COMPARATIVA - - - > Plataformas de almacenamiento cloud

www.revistabyte.es Marzo 2018 • Nº 258 • 5,75 euros

byte TI

Síguenos en twitter: (@BYTE_TI)

ANÁLISIS

• ESET Safica

El estado de la ciberseguridad

- Principales retos y amenazas
- Dónde poner el foco
- El usuario como factor de riesgo

La nueva era de la inteligencia artificial

Movilidad Innovadora

mkm

Javier López Sáez

Barracuda **Essentials para Office 365**

Seguridad multicapa, backup, archivado y eDiscovery para incrementar la protección de todos sus datos en Office 365 y alcanzar el cumplimiento normativo.

ESS

Barracuda
Essentials

Confiar sus datos y documentos más importantes al cloud genera nuevas preocupaciones acerca de su Seguridad, Cumplimiento y Protección frente a pérdidas de información. Barracuda Essentials le proporciona todos los elementos necesarios para realizar su migración y permanencia en el cloud de forma segura y con el más alto nivel de cumplimiento normativo.

Barracuda®

barracuda.com
iberia_team@barracuda.com

Hay que insistir en la excelente organización del Mobile World Congress: están cuidados hasta los más mínimos detalles para que todo funcione como un reloj. Cuentan con la mejor ciudad para acogerla, un emplazamiento perfecto e infraestructuras de sobra. Pero que no se duerman: tienen que volver a potenciar las conferencias y la presencia de gurús de renombre que este año no han brillado como otros. No sé qué cifras de visitantes darán, pero yo he tenido la percepción de más número que en 2017. Y cuidado con los robos, que parece que han aumentado de manera alarmante…

Huawei vs. Samsung

Ramiro Larragán, responsable de Marketing de la División de Consumo de Huawei, me reconocía en el pasado Mobile, a pregunta mía, que su competidor principal es Samsung, muy por delante de Apple. Precisamente, la compañía de la manzana es de las pocas multinacionales de renombre que no han acudido al Mobile World Congress, y nadie la ha echado de menos.

Y es que, a falta de novedades de gran relieve, no ha pasado desapercibido en la feria la pugna entre la marca china Huawei y la coreana Samsung por demostrar quién lo tenía más grande (el stand). No me atrevo a asegurar de quién ha sido la ventaja.

Samsung organizó un mega evento para presentar su S9, con un alarde de medios y de invitados (partners, clientes y prensa de todo el mundo), que yo no he tenido ocasión de presenciar en toda mi vida profesional (por cierto, más larga de la que me gustaría presumir). Pero la firma china montó un stand que ocupaba gran parte del pabellón 1, con un despliegue de medios también impresionante: cientos de personas, decoración de alto nivel, presentaciones continuas de productos, catering permanente para los miles de acreditados…, realmente increíble.

Algún medio ha intentado calcular la inversión aproximada de estas compañías en el certamen barcelonés: se llega a hablar, en el caso de Huawei, de cifras superiores a los diez millones de euros: una auténtica barbaridad, que me encanta ver y contar porque inversión es.

Por lo demás, parece que se despejan los temores que han amenazado la continuidad de la capital catalana como sede del MGC. No por estar más claro ahora, dejó de haber una gran incertidumbre coincidiendo con la inauguración y la irresponsable espantada de la alcaldesa.

Podemos hablar, por tanto, de éxito de todos en la consecución del objetivo de asegurar el certamen en Cataluña. Conviene, de todas formas, no relajarnos y aprender de los riesgos y errores cometidos. No me cansaré de escribir que tener este evento en España es un bien tan enorme que perderlo sería una auténtica ruina.

Sumario

FEBRERO 2018

EN PORTADA

Ciberseguridad

38

N.º 258• ÉPOCA III

Director
Juan Manuel Sáez
(juanmsaez@mkm-pi.com)

Redactor Jefe
Manuel Navarro
(mnavarro@mkm-pi.com)

Coordinador Técnico
Javier Palazon

Colaboradores
S. Velasco, R.de Miguel, I. Pajuelo, O. González, D. Rodríguez, F. Jofre, JL. Valbuena, MªJ. Recio, MA. Gombáu, J. Hermoso, JC. Hernández, C. Hernández, M. Barceló, A.Barba.

Fotógrafos
E. Fidalgo, S. Cogolludo, Vilma Tonda

Ilustración de portada
Javier López Sáez

Diseño y maquetación
El Palíndromo Comunicación S.L.

WebMaster
NEXICA
www.nexica.es

REDACCIÓN
Avda. del Generalísimo, 14 – 2º B
28660 Boadilla del Monte
Madrid
Tel.: 91 632 38 27 / 91 633 39 53
Fax: 91 633 25 64
e-mail: byte@mkm-pi.com

PUBLICIDAD
Directora comercial: Isabel Gallego
(igallego@mkm-pi.com)
Tel.: 91 632 38 27
Ignacio Sáez (nachosaez@mkm-pi.com)

DEPARTAMENTO DE SUSCRIPCIONES
Tel. 91 632 38 27
Fax.: 91 633 25 64
e-mail: suscripciones@mkm-pi.com
Precio de este ejemplar: 5,75 euros
Precio para Canarias, Ceuta y Melilla: 5,75 euros (incluye transporte)

Impresión
Gráficas Monterreina
Distribución
DISPAÑA
Revista mensual de informática
ISSN: 1135-0407

Depósito legal
B-6875/95

© Reservados todos los derechos
Se prohíbe la reproducción total o parcial por ningún medio, electrónico o mecánico, incluyendo fotocopias, grabados o cualquier otro sistema, de los artículos aparecidos en este número sin la autorización expresa por escrito del titular del Copyright. La cabecera de esta revista es Copyright de Publicaciones Informáticas MKM. Todos los derechos reservados. Publicado con la autorización de Publicaciones Informáticas MKM. La reproducción de cualquier forma, en cualquier idioma, en todo o parte sin el consentimiento escrito de Publicaciones Informáticas MKM, queda terminantemente prohibida. Byte ti es una marca registrada de Publicaciones Informáticas MKM.

MARZO de 2018
Printed in Spain

EDITA
Publicaciones Informáticas MKM

8 NOVEDADES

28 COMPARATIVA

TENDENCIAS 58

3 **CARTA DEL DIRECTOR**

6 **RECOMENDAMOS**

8 **NOVEDADES**

22 **DESAYUNO**
Movilidad

26 **ANÁLISIS**

28 **COMPARATIVA**

42 **TEMA DE PORTADA**

52 **UN CIO EN 20 LÍNEAS**

54 **LEGALIDAD TIC**

58 **TENDENCIAS**

64 **ENTREVISTA**

66 **TEMPORAL**
Por Miquel Barceló

25 años. Todo conectado. Ahora el gran cambio: "Tecnología en la Estrategia Corporativa"

Por Markel Gruber, Presidente Asociación @asLAN

El próximo mes de abril tiene lugar en Madrid el Congreso&EXPO que la Asociación @asLAN organiza desde hace 25 años. En esta edición tan especial contaremos con el apoyo de más de 120 empresas y las principales instituciones, lo que nos permitirá batir la cifra de los 6.000 visitantes.

En el año 1993 organizamos el primer Salón monográfico en torno al protocolo TCP/IP y actualmente la red, el eje conductor de estas 25 ediciones, está omnipresente en todos los ámbitos de nuestra sociedad y economía. Ahora la Tecnología está en la Estrategia de cualquier organización que quiera sobrevivir. Con más de 20 billones de dispositivos conectados y la hiperconectividad de personas, cosas e infraestructuras IT, podemos decir que la red ha colonizado el mundo y ofrece una base para comenzar una nueva etapa en la que la seguridad de la información, el análisis de datos y la integración de servicios desde la nube hará cambiar los modelos de negocio de las empresas en los próximos 10 años más de lo que ha cambiado en estos 25.

Disponer de una amplia visión de las oportunidades que ofrecen las últimas innovaciones tecnológicas, ya no es sólo una oportunidad y responsabilidad del CIO, sino que la dirección de la compañía y responsables de las áreas de negocio, están cada vez más interesados en saber cómo las TIC puede generar en su organización una ventaja competitiva.

La tendencia cada vez es más evidente, el CIO tiene que saber más de negocio y los responsables del negocio más de tecnología. Ambos rodearse de un buen ecosistema de proveedores especializados en tecnología.

Tres ejemplos de cómo la innovación IT aporta una ventaja competitiva

Inteligencia de negocio, confianza y flexibilidad, son tres ámbitos en los que la innovación IT puede aportar una ventaja competitiva.

1. Inteligencia de negocio: el usuario hiperconectado La visualización, análisis de los dispositivos y el tráfico de datos que circula por la red permiten tomar decisiones, desarrollar nuevos servicios y mejorar la fidelización de clientes. Un mundo por explorar que no ha hecho más que empezar: desde el SIEM (Security Information and Event Management) hasta el DeepLearning, pasando por el análisis de video, wifi, aplicaciones, etc.

2. Confianza: Seguridad y disponibilidad en la era digital

En un escenario cada vez más digital, la confianza de clientes, proveedores e inversores, dependen de la capacidad de las organizaciones para evitar las ciberamenazas y de su capacidad de recuperación. Desde la Asociación consideramos que debe plantearse la seguridad como parte ineludible de la Transformación Digital de las compañías.

3. Flexibilidad: integración de servicios e infraestructuras desde la nube

Crecer, innovar y diferenciarse.... en un contexto tan dinámico y competitivo como el actual, requiere de infraestructuras y servicios IT de gran elasticidad. En el Congreso ASLAN2018, compañías líderes en innovación IT a nivel mundial, ofrecerán una visión general de las oportunidades y retos para integrar tecnología altamente eficiente: desde el puesto de trabajo hasta el SOC (Security Operation Center), pasando por infraestructuras de las principales plataformas de nube pública

Con este gran cambio en el que la Tecnología cada vez está más en la Estrategia Corporativa, nuestro Sector adquiere mayor relevancia, y todavía tiene mucho que ofrecer: La inteligencia artificial ha comenzado a desarrollarse sobre la red.

Renovación en las cámaras Canon

Canon ha anunciado el lanzamiento de las EOS 2000D y EOS 4000D, sus últimas cámaras réflex digitales (DSLR) para principiantes. Con una amplia variedad de funciones muy prácticas y fáciles de usar, estas cámaras están pensadas para satisfacer las necesidades, al contar historias, de aquellos que comienzan a dar sus primeros pasos en la fotografía con cámaras de objetivos intercambiables, así como para quienes quieran captar con facilidad fotos con un gran detalle y calidad DSLR, así como vídeos Full HD con aspecto cinematográfico.

Las nuevas incorporaciones a la gama DSLR de iniciación de Canon, las EOS 2000D y EOS 4000D, han sido diseñadas para personas que busquen nuevas experiencias y que quieran compartir sus aventuras en las redes sociales rápidamente. La potente combinación de la tecnología del sensor APS-C, el procesador de imagen DIGIC 4+, la conectividad Wi-Fi constante y las sencillas guías de funciones, con la que cuentan las cámaras, permite captar historias y compartirlas mediante fotos con alto nivel de detalle y vídeos Full HD.

El procesador de imagen DIGIC 4+, utilizado en ambas cámaras, potencia el modo de Escenas Inteligente Automático de Canon, que permite fotografiar con tan solo apuntar y disparar, con unos resultados excelentes, ya que este optimiza de forma automática cada toma. El rápido y sensible procesador de imagen DIGIC 4+ permite, también, grabar vídeos Full HD con ambos modelos, dando vida, con vídeos de aspecto cinematográfico, a tus recuerdos.

SAP Business Integrity Screening Solution

SAP ha presentado SAP Business Integrity Screening, una aplicación que ayuda a reducir el riesgo financiero dentro de la actividad empresarial. Analiza datos de transacciones y patrones sospechosos en tiempo real para detectar excepciones, posibles fraudes y fallos de cumplimiento. Esta automatización se traduce en mayores ganancias y en ahorro de costes. Business Integrity Screening permite a las organizaciones adoptar la garantía de cumplimiento en un amplio número de escenarios, mediante la detección temprana de transacciones anómalas antes de que se produzcan pérdidas económicas, y a través de la prevención de futuras contingencias. La aplicación también examina entidades empresariales e individuales frente a grupos/agentes de alto riesgo o incluidos en listas negras para reducir el riesgo de realizar negocios con estos. Todas estas características disminuyen el coste asociado con investigaciones e infracciones de cumplimiento. SAP Business Integrity Screening es una solución completa que combina capacidades analíticas con un proceso holístico que detecta posibles excepciones de forma anticipada para minimizar las pérdidas financieras. La flexibilidad de la plataforma permite a las organizaciones definir reglas que abordan una amplia variedad de escenarios tales como fraude en seguros, auditorías fiscales, anti-soborno y la Ley de Prácticas Corruptas en el Extranjero (FCPA), robo de servicios públicos, evaluación de socios, automatización de auditorías internas, gastos de viaje y ocio, pagos de facturas y pagos al sector público.

