículos de Chrysler conectartse a Internet, además de controlar el sistema de entretenimiento y funciones de navegación, los investigadores pudieron acceder a las funciones más críticas del coche y controlarlo de manera remota.

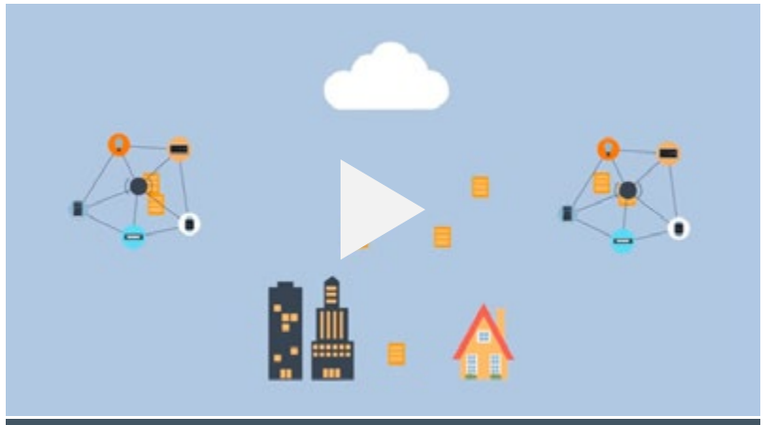
Mientras el coche circulaba a 112km/hora, el conductor pudo sentir cómo el aire acondicionado se ponía a funcionar a máxima potencia, ver fotos en la pantalla de control, escuchar música a todo volumen y activarse los limpiaparabrisas. Todo ello de repente y sin que el conductor tuviera control alguno sobre ello. Finalmente, el motor se apagó de repente.

Al mando del volante el periodista Andy Greenberg, que narró su experiencia en Wired. Estaba avisado, sabía que iba a pasar: "Recuerda Andy, pase lo que pase, no entres en pánico", fue el consejo que le dieron los dos investigadores que, a 16 kilómetros y sentados en un sofá con dos ordenadores, jugaban con el coche. El impacto para Chrysler fue tener que retirar 1,4 millones de vehículos.

Quizá el del Jeep ha sido el más conocido, pero desde luego no ha sido el último. Dieter Spaar, experto de seguridad alemán, descubrió vulnerabilidades en BMW ConnectedDrive, que permite a un hacker abrir el coche de forma remota, además de hacer un seguimiento de la localización y velocidad del vehículo en tiempo real o leer los emails enviados y recibidos a través de BMW Online.

La vulnerabilidad ya fue solucionada, pero es cuestión de tiempo que se detecte alguna más.

La seguridad del IoT se vuelve de vital importancia en determinados escenarios, y los coches conectados son uno de ellos, sobre todo con los enormes avances que se están consiguiendo en torno a los coches autónomos.



"Se han utilizado dispositivos del IoT para realizar ataques de denegación de servicio, minar criptomonedas o robar información confidencial, por poner solo tres ejemplos"

Josep Albors, responsable de concienciación de ESET España

cho de que, además, el ciclo de vida para reemplazar estos sistemas puede ser mucho más largo que con los sistemas informáticos tradicionales.

Está claro que las empresas, la industria en general, se enfrenta a una serie de retos a la hora de integrar la seguridad en el ecosistema del Internet de las Cosas. Para Eutimio Fernández existen dos retos principales; "en primer lugar, la mayoría de los dispositivos IoT no pueden protegerse a sí mismos, creando una gran oportunidad para que los atacantes exploten las vulnerabilidades y obtengan acceso a la red corporativa. El segundo reto es la implementación a escala o masiva, ya que las organizaciones conectarán cientos de miles de dispositivos en los próximos años".

Rodrigo Chávez Rivas, responsable de IT Security Services & Solutions de Unisys, habla del "apetito" de ciertos fabricantes por conseguir un posicionamiento en el mercado, como algo que impacta negativamente en la seguridad del IoT. "Si describimos los desafíos considerando el proceso que hay desde la fabricación hasta llegar al consumidor final, probablemente el primer reto sea conseguir que todos fabricantes de IoT prioricen la seguridad antes que el 'Time to market'", dice Chávez. El resultado es que muchos productos y soluciones llegan al mercado sin los mínimos controles de seguridad

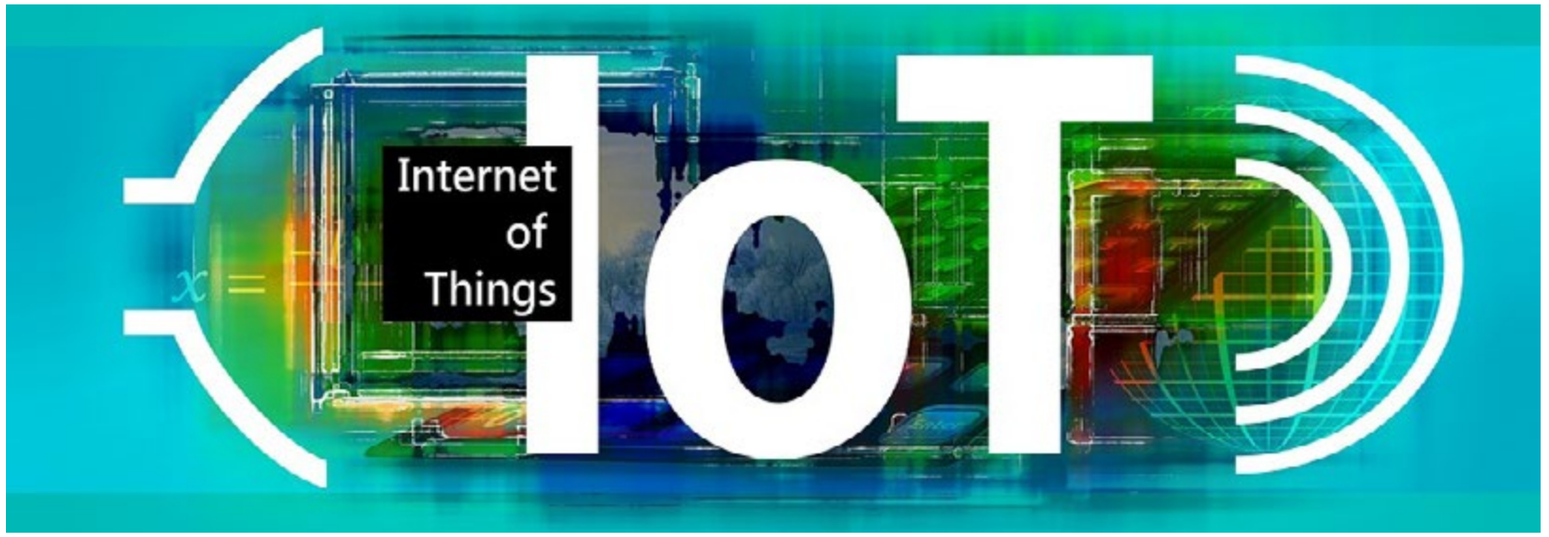
Josep Albors añade que la rapidez con la que se mueve el mercado y con la se añaden nuevas funcionalidades hace que muchos fabricantes se centren en nuevas versiones de productos sin preocuparse por ofrecer soporte de los modelos antiguos, que se quedan obsoletos.

Al preguntarse sobre los retos a la hora de integrar seguridad en el Internet de las Cosas, Pedro Pablo Pérez, CEO de ElevenPaths, enumera algunos retos que afectan principalmente a los dispositivos. Uno de ellos es la heterogeneidad de redes, dispositivos, protocolos, métodos de autenticación y plataformas en la nube; una heterogeneidad que impiden que las soluciones de seguridad puedan generalizarse. Hace referencia también Pablo Pérez a la gestión de la identidad y el acceso de los propios dispositivos, así como de los vínculos con sus propietarios y otros dispositivos, y finaliza hablando de la forma de operar los propios dispositivos, "incluyendo la gestión remota y la actualización del software y su monitorización continua para la detección de incidentes", como retos que dificultan aplicar seguridad el IoT.

Todos estos retos se acrecientan "cuando los dispositivos IoT son además implementados para controlar infraestructuras, como operaciones de fábrica y cadenas de suministro", dice Ricardo Lizarralde, Director Southern Europe Middle East and Africa, AT&T. "A fin de velar por que la integración y aplicación de la seguridad de IoT sea lo más fluida posible, las organizaciones necesitan inyectar los requerimientos y consideraciones de seguridad desde la fase inicial del proceso, para que los dis-

"El mercado está concienciado para aplicar seguridad al IoT, pero no está preparado. El modelo de seguridad de red actual fue diseñado para conectar ordenadores de propósito general, y no miles de millones de dispositivos de propósito específico"

Eutimio Fernández, director de ciberseguridad en Cisco España



positivos IoT sean diseñados con una arquitectura segura por defecto", dice Lizarralde.

En todo caso, los dispositivos de IoT necesitan dos acciones críticas por parte de us administradores para incrementar su seguridad, dice Rodrigo Chávez. Por un lado, una adecuada configuración inicial, que implica un cambio de calves de fábrica, y un adecuado mantenimiento, como es la actualización de parches de seguridad. "Finalmente, y ya en el lado del consumidor final, el reto probablemente consista en proteger cualquier dato tratado en los dispositivos de IoT y cualquier infraestructura conectada al dispositivo IoT", añade el directivo.

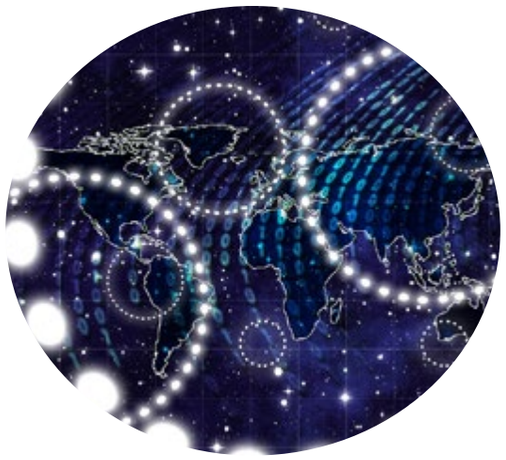
Tecnologías para securizar el IoT

Ni se va a conseguir de la noche a la mañana, ni será una tecnología única la que garantice la seguridad del IoT. Forrester elaboró en el primer trimestre de este año un documento en el que enumera lo que en su opinión son las tecnologías más importantes para proteger el IoT, para securizar el ecosistema de dispositivos conectados.

Proteger la red y los sistemas backend del IoT es una manera de empezar. Explican los expertos que proteger una red de dispositivos conectados es algo más complicado que proteger una red tradicional porque hay más protocolos de comunicación, más estándares y tipos de dispositivos, lo que plantea una mayor complejidad. Se propone asegurar el endpoint mediante soluciones antivirus y antimalware, así como firewalls y sistemas de prevención y detección de intrusiones.

La autenticación puede convertirse en un elemento imprescindible. Proporcionar a los usuarios la capacidad de autenticar un dispositivo IoT, incluso la gestión de varios usuarios para un mismo dispositivo a través de una contraseña o, mejor aún, mecanismos de autenticación de doble factor o incluso biometría. La tarea no es baladí si se tiene en cuenta que la mayoría de los escenarios del IoT contemplan comu-

De las Botnets a los Thingbots



Las Botnets son redes de ordenadores infectados que se utilizan para fines maliciosos. A veces sólo para enviar spam, otras para lanzar ataques de denegación de servicio distribuido, o DDoS, contra determinados objetivos. Actualmente las botnets con capacidades DDoS son un negocio que está disponible en la Darkweb.

Debido a su ubicuidad y al hecho de que normalmente están conectadas directamente a Internet, los routers y módems inalámbricos son uno de los principales objetivos de las thingbots, junto con las cámaras de red. La mayoría de estos dispositivos utilizan Linux como su sistema operativo, lo que permite a los atacantes utilizan un malware diseñado para este sistema operativo y compilarlo para dirigirlo contra arquitecturas específicas en las quer el dispositivo se esté ejecutando.

Lo que ha cambiado en los últimos tiempos en el Internet de las Cosas, el uso de esos miles de millones de dispositivos conectados para crear redes de Thingbots capaces de participar en un ataque DDoS. Es lo que el IBM X-Force ha definido como The Weaponization of IoT Devices en un informe.

Entre los ejemplos más alarmantes, la botnet Mirai. Capaz de infectar cientos de miles de dispositivos de IoT, especialmente cámaras de seguridad, utilizando las contraseñas por defecto para el acceso a Telnet, Mirai se ha convertido en uno de los mayores ejemplos de lo que está por llegar.

Mirai es un tipo de malware que detecta de manera automática dispositivos de IoT para infectarlos e incorporarlos a la red. En solo dos semanas la Thingbot fue capaz de interrumpir el servicio de más de 900.000 clientes de Deutsche Telekom en Alemania o infectar casi 2.500 routers en Reino Unido. En poco tiempo se hizo público que más de 80 modelos de cámaras Sony eran vulnerables a Mirai.

Entre las ventajas de Mirai es que ha probado ser extremadamente flexible y adaptable, lo que permite a los ciberdelincuentes desarrollar variantes capaces de atentar contra otras clases de dispositivos IoT, engrosando la botnet.