LG THINQ

LG presenta su apuesta por la inteligencia artificial: el ecosistema LG ThinQ. Equipado con procesadores propios y con Google Assistant, LG ha conseguido que los electrodomésticos y la tecnología doméstica aprendan del comportamiento humano y puedan así adelantarse a las preferencias de los usuarios.

Una de sus caracterrísticas es su habilidad para evolucionar con el paso del tiempo. Con ThinQ, "vivir" y "aprender" cobran un nuevo y excitante significado. Cuanto más se utilicen los productos de LG, más evolucionan para dar con las necesidades específicas de cada usuario. Por ejemplo, el aire acondicionado LG ThinQ aprende de los hábitos y estilos de vida y crea patrones de comportamiento para ofrecer las soluciones personalizadas más óptimas, como adecuar la temperatura de la casa a la temperatura idónea de cada usuario.

La segunda característica trata de la habilidad para integrar la Inteligencia Artificial en un variado portfolio de productos cotidianos. LG elabora productos de uso diario para distintos entornos. Productos del hogar -como frigoríficos, lavadoras, televisiones, aspiradores…- como productos y servicios que se prestan fuera del hogar -como sistemas de entretenimiento e información para el sector automovilístico, unidades telemáticas, soluciones de climatización, sistemas de gestión de energía, etc-. A través de esta amplia red de productos conectados cualquier usuario será capaz de beneficiarse de la Inteligencia Artificial como una experiencia cotidiana. Por ejemplo, enr el sistema de info-entretenimiento de los coches. Según el usuario vaya acercándose a su casa, se ajusta la temperatura del sistema de climatización y la luz del hogar teniendo en cuenta qué usuario es quién se esté aproximando.

Las principales novedades del MWC: Telefónica, Vodafone, LG

El Mobile World Congress de este año no ha destacado precisamente por las grandes novedades, más allá de la presentación del nuevo buque insignia de Samsung y del que hablamos más adelante.

Dentro del Mobile, curiosamente, lo más destacado se anunció en la jornada anterior a la inauguración. Además de las novedades de Samsung y Huawei (de las que hablamos más adelante), estas han sido las principales novedades del día pre-Mobile:

TELEFÓNICA

Una de las principales novedades del MWC era lo que iba a presentar Telefónica. La operadora anunció en el evento del pasado año el desaroolo de la denominada cuarta plataforma y este año era el momento de ver Aura hecho realidad. Presentado por el presidente de Telefónica, José María Álvarez Pallete Aura se ha convertido en un asistente digital con inteligencia artificial incorporada con el que se pretende cambiar la forma en que los clientes se relacionan con Telefónica y cómo gestionan su vida digital con la compañía. Podrán utilizar una primera versión de Aura en Argentina, Brasil, Chile, Alemania, España y Reino Unido. Aura llegará inicialmente a los dispositivos de los clientes a través de una aplicación móvil y también a través de otros canales de terceros como Facebook, Google y Microsoft. Durante el evento de lanzamiento, Pallete, destacó el potencial de Aura para sus clientes. "Hace un año dijimos que queríamos que la inteligencia artificial fuera la base de la relación con nuestros clientes y ahora cumplimos con nuestra promesa. La digitalización es la esencia de nuestro negocio y gracias a la profunda transformación interna que hemos experimentado en los últimos ocho años nos hemos convertido en una empresa de plataformas inteligentes". Tal y como se puso de manifiesto durante la presentación, Aura aspira a estar donde los clientes de Telefónica quieren estar y, por ello, estará disponible también en otros canales. En esta primera fase, se integrará con Facebook Messenger en Alemania y Chile. Los clientes de Telefónica en estos países pueden incluir a Aura entre sus contactos e interactuar con ella a través del chat cuando lo deseen.

En los próximos meses, Aura estará integrada con Google Assistant y, en 2019, con Microsoft Cortana

Por otro lado, y al igual que ha hecho Vodafone, la operadora ha puesto en el hogar su próximo objetivo. Para ello ha anunciado el lanzamiento de Movistar Home, un dispositivo que integrará en todos sus servicios la inteligencia artificial de Aura. Con capacidades de edge computing para procesar y analizar datos, Movistar Home busca convertirse en un centro de conexión y de todos los dispositivos en el hogar desde el que los usuarios puedan gestionar sus servicios. Equipado con una segunda pantalla, permitirá realizar llamadas y videolla-

madas que podrán proyectarse en la televisión. Movistar Home se lanzará inicialmente en España este otoño.

VODAFONE

Vodafone sigue con su apuesta por IoT bajo la marca presentada a finales del año pasado V by Vodafone. En este caso la apuesta pasa por el hogar conectado y para ello ha presentado en el marco del MWC el acuerdo al que ha llegado con Vodafone para el desarrollo y lanzamiento de V-Home by Vodafone, una plataforma completa de servicios "Smarthome" o de hogar inteligente basados en Internet de las Cosas.

Los nuevos servicios y productos "V-Home by Vodafone" son fruto de la colaboración de ambas marcas y permitirán a los Clientes controlar, desde el smartphone, los dispositivos inteligentes de su hogar, compatibles con el ecosistema SmartThings de Samsung y V by Vodafone. Además, Vodafone creará nuevos servicios para facilitar aún más a sus Clientes la automatización del hogar, aprovechando por un lado el entorno abierto de Samsung SmartThings que permite interconectar una gran variedad de dispositivos y, por otro, la gran capilaridad de la red de Vodafone. El primer producto en el que colaboran ambas compañías es el Starter Kit de "V-Home by Vodafone", un sencillo sistema de monitorización del hogar asequible y fácil de configurar, que también incluye servicios diseñados por Vodafone para que los usuarios puedan estar al tanto en tiempo real de lo que ocurre en su hogar y recibir avisos. El Starter Kit incluye:

- Samsung SmartThings hub.
- Cámara de video inalámbrica.
- Multisensor Samsung SmartThings.
- Sirena Samsung SmartThings.
- Alarm Assistant de Vodafone.
- V-Home Monitor .

LG

LG ha centrado la atención en la presentación del LG V30S y lo ha hecho poniendo el foco en la Inteligencia Artificial. El terminal está desarrollado sobre la plataforma de LG V30, y al centrarse en la parte de Inteligencia Artificial lleva asociada la marca de referencia para AI, como es THINQ. ¿Dónde se encuentra la Inteligencia Artificial en este smartphone? La primera de ellas se encuentra en la cámara que es mucho más intuitiva. Asimismo apuesta por el reconocimiento de voz (Voice AI), ampliando los comandos disponibles.

Empezando por la parte referente a la cámara, la funcionalidad Vision AI tiene tres funcionalidades inteligentes de cámara: AI CAM, QLens y Bright Mode, que automatizan y mejoran la captura de imagen y fotos, y llevan esta experiencia a un nivel nunca antes alcanzado en un Smartphone, tanto para fotógrafos amateurs como profesionales. AI CAM analiza automáticamente los objetos en el encuadre y recomienda a continuación el modo más adecuado para tomar esa foto.

> Las operadoras han apostado por el hogar conectado y la analítica de datos. LG, mejora su mejor terminal

SOBRESALIENTE

TELEFÓNICA

Los resultados de Telefónica han sorprendido a propios y extraños. Nada menos que un 32,2% ha subido su beneficio neto en 2017 alcanzando los 3.132 millones de euros. No sólo eso, sino que ha sido capaz de reducir su deuda en un nada despreciable de un 9%.

ECONOCOM

Econocom alcanzó en 2017 una facturación de 2.980 millones de euros frente a los 2.536 millones de euros de 2016, es decir un incremento del 17,5 %. El crecimiento orgánico ha demostrado su fuerza (+11,2 %), acelerándose durante el segundo trimestre y claramente por encima de la previsión anual ("superior al 5 %"). Todas las actividades del grupo contribuyen a esta tendencia. Durante este período, el grupo se ha confirmado como un interlocutor clave de las grandes cuentas en Europa para desplegar su estrategia digital. La actividad de Servicios representa ahora el 34%.

MUY DEFICIENTE

MEDIDAS DE SEGURIDAD

Pese a que las grandes compañías son cada vez más conscientes del riesgo que supone la creciente sofisticación de los ciberataques, el 89% de los directivos encuestados en el estudio Global Information Security Survey (GISS) de EY señala que las medidas de seguridad implementadas por sus compañías no son capaces de responder totalmente a las necesidades del negocio.

APLICACIONES NOCIVAS

El estudio CA Veracode State of Software Security Report 2017 resaltó que las vulnerabilidades continúan apareciendo a un ritmo alarmante en software que no había sido testado previamente desde el punto de vista de la seguridad y también destacó que organizaciones de todo el mundo revelan que el 77% de las aplicaciones tiene al menos una vulnerabilidad en un análisis inicial.

HP apuesta por Device-as-a-Service con una nueva oferta

HP ha anunciado un nuevo conjunto de ofertas de Device-as-a-Service (DaaS) para clientes y socios que incluyen nuevas capacidades de análisis predictivo, disponibles para ofrecer un servicio más amplio atendiendo a las necesidades de los clientes y opciones mejoradas para simplificar el soporte de TI con HP Tech Café Market, la nueva solución integral de venta y almacenamiento. Montse Serra, directora general de Soluciones para Empresas de HP, fue la encargada de presentarlo a los periodistas.

Tal y como se destacó, los entornos con multitud de dispositivos diferentes, representan una norma habitual en el mundo de hoy, y gestionar múltiples tipologías de equipos, sistemas operativos (OS) y varios proveedores, se está convirtiendo cada vez más en un creciente rompecabezas para las organizaciones. El informe IDC DaaS revela que más del 63% de los responsables de TI encuestados por la consultora IDC afirmaron perder gran cantidad de recursos en la administración de dispositivos.

Las soluciones DaaS se están implementando o están siendo consideradas por el 40 por ciento de las empresas a medida que las compañías se van dando cuenta del valor que tiene transferir recursos a iniciativas más estratégicas en lugar de gastar recursos valiosos de TI en el soporte del ciclo de vida y la gestión del dispositivo. Estos gestores de TI preferirían destinar sus recursos a otras prioridades como son mejorar las SLAs/QoS (37%), usar IT para hacer el negocio más eficiente (30%), generar mejoras operativas (17%) y reducir los costes de TI (16%)2.

"Mediante el continuo desarrollo de nuestras ofertas de servicios, queremos demostrar el profundo compromiso de HP con las cambiantes necesidades del trabajo", explicó Montse Serra. El crecimiento de HP DaaS es resultado de la necesidad que tienen los departamentos de TI de buscar nuevas formas de administrar de manera más eficiente los dispositivos de HP y de otros fabricantes. HP ha logrado un fuerte crecimiento en su negocio de servicios, dado que HP DaaS ya está activo en cerca de 100 socios de canal en todo el mundo.

Este servicio de HP permite a los clientes analizar el rendimiento del hardware, detectar problemas potenciales de antemano e implementar de manera proactiva acciones correctivas.

Por Fernando Jofre

Telefónica entra con fuerza en la IA

En el evento de Predicciones TIC 2018 que organizó IDC a finales de enero, participó Telefónica con una ponencia titulada "Evolución hacia un mundo de plataformas", en la que ya nos anticipaban lo que se ha materializado en los preámbulos del MWC de Barcelona: Aura. En su intervención, Carlos Rabazo destacaba la tendencia de una evolución hacia un ecosistema de servicios y productos, con un Customer & User Experience (UX) excelentes, indicando que precisamente la Inteligencia Artificial será el mecanismo de control de la UX, mediante asistentes personales que atenderán directamente las necesidades de los clientes y consiguiendo experiencias combinadas online y off-line.

Si la primera plataforma de Telefónica fue la red, la segunda estaba constituida por los OSS y BSS, la tercera por los servicios para clientes, ahora la cuarta consiste en servicios de interacción natural con clientes, basados en Datos e Inteligencia Artificial (IA) cognitiva. Para Telefónica, esta cuarta plataforma tendrá como protagonista la IA, consiguiendo un modelo relación con el operador más natural. Y ya nos anticipaba lo que sería Aura, el asistente digital que ha sido presentado en el MWC. La primera versión llegará a nuestro país como primicia junto con otros cinco, y podremos experimentar con Aura a través de una App y también interactuando con Facebook Messenger, Google Assistant y Cortana de Microsoft (en 2019). odremos incorporar a Aura como un contacto más de nuestra agenda de Facebook, e interactuar a través de chat.

¿Para qué va a servir? En principio para tareas básicas: preguntar por facturas, servicios contratados, el uso de datos y poco más… En otro evento organizado por Intel sobre Inteligencia Artificial en el que participó un portavoz de Movistar+ , éste ya nos contaba que la IA la utiliza su compañía para recomendarnos contenidos multimedia en nuestros servicios de Imagenio. No la llamó Aura, pero es otra aplicación práctica de la IA. Lo que ya nos contó y se revela oficialmente ahora, es que nos ayudará a gestionar la conectividad del router, controlar la televisión con la voz o pedir una recomendación. Al final, es ahorro de costes para la operadora. No nos engañemos. Aura crecerá seguro… Esto no ha hecho más que empezar. Que tiemblen los call center

ENJOY SAFER TECHNOLOGY™

Adapta tu empresa a la nueva normativa de protección de datos

ENDPOINT ENCRYPTION

DESCARGA GUÍA GRATUITA GDPR

http://gdpr.eset.es 962913348

@asLAN potencia el Hybrid Cloud

En la nueva era digital, el Centro de Datos se ha convertido en un elemento vital de la empresa en constante evolución. Tendencias como Hybrid Cloud, Industry 4.0, Artificial Intelligence o las nuevas redes 5G impactan directamente en las necesidades de almacenamiento, proceso y conectividad del Data Center.

En el mes de abril se celebra en Madrid el Congreso&EXPO ASLAN2018 bajo el título "Enabling Digital Transformation", en el que ofrecerán su visión cerca de 150 speakers y mostrarán sus soluciones tecnológicas más de 120 expositores especializados en servicios, aplicaciones e infraestructuras conectadas para impulsar la Transformación Digital: IoT, Hybrid Cloud, Artificial Intelligence, CyberSecurity, Software Defined Infrastructure, Wireless Networks, Data Centers, Digital WorkSpacE. Coincidiendo con el 25ª aniversario del Congreso, la Asociación @asLAN prepara una edición muy especial a la que acudirán más de 6.000 profesionales (responsables IT, ingenierías, proveedores de servicios…) y se realizarán eventos específicos sobre temas de actualidad como el Foro Tendencias Tecnológicas "SmartDataCenter: El Corazón de la economía digital", durante el que se abordarán cuestiones como:

- Hybrid Cloud, integración de servicios críticos para la empresa digital.
- "Todo" definido por Software.
- Innovación en el Centro de Datos 4.0.
- Hiperconvergencia e infraestructuras ágiles.

Además de este Foro, en el que ofrecerán su visión fabricantes "líderes&visionarios" de la industria IT internacional y los grandes centros de datos neutrales en España, la EXPO contará con un espacio diferenciado en el que un ecosistema de proveedores especializados en soluciones para mejorar la eficiencia en los Centros de Datos Corporativos, presentarán sus productos y soluciones.

También este año colabora la Plataforma enerTIC.org, impulsando la participación de proveedores especializados en soluciones mejorar la Eficiencia Energética en el DataCenter: El núcleo de la economía digital. En www.congreso.aslan.es puede consultarse ya la relación de expositores y todos los eventos previstos en el marco de ASLAN2018.

Por Manuel Navarro

Un Mobile político

Por primera vez en su historia, el Mobile World Congress a punto estuvo de convertirse en un evento político. Pero aunque les pese a algunos, eso no ocurrió. Dos son los elementos que lo han intentado:

1.- Ada Colau: la alcaldesa de Barcelona quiso tener su papel protagonista como siempre hace. Ese papel lo tiene perfectamente meditado: se trata de estar al plato y a las tajadas, así que primero se niega a recibir al Rey, porque "es un acto de pleitesía", (aunque en las ediciones anteriores no tuvo ningún problema en hacerlo),para a continuación asistir a la cena oficial y aplaudirle el discurso.

2.- La Prensa: es muy llamativo abrir las principales páginas de los periódicos y de las webs con las manifestaciones independentistas y unionistas: eso genera venta de periódicos y aumentos de visitas. Sin embargo, es echar más leña al fuego, toda vez que la representación de ambas manifestaciones era mínima, apenas unos centenares. De ahí, a intentar dar la sensación de que se quería boicotear al MWC dando a entender que en Barcelona, prácticamente había un enfrentamiento brutal entre ambas partes va un trecho. Tal vez si dejáramos de exagerar determinadas noticias, las soluciones al tema catalán sería más fácil.

La realidad es que los cuatro paletos, (los de ambos lados no nos olvidemos), pasaron desapercibidos para la organización del MWC, que encontró el evento que realmente quería:: stands llenos y gente y empresas haciendo negocio.

De hecho, el único pero que se le puede poner al Mobile World Congress de este año corre a cuenta de los propios organizadores: faltaron auténticos gurús y personalidades relevantes. Que Fernando Alonso sea la personalidad más representativa dice que algo se ha hecho mal por parte de la organización. Si esto se mejora y dejamos de analizar el MWC como un elemento distorsionador de la política nacional, no cabe ninguna duda de que el evento se encuentra en el mejor lugar posible para su celebración en futuras ediciones.

phc CS

BUILT FOR MORE

EL **ERP** QUE SE ADAPTA A SU NEGOCIO

Descubra cómo el Software de Gestión puede acelerar su empresa

www.phcsoftware.com

CONOZCA LA V22 DE PHC CS

MÁS AGILIDAD, MEJOR EXPERIENCIA, MÁS INNOVACIÓN.

V22 LIBERTAD DE ACCIÓN
EXCELENCIA EN LA GESTIÓN

Intel rediseña el centro de datos

Intel acaba de anunciar los SSD DC Intel serie P4510 para aplicaciones de centros de datos. La serie P4510 usa una NAND 3D TL de 64 capas de Intel para permitir a los usuarios finales realizar más tareas en cada servidor, además de ofrecer soporte a mayores cargas de trabajo y más capacidad con un ahorro de espacio. La serie P4510 permite hasta cuatro veces más terabytes por servidor y ofrece hasta 10 veces más latencia en lectura aleatoria, con un 99,99% de calidad de servicio en comparación con las generaciones anteriores. La unidad también puede proporcionar hasta el doble de operaciones de E/S por segundo (IOPS) por terabyte. Las unidades de 1 y 2TB se han distribuido a los suministradores de servicios en la nube (CSP) en grandes cantidades desde agosto de 2017, y las de 4y 8TB se encuentran disponibles para los CSP y para los clientes del canal. Todas estas capacidades se encuentran disponibles para formatos U.2 de 2.5" y 15 mm y utilizan una conexión PCIe NVMe 3.0 x4. Para acelerar el rendimiento y para simplificar la gestión de los SSD PCIe serie P4510 y de otros SSD PCIe, Intel también ofrece dos nuevas tecnologías que funcionan juntas para sustituir el hardware de almacenamiento de legado. Los procesadores Escalables Intel Xeon incluyen la tecnología Intel Volume Management Device (VMD), para facilitar la gestión robusta como las retiradas / inserciones inesperadas y la gestión mediante LED de los SSD PCIe conectados directamente al CPU. Basándose en estas prestaciones, el Intel Virtual RAID on CPU (VROC) usa la tecnología Intel VMD para proporcionar RAID a los SSD PCIe. Gracias a la sustitución de las tarjetas RAID por el Intel VROC, los clientes pueden disfrutar hasta del doble de rendimiento de IOPS y hasta un 70% de ahorro de costes con unos SSD PCIe conectados directamente al CPU, mejorando así el rendimiento de las inversiones de los clientes en almacenamiento basado en SSD.

Por Óscar González

El consorcio Alastria

La Red Alastria es un consorcio sin ánimo de lucro, con el fin de proveer a Espana de la Infraestructura Blockchain basica "Red ALASTRIA" y del estandar de Identidad Digital "ID ALASTRIA" que permita que las transacciones sobre dicha red puedan tener validez legal y, con ello, la Sociedad espanola pueda desarrollar su propia estrategia Blockchain y que anunció su creación a finales del año pasado.

El público general está siendo bombardeado de forma constante por noticias que tienen que ver con Bitcoin y redes Blockchain. Pero la tecnología blockchain tiene muchos otros usos además del de ser la implementación bajo la que descansan la mayoría de las criptodivisas. Pero a nivel legal todavía existen muchas dudas y un largo camino que recorrer. Para ello, la red Alastria, que desde cuenta con cerca de 80 miembros, de las mayores empresas de distintos sectores de nuestro país.

La lista de participantes pasa por la gran banca, operadoras y muchas empresas de desarrollo tecnológico, destacando compañías como Telefónica, Santander, Bankia, CaixaBank, BBVA, Sabadell, Kutxabank, Repsol, Cepsa, Indra, BME, Caja Rural, Cajamar o empresas de desarrollo fuertemente orientadas hacia esta tecnología, como SameLAN, entre muchas otras.

El trabajo está ya en marcha y desde aquí esperamos que la Red Alastria sea una realidad en el corto plazo, y que abra el camino para asentar los beneficios de la tecnología blockchain en nuestro cuerpo jurídico y social, para que de esta forma se produzca una verdadera transformación digital en multitud de procesos y operativas de negocio.

Mientras tanto, todo el trabajo tecnológico se publica en su propio github, accesible en https://github.com/alastria.

CLOUD
by
arsys

¡SEGUIMOS DANDO LA VUELTA AL CLOUD!

TE PRESENTAMOS EL NUEVO CLOUD HIBRIDO

© 2018. Arsys Internet S.L.U. Promoción válida desde el 1 al 31 de marzo de 2018. Consulta condiciones en www.arsys.es/legal

CLOUD

30 DÍAS GRATIS

PRUÉBALO

- SERVIDORES CLOUD Y DEDICADOS EN UN ÚNICO PANEL
- FÁCIL Y RÁPIDO, DESPLIEGUE EN MINUTOS
- PAGO POR USO, SIN INVERSIÓN INICIAL
- ALTO RENDIMIENTO, DISPONIBILIDAD Y FIABILIDAD
- CENTROS DE DATOS EN ESPAÑA, EUROPA Y EEUU
- INNOVACIÓN Y ALTA TECNOLOGÍA A TU ALCANCE

EL MEJOR SERVICIO AL CLIENTE | INNOVACIÓN TECNOLÓGICA | MÁS DE 20 AÑOS DE EXPERIENCIA

www.arsys.es/cloudhibrido | 902115530

arsys

Huawei se adentra en el mercado del portátil profesional

Huawei ha presentado en la inauguración del Mobile World Congress 2018, el primer portátil con pantalla FullView del mundo

El Huawei MateBook X Pro (a partir de 1,500 euros), además de la serie de tablets Huawei MediaPad M5 (a partir de 349 euros). Con un cuidado diseño tanto en su interior, como en su exterior, los nuevos portátiles y tablets llegan con un conjunto de exclusivas prestaciones.

Los equipos estarán disponibles en España a partir del segundo trimestre y, a pesar de que el mercado de portátiles y tablets se han incorporado después que los móviles, la filial española se toma muy en serio este segmento, tal como destacó a este Diario Informático, Ramiro Larragán, Marketing Manager de Huawei Consumer BG. "No trabajamos prácticamente nada la gama de entrada: los productos que comercializamos están situados en el terreno medio-alto del mercado, con un nivel de calidad muy elevado", agregó.

Tanto Huawei MateBook X Pro como Huawei MediaPad M5 combinan pantallas nítidas y claras, potentes actualizaciones de hardware y avances inteligentes de software: Core i7/i5 de octava generación, gráficos NVIDIAGeForceMX150 GPU con 2GB de GDDR5, una batería duradera de 57.4Wh (capacidad típica). Huawei Matebook X Pro es cuenta además con sistema de sonido Dolby Atmos Sound System, y altavoces personalizados que ofrecen un sonido envolvente e inmersivo.

Serie Huawei MediaPad M5: Ergonómicamente diseñada con un cristal 2.5D y una pantalla de 2K, y mejorada con ClariVu 5.0, las tablets de 8.4 o 10.8 pulgadas cuentan con altavoces estéreo sintonizados por Harman Kardon. La tecnología Huawei Histen proporciona audio 3D inmersivo y admite audio de alta resolución para una calidad de sonido excepcional.

Huawei MateBook X Pro: un portátil ultra delgado de 13.9, con pantalla Huawei FullView 3K totalmente táctil y con un ratio de pantalla del 91%. Incluye un potente procesador Intel®Huawei MediaPad M5 Pro de 10.8 pulgadas viene con un ultra preciso Huawei M-Pen con 4.096 niveles de sensibilidad para tomar notas sin esfuerzo.

HUAWEI MATEBOOK X PRO

Huawei MateBook X Pro es el primer portátil que cuenta con pantalla Huawei FullView. El portátil de 13,9 pulgadas y 3K con una pantalla táctil de 10 puntos tiene una resolución de 3000 x 2000 píxeles y un ratio de aspecto de 3:2, perfecto para la creación de contenido. Cuenta con acabado de corte de diamante y chorro de arena para crear un cuerpo ultra delgado de tan solo 14,6 mm de grosor y un peso de 1,33 kg. Huawei MateBook X Pro está disponible en dos colores: Space Grey y Mystic Silver. Con un poderoso procesador IntelCore i7 / i5 de octava generación y gráficos NVIDIAGeForceMX150 con 2GB de GDDR5, Huawei MateBook X Pro presenta Dolby Atmos Sound System, audio en movimiento con Dolby Atmos y altavoces personalizados. Con Dolby Atmos Sound System,. Una batería de 57.4Wh y el diseño de bajo consumo de energía de Huawei proporcionan hasta 12 horas de reproducción de video 1080P, 14 horas de trabajo o 15 horas de navegación por páginas web. Huawei ha aplicado muchas de sus innovadoras tecnologías de teléfonos inteligentes a Huawei MateBook X Pro para crear experiencias de usuario intuitivas y sin esfuerzo.