En lo que va de año han llegado al mercado 98 millones de cámaras IP, según IHS. Y la mayoría de ellas utilizan nombres y contraseñas por defecto

nicaciones machine to machine, por lo que en este caso el proceso de autenticación debe poder realizarse a través de máquinas mediante algún tipo de certificado digital y sin intervención humana.

El cifrado es otro elemento que puede jugar un papel fundamental en la seguridad del IoT. Cifrar los datos y las comunicaciones entre dispositivos y sistemas de back-end mediante algoritmos estándar ayuda a mantener la integridad de los datos y evitar que los hackers detecten los datos.

Mencionábamos antes la posibilidad de utilizar certificados digitales. Aunque las especificaciones de hardware de algunos dispositivos del IoT pueden limitar o impedir el uso de PKI, los certificados digitales podrán cargarse de forma segura en el momento de fabricación del dispositivo para después habilitarse o activarse mediante PKI de terceros. Como es lógico también sería posible instalar los certificados después de la fabricación.

La analítica de conducta podría llegar también al IoT de forma que monitorizando las actividades se detecten las sospechosas. Este tipo de soluciones, que incorporan tecnologías de machine learning, big data e inteligencia artificial permiten detectar anomalías pero son muy nuevas. Por el momento quizá deberíamos conformarnos con que la capacidad de análisis del IoT se limite a poder detectar ataques o intrusiones específicas que soluciones de red tradicionales como los firewalls no pudieran identificar.

La seguridad de las API será esencial para proteger la integridad de los datos que se mueven entre los dispositivos del borde de la red y los sistemas de back-end para asegurar que sólo los dispositivos, desarrolladores y aplicaciones autorizados se comunican con las APIs. De forma que otra de las medidas propuestas de Forrester para asegurar el internet de las cosas habla de proporcionar la capacidad de autenticar y autorizar el movimiento de datos entre dispositivos IoT, sistemas back-end y aplicaciones que utilizan APIs basadas en REST documentadas.

RIESGOS DE IOT EN LAS EMPRESAS

La proliferación y ubicuidad de los dispositivos IoT en las empresas está generando una mayor superficie de ataque y sencillos puntos de entrada que permiten a los hackers acceder a la red. Este estudio de ForeScout se ha centrado en siete dispositivos conectados a Internet comunes en las empresas y ha detectado lo fácil que es atacarlos, además de lo complicado que es implementar seguridad en ellos por sus propias tecnologías, métodos de desarrollo y producción.

IoT, la nueva arma de los ciberdelincuentes

Las posibilidades que el IoT ofrece a los delincuentes "son bastante amplias y llevamos años viendo ejemplos", dice Josep Albors, quien recuerda que ya se han utilizado dispositivos del IoT para realizar ataques de denegación de servicio, minar criptomonedas o robar información confidencial, por poner solo tres ejemplos. "El problema es que el futuro no pinta nada esperanzador si no hacemos algo al respecto", asegura.

Ricardo Lizarralde, de AT&T, recuerda que casa vez es más difícil detectar amenazas y que "los cibercriminales están desarrollando continuamente nuevas formas de abrir brechas en los sistemas de datos". La innovación camina del lado de los ciberdelincuentes; "utilizar 100,000 dispositivos IoT para lanzar un ataque DDoS ya no es sólo una teoría; esta es la última prueba de que la innovación en el cybercrimen está prosperando", recuerda.

Precisamente Eutimio Fernández habla de ataques de denegación de servicios (DDoS) que utilizan botnets de objetos conectados para colapsar servidores con tráfico procedente de múltiples fuentes como uno de los usos que los ciberdelincuentes harán del Internet de las cosas. El gran desafío, dice el responsable del negocio de seguridad de Cisco, es que "esos ataques pueden detener servicios básicos como el suministro de electricidad, gas o agua. Y es que el tamaño medio de los ataques DDoS se ha incrementado un 22% hasta los 1,2 Gbps, suficiente para dejar completamente 'offline' a la mayoría de organizaciones; e incluso provocar un ataque de enormes dimensiones o derivar en ataques de destrucción de servicio (DeOS, Destruction of Service), capaces de eliminar las redes seguras y de backup que utilizan las organizaciones para restaurar sus sistemas y datos tras un incidente de ciber-seguridad".

Para Chávez el IoT se está convirtiendo en un "interesante objetivo de ataque". Ser un entorno relativamente nuevo donde existe un enorme volumen de dispositivos pobremente configurados y peor mantenidos es una gran oportunidad para, en

"La diversidad de dispositivos personales, de fabricantes y su falta de estandarización en cuestiones de seguridad, hacen que muchos de ellos vengan de fábrica con vulnerabilidades fácilmente explotables"

Pedro Pablo Pérez, CEO de ElevenPaths

Proteger el dato, no el dispositivo

IoT por Internet of Things, pero también por Internet of Troubles o Internet of Threats. Es una chanza habitual en el sector. Se dice con convicción. Y es que la adopción masiva y acelerada del IoT no deja tiempo para casi nada y la seguridad, como casi siempre, queda por detrás de la operatividad.

La seguridad del IoT es un reto enorme. Hay propuestas que combinan segmentación, inteligencia de amenazas, automatización, filtrado de tráfico, pentesting persistente, control de accesos... y un sinfín de tecnologías para hacer frente a una amenaza.

Ante la variedad de dispositivos, hay quienes prefieren proteger el dato. No es un tema baladí. Según un informe de Cisco los miles de millones de dispositivos que formarán parte del Internet de las Cosas generan miles de billones de datos para 2018; cerca de 400 zettabyttes al año. Y esos datos deben protegerse. Asegurarlos pasas por identificarlos, autenticarlos y cifrarlos, de forma que se conviertan en datos íntegros y confidenciales.

Identificación y autenticación van de la mano. Su objetivo es asegurar que la información se está comunicando al dispositivo correcto y que la fuente es de confianza. Si no se hiciera uso de la autenticación un hacker podría comunicarse directamente con un sistema de alarma para desactivarlo o desbloquear una puerta y acceder a una casa.

La autenticación e identificación son, por tanto, necesarias, pero además de estar seguros de que nos conectamos con el dispositivo adecuado, conviene evitar escuchas, saber que no hay nadie espiando esas comunicaciones entre dispositivos o incluso pueda manipular esas conversaciones. Por eso el cifrado es la otra capa de protección importante para el IoT. Algoritmos de cifrado como AES pueden hacer que el dato sea inútil para los ciberdelincuentes

Pero el cifrado también debe aplicarse cuando el dato está en reposo. Y esto significa que los datos no sean modificados, y que no puedan ser leídos o entendidos por nadie sin las claves adecuadas.

primer lugar, acceder a datos fáciles de monetizar, y en segundo y mucho más peligroso, acceder a infraestructuras críticas.

Pablo Pérez, de ElevenPaths, dice que se puede clasificar los ataques al IoT en función del objetivo que persiguen, bien sea utilizar los dispositivos conectados como medio para atacar otro objetivo, o atacar al IoT en sí mismo. “Los ataques del segundo tipo seguramente serán menos frecuentes, pues es de esperar que se hayan concebido con la seguridad como propiedad fundamental, pero su impacto puede ser mayor, ya que uno de los objetivos puede ser las infraestructuras críticas de un país”, dice el ejecutivo.

Un perfecto caso de lo que los ciberdelincuentes pueden hacer con el IoT es Mirai, la botnet que el pasado otoño hackeo millones de cámaras para crear un ataque de DDoS. Lo que hizo único aquel ataque, que marcó un antes y un después, es la capacidad del gusano de extenderse rápidamente entre dispositivos conectados que se han desplegado sin ningún tipo de seguridad.

Pero Mirai fue sólo un ejemplo al que siguieron los ataques de Haijme y Devil Ivi, que no sólo utilizaban el mismo tipo de mecanismo para atacar dispositivos del IoT, sino que añadía herramientas que les permitían identificar diferentes dispositivos, seleccionar las contraseñas conocidas y explotar las vulnerabilidades adecuadas, comprometer el dispositivo y después utilizar su protocolo de comunicación para extender la infección a otros dispositivos.

Recomendaciones básicas de seguridad

Está claro que Interconectar dispositivos IoT y redes que utilizan diferentes grupos de especificaciones no solo genera ineficiencias, sino que incrementa los puntos en los que las vulnerabilidades de seguridad pueden existir. También ha quedado claro que en lo que respecta a la seguridad, el Internet de las cosas tiene mucho que evolucionar.

A veces nada más fácil que aplicar las mismas recomendaciones que para otros dispositivos. Ese parece ser el caso de Ricardo Lizarralde, de AT&T,

que habla de una necesaria actualización del software/firmware de los dispositivos conectados, seguido de contar con una formad e restablecer su estado original o no utilizar contraseñas predeterminadas. Además, “un dispositivo no debería ofrecer ningún servicio a la red que no sea necesario para soportar sus funciones principales; no debe tener puntos de entrada ocultos o conocidos que puedan ser atacados por el fabricante u otros y los fabricantes deberían proporcionar acceso online a los manuales de los operadores, así como acceso a las instrucciones de actualización. La información de soporte debería incluir una explicación clara de su mantenimiento a lo largo del ciclo de vida del producto”.

“Establecer la seguridad desde el diseño y concretar una normativa que obligue a los fabricantes a cumplir unas condiciones mínimas. Luego se tendrá que concienciar y educar a los usuarios para que hagan uso de esas características de seguridad incluidas y se preocupen de actualizar los dispositivos”, dice Josep Albors, de Eset.

Parecida es la opinión de Rodrigo Chávez, que apuesta por: Comprar dispositivos IoT que cumplan de fábrica con los requisitos de seguridad recomendados para el escenario al que vayan a estar expuestos; realizar configuraciones de seguridad adecuadas (cambio de contraseñas de fábrica como mínimo) y tomar las acciones recomendadas por los fabricantes; y restringir el acceso a los dispositivos IoT sólo a quienes sea estrictamente necesario, como las principales recomendaciones de seguridad.

"Utilizar 100,000 dispositivos IoT para lanzar un ataque DDoS ya no es solo una teoría; esta es la última prueba de que la innovación en el cibercrimen está prosperando"

Ricardo Lizarralde, Director Southern Europe Middle East and Africa, AT&T

La propuesta de Cisco es también muy clara. Para Eutimio Fernández, nada mejor que segmentar el tráfico IoT y el tráfico habitual de la red de TI; adoptar una arquitectura de seguridad integrada, que abarque las IT, OT y la nube, capaz de establecer políticas de seguridad una vez e implementarlas en múltiples ámbitos; automatizar. Nadie podrá gestionar los miles de dispositivos conectados a la red corporativa de forma manual, salvo con herramientas automatizadas (con funcionalidades de autoprotección y auto-reparación), inteligentes (basadas en políticas) y escalables; mantener actualizados los sistemas, implementar firewalls y sistemas IDS/IPS y aplicar ciber-inteligencia de extremo a extremo, utilizando la red como sensor para bloquear los ataques y como reforzador de las políticas de defensa; unificar los estándares, insistiendo a los proveedores para que los utilicen; convertir la seguridad en elemento básico de las implementaciones IoT desde el principio; si los dispositivos resultan comprometidos, activar procesos de respuesta frente a incidentes con tolerancia a fallos para proteger el negocio.

Junto con las recomendaciones de seguridad que se deben seguir, hay que tener en cuenta el uso de estándares, que permite no sólo una mejor interrelación entre productos, protocolos, formatos y especificaciones, sino menores riesgos de seguridad.

La primera de las cinco iniciativas más importantes en lo que respecta a estándares del IoT, según AT&T, es oneM2M, un consorcio de cerca de 230 vendedores, asociaciones industriales y agencias gubernamentales que desarrollan especificaciones

Enlaces de interés...

- TechRadar: Internet Of Things Security, Q1 2017
- Estudio 2017 sobre la seguridad de la movilidad y el IoT
- WP. Riesgos de IoT en las empresas
- Seguridad en el Internet de las Cosas

para una capa de middleware distribuido (dispositivo, pasarela, nube) que proporcione gestión de dispositivos y otros servicios comunes a todas las aplicaciones M2M.

Allseen Alliance agrupa a cerca de 185 miembros y promueve el Open Source AllJoyn Framework (inicialmente promovido por Qualcomm y ahora gestionado por la Fundación Linux), cuyo objetivo es permitir a los dispositivos descubrirse y comunicarse entre sí, y dar a los desarrolladores herramientas para crear aplicaciones IoT compatibles.

Open Internet Consortium es un consorcio de cerca de cien vendedores que promueven el IoTivity Project, un marco de código abierto (también alojado por la Fundación Linux) destinado a permitir la conectividad perfecta de dispositivo a dispositivo.

El Industrial Internet Consortium es una organización global de asociaciones público-privadas administrada por el Object Management Group. Cuenta con más de 200 miembros y fue creado para acelerar el desarrollo, adopción y uso generalizado de máquinas y dispositivos interconectados, analítica inteligente y personas en el trabajo.

Por último, la 3rd Generation Partnership Project (3GPP). Se trata de una iniciativa global que une a siete organizaciones de desarrollo de estándares de telecomunicaciones que desarrollan especificaciones que cubren tecnologías de redes celulares, incluyendo estándares de acceso por radio. Lanzado en 1998, el 3GPP se está moviendo ahora para abordar las cuestiones de telecomunicaciones, incluida la seguridad.

netskope

¿Cuántos servicios Cloud está utilizando su compañia?