Anatomía de un ataque dirigido

Por Alfonso Ramírez
director general de Kaspersky Lab Iberia

Los ataques dirigidos son procesos a largo plazo que pueden comprometer la seguridad y dan acceso a los atacantes el control de los sistemas TI de la víctima. Aunque algunos ataques utilicen APTs –muy efectivas, pero costosas de implementar—, otros pueden usar técnicas mucho más sencillas como malware avanzado o exploits de día cero.

En teoría, la cadena de un ataque dirigido parece bastante sencilla: Reconocimiento & Testing, Penetración, Propagación, Ejecución y Resultado. Esto podría dar a entender que bloquear de forma automática las primeras fases de un ataque podría ser suficiente para neutralizarlo. Pero, en realidad, los ataques dirigidos son muy sofisticados y no lineales, en términos de progresión y ejecución. Así, las funcionalidades de detección automática, monitorización continua y "threat hunting" deben ser parte de una estrategia en varias etapas.

Un ataque dirigido es un proceso lento que viola la seguridad y permite al cibercriminal evitar los procesos de autorización e interactuar con la infraestructura TI; es decir, "esquivando" las tradicionales medidas de detección.

En primer lugar, hay que ver estos ataques como proyectos en constante evolución más que como una acción maliciosa única. Según nuestra experiencia en la monitorización de ataques globales, este tipo de operaciones duran al menos 100 días e incluso años para agencias gubernamentales, grandes empresas e infraestructuras críticas.

En segundo lugar, el proceso de estos ataques suele centrarse en determinadas infraestructuras y está diseñado para acabar con ciertos mecanismos de seguridad e incluso pueden inicialmente dirigirse a determinados empleados a través del email o incluso de las redes sociales.

En tercer lugar, la operación es gestionada por un grupo organizado o grupo de profesionales, armados con las herramientas más sofisticadas. Sus actividades van más allá de un proceso y podrían definirse como una operación de combate. Por ejemplo, los atacantes recopilan una lista de empleados que podrían convertirse en la puerta de entrada de esa organización, y estudian sus perfiles online y su actividad en redes sociales. Después, toman el control del dispositivo de la víctima y una vez infectado, los intrusos se apoderan de las redes desde donde dirigen todas sus actividades criminales.

UN MARCO ADAPTATIVO DE SEGURIDAD

Implementar un enfoque de seguridad adaptativo reduce de forma significativa el riesgo de ataques y, obviamente, los daños. Muchas de las amenazas pueden ser identificadas con tecnologías analíticas y preventivas; mientras que otras pueden ser detectadas y resultar inocuas a través de enfoques de protección más tradicionales. La prevención y predicción trabajan para parar un incidente antes de que se convierta en un "accidente". La detección y la respuesta definen el descubrimiento y la remediación de un "accidente". En este paradigma, cada paso supone un mayor coste en recursos para reaccionar que en el estadio anterior. A menudo, la seguridad recibe el presupuesto que se estima que merece, no el que en realidad necesita. La seguridad ha de ser prioritaria, también en cuanto a la inversión, para un despliegue con éxito y un tiempo de recuperación (RTO) óptimo.

Esencialmente, supone que los sistemas de prevención tradicional han de funcionar en coordinación con tecnologías de detección, analíticas de amenazas, capacidades de respuesta t técnicas de seguridad predictivas. Esto ayuda a crear un sistema de seguridad que constantemente se adapta y responde a los retos emergentes de las empresas.

Así, la implementación de una estrategia de seguridad adaptativa permite PREVENIR y reducir el número de amenazas avanzadas y ataques dirigidos; DETECTAR e identificar las actividades sospechosas (ataques dirigidos); RESPONDER, reducir las brechas de seguridad e investigar los ataques y PREDECIR dónde y cómo se producirán los próximos ataques

Samsung: los Rolling Stones de la movilidad

Como si fuera un megaconcierto de los Stones, Samsung se ha convertido en la estrella del día previo a la inauguración del MWC.

Manuel Navarro

Al igual que los viejos rockeros cada vez que salen de gira, Samsung puede presumir de ser la principal atracción del Mobile World Congress 2018. Para acceder a Unpacked 2018 hay que aguantar una cola kilométrica para acceder al recinto, pasar un control de seguridad y enseñar tu pase acompañado del DNI para asegurar que nadie que no esté invitado acceda al recinto en el que se va a producir la presentación. Una vez dentro, toca esperar alrededor de una hora y media para que el show comience.

En Samsung saben que son las estrellas. Ya es tradición que el buque insignia de la compañía se presente en este mega-evento que, de momento, se sigue celebrando en Barcelona. Al igual que sucede con los Jagger, Richards y compañía, los surcoreanos saben lo que demanda la audiencia… y se lo dan. Los Stones tocan Satisfaction y el público se entrega. Samsung lanza su nuevo smartphone y los aplausos se generalizan, incluso entre la prensa especializada. Sólo faltan unos pocos y efectistas trucos, como utilizar la realidad virtual para que se simule que los asistentes tienen el nuevo dispositivo en la palma de la mano, y la entrada al show habrá merecido las colas y las esperas.

Porque el S9 y su hermano mayor el S9+ son unos terminales con unas excelentes características. La compañía se ha centrado en tres apartados para su desarrollo: la cámara, la seguridad y la pantalla. La surcoreana sigue apostando por la pantalla infinita, algo que ha sido muy del gusto de los consumidores y que ya es algo más que probado, toda vez que son muchos los fabricantes que han incorporado estas pantallas en sus tecnologías.

Es la cámara donde Samsung ha realizado un mayor esfuerzo. La novedad radica en que cuenta con un sensor Super Speed Dual Pixel con procesador y memoria dedicados y capacidad para combinar hasta 12 tomas en una única imagen, para producir fotografías en alta calidad. De esta forma, los nuevos terminales cuentan con Grabación de vídeo Super Slow-mo que permite la grabación en vídeo a 960 fotogramas por segundo. Los Galaxy S9 y S9+ también disponen de detección automática del movimiento (Motion Detection), una función inteligente que comienza a grabar automáticamente cuando detecta movimiento dentro del encuadre. Además destaca la cámara Super Low Light: La iluminación es el secreto de toda buena fotografía. Pero a menudo las fotos se toman en condiciones de luz que no son las ideales, y la mayoría de las cámaras de smartphone tienen una apertura fija que no puede ajustarse ni para ambientes con poca luz ni para escenas con demasiada iluminación. Esto resulta en imágenes granulosas por la falta de luz o quemadas por el exceso de luz. De forma parecida a como el iris del ojo humano se dilata y se contrae, la apertura dual de Samsung (f1,5 – f2,4) se ajusta automática para dejar entrar más luz cuando la escena está oscura y para impedir el exceso de luz cuando la escena es demasiado luminosa, consiguiendo fotografías nítidas y claras.

Y finalmente, uno de los apartados más destacados aunque la verdad, no como característica importante del teléfono sino como un aspecto que pueden valorar por los usuarios, cada vez más ávidos de encontrar aplicaciones destinadas al ocio más barato. En este caso se llama AR Emojis y gracias a ella el usuario puede crear un emoji que se parece, suena y actúa igual que él. Los AR Emojis utilizan un algoritmo de inteligencia artificial que analiza una imagen 2D del usuario y que a la vez traza un modelo 3D de su rostro basado en más de 100 rasgos faciales para representar e imitar expresiones como guiños y movimientos de cabeza, logrando una personalización realista.

En definitiva, nos encontramos ante un terminal que aporta novedades interesantes pero no llamativas. Un smartphone que seguramente liderará, al menos durante unos meses, el mercado de ventas premium. Un smartphone que se queda en una buena canción compuesta para satisfacer a los fans más acérrimos pero que no es un “Paint it Black”.

Synology C2 Backup, rentable solución de copia de seguridad en la nube

Los datos importantes de una empresa pueden perderse debido a fallos de hardware, errores humanos u otros tipos de desastres. Las compañías necesitan garantizar la gestión de las copias de seguridad de los datos que manejan con soluciones fiables y seguras, pero también fáciles de utilizar, rápidas y manejables. Y, por supuesto, rentables. Synology C2 backup garantiza todo ello y aporta una experiencia uniforme en copias de seguridad locales y en la nube para sus usuarios.

Los principales puntos fuertes de Synology C2 Backup son: garantizar la disponibilidad de todos los datos en la nube, posibilitar la programación de copias de seguridad en la nube y copias de seguridad diferenciales y la restauración granular de la que hablaremos más adelante.

Esta solución de Synology se ofrece como un servicio dentro del llamado Synology Cloud² (Synology C2) diseñado tanto para usuarios empresariales como domésticos. Gracias a las copias adicionales de los archivos importantes almacenados en Synology C2, es posible garantizar la seguridad y disponibilidad de los datos en caso de desastre. Synology C2 Backup ofrece dos planes flexibles para satisfacer las diversas necesidades de los clientes. El primer plan ofrece un backup diario con retención regular, 11 versiones de respaldo durante los últimos 30 días sin cargo adicional y posibilidad de elección de plan flexible para capacidad de almacenamiento entre 100 GB, 300 GB y 1 TB. El segundo plan, que es más avanzado y ofrece horarios flexibles para realizar el backup, tiene políticas de retención personalizables, duplicación de datos para optimizar el uso del almacenamiento e incluye desde 1TB hasta 10 Terabytes de capacidad de almacenamiento.

Asimismo, es posible contratar más de 10 TB previa demanda a los profesionales de Synology.

La protección de los datos de este servicio tiene garantías de fiabilidad asimilables a un nivel de seguridad militar. Asegura la protección de los datos importantes frente a accesos no autorizados gracias al uso de tecnologías de cifrado avanzadas, como AES-256, Advanced Encryption Estándar, que son los algoritmos de cifrado más utilizados y seguros en la actualidad, y RSA2048, los sistemas de cifrado asimétricos más exitosos hasta el momento. Con Synology C2 Backup, nadie puede acceder a los datos si no conoce la clave privada del usuario, ni siquiera Synology.

Si tenemos que destacar algunas de las funciones más relevantes de esta solución podemos mencionar, entre otras, que las tareas de copia de seguridad pueden ejecutarse automáticamente a una hora programada o repetirse periódicamente de la forma elegida, de modo que no afecten a la producción de la empresa. Además, la compatibilidad con diferentes versiones de copia de seguridad de Synology C2 Backup presenta la ventaja de ofrecer varios puntos de recuperación de datos, y posibilita navegar fácilmente por las distintas versiones de los archivos. Es interesante también la función de restauración de archivos granulares que permite recuperar un archivo específico sin tener que restaurar todo en la misma tarea de copia de seguridad y así ahorrar un tiempo precioso. Incluso sin un Synology NAS, es posible acceder a los datos importantes almacenados en Synology C2 desde cualquier navegador y con una gran flexibilidad.

SOLUCIÓN ASEQUIBLE Y COMPLETA

Aparte del coste de suscripción, que dependerá del plan contratado, el uso de este servicio no tiene ningún otro coste oculto. Con Synology C2 Backup, se dispone de tamaño y acceso de archivos ilimitados y recuperación de datos y velocidad ilimitada en las copias de seguridad y en las recuperaciones de datos. Synology no realiza cargos adicionales por cargar, restaurar o explorar archivos en la consola C2, por ejemplo. Además, la marca invita a probar completamente gratis C2 durante 30 días para probar todas las funcionalidades antes de realizar la compra. El almacenamiento de copia de seguridad en Synology C2 puede adquirirse a través de una cuenta Synology y compartirse con varios servidores Synology NAS asociados a esa cuenta, lo que permite aumentar la flexibilidad del uso de almacenamiento. Además, es posible actualizar el plan de copia de seguridad durante el periodo de suscripción en caso de que se necesite más espacio.

d!talk en CEBIT 2018: nueva fórmula de conferencias

Uno de los apartados más interesantes de la feria tecnológica CEBIT que se celebrará del 11 al 15 de junio en los recintos feriales de Hannover es, sin duda, el dedicado a las charlas y conferencias.

La organización de CEBIT 2018 ha diseñado un nuevo formato de conferencias que complementan la exposición centrándose en crear un ambiente especial y ampliando el horario hasta las 19:00h con el fin de incrementar aún más las oportunidades del networking profesional.

En d!talk y, por primera vez, los gurús y los pioneros de la digitalización tendrán a su disposición más de 10 salas dentro de las exposiciones en las que compartirán conocimientos

Al igual que ocurre con el evento, la transformación también se ha realizado en este apartado y se ha adaptado a los nuevos tiempos que corren en el mundo de la tecnología de tal forma que hay charlas y conferencias de interés para todo tipo de público, usuarios y profesionales. El nuevo formato estrena, además, un nuevo nombre: d!talk.