¿Está seguro?

JORGE GIL

Director General de IDC España
Con más de veinte años de experiencia en el sector tecnológico, en los últimos siete Jorge Gil ha desarrollado un papel activo en el área de la transformación empresarial, ayudando y asesorando a compañías de diferentes tamaños, desde grandes corporaciones hasta medianas empresas y startups españolas, formando parte de varios espacios coworking de ayuda a emprendedores.
Jorge es socio fundador de Go2Do, consultora especializada en el asesoramiento y ayuda a la creación de empresas y desarrollo de estrategia de marketing. Anteriormente, ha ocupado los puestos de director general en Panda Security y de consejero y asesor en Afina y Epson respectivamente, además de dirigir el equipo de marketing y desarrollo de negocio a nivel global en Microsoft.

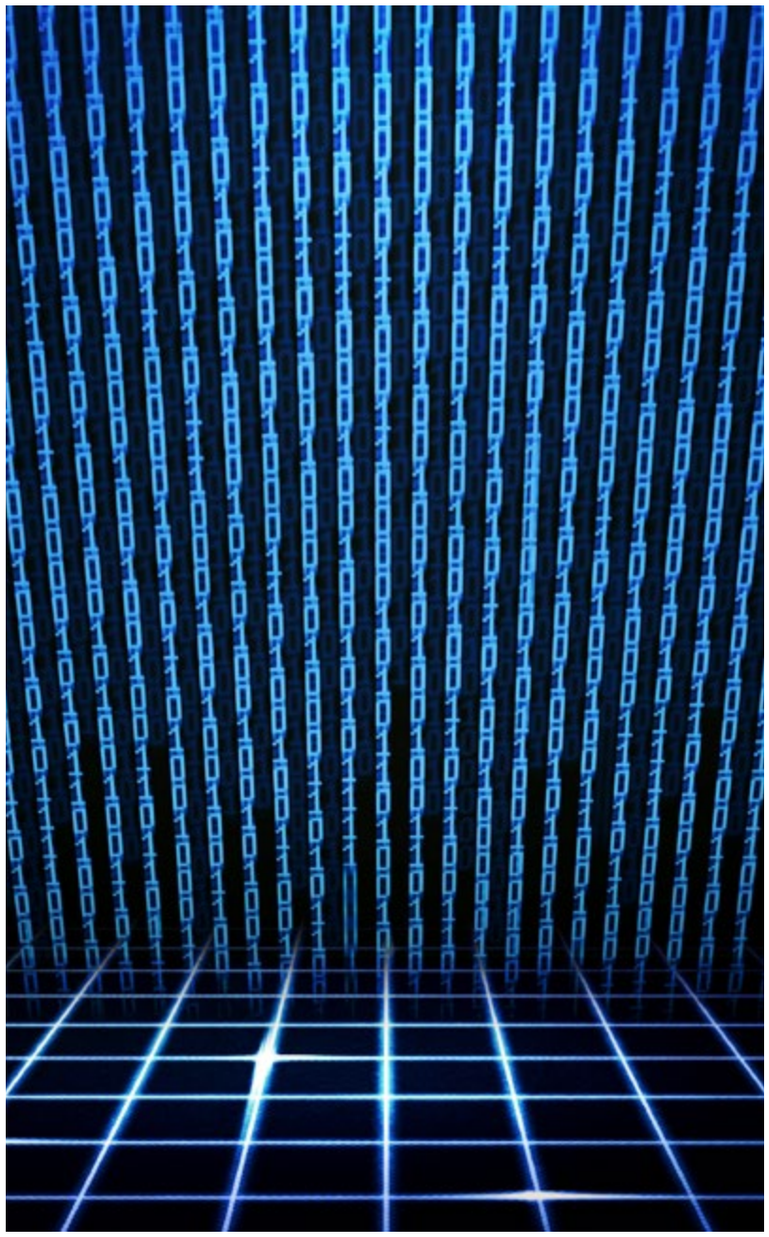
El actual contexto europeo de ciberseguridad

En IDC, estimamos que, para 2019, el 70% de las grandes empresas con sede en EE.UU. y Europa serán objeto de ataques de ciberseguridad. Este es un dato representativo de lo que constituye el actual contexto europeo de ciberseguridad, y consideramos que son tres los principales factores que ayudan a explicarlo:

1) El actual contexto de amenazas
El número de actores del crimen cibernético se está expandiendo y la sofisticación de los ataques que son capaces de lanzar está creciendo. Hoy, con frecuencia, asistimos a casos de Ransomware, y nos damos cuenta de la impresionante profesionalización de los hackers, siendo un ejemplo claro la existencia de marketplaces donde el hacking-as-a-service es un concepto ampliamente practicado que pone en evidencia el desarrollo y la madurez de las organizaciones criminales, que cada vez más comparten y evolucionan amenazas de forma colaborativa, como lo hacen las comunidades Open Source. Agravando esta situación, está el hecho de

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?



El hacking-as-a-service es un concepto ampliamente practicado que pone en evidencia el desarrollo y la madurez de las organizaciones criminales

que esto es un fenómeno global, disperso geográficamente, con lo que se vuelve todavía más difícil de combatir.

Esto tiene un efecto claro: el número de amenazas lanzadas sobre empresas e individuos está creciendo exponencialmente. Tomemos conciencia de que hoy son lanzados más de un millón de tipos de malware por día. WannaCry fue solo uno entre un millón de otros tantos virus. Esto significa que los enfoques tradicionales de seguridad ya no son efectivos para lidiar con esta escala de amenazas, siendo necesario cambiarlos. Será, por tanto, fundamental cambiar la mentalidad de las empresas y pasar de la reacción a la proactividad, asumiendo un papel importante el análisis del comportamiento y del contexto, así como adoptar una mentalidad de gestión del riesgo.

Además, la tecnología cobra aquí un papel fundamental, debiendo las organizaciones apostar por soluciones que les proporcionen capacidades de Automatización de procesos de seguridad, tanto los de prevención, como los de detección y de remediación; Integración: ser capaz de gestionar de forma integrada los distintos entornos de tecnológicos; Visibilidad: ser capaz de conocer el estado de seguridad del entorno tecnológico y ser capaz de identificar los impactos en procesos, servicios y activos de negocio.

2) La Transformación Digital de las empresas: Sabemos que la Transformación Digital es hoy una clave de la estratégia del 92% de empresas en España. En IDC la definimos como el proceso continuo a través del cual las empresas se adaptan a o generan cambios disruptivos en sus clientes y mercados mediante el aprovechamiento de competencias digitales para innovar en nuevos modelos de negocio, productos, y servicios que combinan las experiencias física y digital de sus clientes, mientras mejoran la eficiencia operacional y el desempeño organizacional.

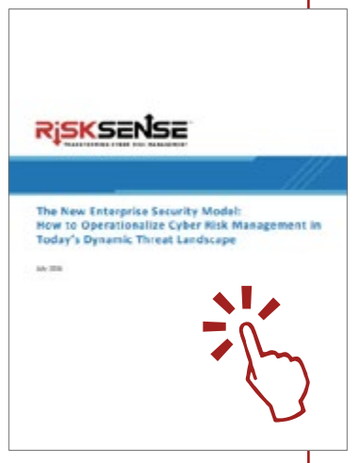
Es importante entender que este momento de transformación digital es motivado por el aparecimiento de empresas nativas digitales, que sabemos sobejamente quien son, y que están provocando una auténtica revolución en los modelos de negocio de las empresas tradicionales a través del uso de tecnología de la Tercera Plataforma. Por ello, para las empresas que se están transformando, entender y explorar la Tercera Plataformas es fundamental. Constituida sobre los pilares de Cloud, Big Data, Movilidad y Social, la Tercera Plataforma es donde hoy el gasto mundial de TI (y el español, por supuesto) está creciendo, lo que evidencia el uso que están haciendo las empresas.

Tenemos que reconocer que cada uno de los pilares de la Tercera Plataforma representa un factor de exposición al riesgo

Sin embargo, tenemos que reconocer que cada uno de los pilares de la Tercera Plataforma representa un factor de exposición al riesgo. Esto nos lo confirman todos los estudios y encuestas que hacemos en IDC: la seguridad es la principal preocupación de las empresas en su viaje de Transformación Digital. ¿Significa esto, entonces, que las empresas están bloqueadas? No. Hemos identificado dos grandes grupos de empresas: las pragmáticas, que ven que en la nube y en otros pilares de la Tercera Plataforma hay formas de seguridad que están alineadas con algunos de sus objetivos de negocio (o bien financieramente, o bien por el aporte de funcionalidades, agilidad y flexibilidad, o por otro beneficio); y las escépticas, que no confían en la nube. Pero, vemos que el escepticismo está cediendo posición al pragmatismo. Con el tiempo, la seguridad dejará de ser una preocupación tan grande como es hoy. No obstante, cabe a los proveedores de soluciones de seguridad proporcionar esa tranquilidad, garantizando, por un lado, la clareza de sus mensajes y demostrando cabalmente, por otro, las capacidades de sus soluciones.

EL NUEVO MODELO DE SEGURIAD EMPRESARIAL

Uno de los mayores retos de la ciberseguridad es cómo gestionar el volumen, la velocidad y la complejidad de los datos generados por las herramientas de seguridad de TI. Cuantas más herramientas, más difícil es el desafío a la hora de analizar los datos y priorizar los esfuerzos hacia la remediación de un ataque. En lugar de agregar más herramientas, las organizaciones necesitan implementar un nuevo modelo de seguridad empresarial más eficiente. Hablamos de la gestión del riesgo que utiliza el análisis basado en inteligencia para ayudar a las organizaciones a gestionar mejor su seguridad, acabar con los silos y mejorar las tareas de seguridad a través de la automatización.



Enlaces de interés...

- Un entorno Seguro: base para la Transformación Digital
- La tribuna de GDPR: Situación Actual
- 10 mitos alrededor de GDPR
- Guías de Inversión de Seguridad de IDC
- Cómo defender mi empresa híbrida de brechas y amenazas

3) GDPR:

Dentro del contexto regulatorio europeo, aunque cada sector posea su regulación específica, GDPR es el reglamento más importante e impactante para las organizaciones. Desde luego, por su urgencia. En 25 de mayo de 2018, el periodo actual de transición acabará y el reglamento será de carácter obligatorio. Sin embargo, en las conversaciones que mantenemos con las empresas, constatamos que hay un desconocimiento significativo sobre lo que representa e implica esta normativa.

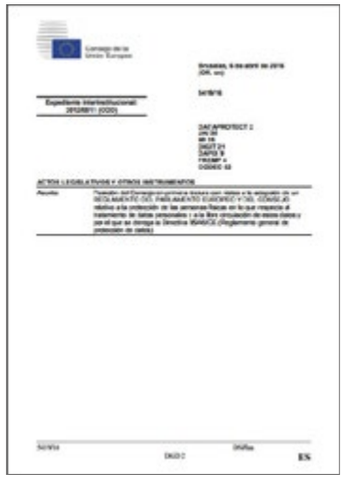
En primer lugar, no es una directiva, sino un reglamento. Una directiva es un acto legislativo global que reserva a cada país miembro la jurisprudencia para definir cómo implementarla. Un reglamento es un acto legislativo vinculante – todos los países tendrán que implementarla de acuerdo con las mismas reglas. En segundo lugar, reemplaza una directiva europea obsoleta, implementada en 1995, anterior a las empresas nativas digitales que han impulsado la creación de la actual economía digital.

Este reglamento destinase a la protección de datos personales (todos los que permitan identificar una persona) de los ciudadanos de la Unión Europea y codifica los derechos que a partir de hoy todas las entidades que procesen datos de ciudadanos de la UE están obligadas a respectar. A título de ejemplo, preconiza para el ciudadano el derecho a acceder a los datos que una entidad posee sobre uno mismo, el derecho al olvido, y el derecho al consentimiento explícito. Representa, por tanto, un aumento de los derechos de los ciudadanos europeos. Además, conlleva para las empresas un conjunto de nuevas obligaciones, como, por ejemplo, la comunicación obligatoria de las brechas de seguridad en 72 horas.

Las consecuencias para las empresas que no estén en conformidad con el reglamento GDPR son severas: podrán ser objeto de multas hasta el 4% de sus ingresos o € 20M, lo que sea más elevado. Podrán también ser prohibidas de procesas datos personales, lo que puede ser sinónimo de prohibición de facturar. Esto significa que la gestión del riesgo en las empresas va a cambiar definitivamente. Podemos, efectivamente, decir que habrá un antes y un después de la GDPR.

Ante este escenario polifacético y complejo, importa referir que el modelo de seguridad empresarial del futuro debe acomodar estos tres factores, esperándose que las empresas apuesten por racionalizar la tecnología y simplificar el propio entorno de seguridad, para que puedan ser más ágiles y efectivas las empresas a la hora de afrontar las amenazas, y por implementar el liderazgo y los modelos organizativos necesarios. En este sentido, la figura del director de seguridad de la información (CISO) se asume como fundamental, pues debe aunar tanto el conocimiento de la seguridad y de la regulación como del negocio, de tal forma que pueda entender los riesgos asociados a las nuevas oportunidades, influyendo en las decisiones que desde la alta dirección se lleven a cabo.