En d!talk y, por primera vez, los gurús y los pioneros de la digitalización tendrán a su disposición más de 10 salas dentro de las exposiciones en las que compartirán conocimientos y visiones de especial relevancia con todos los visitantes interesados. Los que asistan a cada una de estas conferencias podrán obtener los conocimientos que pueden marcar la diferencia para el éxito futuro. Temas como el poder que ofrece la realidad aumentada o los peligros que pueda suponer la inteligencia artificial son sólo algunos de los ejemplos de las conferencias que tendrán lugar en CEBIT. Para ello contará con ponentes de primera línea como Max Amordeluso, evengelista para Europa de Amazon Alexa; la psicóloga forense Julia Shaw, conocida mundialmente por su best-seller "The Memory Illusion" y su trabajo en el área de falsos recuerdos; Jaron Lanier, escritor e informático y uno de los pioneros en el campo de la realidad virtual; el experto en ciberseguridad Mikko Hypponen o la emprendedora y coach Susanne Birgersdotter, entre muchos otros.

Signals

Dentro del capítulo que en esta nueva era emprendida por CEBIT tienen las conferencias destaca Signals. Se trata de un nuevo tipo de conferencia centrada de manera exclusiva en Influencer Marketing, Social Media y Networking. Signal es un lugar perfecto en el que personas influyentes, bloggers y creadores digitales pueden encontrarse con profesionales del marketing y las relaciones públicas. Más de 50 oradores, divididos en dos etapas, estarán presentes en Signal. Los asistentes además, podrán participar en talleres de expertos sobre mejores prácticas, tendencias y desafíos en Influencer Marketing.

Lo más importante de d!talk son los múltiples formatos de charla y conferencias que tendrán lugar, de tal forma que prácticamente no hay excusa para no poder asistir a ninguna de ellas. Los visitantes podrán elegir entre las clásicas keynotes, charlas entre varios expertos, paneles, lanzamientos y un largo etcétera de opciones.

Por supuesto la temática de la mismas abarcan todos los temas y las tendencias del momento:

- Inteligencia artificial,
- Realidad Aumentada y Virtual
- Blockchain
- Centro de datos, servidor y soluciones de almacenamiento
- Administración digital
- Movilidad futura
- Robots humanoides
- Internet de las Cosas
- Nueva tecnología y tecnologías disruptivas
- Investigación e Innovación
- Seguridad
- Startups
- Sistemas no tripulados y aviones no tripulados
- Mujeres en negocios digitales

En definitiva, d!talk será el espacio de referencia para saber cuáles van a ser las próximas tendencias en el mundo TIC de la mano de los principales expertos e influencers de la actualidad.

Trabajamos para Ti

Ingecom

Si te gusta la CiberSeguridad y quieres unirte a un equipo de profesionales de la misma, ponte en contacto con nosotros

www.ingecom.net info@ingecom.net

MADRID C/ Infanta Mercedes, 90 - 8ª Planta – 28020 Madrid – Tel.: +34 91 571 51 96 Fax: +34 94 441 05 39
BILBAO C/ Máximo Aguirre, 18 Bis - 8ª Pl. – 48011 Bilbao (Bizkaia) – Tel.: +34 94 439 56 78 Fax: +34 94 441 05 39
LISBOA Edificio Infante, Avenida D. João II, 35, 11°A – 1990-083 Lisboa – Tel.: +351 21 012 65 65

Movilidad, un camino por recorrer

La práctica totalidad de la población ya está acostumbrada a trabajar en movilidad. Las empresas también. Sin embargo, aunque se trata de un mercado asentado, las organizaciones todavía tienen que recorrer mucho camino. Para tratar este tema Byte TI juntó en un desayuno tecnológico a Javier Naranjo, BDM Mobile SSP Red Hat Iberia; Enilio Álvarez, Strategic Accounts and Business Solutions Director de Econocom; Iván Abad, Technical Services Manager para Iberia de Commvault de Commvault; Carlos Marina, responsable de dispositivos móviles profesionales de HP y Miguel Hernández, Director de producto para Iberia de Lenovo.

El primer aspecto que se trató durante el evento fue el análisis de las tendencias del mercado y cuál es su situación actual. En este sentido, Javier Naranjo, BDM Mobile SSP Red Hat Iberia aseguró que "el mercado se está enfocando a la modernidad de las aplicaciones en las que el usuario usa el móvil prácticamente para todo en el que entran en juego otros elementos. Por ejemplo, ya no se buscan las prestaciones clásicas de un coche sino otro tipo de prestaciones más tecnológicas. La movilidad es un elemento al servicio del usuario y es la puerta de entrada a las TIC". Por su parte, Enilio Álvarez, Strategic Accounts and Business Solutions Director de Econocom afirmó que "la movilidad ha dejado de ser una tendencia. Ninguna empresa hace ya un cambio sin contemplar la movilidad. Ya han asimilado que tienen que hacer las cosas de otra manera y que sus empleados no van a aceptar unas herramientas con menores capacidades a las que utilizan para uso personal. No van a aceptar, por ejemplo, que para pedir un viaje de empresa tengan que firmar un papel, cuando en su vida real no lo hacen". En la misma línea se situó Iván Abad, Technical Services Manager para Iberia de Commvault para quien la movilidad "ya es una realidad. Todos estamos acostumbrados a trabajar con dispositivos móviles. Obviamente, la tendencia es a lo contrario, es decir que desaparezca el "legacy": todo lo que sea escrito, ir a firmar un documento a un banco, etc. todo eso tiene que desaparecer. Cuando un niño de 10 años se incorpore al mundo laboral no va a entender que se tenga que trasladar a otro sitio a firmar un papel". Carlos Marina, responsable de dispositivos móviles profesionales de HP cree que en la actualidad, "hay muchas tendencias pero lo que hay a día de hoy en torno a la movilidad son realidades. El 50% de los empleados ya está adaptado a esta realidad. Se ven tendencias, como que cada vez más aplicativos en la nube, aplicaciones empresariales desarrolladas en movilidad, el IoT, etc.. Ya no se puede trazar una línea en la que se separe la vida laboral de la vida privada. Se ha mezclado todo: los usuarios trabajan en su horario no laboral y hacen gestiones personales en su horario laboral". Finalmente, Miguel Hernández, director de producto para Iberia de Lenovo afirmó que "hace cuatro o cinco años años, cuando se hablaba de movilidad, lo estábamos haciendo sobre un perfil de usuario que estaba viajando de forma constante. Hoy no es así: la movilidad está dentro de la misma oficina. En el tema de hardware, los fabricantes tenemos el reto de facilitar las cosas. Otro reto está en el uso del software en cualquier tipo de dispositivo: se pueden hacer las mismas cosas con diferentes dispositivos y cualquier app. Esas aplicaciones tiene que estar disponible en cualquier tipo de hardware".

MEJORAR LA MOVILIDAD

Aunque la movilidad se ha extendido entre usuarios y organizaciones lo cierto es que éstas últimas todavía tienen mucho camino por recorrer sobre todo para adaptarse a las necesidades que requieren sus trabajadores y que permitirían implementar la productividad de éstos. En este sentido, el portavoz de Red Hat afirmó que "las empresas se están adaptando aunque no a la velocidad que se desarrolla la tecnología. Sin embargo, se han dado cuenta de que, para poder sacar el máximo rendimiento al empleado, tiene que proporcionarle las herramientas adecuadas. El horario laboral se ha extendido y hoy los trabajadores adaptan su horario para sacar adelante el trabajo que tienen que hacer independientemente de dónde estén". Carlos Marina de HP cree que "lo que no hay que olvidar es que estamos en una transformación muy importante que viene desde lo más profundo de la empresa. Es

cierto que se requiere de inversiones potentes pero el efecto startup ha ayudado a que las grandes empresas se suban al carro de apostar por las nuevas tendencias tecnológicas". En este sentido, el representante de Commvault considera que "las grandes cuentas están entrando en herramientas de adaptación a los dispositivos móviles porque los usuarios les han obligado a ello. Por ello han acometido la transformación digital porque si no, se veían fuera del mercado. Las empresas se están adaptando a la velocidad de las exigencias de los usuarios. A nivel personal somos muy exigentes y queremos las cosas inmediatamente, por ello exigimos a nuestras empresas lo mismo".

El cambio se está produciendo y ya no hay marcha atrás. Las empresas lo saben y están empezando a apostar de forma rápida por las soluciones móviles. Para Enilio Álvarez de Econocom, "hemos notado un cambio en las empresas. Hay un montón de proyectos para renovar el puesto de trabajo, darle un nuevo modelo de puesto de trabajo para adaptarnos a sus necesidades. La empresa está invirtiendo en rediseñar el entorno de trabajo, no sólo en cuanto a equipamiento, sino también en renovación de los espacios de trabajo. Además las empresas, cada vez más, están desarrollando productos 100% digital. Por primera vez se está invirtiendo en el puesto de trabajo y la otra cosa en la que se está invirtiendo en el desarrollo del software". Por su parte, el portavoz de Red Hat aseguró que "la velocidad que piden los usuarios es básica y la empresa se ha subido a ese carro. La empresa, por ejemplo, tiene que ser capaz de sacar muy rápido las apps, para que el empleado sea igual de rápido".

AA.PP.

¿Todo el mundo se está adaptando de forma rápida a los entornos de movilidad? Todos no. Hay un sector en el que la movilidad no ha calado ni tiene visos de calar a corto plazo: se trata del de las Administraciones Públicas. Tal y como aseguró Javier Naranjo, "el sector que está más retrasado y que debería ser al contrario, es el de las Administraciones Públicas. Por contra, donde vemos que se están poniendo las pilas es en el sector de la banca y sectores como el industrial. Este tipo de empresas se están empezando a poner las pilas porque los ciudadanos se lo están exigiendo". Para Enilio Álvarez, "en el caso de las Administraciones Públicas hay una gran demanda por parte de los usuarios pero no hay tanta presión interna por parte de los trabajadores y por eso no van tan rápido como sucede en el resto de empresas y esto es un problema. Nosotros notamos que en las grandes organizaciones se mueven pero sobre todo las que se mueven de forma rápida y aborda proyectos muy interesantes son las pymes". En la misma línea se situó Iván Abad de Commvault. En su opinión "efectivamente el desarrollo más lento se está produciendo en la Administración Pública porque quizá tienen otra mentalidad y ni siquiera han pensado en cuánto dinero se podrían ahorrar teniendo menos oficinas o locales. Además, también son más reacios también a la hora de facilitar información por Internet por un tema, que según dicen ellos, es por motivos de seguridad". El portavoz de HP afirmó que "efectivamente la Administración Pública es el sector que está más lejos de adaptarse a los entornos móviles y según lo veo yo es por varios aspectos: uno por motivo de cultura, otro porque no necesita tener el ROI y luego por un tema de productividad. En el caso de la empresa privada queremos ser más productivos porque queremos vivir mejor en nuestro entorno laboral, pero eso no ocurre en la Administración. Ahora mismo en las AA.PP., el 70% de los puestos de trabajo son un ordenador fijo en una mesa. Hay un tema que es muy importante que es que la movilidad atrae talento y lo que no sabe la Administración Pública es que en un futuro la gente no va a a querer trabajar en ella ya que se ha quedado totalmente desfasada". Finalmente el portavoz de Lenovo cree que "se trata de un tema cultural y de necesidad. La Administración Pública no necesita captar ningún cliente. Al final, en el mundo privado se mezcla todo. Puedes llegar a las 11:30 de la mañana y estar trabajando a las 23:00 en tu casa. En la Administración al final, sus trabajadores tienen un horario fijo y de ahí no se mueven".

TRANSFORMACIÓN DIGITAL

La movilidad es uno de los pilares de la

transformación digital. Sin ella, esa transformación seguramente no existiría. Tal y como afirma Miguel Hernández, "en estos momentos hay un cambio de paradigma a la hora de desarrollar productos y soluciones. Si no se hace esto la transformación digital no va a ocurrir. Hoy en día es obligatorio ser móvil". De la misma opinión es Carlos Marina de HP quien asegura que "no hay transformación digital sin movilidad. Es un cambio profundo que no consiste sólo en comprar móviles, tabletas o hacer una aplicación para el empleado. Se trata de diseñar una estrategia a medio plazo. Se ha inundado a los departamentos comerciales de tabletas, portátiles y móviles, y esto es de locos. Es necesario que tengan una estrategia definida a medio plazo y no comprar equipos por comprarlos". La clave, según Iván Abad, "los usuarios estamos empujando a las empresas a que hagan esa transformación digital, y esa se tiene que hacer a través de los dispositivos móviles. No hay transformación digital sin movilidad". Para el portavoz de Econocom, "la movilidad es un elemento para conseguir la transformación digital. Para ello, hay que rediseñar los procesos existentes en una empresa. Hay que ver cómo se adaptan y como se hacen esos cambios. O se piensa esto o al final, las tabletas las usaran los hijos de los comerciales para jugar". Finalmente, y en la misma corriente de opinión se situó Javier Naranjo de Red Hat: "No se trata de recibir un terminal. Se trata de que el empleado sepa trabajar desde ese terminal o desde cualquier otro, en cualquier lugar y a cualquier hora. La empresa tiene que entender que para entrar en la transformación digital tiene que entender la movilidad".

SEGURIDAD

El último de los elementos clave, o al menos que está teniendo bastante impacto en los últimos meses, se encuentra en la seguridad. Para Miguel Hernández de Lenovo, "la falta de seguridad es una realidad a día de hoy. El problema no es que haya o no haya seguridad. Lo primero que hace falta es educar a los usuarios en seguridad. Las empresas tampoco estaban concienciadas hasta hace poco. Tenemos que reconocer que la seguridad al 100% no va a existir. Lo que hay que hacer es educar al usuario para que proteja los datos". Para el portavoz de HP, la seguridad "es el tema de moda. También hay un poco de marketing para que todos se conciencien sobre ello, pero las brechas de seguridad ya existían en el mundo analógico. Lo que es cierto es que como los entornos no están compartimentados, debe haber un tema de educación con respecto a la seguridad. Hay que tomar una serie de medidas para que la seguridad esté controlada. Hay que tener en cuenta también otras cosas: por ejemplo, a día de hoy, hay muchas empresas que utilizan software ilegal y eso provoca fallos". Desde Econocom, su portavoz Enilio Álvarez, cree que "la seguridad es la disculpa para no hacer cosas. Además también creo que el mundo digital es más seguro que el mundo físico. Por supuesto puede ser más seguro, pero eso no quiere decir que no lo sea". Finalmente el representante de Red Hat cree que la clave hay que buscarla en "enseñar al usuario que es el eslabón más peligroso. Otro aspecto importante es de tratar de alejar el dato del usuario en una nube securizada".

LOS PROTAGONISTAS

Enilio Álvarez, Strategic Accounts and Business Solutions Director de Econocom

Iván Abad, Technical Services Manager para Iberia de Commvault

Carlos Marina, responsable de dispositivos móviles profesionales de HP

Miguel Hernández, Director de producto para Iberia de Lenovo

Javier Naranjo, BDM Mobile SSP de Red Hat Iberia

HP: La movilidad profesional es uno de los factores más demandados por las empresas, porque a las cada vez mayores demandas en seguridad y fiabilidad, se suman requisitos como un diseño atractivo y la posibilidad de trabajar en cualquier momento y lugar, sin que el ritmo de trabajo se vea afectado. Buscamos por lo tanto, dispositivos táctiles, ligeros y potentes, con gran autonomía. También destacar las workstations portátiles para trabajos de campo que requieran altos niveles de potencia y rendimiento e incluso mochilas de realidad virtual para entornos profesionales avanzados.

COMMVAULT: Los datos de puestos de trabajo son a menudo uno de los aspectos más olvidados en la estrategia de protección de datos de una empresa, si bien el contenido de los portátiles, ordenadores de sobremesa y dispositivos móviles es uno de los activos más valiosos de una compañía e incluso cuando pueden correr el mayor riesgo. Sin embargo, solamente la mitad de las empresas usa actualmente algún tipo de proceso de copia de seguridad en el puesto de trabajo. Este hecho implica que la cantidad de datos de puestos de trabajo que están en peligro es bastante considerable. Commvault protege la información allí donde esté y permite a los usuarios acceder a sus datos y archivos con cualquier dispositivo, en cualquier lugar y en cualquier momento. La tecnología de Commvault permite ganar control sobre los datos de puestos de trabajo con una protección rápida, eficaz, segura y transparente en equipos de sobremesa y portátiles, que ofrece funciones de deduplicación en origen, programación flexible y gestión de ancho de banda.

RED HAT: Red Hat Mobile es la solución basada en el valor del open source empresarial para aportar flexibilidad, agilidad y rapidez a las organizaciones, los tres pilares que resumen la necesidad y la tendencia del mercado actual.Red Hat entiende la movilidad como pieza esencial en la transformación digital, al considerar la aplicación moderna como el activo clave que tiene la empresa para acelerar su transformación. Por ello, Red Hat Mobile conjuga el valor de negocio con las capacidades de los desarrolladores, para lo que se articula sobre Red Hat Opeshift, tecnología PaaS servicio líder del mercado y cimentada n los pilares modernos de contenedores, micro-servicios y DevOps. Entendiendo la casuística específica de las aplicaciones móviles, Red Hat Mobile es además una solución abierta y totalmente integrable con IoT, Machine Learning, Inteligencia Artificial y gestión de APIs.

LENOVO: En Lenovo siempre hemos tenido como premisa adaptarnos a las necesidades de los usuarios más exigentes y la movilidad es una de las prestaciones más demandas hoy en día. Es por ello que hemos sido pioneros en el mercado de los convertibles y actualmente contamos con el convertible más delgado del mundo, el Yoga 920, un dispositivo perfecto tanto para el trabajo como para el entretenimiento que los usuarios podrán transportar a cualquier parte. En nuestra gama profesional, la gama ThinkPad Yoga X1 es uno de nuestros equipos más potentes, para todos aquellos que necesiten las prestaciones de un portátil y la movilidad de una tablet. En los próximos años es previsible que el sector siga creciendo en cuanto a movilidad se refiere, y necesitamos estar a la vanguardia para poder afrontar un futuro cada vez más móvil.

ECONOCOM: "Desde Grupo Econocom pensamos que la transformación digital está impactando en los modelos de negocio de las empresas. Por ello, nuestra misión es potenciar las soluciones de movilidad para poder ofrecer a nuestros clientes la agilidad necesaria que demanda el entorno digital a partir de soluciones innovadoras y flexibles" – Enilio Alvarez - Director de Cuentas Estratégicas y Soluciones de Negocio.

Safetica DLP Suite

Los clientes de ESET pueden agregar Safetica DLP Suite a su estrategia de seguridad lo que les permitirá tener una herramienta líder en prevención de pérdida de datos

ESET ESPAÑA

C/ Martínez Valls, 56
46870 Ontinyent, Valencia

Precio
consultar

Teléfono
96 029 133 48

WEB
www.eset.es

EXCELENTE
MUY BUENO
BUENO
ACEPTABLE
POBRE

TECNOLOGÍA

IMPLEMENTACIÓN

RENDIMIENTO

La herramienta Safetica DLP se caracteriza por ofrecer una solución completa para la prevención de fugas de información (DLP). La principal ventaja es que esta solución puede proteger a las organizaciones frente a una amplia gama de amenazas de seguridad y que son las que ocurren con una mayor probabilidad y en la que están implicadas las principales amenazas actuales: se trata de mitigar todas aquellas que tiene como origen al factor humano

Safetica DL protege a las empresas contra fugas de información planificadas o accidentales, acciones internas maliciosas, problemas de productividad, los peligros que comporta la política BYOD (trae tu propio dispositivo) y mucho más.

Gracias a una alianza con ESET, los usuarios pueden beneficiarse de las ventajas que proporciona Safetica DLP. Entre otras, este producto proporciona una solución completa para la prevención de fugas de información a nivel corporativo, enviando a los administradores informes completos de la actividad y aplicando las políticas de seguridad de la empresa en las actividades de los usuarios. Además, cuenta con una gran ventaja como es la de ofrecer este conjunto de herramientas de seguridad en un solo programa, algo que no ocurre en el caso de otros fabricantes, por lo que se requieren diversas soluciones de seguridad.

El funcionamiento de la herramienta es simple. En general, los trabajadores de una compañía utilizan información crítica de la empresa para hacer su labor, acceden a Internet, leen correos electrónicos, envían documentos a la impresora y conectan sus dispositivos portátiles. Lo que hace Safetica es instalar un agente (Safetica Endpoint Client) en los equipos deseados y manteniendo una conexión regular con ellos a través del servidor (Safetica Management Service). A su vez, este servidor construye una base de datos con la actividad de este puesto de trabajo y distribuye nuevas políticas y regulaciones para proteger la información en cada equipo.

Entre otras características destacan las siguientes:

Safetica avisa a los administradores de la empresa en caso de cambios repentinos en el rendimiento del empleado y muestra los cambios de productividad por departamento en una gráfica temporal. Estos cambios son indicaciones de posibles riesgos de seguridad.

Además, es capaz de descubrir los riesgos de seguridad

en muchos frentes revisando todas las actividades de los usuarios en busca de signos de un posible peligro, incluso antes de la transferencia misma de la información.

También puede prevenir fugas de información que se puedan realizar por correo electrónico y a la vez garantiza que la información protegida no se envía a la cuenta de correo equivocada.

Otra ventaja es que Safetica registra dónde se han enviado los archivos con información sensible y almacena esta información para futuros informes. La herramienta incluye también el control de aplicaciones con reglas de tiempo lo que hace que pueda permitir el uso de aplicaciones relacionadas con el trabajo y bloquea otras para conseguir un entorno más seguro. Además, puede establecerse que las aplicaciones estén disponibles solo durante un período determinado de tiempo.

Otra de las características que destaca es el filtro web por el que gracias a él, se pueden aplicar fácilmente las Políticas de uso aceptable en la empresa con categorías seleccionadas y filtro de palabras clave.

IMPRESIÓN Y DISPOSITIVOS

La solución permite el control de dispositivos, lo que supone una ventaja para los administradores ya que en una sola herramienta pueden establecer tanto un contro de impresión como un control de dispositivos, por lo que ya no es necesario recurrir a herramientas de terceros. El control de impresión, limita qué puede ser impreso y por quién estableciendo cuotas para usuarios y departamentos. Por su parte, el control de dispositivos evita que los empleados puedan conectar dispositivos no autorizados en el trabajo. Los puertos comunes pueden activarse para ciertos dispositivos o bloquearse para todos.

ASLAN 2018 CONGRESS & EXPO

25 AÑOS TODO CONECTADO

ENABLING
DIGITAL TRANSFORMATION

11 & 12 ABRIL MADRID

Security · Cloud · Mobility · Collaboration

Networks · IoT · DataCenter

Analytics · Artificial Intelligence

PALACIO MUNICIPAL DE CONGRESOS MADRID

+2.500 m²

+10 Espacios y Salas de Conferencias

+6.000 asistentes procedentes de...

+3.000 ...empresas de toda España

+100 compañías líderes en tecnologías y servicios IT

+150 speakers

EXPO IT Innovation Areas · IT Leaders Forum · Enterprise & Government IT Managers Meetings · KeyNotes · Speakers Corners · Digital Transformation Awards · VIP & Institucional Relationship Area · Company WorkShops

Impulsar la tecnología para acelerar la Transformación de empresas y administraciones: *IT managers, partners, service providers* y *startups* tienen la oportunidad de liderar la Transformación Digital aportando su talento y experiencia. Conocer las últimas innovaciones tecnológicas, y cómo transformar las organizaciones, es su gran reto en la nueva era digital y el foco principal del Congreso ASLAN2018.

GLOBAL SPONSORS

DELL EMC · vmware · EQUINIX itconic · WALHALLA · econocom · eset · Hewlett Packard Enterprise

EVENT SPONSORS

COMMVAULT · Extreme · interCloud · KASPERSKY · SOPHOS · CenturyLink · vodafone

Inscripción gratuita en **www.congreso.aslan.es**

Síguenos y participa **#ASLAN2018**

CELEBRACION SIMULTÁNEA

smart energy CONGRESS

ORGANIZA

@asLAN

Creamos espacios de encuentro y divulgación tecnológica gracias al apoyo de más de 100 empresas asociadas

Plataformas de almacenamiento cloud

Cada negocio tiene unas necesidades distintas y a la hora de valorar la adquisición de una plataforma de almacenamiento cloud se han de tener en cuenta diferentes criterios. Repasamos la oferta actual de este tipo de soluciones.

La nube informática o cloud computing prosigue con su éxito y son cada vez más las empresas que apuestan por su contratación: las hay públicas, privadas o una combinación de ambas. Además, es posible elegir si se prefiere optar a una plataforma, infraestuctura, software como servicio…

Dentro de este contexto, la contratación de una plataforma de almacenamiento cloud exige que los negocios interesados en este tipo de soluciones estudien no sólo el desembolso que están dispuestas a realizar, también deben analizar necesidades y comparar las características y ventajas que unas y otras ofrecen.