GDPR es el reglamento más importante e impactante para las organizaciones



La GDPR en Español, que no te la cuenten

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

Gestión del riesgo y la seguridad a la velocidad del negocio digital

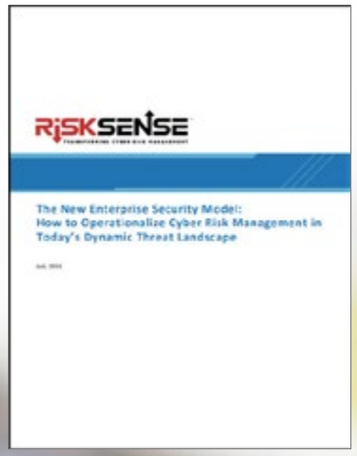
La Transformación Digital está cambiando el paisaje tradicional de gobierno y control de TI. Por un lado, la autoridad del responsable de las Tic se ve a menudo superada a favor de una mayor autonomía en el despliegue de nuevas tecnologías digitales. Por otro, el incremento de nuevos elementos (sistemas, dispositivos e incluso datos) genera problemas de escalabilidad para los que algunas soluciones de seguridad no están preparadas. ¿Cómo hacer frente a esta nueva realidad manteniendo bajo control la gestión del riesgo y la seguridad?

Cómo defender mi empresa híbrida de brechas y amenazas

Para acceder a recursos no autorizados, los hackers apuntan a cuentas de usuario privilegiadas, porque cuantos más privilegios más poder. Sin un control adecuado, un hacker con una sola cuenta privilegiada comprometida puede causar un daño generalizado e irreparable a la infraestructura de una organización, la propiedad intelectual y el valor de marca. En este documento se ofrecen las claves para proporcionar una protección amplia y coherente entre las credenciales y los niveles de acceso.

El nuevo modelo de Seguridad Empresarial

Uno de los mayores retos de la ciberseguridad es cómo gestionar el volumen, la velocidad y la complejidad de los datos generados por las herramientas de seguridad de TI. Cuantas más herramientas, más difícil es el desafío a la hora de analizar los datos y priorizar los esfuerzos hacia la remediación de un ataque. Este documento explora la emergente disciplina de la gestión de riesgos impulsada por la inteligencia como una respuesta a los ciberataques, las amenazas persistentes avanzadas y las fugas de información privilegiada.



La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

DANIEL LARGACHA

Director del Centro de Ciberseguridad de ISMS Forum
Head of CCG-CERT MAPFRE

Daniel Largacha Lamela es Global Control Center Assistant Director en MAPFRE, puesto en el que confluyen en el plano operativo los ámbitos tradicionales de seguridad física y seguridad de la información. Asímismo Daniel colabora en los subgrupos de Cyber-riesgos del CROF (Chief Risk Officer Forum de entidades aseguradoras europeas) y de transformación digital del EFR (European Financial Services Round Table).

La carrera de Largacha ha estado siempre vinculada a las Tecnologías de Información principalmente en el ámbito de la Seguridad, actividades que ha desarrollado en grandes empresas como Telefónica, Deloitte, y Azertia. Largacha es Ingeniero Superior en Informática por la Universidad Politécnica de Madrid y Máster en Dirección Aseguradora por el ICEA (Investigación Cooperativa de Entidades Aseguradoras y Fondos de Pensiones).

El estado de la ciberseguridad en España

La base del estado del bienestar en la sociedad actual está arraigada en pilares como la sanidad, la educación y la satisfacción de las necesidades básicas, pero además está también ligado necesariamente a algunos aspectos más básicos como el agua corriente, el suministro eléctrico que por lo esencial de su naturaleza (en la sociedad actual) pasan inadvertidas. Con la ciberseguridad, nos ocurre algo parecido, es una cuestión que está intrínsecamente relacionada con la tecnología, aunque a diferencia de lo comentado anteriormente, es completamente intangible y su ausencia puede pasar desapercibida o no apreciada hasta que realmente se hace evidente y necesaria.

Lo cierto es que, gracias a la adopción de la tecnología por parte de los individuos en los años 90

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

El concepto de seguro no existe y no es algo propio de la tecnología

con la aparición de Internet en los hogares, los ordenadores personales tomaron un nuevo hueco, motivando la primera burbuja tecnológica. En el ámbito de la ciberseguridad, la rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad. Algunos fabricantes atendiendo al riesgo potencial en el que nos encontrábamos inmersos, decidieron entonces cambiar sus estrategias de desarrollo de productos limitando su expansión y elevando el peso de los requisitos de ciberseguridad.

En la situación actual, el número de ordenadores ha aumentado geométricamente con la introducción de los smartphones, tablets, dispositivos IoT (que entran dentro de lo que se entiende por un ordenador), hasta el punto de que en los países desarrollados se ha pasado de uno por hogar a más de uno por persona. Esta tendencia ha despertado el interés de todos los sectores, cuestión que podemos ver en la “smartización” de bienes de consumo no vinculados históricamente con la informática, como por ejemplo los electrodomésticos (neveras, lavadoras…), automóviles, etc.

Sin embargo, en el ámbito de la ciberseguridad, aunque también se ha despertado cierto interés, mejorando en términos relativos, el crecimiento no ha seguido la misma proporción, y su evolución no ha ido necesariamente en la misma medida que la tecnología. Para ayudarnos a entender bien el escenario vamos a exponer cuales son los principales factores que influyen sobre este:

- **El concepto de seguro no existe y no es algo propio de la tecnología.** En muchos ámbitos no hablamos de ignífugo o impermeable sino realmente de resistente al fuego o resistente al agua. En la tecnología hay que partir de la base que el software es imperfecto per se, por lo que nunca podemos asegurar con certeza que un sistema es seguro.
- **Mayor exposición:** la aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software (imperfecto) aumenta la posibilidad de éxito que tendría un potencial atacante.
- **La falta de equilibrio que existe en escenarios de proteger versus atacar.** La globalización y la conexión desde cualquier punto del mundo muestra un escenario desigual a la hora definir estrategias o medidas de protección frente a posibles ataques.
- **Aumento de tamaño de la amenaza, debido principalmente a dos factores.** El aumento de los “actores” que destinan sus esfuerzos a atacar y la mayor sofisticación de estos ataques.

A todos estos factores además hay que añadirle el más importante, y es la dependencia actual que tenemos tanto la sociedad en su conjunto, como

DOLPHINATTACK, O LOS FALLOS DE SEGURIDAD DE SIRI, ALEXA O GOOGLE NOW

Se trata de susurrar, de hablar tan bajito que el oído humano no lo detecte, pero sí los micrófonos de los dispositivos móviles. Se trata de hablar por debajo de los 20kHz. Después de esto basta con decir "activar modo avión" para que el usuario quede desconectado de la red; o susurrar la dirección de una página web para acceder a una que pudiera ser maliciosa. Por ahora es un estudio, una prueba de concepto, pero quién sabe.

> La aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software aumenta la posibilidad de éxito que tendría un potencial atacante

las personas de manera individual sobre las tecnologías de información. La tecnología juega hoy un rol crítico en todo lo que hacemos en nuestro día a día, y nadie es ajeno a ello. Desde que nos levantamos y encendemos la luz del dormitorio, hasta que bebemos el último vaso de agua. Tanto gobiernos como empresas son conscientes de la sensibilidad del escenario actual, y desde ambos frentes se trata de mejorar lo máximo posible este escenario, que pasa inexorablemente por sensibilizar a los principales grupos de interés (ciudadanos, accionistas, consumidor, empleados… etc.).

La situación actual requiere el compromiso por todas las partes, gobiernos, empresas y la sociedad. La comprensión y aceptación de la situación es uno de los factores críticos de éxito. El otro es el consenso de los compromisos en seguridad que sean necesarios acometer. Un elemento catalizador que puede favorecer la aparición y persistencia de estos factores críticos de éxito es el papel que juegan las asociaciones como el ISMS, ya que pueden acercar las posturas de éstos, así como facilitar recursos, actividades, o capacidades desde una posición más neutra que facilite el entorno de colaboración.

¿Te avisamos del próximo IT Digital Security?

La rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad

Existen tres pilares sobre los que los que se puede cimentar una mejora sostenible del escenario actual:

- **La mejora de la capacidad de las organizaciones: aumentando la capacidad de detección y prevención ante un ataque para una entidad, es un aspecto crítico que puede permitir el bloqueo o minimización del ataque.** Para este punto la colaboración entre entidades en la compartición de información de eventos que puedan ser dañinos posibilita que el resto de entidades puedan estar preparadas ante eventos similares.
Otro factor que afecta directamente a la capacidad de reacción de las organizaciones tiene que ver con los planes de respuesta y gestión de crisis ante incidentes de seguridad. Estas situaciones requieren de la toma de decisión de alto calado, en periodos de tiempo críticas, una buena preparación de estos escenarios minimiza los impactos que pueden tener los incidentes de seguridad en las organizaciones.
- **El fomento de la seguridad: tanto en la sociedad en su conjunto, tanto a individuos como organizaciones empresariales.** La creación de escenarios de colaboración a través de los cuales las organizaciones puedan compartir sus experiencias y necesidades con otras organizaciones, de forma que se optimicen esfuerzos tanto internos como externos, potenciando su capacidad de influencia en la sociedad.
- **La capacitación y especialización de profesionales: enfocados en la seguridad de la tecnología.** Tanto universidades, como entidades privadas deben de facilitar a la sociedad la creación de perfiles con capacidad suficiente, que abarquen todos los ámbitos, desde los perfiles más técnicos, pasando por perfiles de especialistas en procesos y gestión, hasta perfiles directivos.

Enlaces de interés...

- ISMS Fórum
- Incibe

#ITWEBINARS

it Digital Security

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

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

Registro

Martes, 28 de noviembre – 11:00 (CET)

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

Registro

PABLO FERNÁNDEZ BURGUEÑO

@Pablofb

Abogado y socio en NevTrace y Abanlex

Pablo es jurista especializado en ciberseguridad, derecho del entretenimiento y modelos de negocio basados en el uso de blockchains. Es abogado en ejercicio, fundador de Abanlex y NevTrace, un laboratorio de criptografía aplicada desde el que realiza investigaciones sobre big data contra la ciberdelincuencia.

Seguridad Informática y previsiones de futuro

para el sector financiero

El sector financiero y bancario se enfrenta principalmente a los desafíos derivados de los avances informáticos y, en especial, a los vinculados con fintech, blockchain y seguridad informática.

Las fintech son empresas que unen las finanzas y la tecnología para prestar servicios financieros a los usuarios a través del uso de sitios webs y aplicaciones móviles haciendo extraordinariamente fáciles operaciones tales como la inversión en empresas o en proyectos de terceros, el cambio de divisas, las transferencias internacionales o el envío de dinero entre personas. Sus creadores emprenden nuevos modelos de negocio basados en la automatización de procesos sobre los pilares de la informática, la posibilidad de replicar acciones y la escalabilidad del producto.

El sector financiero y bancario también se enfrenta al reto surgido del nacimiento de soluciones basadas en la tecnología blockchain. A partir de esta se derivan las monedas virtuales, como el Bitcoin o el Monero y los smart contract, que permiten la creación de sistemas monetarios alternativos y la programación del dinero, respectivamente.

Gracias a la tecnología blockchain es posible mantener un libro contable único cuyo contenido se encuentra repetido íntegramente en diferentes ordenadores conectados. En la blockchain pueden escribirse transacciones monetarias, códigos informáticos o simples cadenas de caracteres alfanuméricos.

La confianza que se deposita en las anotaciones que se escriben en la blockchain se ve reforzado por la siguiente norma: aquel ordenador que trate de editar o borrar alguna de ellas es inmediatamente expulsado de la red. Esta garantía de integridad es la que ha permitido que determinadas blockchains, como la de Bitcoin, se abriera a Internet y se mantenga de forma simultánea en decenas de

Compartir en RRSS

La tecnología avanza mientras el sector financiero trabaja para conseguir integrar y mantener medidas suficientes de seguridad informática para combatir los ataques constantes y masivos que sufre

miles de ordenadores no identificados alrededor del mundo. A más ordenadores conectados, mayor es la seguridad que ofrece.

La tecnología avanza mientras el sector financiero trabaja para conseguir integrar y mantener medidas suficientes de seguridad informática para combatir los ataques constantes y masivos que sufre.

Estos ataques son a veces dirigidos contra las entidades con la finalidad de sustraer grandes cantidades de dinero o, aún más valioso, de secretos comerciales o datos de carácter personal; otras veces son el resultado de infecciones aleatorias sufridas por los clientes o los propios empleados de las sucursales.

Las estafas informáticas representan casi siempre más del 80% de los delitos informáticos, según los últimos informes anuales publicados por la Fiscalía General del Estado, aunque hay otra gran variedad de acciones ilícitas que llegan a los tribunales. La implementación inmediata de medidas de seguridad técnicas específicas, para evitar las brechas de seguridad o las consecuencias de estas, es exigida por las diferentes normas que ya están en vigor como, por ejemplo, la Directiva NIS o el Reglamento General de Protección de Datos. Si bien ya están en vigor, la exigibilidad de las mismas comenzará en el año 2018, con sanciones por su incumplimiento con multas de hasta 20 millones de euros o de hasta el 4% de la facturación global del año financiero anterior, eligiéndose la cifra más alta.