Las pequeñas y medianas empresas, así como integradores de sistemas y desarrolladores, tienen a su disposición la solución Cloud Server del proveedor 1&1: se trata de una solución de servidor raíz que ofrece configuración individual de los recursos y facturación por minuto que emplea la tecnología de almacenamiento NetApp SolidFire Allflash. Por su parte, el proveedor Arsys, de la mano de su plataforma Cloud Storage está disponible en cuatro modalidades según las necesidades que un cliente necesite cubrir. Para labores de almacenamiento, archivo, procesamiento y copias de seguridad. Otro proveedor de hosting gestionado es Claranet que, a través de su producto Cloud Hosting, despliega plataformas de cloud tanto públicas, privadas e híbridas, tanto en infraestructura propia como de otros proveedores (por ejemplo, brinda servicios sobre Amazon Web Services). También hemos seleccionado Interoute Virtual Data Centre (VDC) Storage, una solución de Infraestructura como Servicios (IaaS) automatizada y escalable que brinda computación, red y almacenamiento para grandes empresas, y a Microsoft Azure Storage, la ya conocida propuesta del gigante de Redmond. Interesante resulta también ONTAP Cloud de NetApp para Azure y AWS que propone una plataforma de almacenamiento universal desde sus instalaciones del centro de datos hasta el cloud.

En el caso de Oracle Content and Experience Cloud, las organizaciones empresariales tienen la oportunidad de optimizar la experiencia de sus trabajadores con independencia de su ubicación de la mano de este hub o concentrador. Otras alternativas son Sarenet Plataforma Cloud y VMware vSan enfocado a cargas de trabajo virtualizadas.

Para finalizar, indicar la presencia también de la solución de gestión de datos IBM Spectrum Protect Plus y Openbravo Cloud. Es la solución de Openbravo a los minoristas interesados en adoptar la nueva solución de esta firma en la nube informática y se presenta como plataforma como servicio sobre Amazon Web Services, asignando a cada cliente recursos dedicados.

1&1 Cloud Server

Una solución de servidor raíz a medida para PYMES que emplea almacenamiento NetApp SolidFire Allflash y con un sistema de configuración individual de los recursos.

Con 1&1 Cloud Server (o Servidor Cloud), este conocido proveedor de hosting web propone una solución de servidor raíz adaptada a las necesidades de las pequeñas y las medianas empresas, así como desarrolladores e integradores de sistemas que necesitan trasladar sus proyectos web y aplicaciones de negocio a un entorno flexible y eficiente, combinando funcionalidades técnicas avanzadas y facilidad de uso. De hecho, la infraestructura cloud de 1&1 permite crear servidores operativos en menos de un minuto según señala la propia 1&1.

Los usuarios profesionales pueden, además, tomar el control de toda la infraestructura de hardware y software en tiempo real. Además, y gracias a la presencia de un panel de control intuitivo y sencillo de manejar, activan y gestionan tanto servidores en la nube informática como sistemas de almacenamiento, junto a características como cortafuegos, balanceadores de carga, API y backups, adaptándolos de forma flexible a medida que sus proyectos evolucionan de forma fácil. Los clientes también poseen la opción de ajustar el número de CPUs, RAM y almacenamiento SSD siempre que lo consideren necesario.

Por otra parte, la función de redimensionamiento hot-add ayuda a escalar los recursos sin reiniciar el servidor y evitando tiempos de inactividad. Y con el sistema de gestión de derechos multiusuario, es posible añadir varias cuentas de usuario con diferentes derechos de acceso. De igual forma, 1&1 Cloud Server da la oportunidad de seleccionar la ubicación del centro de datos del servidor y así ejecutar las máquinas virtuales (VMs) en centros de datos no sólo de España sino de Alemania o de Estados Unidos. La seguridad en estos centros de datos se encuentra certificada según la norma internacional ISO/IEC 27001:2013 y asienta sus bases en las directrices europeas de protección de datos, así como en otra serie de medidas de protección de datos que garantizan un alta seguridad para los sistemas y clientes (esta información se puede proteger todavía más con soluciones de copias de seguridad a crear en cualquier momento).

Para garantizar el máximo rendimiento de los proyectos web de los clientes, este proveedor pone a su alcance una potente infraestructura que sólo utiliza componentes técnicos de alta calidad, como el almacenamiento flash integral de NetApp SolidFire. La tecnología ofrece a los profesionales IT no solo una mayor fiabilidad de los servicios, también la flexibilidad de la nube para sus proyectos web. Cloud Server se basa en un sistema de facturación de pago por uso. De esta forma, los clientes pueden realizar un seguimiento del tiempo de actividad y de sus costes en términos de servidores usados, almacenamiento compartido, balanceadores de carga, imágenes y direcciones IP públicas. Así, los costes pueden ser fácilmente seguidos, asignados a proyectos individuales y manteniendo el control respectivo. Adicionalmente, un sistema de facturación interactivo muestra la evolución de los costes.

Gracias a la presencia de un panel de control intuitivo activan y gestionan servidores en la nube informática y almacenamiento

1&1
Avenida de La Vega, número 128108
Alcobendas (Madrid)
Teléfono: 91 136 0000
Web: www.1and1.es
Precio: Desde 9,99 euros

DIGITAL BUSINESS WORLD CONGRESS

Madrid 2018
22-24 May

FACING THE DIGITAL
AVALANCHE

Discover #DES2018 Top Speakers

Stuart Russell
Computer Science Professor
Berkeley University
Artificial Intelligence

Tamara McCleary
CEO
Thulium
Brand Marketing

Arun Sundararajan
Professor
NY Stern University
Sharing Economy

Aristedes Mahairas
Head of NY Special Operations
FBI
Cybersecurity

Hanna Niemi-Hugaert
IoT Manager
City of Helsinki
Smart City

Digital Transformation:
a growing market you should take advantage of

ARTIFICIAL INTELLIGENCE

BLOCKCHAIN

CLOUD

CYBERSECURITY

DIGITAL MARKETING

INTERNET OF THINGS

Follow us:

www.des-madrid.com

An event of:
NEBEXT

Arsys Cloud Storage

Se encuentra disponible en cuatro modalidades entre las que elegir, almacenando, archivando y realizando copias de seguridad de toda clase de información.

Las soluciones a medida de este proveedor de servicios de Internet para las necesidades y los requerimientos de almacenamiento cloud (y distintos proyectos IT) permiten almacenar, archivar, procesar y hacer backups de grandes volúmenes de información; y ello, garantizando la protección de datos críticos, confidenciales o sensibles con absoluta flexibilidad y eficiencia.

Disponibles en cuatro modalidades, estas soluciones Cloud Storage se encuentran alojadas en la plataforma cloud de Arsys, ubicada físicamente en los centros de datos de la compañía en España y desarrolladas en colaboración con fabricantes del sector tecnológico como HP, NetApp e IBM, entre otros.

Comenzamos hablando de Efficient Cloud Storage (ECS). Se trata de un servicio de almacenamiento concebido en la nube y diseñado para la nube informática. Entre sus ventajas, destaca la posibilidad de almacenar ficheros y objetos en una arquitectura flexible y escalable a unos costes inferiores a los de las arquitecturas tradicionales de almacenamiento. Para tareas de archivado y copias de seguridad, apoyo en recuperación de desastres, así como desarrollo de software y aplicaciones nativas para smartphones y tabletas es una solución recomendable.

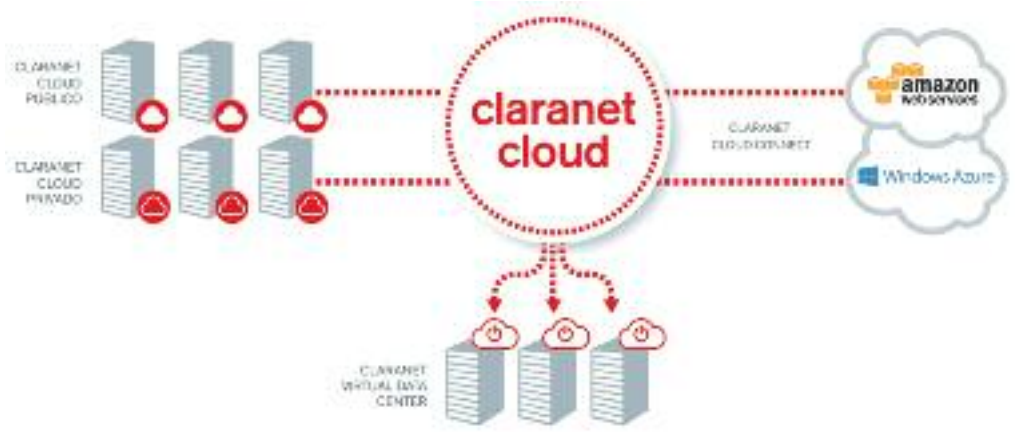
Efficient Plus Cloud Storage (EPCS) es la segunda modalidad que indicamos, perfilándose como una alternativa de rendimiento medio para el almacenamiento de los servicios de proceso en la nube a los que hay que dotar de almacenamiento externo: desarrollo de aplicaciones de negocio, gestión de bases de datos y correo Exchange corporativo. Mientras, High Cloud Storage (HCS), la tercera, es una alternativa de alto rendimiento para el almacenamiento de soluciones cloud a las que es necesario dotar de almacenamiento externo. Se concibe también para aplicaciones de negocio, gestión de bases de datos, servicios de correo Exchange corporativo o proyectos de Big Data e Internet de las Cosas. Tanto en el caso de EPCS como HCS, los servicios de almacenamiento son accesibles por protocolos de fichero (NFS o CIFS) desde servidores cloud localizados en centros de datos de Arsys. La principal diferencia se halla en el apartado del rendimiento. El primero es un servicio de rendimiento medio y el segundo de alto rendimiento.

Finalmente, se encuentra Disco iSCSI, una solución adecuada para aquellos proyectos que se despliegan en entornos de cloud híbrido donde conviven servidores cloud y dedicados. Este modelo de Cloud Storage sirve a los equipos físicos de estos entornos como almacenamiento externo accedido por protocolo de bloques. Un ejemplo son los backend de bases de datos en los cuales varios nodos físicos comparten almacenamiento externo.

Arsys
Avenida de La Vega, número 1
28108 Alcobendas (Madrid)
Teléfono: 902 115 530
Web: www.arsys.es
Precio: A consultar

Claranet Cloud Hosting

Destaca la realización de copias de seguridad de los datos del cliente en un datacenter diferente de donde se hospeda esta información para que el grado de seguridad y redundancia ante una catástrofe o accidente sea máximo.



Este proveedor europeo de cloud hosting gestionado despliega plataformas de cloud público, privado e híbrido, tanto en infraestructura propia (dispone de 43 datacenters donde almacena miles de terabytes de datos) como de grandes proveedores: Microsoft Azure, Google Cloud Platform y Amazon Web Services. Los servicios de cloud hosting gestionado que ofrece se caracterizan por su flexibilidad, integración y pago por uso, lo que permite adaptarlos a diversos entornos empresariales. Por ejemplo, hablaríamos de aquellos negocios que precisan de una inversión inicial baja pero quieren una infraestructura que crezca a la par –aumentando sus recursos en base a su demanda- o grandes proyectos que requieren de procesos de migraciones a entornos de nube pública o híbrida complejos, sacando el máximo beneficio de las características que proporciona cada modelo cloud disponible.

A este respecto, Claranet brinda servicios especializados sobre la infraestructura de Amazon Web Services y diseña (pero también despliega) entornos que responden a necesidades concretas. De la misma forma, audita y monitoriza entornos existentes, detectando puntos de mejora para ofrecer a sus clientes un incremento del rendimiento de sus servicios contratados con AWS. Como partner, además, no solo optimiza el rendimiento de los servicios contratados con AWS, sino también su coste al estudiar la fórmula más rentable para sus clientes.

Su servicio de almacenamiento en la nube está pensado para empresas y corporaciones que deseen almacenar sus datos en centros localizados en su propio país y basándose en la utilización de plataformas de fabricantes como son Dell EMC, Netapp o IBM. Así, siendo las plataformas de almacenamiento un elemento estructural de la infraestructura de Claranet, los clientes con más demanda de recursos pueden disponer de un acceso a disco más veloz y estable en sus màquines; queda así asegurado -en todo momento- que reciben el servicio contratado y que se abren posibilidades de expandir los acuerdos de nivel de servicio a cotas que antes de este cambio no eran posibles.

Las tecnologías de almacenamiento empleada está basada tanto en discos mecánicos como en discos SSD que se combinan para sugerir desde soluciones híbridas hasta soluciones SSD puras, según las necesidades de rendimiento de cada negocio. No obstante, la principal apuesta de Claranet para el almacenamiento de datos calientes en producción está basada desde hace ya un tiempo en discos SSD. Los discos SSD o de estado solido eliminan la mecánica del disco tradicional, suplantándola por tecnología de memorias flash mucho más rápida. Las soluciones de almacenamiento SSD de este proveedor garantizan las IOPS en función de la capacidad de almacenamiento contratada, pudiendo llegar hasta las 3000 IOPS por cada Terabyte de capacidad. Un elemento clave de las soluciones de Claranet es la realización de los backup de los datos originales del cliente en un datacenter físico, distinto del datacenter donde se hospedan los datos de producción, para que el grado de Seguridad y redundància en caso de accidente o catàstrofe sea el máximo possible.