Ante esta situación, las empresas del sector deben tomar decisiones estratégicas de transformación digital para aprender a convivir con la nuevas fintech, convertirse en una de ellas, comprar sus proyectos o invertir en ellos; desarrollar productos basados en blockchain, usar las monedas virtuales para optimizar los tiempos y mejorar los procesos y comenzar a programar smart contracts con el objetivo de programar el dinero; y adecuarse de manera urgente a las nuevas normas en materia de seguridad informática invirtiendo en personal legal y téc-

A partir de 2016 se obliga a un banco español a indemnizar a un usuario que sufrió un ataque informático en su ordenador

nico capaz de evaluar el impacto de los potenciales ataques, seleccionar las soluciones adecuadas e implementarlas de manera eficiente y resiliente.

Así son los ataques informáticos que sufre el sector financiero

Los ataques informáticos que sufre el sector financiero son dirigidos o aleatorios, persistentes... Debería bastar con saber que los ataques son constantes, tanto a entidades como a clientes, que muchos de ellos son exitosos y que la mayor parte de los afectados ni siquiera se dará cuenta de haberlos sufrido hasta ver las consecuencias. Con esta información, las medidas de seguridad implementadas deberían ser suficientes, pero no lo son.

Las estafas, por poner un ejemplo, representan el 80% del total de los delitos informáticos denunciados en España, alcanzando la cifra anual de 17.328 en el periodo 2014 – 2015, según publica en su Memoria Anual de 2016 la Fiscalía General del Estado. Esta sólo es la punta del iceberg o la cresta de una ola de ciberataques que convierten a España en el país más infectado del mundo en determinadas versiones de malware, como es en el caso del ransomware CryptoLocker, que exige rescates en bitcoins a los usuarios afectados.

En el ámbito de la seguridad, el Reglamento General de Protección de Datos, que entró en vigor en 2016, exige a los bancos y las empresas fintech la implantación de medidas de seguridad acordes a los resultados de un análisis de riesgo denominado Evaluación de Impacto. El cumplimiento de esta norma europea de aplicación directa será exigible a partir del 25 de mayo de 2018, por lo que es ahora el momento de adecuar los procesos a lo que ya es imperativo. El Reglamento trae algunas consecuencias interesantes para los casos de incumplimiento como son, por ejemplo, estas dos: se establece una obligación para que las empresas comuniquen, a través de un medio de comunicación social, los ataques informáticos que sufran y que hayan podido afectar a los datos de los usuarios, salvo si pueden comunicarse con ellos directamente; y las sanciones por incumplimiento podrán suponer multas de hasta 20 millones de euros o de hasta el 4% de la facturación global del año financiero anterior, eligiendo la cifra más alta.

Una novedad interesante, también en materia de ciberseguridad, es la lograda en 2016 a través de los Tribunales españoles por la cual se obliga a un

PASADO, PRESENTE Y FUTURO DEL RANSOMWARE

Puede que no sea la más peligrosa, pero no cabe dura de que el ransomware es una amenaza formidable, y lo es porque funciona, y funciona porque son muchos, demasiados, los que pagan. En cualquier caso, existe y a pesar de los esfuerzos por parte de las empresas y de la industria en general para impedir las infecciones o saber reaccionar adecuadamente cuando se produzcan, los ataques de ransomware existen... y seguirán existiendo.

según se indica en la sentencia, la entidad podía haber aplicado y no aplicó medidas de seguridad técnicas suficientes que impidiesen la consecuencia. Aquí es donde empresas como F5, Exclusive, ESET o VMware, principalmente, están apostando por ofrecer sistemas que permiten al banco analizar el dispositivo con el que se está conectando el usuario para detectar malware instalado, para cifrar los datos o, en los servidores del operador, para implementar sistemas de micro-segmentación con el objetivo de detener intrusiones o evitar consecuencias mayores.

Previsiones de futuro para el sector financiero

Estamos en un momento de la historia en la que el avance tecnológico permite la creación de sustitutos eficientes a los operadores tradicionales.

Enlaces de interés...

- La digitalización aumenta los riesgos de fraude
- Criptodivisas, el próximo gran objetivo de los hackers
- W Ciberseguridad y Servicios financieros
- W Las claves de la ciberseguridad de los servicios financieros
- V F5 y Abanlex hablan sobre la responsabilidad del ciberfraude bancario

Las entidades del sector financiero tienen la misión de aprender en poco tiempo lo que sucede a su alrededor

banco español a indemnizar a un usuario que sufrió un ataque informático en su ordenador. El cliente fue infectado con el troyano Citadel, que es un tipo de software malicioso que extrae contraseñas, gracias al cual le fueron sustraídos más de 55.000 euros de su cuenta bancaria. El juez ordenó al banco entregar dicha cantidad al cliente puesto que,

Los nuevos operadores ofrecen sistemas basados en la economía colaborativa. Se benefician de las posibilidades que abren las redes que permiten conectar personas para que, entre ellas, se transmitan todo tipo de información digital. Hasta ahora, el mensaje era texto; ahora, el mensaje puede ser dinero.

Las entidades del sector financiero tienen la misión de aprender en poco tiempo lo que sucede a su alrededor. Si siguen mejorando lo que tienen, van a ser fagocitadas en breve por las que crean algo mejor. Pueden mantenerse estáticas para analizar la situación y actuar después, como buenas fast followers. Quizá sea suficiente, aunque quizá lo recomendable sea experimentar y convertirse en lo que se demanda o comprar a las que ya han nacido convertidas.

El surgimiento de las fintech, la innovación con blockchain y la lucha por la ciberdefensa ponen de relieve una realidad: el mundo financiero ya ha cambiado.

NO SOLO it

Psicobusiness

Llamar al orden sin conflictos y con efectividad

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

En la nube

La gestión de nuestros activos virtuales

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

Tecnología y Negocio

Sin digitalización de la PYME española no habrá paraíso ni tierra prometida

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

Desde mi análisis

RPA, el acrónimo que toda empresa debería conocer

Por Fernando Maldonado, analista asociado en Delfos Research

Transformación Digital

El dato y la Transformación Digital

Por Ramón Puchades, profesor colaborador de MBIT School

Asier de Artaza Azumendi
Director de
www.yesmanagement.es

Llamar al orden, sin conflictos y con efectividad

Emociones del momento, relaciones de tiempo; una materia compleja

RESOLUCIÓN DE CONFLICTOS

CLICAR PARA VER EL VÍDEO

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

"¡Otra vez igual! No puedo con él. ¿Cuántas veces se lo habré dicho? Así no podemos seguir; no sé si seguir dejándolo estar o… ¡poner firme a Julián!"

Ejem, quién no se ha visto alguna vez así, o, mejor dicho, habitualmente así. No hay duda de que los conflictos tienden una tendencia natural a ser evitados. Porque realmente tener que llamar al orden a una persona es un tipo de conflicto. En fin, algo incómodo y, a su vez, bonita materia en el desarrollo del liderazgo individual.

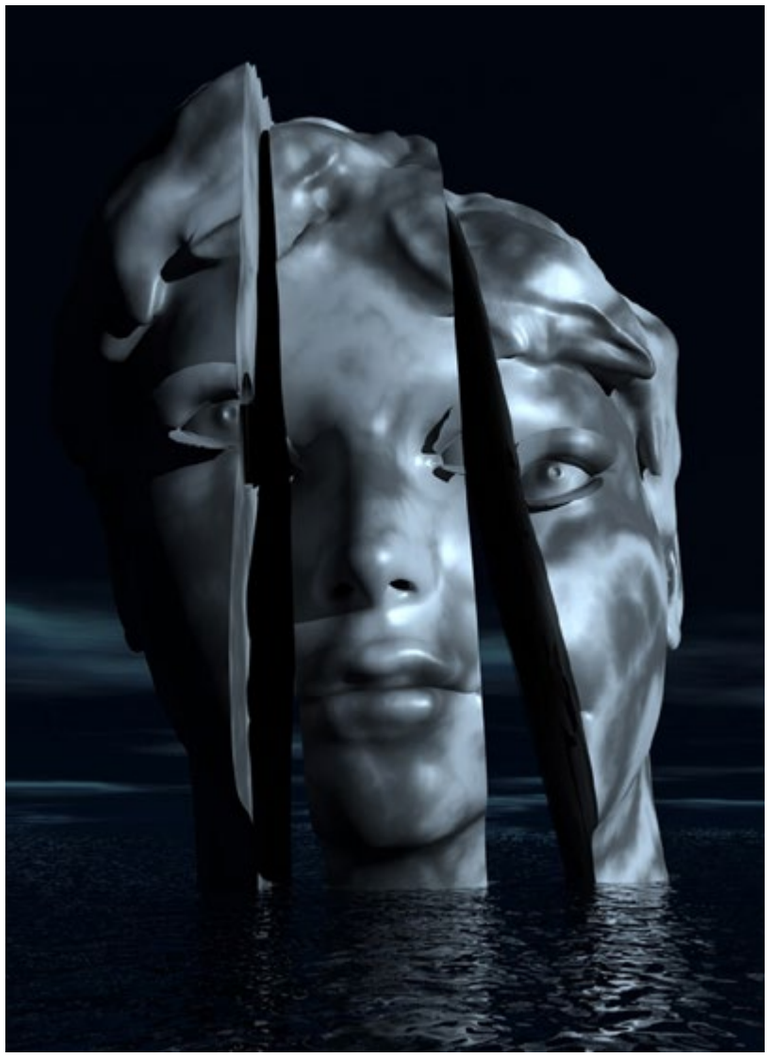
En este artículo pasaremos ligeramente por algunas cuestiones comunes a la resolución de conflictos, de los que ya hablamos en algunos de los primeros números de esta publicación. Pero, en fin, ahí están, otra vez, como protagonistas, las emociones negativas, la comunicación ineficaz, la empatía y asertividad, la falta de inteligencia de emocional y de gestión de los errores cognitivos. Así que, a lo dicho, vayamos directos al proceso.

Nos encontramos que el empleado o compañero sigue actuando de una manera incorrecta con las normas claramente conocidas en nuestra organización o de las obligaciones de su trabajo; vamos que está pasando en

cuestiones que no merecen discusión. Matizo el concepto de normas u obligaciones claramente conocidas ya que ésta es la condición preliminar. Si a alguien le vamos a llamar al orden debemos de estar seguros de que o son "cosas de cajón" o claramente transmitidas, porque, si no, estaríamos hablando de nuestras expectativas respecto a las personas, y nos meteríamos en el complejo mundo de los principio y valores personales de cada uno.

Hechas estas aclaraciones, ahora sí, nos metemos con el proceso que debemos llevar a cabo. El primer punto es trasladar a esta persona los hechos acontecidos. Atención, ¡los hechos! Es habitual entrar a las opiniones arbitrarias que uno tiene sobre lo acontecido, que suelen, además, ir acompañadas del uso del verbo ser en vez del verbo hacer, estar u otro no identitario y estigmatizador.

Por ejemplo, le llamamos al orden: "Julián no puedes llegar siempre a las 9:25, cuando la hora de entrada es a las 9; qué quieres que te diga, eres un jeta y un informal"; y remato "que no vuelva a pasar, aquí entramos todos a las 9 en punto."



Vale la típica chapuza. ¿Cómo se debería hacer de forma eficaz con un poco de aplicación de Psicobusiness, la psicología al servicio del negocio? "Julián, en los últimos seis meses, tu entrada a la empresa ha sido 25 minutos más tarde de la hora y ello ha generado que tus compañeros hayan tenido que trabajar muy agobiados para cubrir tu puesto de atención al cliente, no atendiendo de la forma adecuada y recibiendo dos bajas de clientes".

Como vemos, en la segunda forma no se aplica el verbo ser, no se le identifica, no se le condena a ser un jeta, y no hacemos juicios ni generamos opiniones. Nos centramos en los hechos, y es que la evidencia es inquebrantable. Así estamos siendo profesionales desde tierra firme. ¿Por qué desde tierra firme? Porque, por un lado, no hemos descalificado a nadie, que en el mismo momento nos quita posición. También nos da profesionalidad el trabajar no sacando una conclusión subjetiva del hecho, le asignamos el "eres un jeta", y por tanto cada uno puede sacar su conclusión subjetiva y ponerse a discutir sin llegar a ningún puerto. ¿Qué es ser un jeta y qué no? ¿Cuánto hay qué hacer para

whitepapers

EL OMNINEGOCIO:
ENFOCADOS EN EL CLIENTE

En esta encuesta anual a 400 de los mayores fabricantes y minoristas del sector de bienes de consumo del mundo se examinan las prioridades de los directivos de las empresas de este sector y los retos en los próximos dos años. El informe también contrasta los resultados seleccionados con las conclusiones de una encuesta global a 7.100 consumidores sobre sus conductas y preferencias a la hora de comprar.

ganarse el adjetivo? ¿Quién eres tú para faltarme al respecto…? En fin, tierra resbaladiza, fea y, sobre todo, nada eficaz.

Vayamos al segundo punto que muestra claramente el ejemplo. Los hechos van acompañados de la trascendencia de los mismos. Los hechos en sí mismos son meramente descriptivos, "llegas siempre a las 9:25"; realmente no tiene mucho valor, mucha fuerza. El añadir a la frase "…y ello ha generado que tus compañeros hayan tenido que trabajar muy agobiados para cubrir tu puesto de atención al cliente, no atendiendo de la forma adecuada y recibiendo dos bajas de clientes", especifican la trascendencia del hecho, el efecto negativo que han producido, les dan valor y, sobre todo, les dotan de carga emocional.

TÉCNICAS DE ASERTIVIDAD

CLICAR PARA VER EL VÍDEO

Analicemos hasta aquí, por qué las consecuencias deben seguir a los hechos. Para producir el cambio en una persona, es obligatorio que la persona haga suya la cuestión, si no, casi estaremos hablando para la pared, o el efecto será momentáneo por el malestar emocional que le causa tu cabreo, pero no la cuestión a resolver. Y para qué alguien haga algo suyo tiene que provocarle una emoción, acordémonos que sólo nos movemos por emociones, emotión igual a e motion, e motion igual a motion que, a su vez, es motor, el motor que nos mueve a la acción.

Para producir el cambio en una persona, es obligatorio que la persona haga suya la cuestión, si no, casi estaremos hablando para la pared

Así que debemos reparar en la condición indispensable, que es que la persona se cargue de emoción sobre el hecho, generando una asociación emoción-hecho que le produzca una fuerza interna que trate de rechazar la realización de ese hecho.

Seguimos, para anclar mejor este aspecto. Llega el tercer punto, en el que se le pide a la persona que haga una reflexión sobre qué le parece esto que se le acaba de trasladar. Se trata de que lo haga suyo, de ver hasta qué punto se está consiguiendo su sensibilización. Una

Discover the New

Una nueva dimensión para la tecnología

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

Patrocinado por MICRO FOCUS

Cuando tenemos a la persona dispuesta, comprendiendo lo que ocurre y con interés por el cambio es cuando tenemos que aterrizarlo bien

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

vez que él se haya explicado de forma suficiente sobre cómo ve las cosas, cómo ve que eso que ha hecho no le gusta por los perjuicios que ha creado.... se llega al cuarto punto.

Estamos en el aviso de penalización, es decir, no sólo estamos dialogando y él está ganando una actitud positiva para que no vuelva a pasar, sino que le advertimos que si vuelve a pasar tendrá una sanción (del tipo que tengamos disponible, siempre hay algunas). Pero que no es nuestra intención, sino que lo que buscamos es que todo funcione, estemos todos a gusto y aportemos a la empresa en lo que nos toca.

Finalmente, se debe establecer un plan para conseguir el cambio. Esto sí que no se hace nunca, y fijémonos que poco sensata es la práctica habitual: cojo, te echo la bronca, que incluso puede conllevar ataques a la persona más directos o indirectos, y ya está todo.

Bueno, pues no, ahora que tenemos a la persona dispuesta, comprendiendo lo que ocurre y con interés por el cambio es cuando tenemos que aterrizarlo bien.

El plan debe realizarlo él, nosotros solo seremos unos espectadores que peritaremos y validaremos o no su plan, nunca metiéndonos en la cuestión del mismo, el problema es de él, no nuestro, es de él y no de otras partes de la compañía. Este último aspecto es importante también, el foro es él, su comportamiento, no el que si la empresa tendría que poner horarios flexibles, o los compañeros organizarse de otra manera si no está el.

Llegados a un plan final, desarrollado por él, consistente en varias acciones que nos parecen que resolverán el tema, sólo nos quedará el último punto, la revisión periódica y constante de sus resultados, hasta que el nuevo comportamiento queda instaurado. Así que la reunión debe terminar, con un "muy bien, parece que tienes; el plan el viernes que viene nos volvemos a ver, Julián". it

Enlaces relacionados

- V Resolución de conflictos
- V Técnicas de asertividad
- V Técnicas de sintonización de Nicholas Boothman
- W La verdad sobre el ecosistema de IoT
- W Inspiración para PYMES: cómo transformar 4 sectores clave
- W La reinvención digital: una oportunidad para España

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

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

La gestión de nuestros activos virtuales

Las empresas de hoy operan en un mundo virtual; desde las máquinas virtuales hasta los chatbots, pasando por Bitcoin, lo físico se ha convertido en el modus operandi del pasado, y la respuesta a los cambios que se están produciendo ha llevado incluso a acuñar su propia denominación: la transformación digital

Desde el punto de vista de la operativa de sistemas, esto se ha traducido en un mayor uso de la nube, donde organizaciones de todo tipo están colocando aplicaciones, servidores virtuales, plataformas de almacenamiento, redes, servicios gestionados y otros tipos de activos virtuales, cuya gestión puede resultar mucho más compleja que la de los activos físicos convencionales en un centro de datos, y cuya administración y control de costes son muy distintos de sus equivalentes en el mundo material. Las dificultades aparecen con frecuencia a la hora de monitorizar y evaluar las inversiones en cloud computing, gestionar los costes asociados y aumentar su eficiencia. Los responsables de sistemas deben hacer un seguimiento de los gastos y el uso de los activos en la nube, comparar costes con presupuestos, y llegar a las conclusiones necesarias para establecer políticas apropiadas de buen gobierno.

El modelo de gasto de explotación -OPEX- en cloud computing debe ir acompañado de un enfoque de gestión integral que permita monitorizar y actuar en entornos muy heterogéneos, en los que es probable que se utilicen servicios cloud de múltiples fabricantes y proveedores de servicios gestionados, y donde cada empresa necesitará administrar sus servicios desde el punto de vista del consumo. Este último aspecto incluye todo, desde los servicios necesarios para cada aplicación has-

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.

La analítica permite recalibrar los costes, comparando los gastos planificados con los gastos operativos reales

ta los recursos informáticos concretos requeridos en cada caso, como el almacenamiento o las bases de datos. Para poder alcanzar el éxito en este nuevo modelo, las compañías deben marcarse, entre otros, los siguientes objetivos:

- Visibilizar de forma permanente el inventario cloud en entornos reales.
- Visualizar los costes actuales y los costes previstos frente a los referentes del sector.
- Establecer y aplicar puntos de control para el governance mediante políticas técnicas y financieras.
- Detectar y responder de manera proactiva a las variaciones y desviaciones en los costes y la operativa de la actividad cloud.
- Adquirir ventajas operativas mediante capacidades avanzadas en analítica y computación cognitiva.
- Simular cambios en inventarios, objetivos de gasto y prioridades operativas antes de la toma de decisiones.
- Gestionar políticas mediante el asset tagging -etiquetado de activos- para distintos proveedores y servicios.
- Identificar y mantener informada a la alta dirección sobre ineficiencias y oportunidades de ahorro de costes.

Para alcanzar estos objetivos en entornos de sistemas híbridos será necesario disponer de información ágil, precisa y coherente para las organizaciones, sus directores de sistemas, directores financieros, controllers, y responsables de infraestructuras y operativa, que podría facilitarse, preferentemente, mediante un cuadro de mando tipo "panel único".

Una posible forma de contar con estas capacidades podría ser la explotación de una plataforma de intermediación de servicios cloud. Este servicio, tipo "plug & play", puede ser muy útil en la gestión del gasto y los activos en nubes híbridas, con indicadores visuales de rendimiento de dichos activos, y donde la analítica predictiva puede proporcionar recomendaciones que ayuden a definir prioridades de los cambios a implantar, según el nivel de impacto de cada uno de ellos. La analítica permite, además, recalibrar los costes, comparando

CÓMO DIFERENCIAR PROVEEDORES CLOUD

CLICAR PARA VER EL VÍDEO

it whitepapers

INFRAESTRUCTURA EN CLOUD

A partir de la encuesta realizada a más de 45 empresas y de entrevistas, tanto con compañías cliente como proveedoras, el informe de Penteo analiza las tendencias en relación con los servicios en la nube y, especialmente en la infraestructura, describiendo el grado de adopción en la empresa española, la previsión de crecimiento, los beneficios esperados y obtenidos, así como los principales drivers y barreras de adopción.

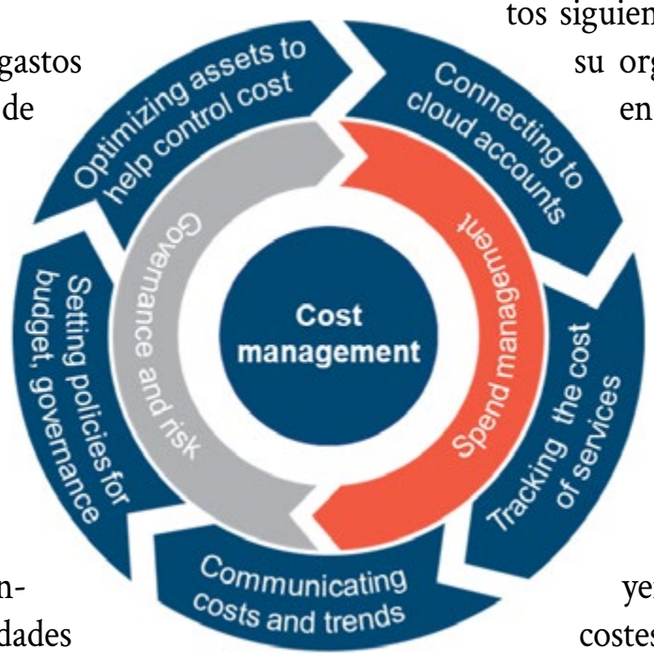
¿Te avisamos del próximo IT User?

Octubre 2017

La gestión del negocio desde una plataforma de sistemas virtual es otra historia. Aquí es donde debemos contar con habilidades, funcionalidades y herramientas avanzadas de gestión de costes y activos

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

los gastos planificados con los gastos operativos reales, y el catálogo de servicios, la estructura de precios, los motores de análisis y la compilación de las mejores prácticas de la industria simplifican la elección de proveedores cloud alternativos.



Pero la gestión del negocio desde una plataforma de sistemas virtual es otra historia. Aquí es donde debemos contar con habilidades, funcionalidades y herramientas avanzadas de gestión de costes y activos. Según Gartner, la transición a la nube conllevará una inversión asociada de más de un billón de dólares en sistemas informáticos durante los próximos cinco años, algo que convierte al cloud computing en una de las fuerzas más disruptivas en el sector TIC desde el inicio de la era digital. Valore los elementos siguientes si quiere asegurarse de que su organización esté lista para estos enormes cambios:

1. Establecimiento de políticas y umbrales de governance para cada servicio.
2. Conexión de la plataforma avanzada de gestión con todas las cuentas de servicios cloud.
3. Monitorización de los costes de todos los servicios, incluyendo los costes recurrentes y los costes por uso.
4. Control efectivo de los costes y el uso de los activos mediante motores de analítica de costes diseñados específicamente para ello.
5. Simulación y optimización de las acciones de control y compliance para un mejor control global de los costes.

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

Enlaces relacionados

- La transformación digital
- Una plataforma de intermediación de servicios cloud
- La invertión en TI por el pao a Cloud hasta 2020
- Ataques con exploits, de las amenazas diarias a las campañas dirigidas
- Informe Symantec sobre la seguridad en 2017
- Informe sobre la responsabilidad de las entidades financieras en el fraude
- La paradoja tras la experiencia del usuario con el criptoransomware
- 7 beneficios de un enfoque holístico de la protección de datos
- 4 formas de protegerse y recuperarse de ataques de ransomware
- Ciberrriesgos y reputación en las pequeñas empresas

Sin digitalización de la PYME española no habrá paraíso ni tierra prometida

Jorge Díaz-Cardiel
Socio director general de Advice Strategic Consultants

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

2017 no es 2013. En el primer semestre de 2013, la economía española todavía vivía en recesión y no empezó a ver la luz hasta la segunda mitad del año. Como dijimos en el Contexto Económico, Empresarial y Social de la Radiografía de la Pyme de Sage España, 2014 fue el año bisagra de la recuperación, con un crecimiento positivo anual del PIB del 1,4%. En 2015, España creció el 3%. Coinciden los Servicios de Estudios Económicos Nacionales e internacionales, con pocas diferencias de matiz. Y el crecimiento se repitió en 2016 (3,2%).

El programa de reformas del Gobierno de España, el peso –primero- de las exportaciones en la composición del PIB, y del consumo interno en la segunda fase de la recuperación, la caída de los precios del petróleo, la devaluación del euro, los aumentos de competitividad de la economía española vía reducción de costes laborales, la creación de empleo y la reciente nueva política del Banco Central Europeo son algunos de los parámetros del éxito de la salida de la crisis que ahora hay que consolidar.

El tejido empresarial español es pyme

La macroeconomía ha evolucionado favorablemente, por tanto, en los dos últimos años. Donde no ha habido cambios ha sido en la composición del tejido empresarial español: sigue estando compuesto mayoritariamente por pymes. Concretamente, el 99,88% de nuestras empresas son pyme (entre 0 y 249 asalariados) y, de ellas, el 97,6% facturan menos de dos millones de euros. En los últimos doce meses ha habido, al mismo tiempo, algunos cambios en la pyme. Primero, el sector de actividad: aumenta el peso del sector Servicios, hasta el 80,5%. También se incrementa la importancia de

la pyme para el empleo: del 62,9% se pasa al 66% de la fuerza laboral española soportada por la pyme. Esto es compatible con que haya aumentado la productividad de nuestras pymes un 2,21% debido a que las ventas globales han aumentado, pero el empleo total disminuyó: el valor añadido bruto (VAB) por ocupado de la economía española fue de 58.619 euros, por encima de los 47.485 euros de la UE-28. El comercio al por menor es donde más pymes se han creado y, de estas, son mayoría las que se acogen a la fórmula jurídica de autónomo.

Pymes y sociedad española tecnologizada

Un país económicamente formado por pymes, que soportan la mayor parte del empleo, se identifica fácilmente con la sociedad en la que vive. O, mejor aún, pyme y sociedad españolas se sienten muy reflejadas la una en la otra, como no podía ser de otra manera. La española es una sociedad cada más conectada en red: son 27 millones de españoles los que acceden regularmente a Internet, 1,45 millones más que el año anterior. Y la Banda Ancha Móvil (BAM) continúa siendo la tecnología clave en el avance de la Sociedad de la Información: en 2014, 21,44 millones de españoles accedieron a internet en movilidad, 4 millones más que en 2013. En 2015 y 2016, parecen ser mejores. Las redes sociales están para quedarse: su uso ha aumentado tres puntos hasta el 67,1 por cien.

El comercio electrónico es una tendencia imparable: Un total de 14,9 millones de personas han realizado alguna compra a través de internet en 2014, de los cuales 1,9 millones lo hicieron por primera vez el pasado año. Una de cada tres visitas a tiendas online se produce con dispositivos en movilidad. El comercio electrónico sube un 29,2% con respecto a un año antes, al tiempo que las ventas online españolas en el exterior aumentan un 44,6%.

Y la Administración electrónica, tal y como estaba previsto en la Agenda Digital del Gobierno de España, ha seguido avanzando a buen ritmo: el 76,5 por cien de los trámites realizados por la Administración General del Estado (AGE) han sido por vía electrónica, que ha calculado unos ahorros para ciudadanos y empresas, en 2013 y 2014, de 31.000 millones de euros, más otros 22.000 millones en 2015 y 2016.

La Sociedad de la Información sigue avanzando en España: el 74,8% de los hogares con, al menos, un miembro de 16 a 74 años dispone de ordenador. Y el 74,4% de los hogares españoles tiene acceso a la Red, frente al 69,7% del año anterior.

2015 y 2016 fueron años de mayor dinamismo empresarial

En 2014 y 2015 se crearon más sociedades mercantiles (un 0,8% más) y aumentó la cifra de negocio empresarial (+1,9%). La confianza de los empresarios también

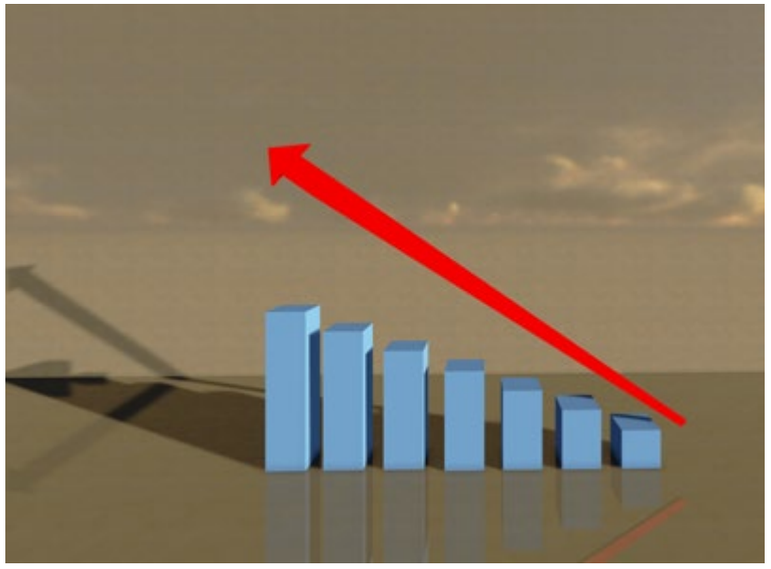
La macroeconomía ha evolucionado favorablemente en los dos últimos años. Donde no ha habido cambios ha sido en la composición del tejido empresarial español: sigue estando compuesto mayoritariamente por pymes

ha mejorado: El Índice de Confianza Empresarial Armonizado (ICEA) en el segundo trimestre de 2017 aumenta un 4% respecto al primer trimestre de 2016; todos los sectores económicos analizados presentan una mejora de la confianza respecto al trimestre anterior.

También analizamos los componentes del entorno empresarial, considerando las pymes que los de mayor importancia en el año 2016 fueron la demanda de sus productos (con un 58,5% de las respuestas con una importancia alta), el entorno macroeconómico (con un 43,7%) y la morosidad (con un 42,7%).

Aumentan las exportaciones, pero las importaciones lo hacen más

En 2016, España siguió exportando, aunque hubo un crecimiento mayor de las importaciones, fruto del aumento de la demanda interna y la mayor inversión. La Unión Europea siguió siendo el destino geográfico más importante de nuestras exportaciones, con el 63,4% del total. En términos sectoriales exportadores sobresalió el sector del automóvil, cuyas ventas al exterior aumentaron un 6,2% y supusieron el 14,8% del total.



Cataluña fue la Comunidad Autónoma que más contribuyó al crecimiento anual de las exportaciones: sus exportaciones representaron el 25,1% del total y crecieron un 3,1%.

Sobre las empresas exportadoras, en 2016, su número descendió un 2,2% y se situó en 147.731 compañías. Un dato que, sin embargo, se vio compensado por el impulso experimentado por las empresas que exportan regularmente (cuatro años consecutivos). En ese año, la cifra ascendió a 45.842 empresas, lo que supuso un 11,4% más que el año anterior y un nuevo máximo histórico. Y, sobre las pymes exportadoras, un análisis más detallado muestra cómo la variación más importante se ha producido entre las empresas que venden menos de 5.000 euros. En 2013, apenas había 6.548, un 4,3% del total; un año después, la cifra creció hasta las 9.058, un incremento del 38,3% o que 2.510 pymes lograron concatenar en 2014 cuatro años seguidos exportando.

Vías alternativas a la financiación bancaria para pymes

La financiación bancaria sigue siendo la principal forma de financiación de las empresas y pymes españolas. Pero también han surgido nuevas formas de financiación alternativa. El Gobierno ha querido recoger esas figuras en la Ley para el Fomento de la Financiación Empresarial y en la Ley de Entidades de Capital Riesgo. Y, aunque todavía son marginales frente a la financiación bancaria, cada vez son más conocidas y utilizadas, como: Private Equity, Venture Capital, Business Angels y Crowdfunding, por sus denominaciones en inglés.

it whitepapers

PERSPECTIVAS DE LA PEQUEÑA EMPRESA EN ESPAÑA

La digitalización podría tener un impacto de hasta el 1,8% anual en el PIB en España hasta 2025, y la creación del Digital Single Market podría contribuir con hasta un 0,5% anual adicional hasta 2022. Así lo indica un informe de Digital McKinsey y la Fundación Cotec, que apunta a la baja digitalización de algunos sectores económicos y de las pymes, un ecosistema de start-ups aún en desarrollo y la escasez relativa de inversión, como los principales obstáculos en la transición digital.

¿Te avisamos del próximo IT User?

ranual del 29,2%. Otra tendencia ascendente es el Big Data, para analizar el comportamiento de los usuarios. El uso del Big Data en el comercio electrónico permite a las empresas promover una experiencia personalizada de usuario (basada en su interacción con la plataforma B2C) y un servicio al cliente perfectamente adaptado (identificando al mismo usuario en distintas plataformas). Cada vez más, la pyme participa de este proceso como actor protagonista.

El sector económico más importante de España en estos años, el turismo (11% del PIB) ha utilizado intensivamente las TIC para crecer rentablemente; en su afán de innovación y renovación se ha servido de las tecnologías de la información y las comunicaciones para ofrecer nuevos servicios y mejorar la experiencia turística de los usuarios.

Como ya vimos, la Administración Electrónica ha dado un fuerte salto cualitativo y cuantitativo: La Administración General del Estado (AGE) afirma que los ahorros conseguidos por los ciudadanos y empresas durante 2012 y 2013 debido al uso de la Administración Electrónica ascienden a 31.000 millones de euros y 22.000 millones entre 2015 y 2016. En España, en 2016, el 59% de los ciudadanos entre los 16 y los 74 años interactuaba con las autoridades públicas a través de la Red.

La pyme es la columna vertebral de la economía española. Con la recuperación económica y con su mayor adopción de las TIC, pensamos que esa afirmación es más cierta que nunca

Por ejemplo, el capital riesgo invirtió 3.000 millones de euros en 2014 en proyectos de financiación de pymes españolas. En 2015 y 2016 la cifra fue estable en los 4.000 millones de euros.

TIC y Economía

Las Tecnologías de la Información (TIC) siguen impactando positivamente en la economía y en los sectores de actividad económicos españoles. Un buen ejemplo es el comercio electrónico: en el cuarto trimestre de 2016, el volumen de negocio generado en nuestro país por el comercio electrónico ascendió a casi 6.000 millones de euros, lo que supuso un incremento inte-

Las TIC son esenciales para las pymes

Como en años anteriores, las TIC siguen estando en el corazón de las pymes españolas para ser más productivas y competitivas, aunque en 2016 se ha dado un salto importante, fruto de la mayor inversión empresarial: el 84% de las pequeñas empresas otorgan a las tecnologías de la información un papel muy importante en sus empresas, cifra que sube hasta el 86% en el caso de la mediana empresa. Además, también realizan un importante esfuerzo para conocer estas tecnologías, y así el 78% de las pequeñas empresas y el 81% de las medianas aseguran que están muy familiarizadas o bastante familiarizadas con ellas. El interés por el Cloud Computing es creciente, con un 69% de las pequeñas empresas y un 83% de las medianas que han oído hablar de él y entienden su concepto. Algo similar sucede con el comercio local y el teléfono móvil, con un usuario que empieza a no diferenciar entre canal físico y canal online, y valora aspectos que suponen la integración de ambos canales: el 47% no quiere pagar por el envío, el 23% no quiere esperar, el 46% quiere tocar el producto antes de comprarlo y el 37% desea la opción de devolverlo en la tienda si es necesario. Todo ello está transformando tecnológicamente el comercio local en España, gracias a Internet y a los teléfonos inteligentes.

Desciende la inversión en I+D

España invirtió menos en I+D en 2016: el gasto interno en Investigación y Desarrollo (I+D) descendió un descenso del 2,8% respecto al año anterior. Dicho gasto representó el 1,24% del Producto Interior Bruto (PIB),

frente al 1,27% del año anterior. Empresas (un 46,3%) y la Administración Pública (un 41,6%) fueron quienes financiaron fundamentalmente las actividades de I+D, aunque como las Organizaciones Empresariales no han dejado de repetir, la inversión en I+D en España debe aumentar para cambiar el modelo productivo del país hacia la Sociedad del Conocimiento.

Las empresas del sector Servicios concentraron el 49,9% del gasto en I+D empresarial. Al mismo tiempo, el volumen de negocio de las empresas manufactureras del sector de alta y media-alta tecnología se situó en 150.238 millones de euros en el año 2016.

Por Comunidades Autónomas, las que presentaron mayores porcentajes de empresas con innovaciones tecnológicas durante el periodo 2011-2016 fueron País Vasco (un 19,6% de sus empresas introdujeron innovaciones tecnológicas en dicho periodo), La Rioja (19,3%) y Comunidad Foral de Navarra (17,9%).

Las pymes han seguido invirtiendo en TIC

Algunos datos son relevadores: el 98,3% de las empresas españolas dispone de conexión a Internet. Siete de cada 10 tienen página web. El porcentaje de empresas que utiliza banda ancha móvil sube cuatro puntos, hasta el 78,3%. El 91,1% de las empresas interactuó a través de Internet con las Administraciones Públicas. El volumen de negocio generado en las empresas por las ventas de comercio electrónico alcanzó el 15,1% del total de ventas durante 2013, un 6,7% superior al del 2012. El 54,6% de las empresas proporciona a sus empleados dispositivos portátiles que permiten la conexión a Internet para uso empresarial. El 22,9% de empresas invirtieron en formación en TIC.

El 36,9% de las empresas usaron alguno de los medios sociales por motivos de trabajo. De éstas, el 92,4% utilizaron las redes sociales.

A comienzos de 2016, el 15% de las pymes compraban soluciones de Cloud Computing. Las más compradas fueron almacenamiento de ficheros (69%), servicio de e-mail (61,4%) y como servidor de bases de datos de la empresa (54,7%).

En cuanto al uso de las TIC por comunidades autónomas, las empresas cuyas sedes sociales están ubicadas en Cataluña, Comunidad de Madrid y Principado de Asturias presentan las mayores intensidades en el uso de las TIC (Conexión a Internet, Interacción con las Administraciones Públicas (AAPP), Banda Ancha móvil, Página Web, Uso de Medios Sociales y Cloud Computing).

El 17,8% de las empresas realizaron ventas mediante comercio electrónico. El volumen de negocio generado por estas ventas alcanzó los 195.443 millones de euros, un 6,7% más que en el año anterior. Las ventas a través de comercio electrónico representaron, el 15,1% del

it whitepapers

ANÁLISIS ESTRATÉGICO PARA EL DESARROLLO DE LA PYME EN ESPAÑA

El Informe Pyme España 2016, en el que colaboran la Fundación para el Análisis Estratégico y Desarrollo de la Pequeña y Mediana Empresa (FAEDPYME), CEPYME y la Asociación Española de Contabilidad y Administración de Empresas (AECA), aporta información sobre la situación y perspectivas de las pymes españolas, con la finalidad de ser de utilidad a las empresas y a los distintos agentes económicos que toman decisiones que puedan favorecer el entorno de la competitividad de las pymes.

¿Te avisamos del próximo IT User?

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

total de ventas efectuadas por las empresas, frente al 14,0% del año anterior.

En el caso de las microempresas, el 72,3% dispone de ordenadores y el 24,4% tiene instalada una Red de Área Local (LAN). El 67,7% dispone de acceso a Internet y el 99% de ellas accede mediante alguna solución de banda ancha. En cuanto a las comunicaciones, el 76,5% usa telefonía móvil, frente al 74,6% del año anterior. Por su parte, el 21,7% utiliza otras tecnologías (GPS, TPV...).

Cabe destacar la banda ancha móvil, que ha experimentado el incremento más elevado al pasar del 56,8% al 66,4%, en el caso de las microempresas.

Como dijimos al principio de este ensayo, 2017 no es 2013. En estos años han avanzado la Sociedad de la Información y la recuperación económica. Las pymes españolas cada vez consideran más importante las TIC para la gestión de su negocio, por lo que la inversión en Tecnologías de la Información ha continuado en estos años. La pyme ya no es ajena al Big Data o las Redes Sociales. La pyme realiza negocios en movilidad. Busca nuevas formas de financiación alternativa a la bancaria y, cada vez, exporta más. La pyme, empujada por la gran empresa española -Telefónica, La Caixa, CaixaBank, Abertis, Gas Natural Fenosa, El Corte Inglés, Cellnex Telecom…- y las compañías TIC -SAGE, Microsoft, Salesforce.com, Oracle, HP, IBM… y las Telcos Digitales -Telefónica, Vodafone, Orange- está cambiando a marchas forzadas hacia la digitalización, como explicaremos en detalle en el segundo ensayo.

Siempre hemos sostenido que la pyme era la columna vertebral de la economía española. Con la recuperación económica y con su mayor adopción de las TIC, pensamos que esa afirmación es más cierta que nunca.

Las pymes españolas cada vez consideran más importante las TIC para la gestión de su negocio, por lo que la inversión en Tecnologías de la Información ha continuado en estos años

Enlaces relacionados

- Observatorio Sage
- Ministerio de Economía, Industria y Competitividad
- Ranking Global de Cloud Computing de la BSA
- Hábitos sobre una TI híbrida
- Barómetro de emprendimiento de éxito en España

Fernando Maldonado
Analista asociado a Delfos Research

RPA, el nuevo acrónimo que toda empresa debe conocer

Durante los últimos años, en la periferia de la industria TI, una tecnología ha ido madurando y preparándose para revolucionar el mercado empresarial. Hoy todas las empresas deberían conocer el significado del acrónimo RPA. Quizá una imagen que ayude a visualizar su impacto en la empresa es la de un ejército de trabajadores virtuales realizando tareas rutinarias.

Esta tecnología ha crecido en el seno de outsourcers, ocupándose de un creciente número de tareas de back office. Por ejemplo, en modelos de servicios compartidos. Así, empresas como Everis, anunciaban a principios de año la creación de un centro de excelencia sobre RPA en España.

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

Todas las proyecciones para los próximos años apuntan a una explosión del mercado RPA

En realidad, se trata de un software que automatiza tareas rutinarias como la extracción y limpieza de datos a través de interfaces de usuario existentes. El robot tiene un ID de usuario al igual que una persona y puede realizar tareas basadas en reglas como por ejemplo acceder al correo electrónico, realizar cálculos, crear documentos e informes y revisar archivos.

Estos robots están centrados en la ejecución de tareas rutinarias, y prometen liberar al empleado de tareas de escaso valor añadido y a las que frecuentemente dedican una parte significativa de su tiempo.

A la espera de una mayor integración de esta tecnología con sistemas BPM, herramientas de workflow o la inminente incorporación de inteligencia artificial, su ámbito de aplicación actual se centra en procesos claramente definidos, repetibles y basados en reglas. Estos criterios, pueden ayudar a las empresas de numerosas industrias a automatizar la realización de una amplia gama de tareas.

Una parte importante del debate actual en torno a cómo la tecnología, y más concretamente la inteligencia artificial, impactará en el empleo gira, sin que lo mencionemos de forma expresa, sobre RPA. Pero mientras que la inteligencia artificial se está desarrollando para potenciar nuestro trabajo -por ejemplo, en la forma de asistentes personales-, la robotización de procesos tiene una propuesta de valor menos elevada: promete liberarnos sencillamente de tareas tediosas.

Los beneficios para la empresa incluyen menores costes, aceleración de procesos, mayor precisión, operar de forma ininterrumpida, mayor trasparencia… En fin, son muchos los motivos por los que esta tecnología comienza a ganar adeptos.

Sin embargo, ahora que las empresas comienzan a adoptarlo comienzan a surgir casos en los que su implantación ha fallado. A veces, sencillamente se buscan procesos muy complejos para los que la empresa no está preparada. Los procesos deben ser cuidadosamente seleccionados y deben someterse sometidos a un análisis

BREVE INTRODUCCIÓN A RPA

CLICAR PARA VER EL VÍDEO

it whitepapers

IMPACTO DE LA AUTOMATIZACIÓN EN LAS OPERACIONES DE IT

La automatización de las operaciones de TI ofrece grandes oportunidades para reorientar el personal de las empresas en actividades de más valor y de esta manera responder a necesidades de los negocios, ya que se libera tiempo que hoy en día se usa para tareas administrativas rutinarias. Según se desvela en este estudio, la mayor parte de las compañías consultadas considera que se necesita automatizar las tecnologías para hacer frente a las crecientes presiones y de entrega de valor al negocio, aunque según la encuesta muchos afirman que aún les queda un largo camino por recorrer.

preliminar sobre su idoneidad para ser automatizados, además, este análisis, deben acompañarse de una posible reingeniería del proceso. Solo entonces RPA realizará su promesa.

Los beneficios para la empresa incluyen menores costes, aceleración de procesos, mayor precisión, operar de forma ininterrumpida y mayor trasparencia, entre otros

ROBOTIC PROCESS AUTOMATION

CLICAR PARA VER EL VÍDEO

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkdIn beBee

De momento, lo que está claro es que RPA (Robotic Process Automation) ha venido para quedarse. Todas las proyecciones para los próximos años apuntan a una explosión de este mercado.

Algo seductor tendrá su propuesta de valor. Aunque solo sea por eso, bien merece la pena que le dediquemos parte de nuestra atención.

Enlaces relacionados

- Everis crea un centro de excelencia RPA
- Expectativas de crecimiento del mercado
- Cómo ser flexible y apto para la Transformación Digital
- Cinco capacidades de un servidor para la Transformación Digital de la PYME
- Oportunidades de uso de software legal
- Barómetro de Talento y Cultura Digital
- La reinvención digital: una oportunidad para España

El dato y la Transformación Digital

Ramón Puchades,
profesor colaborador de MBIT School

Los datos son uno de los pilares sobre los que se asienta la transformación digital. Es evidente que una de las características de la disrupción tecnológica es la abundancia de datos. La tecnología, ahora mismo, nos permite capturarlos en los puntos precisos donde se generan; solo hay que decidir qué dato es relevante y orquestar la tecnología para capturarlo y almacenarlo. Generar información con los datos almacenados es más complicado, pero las herramientas de Machine Learning e Inteligencia Artificial y los científicos de datos pelean cada día para resolver el problema.

Todo este escenario pone a disposición de empresas e instituciones mucha información valiosa que habría hecho feliz a Jim Barksdale cuando, siendo CEO de

Profesor en diferentes escuelas de negocios como EAE Business School, EOI o MBIT Business School, ha sido CTO del Grupo Prisa; CEO de la startup Talents United; director de Redes Sociales y Head of Innovation Spain de Unidad Editorial; director Web 2.0 de Barrabés Internet, consultora especializada en estrategia y comunicación en el mundo de la PYME y las nuevas tecnologías; participó con el Grupo Netjuice en el desarrollo y consolidación internacional de Baquia.com, como CTO de la compañía; y, en especial, fue director de Internet en la concepción y nacimiento de Barrabes.com en el año 1998, donde se inició con la innovación, la internacionalización y el emprendimiento.

Netscape, pronunció su famosa frase: "Si tenemos datos, miremos los datos. Si todo lo que tenemos son opiniones, la mía es la que cuenta". Sin embargo, no todos los directivos tienen el hambre de datos que tenía Jim; la cruda realidad es que las empresas e instituciones no están preparadas para absorber esa gran cantidad de información y solo emprendiendo una profunda transformación podrán llegar a aprovecharla.

Tres ámbitos principales de transformación

Los ámbitos que requieren transformación para aprovechar la abundancia de datos son muchos, pero hay tres campos especialmente relevantes: la toma de decisiones, la experiencia del cliente y el desarrollo de producto.

Las empresas toman decisiones en base a una combinación de información y de análisis basado en la experiencia. Los equipos directivos son una especie de oráculos que, leyendo cuadros de mando e informes periódicos, toman sus decisiones basándose en su intuición y experiencia. La información que gestionan está agrupada en grandes bloques y largos períodos de tiempo y basada en estimaciones. Sin embargo, el conjunto de información disponible está cambiando, los cuadros de mando se convierten en paneles de información en tiempo real y los informes en datos precisos que permiten a los científicos de datos hacer predicciones y correlaciones más acertadas para tomar decisiones con mayor agilidad, en tiempo real y basadas más en la creatividad que en la repetición de experiencias.

Los ámbitos que requieren transformación para aprovechar la abundancia de datos son muchos, pero hay tres campos especialmente relevantes: la toma de decisiones, la experiencia del cliente y el desarrollo de producto

El desarrollo de producto, por su parte, debería ser un proceso continuo de colaboración con los usuarios destinatarios. Las nuevas técnicas de Big Data permiten constatar el nivel de eficacia de un producto y los nuevos entornos de seguimiento de interacción en tiempo real permiten, además, hacer ajustes al vuelo para mejorar el servicio de modo ágil y con un tiempo de respuesta casi instantáneo. Sin embargo, la mayoría de las empresas han construido sistemas de

it whitepapers

LA TI HÍBRIDA AYUDA A LAS EMPRESAS A NAVEGAR POR LA TRANSFORMACIÓN DIGITAL

En esta era de revolución digital, las empresas deben ser más ágiles para captar las oportunidades. Muchas consideraron que el cloud computing puro era una manera de conseguirlo, puesto que prometía agilidad, escalabilidad y coste. Sin embargo, con el traslado a la nube, muchas descubrieron que su seguridad, cumplimiento y rendimiento no estaban realmente a la altura de sus necesidades. Las empresas más avanzadas adoptaron la TI híbrida, que incluye servicios locales y externos. En este informe podrás leer las razones que las llevaron a ello.

¿Te avisamos del próximo IT User?

La Transformación Digital es mucho más que Big Data, pero una de sus inexorables consecuencias es que uno de los principales focos de la organización sean los datos

desarrollo de producto, incluso de innovación, poco ágiles y basados en estructuras pesadas y burocráticas. Es necesario evolucionar hacia estructuras de producción más flexibles, que permitan cerrar el ciclo propuesta de producto → análisis → rediseño → propuesta de producto.

La experiencia del cliente, por último, se basaba en encuestas alejadas del propio cliente y en poblaciones pequeñas como muestra; a lo que se le podían unir datos deducidos de las ventas y de los costosos departamentos de atención al cliente. La disrupción digital ha construido varias piezas que han roto esta inercia y que harán que las empresas tengan que transformar sus estructuras y sus canales de comunicación. Técnicas de análisis de redes, de análisis del lenguaje natural, etiquetado... son imprescindibles para escuchar la conversación de los usuarios allá donde sucede y permitir a las empresas mejorar la experiencia del cliente. La personalización de productos y servicios es otra de las virtudes de la abundancia del dato, al permitir a las organizaciones construir una solución particular para él en su contexto específico.

La Transformación Digital, por tanto, es mucho más que Big Data, pero una de sus inexorables consecuencias es que uno de los principales focos de la organización sean los datos.

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn beBee

Enlaces relacionados

- Jim Barksdale
- Cómo la Transformación Digital impacta en los OEM
- Cómo ser flexible y apto para la Transformación Digital
- Las operadoras de telecomunicaciones en la era digital
- GMV: Transformación Digital
- La Transformación Digital como eje estratégico
- Como transformar cuatro sectores clave

it Digital MEDIA GROUP

it Reseller TECH&CONSULTING

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