Claranet
Calle Juan Gris, número 10-18, planta 5, Torres Cerdà08014 Barcelona2
Teléfono: 934 452 650
Web: www.claranet.es
Precio: Consultar

Interoute VDC Storage

Solución orientada a grandes empresas que resuelve toda clase de necesidades de almacenamiento como bases de datos, aplicaciones basadas en sistemas de archivos o grandes almacenes de datos para el archivado de la información.

Nos encontramos ante una solución de Infraestructura como Servicios (IaaS) automatizada y escalable que brinda computación, red y almacenamiento. Lo característico de esta propuesta es que se trata de una plataforma cloud privada de ámbito mundial que dispone de conectividad de red propia gestionada por la propia Interoute. Con una extensión de más de 70.000 kilómetros de fibra, se contabilizan hasta 17 centros de datos localizados en Europa, Asia y Estados Unidos. Al contar con una automatización de la infraestructura IaaS añadir nuevas zonas y redes resulta sencillo. Otro dato de interés se refiere a su baja latencia y a la alta velocidad de transferencia para aplicaciones exigentes y de alto rendimiento, aglutinando más de 300 puntos de conexión directa con acceso tanto privado como público.
Profundizando en esta propuesta, todo el almacenamiento se implementa en hardware de nivel empresarial, redundante (RAID) y HA hardware, mientras que los volúmenes de almacenamiento se pueden implementar y administrar a través de la API o la interfaz de control gráfico que se sugiere. Asimismo, estos volúmenes se pueden desmontar en cualquier máquina virtual en la misma zona de implementación (en este caso, el acuerdo de nivel de servicio cubre los servicios de mantenimiento).
Se hace uso, por otro lado, de unidades SSD y de un sistema de almacenamiento externo por bloques (EBS) magnéticos, con un volumen modificable de hasta 2.000 GB. Los niveles de protección de VDC Storage son dos: uno de tipo local y otro remoto, y ambos mantienen un objetivo de punto de recuperación (o RPO) de cuatro horas que garantiza un completo sistema de recuperación de datos. El objetivo de tiempo de recuperación (RTO) asociado también es de cuatro horas.
¿Cómo elegir uno u otro? Se seleccionará desde la propia consola de VDC cuando haya que configurar las necesidades de espacio de almacenamiento. Asociado este espacio, las copias de seguridad comenzarán a realizarse de manera automática.
A la solución de almacenamiento externo por bloques antes citada, se le puede añadir la opción de protección Protected Tier, incluye una copia de seguridad automática, o de replicación en espejo que responde al nombre de Mirrored Tier: en este caso, se combina una copia de seguridad local con la replicación en otra zona VDC distinta) A partir de aquí, de los volúmenes EBS que permanecen protegidos se capturan instantáneas cada cuatro horas que, a su vez, se conservan hasta 48 horas. Luego están las que se conservan una semana e, incluso, un mes.

Interoute
Calle Lezama, número 4. 28034 Madrid
Teléfono: 91 515 96 80
Web: www.interoute.es
Precio: consultar

Encuentros tecnológicos

¿Quieres tener un contacto directo con los CIOs de las grandes empresas españolas?

Byte TI te organiza un encuentro a medida con ellos.

Convénceles de que tus soluciones son las mejores.

- Sector Público
- Banca
- Sanidad
- Seguros
- Alimentación
- Farmacéutico

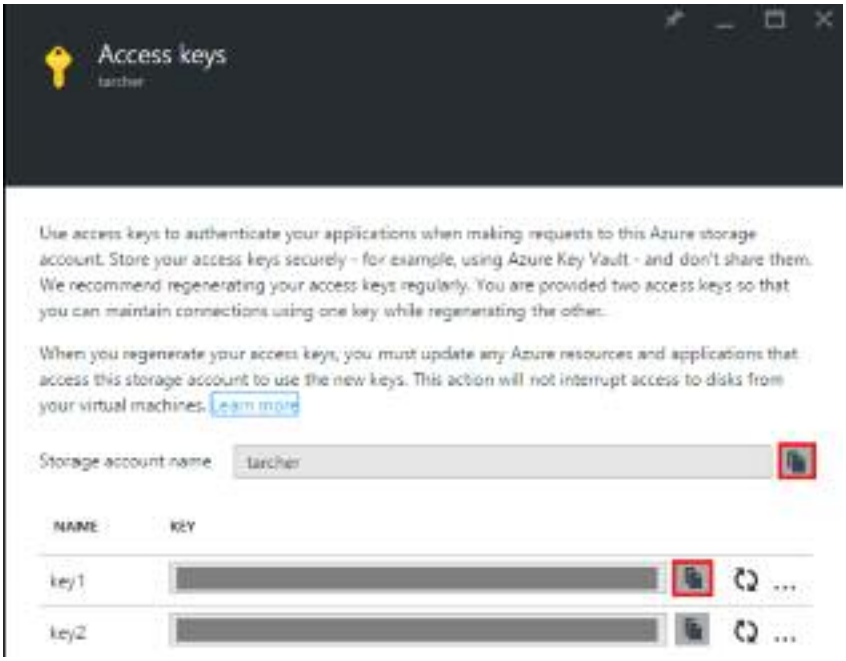
Y muchos más a tu alcance

Infórmate sin compromiso

Encuentros tecnológicos byte TI

Microsoft Azure Storage

Bajo el paraguas de Azure, se engloba todo lo relacionado con la nube de Microsoft. Entre estos servicios se encuentra Azure Data Storage, que permite directamente llevar el almacenamiento de los centros de datos a la nube.



El servicio en la nube administrado por el gigante de Redmond proporciona almacenamiento altamente disponible, seguro, duradero, escalable y redundante donde Microsoft se encarga del mantenimiento y soluciona automáticamente los problemas críticos.

Profundizando en sus características, esta propuesta está formada por tres servicios de datos y, además, cuenta con almacenamiento de acceso esporádico para guardar grandes cantidades de datos a los que se accede con muy poca frecuencia a costo reducido.

Está formado por tres servicios de datos y del primero del que vamos a hablar es Blob Storage, que admite almacenamiento estándar y premium. Básicamente, los blobs son archivos como los que se almacenan en el equipo (o en tabletas, dispositivos móviles...): imágenes, archivos de Microsoft Excel o HTML, discos duros virtuales, macrodatos o copias de seguridad de bases de datos, entre otros ejemplos. En este caso, los blobs se almacenan en contenedores que son similares a las carpetas. Al almacenar estos archivos en Blob Storage, es posible acceder a ellos desde cualquier lugar mediante direcciones URL, la interfaz de REST o una de las bibliotecas de cliente de almacenamiento de SDK de Azure (las bibliotecas de cliente de almacenamiento están disponibles en lenguajes como Node.js, Java, PHP, Ruby, Python y .NET).

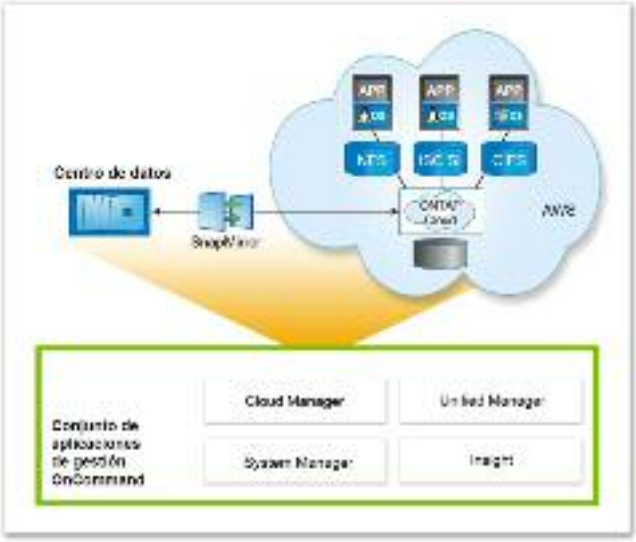
Azure Files (el segundo) se emplea para configurar recursos compartidos de archivos de red de alta disponibilidad a los que se puede acceder mediante el protocolo bloque de mensajes del servidor (SMB) estándar. Esto significa que varias máquinas virtuales pueden compartir los mismos archivos con acceso de lectura y escritura y también leer estos ficheros mediante la interfaz REST o las bibliotecas de cliente de Storage. Lo que distingue Azure Files de los archivos en un recurso compartido de archivos corporativo es que es posible acceder a ellos desde cualquier lugar del mundo mediante una dirección URL que apunte al archivo e incluya un token de firma de acceso compartido (SAS). Puede generar tokens SAS y se permite el acceso específico a un recurso privado durante un período de tiempo determinado. El servicio Azure Queue (el tercero) se emplea para almacenar y recuperar mensajes. En este caso, la cola de mensajes puede ser de hasta 64 KB de tamaño y contener millones de mensajes (las colas se emplean por lo general para guardar listas de mensajes y procesarlas de forma asincrónica). Esta propuesta, en otro orden de cosas, incluye todas las funcionalidades de disco administrado y no administrado que utilizan las máquinas virtuales y para los servicios de almacenamiento brinda cifrado en reposo y de cliente, además de una opción de cifrado durante el tránsito con recursos compartidos de Azure Files. Para asegurarse de que los datos sean duraderos, Azure Storage mantendrá (y administrará) varias copias de los mismos. Esto se denomina replicación y, a veces, redundancia. Al configurar la cuenta de almacenamiento, hay que seleccionar un tipo de replicación y las posibilidades son: almacenamiento con redundancia local (LRS); con redundancia de zona (ZRS); con redundancia geográfica (GRS); y con redundancia geográfica con acceso de lectura (RA-GRS).

Microsoft
Paseo Club Deportivo, número 1
28223 Pozuelo de Alarcón (Madrid)
Teléfono: 91 391 90 00
Web: www.microsoft.es
Precio: consultar

ONTAP Cloud de NetApp

Una solución de almacenamiento de datos que se adapta a muchas cargas de trabajo, como la recuperación ante desastres, las cargas de trabajo de producción y los entornos de desarrollo y pruebas en el cloud.

NetApp ayuda a las organizaciones a gestionar sus datos de distintas maneras, por ejemplo controlando recursos de almacenamiento en el cloud público con el software de almacenamiento NetApp ONTAP; pero también ofreciendo una rápida puesta en marcha de almacenamiento con un entorno de gestión simple (de la mano de OnCommand Cloud Manager y ONTAP Cloud) y e implementando aplicaciones en el cloud con varios modelos de consumo de almacenamiento que incluyen servicios de archivos (NFS y CIFS).
ONTAP Cloud es un dispositivo de almacenamiento de software sin interrupciones basado en el software ONTAP de NetApp y proporciona una plataforma de almacenamiento universal desde sus instalaciones del centro de datos hasta el cloud.
Adaptable a distintas cargas de trabajo, se puede poner en marcha y gestionar desde OnCommand Cloud Manager como máquina virtual en instancias de Amazon EC2 (gestiona el almacenamiento de Amazon EBS) o Microsoft Azure (gestión del almacenamiento de Azure también). ¿El resultado? La creación de una solución de almacenamiento para empresas basada directamente tanto en recursos de Amazon como cloud de Azure respectivamente.
En ambos casos, las soluciones de ONTAP reducen al mínimo los recursos de almacenamiento en cloud con funciones eficientes como la deduplicación de datos o las copias de snapshot con compresión y capacidad cero, que pueden actuar como datos principales. Asimismo, aprovisionan de almacenamiento tanto NAS como SAN -para el entorno de sus aplicaciones con compatibilidad con CIFS, NFS y arrojan backups de los datos de



un momento específico casi instantáneos a través de copias snapshot de NetApp con un impacto nulo. Mientras, mediante la suite de herramientas ONTAP SnapManager se obtienen copias snapshot coherentes con las aplicaciones. ONTAP ofrece de igual forma SnapMirror, una tecnología que reúne su cloud híbrido vinculando su almacenamiento FAS en las instalaciones con su entorno de ONTAP Cloud.
ONTAP Cloud se pone en marcha a través de OnCommand Cloud Manager (como ante hemos indicado) y proporciona la instalación, la asignación de recursos, el aprovisionamiento de datos y la configuración de replicación necesarios. En este caso, Cloud Manager se emplea para actividades de gestión diaria de los recursos de datos del cloud: al integrarse en el entorno cloud del cliente, éste pueda usar sus credenciales de AWS o Azure con el fin de reunir los recursos necesarios para satisfacer sus requisitos de almacenamiento. Por otro lado, y dado que facilita una visibilidad de los recursos consumidos por cada instancia, también arroja supervisión y comentarios de interés sobre el coste de estos mismos recursos, pudiendo identificar y mover cargas de trabajo al entorno más eficiente.
Los modos de consumo son dos: pago por uso y suscripción. En el primero, el almacenamiento se adquiere directamente desde la cuenta de Amazon o Azure y se factura de acuerdo con el uso por horas (opción adecuada para necesidades de aplicaciones a corto plazo o para entornos que deban acelerarse o decelerarse bajo demanda). Para el segundo, cada modelo de consumo incluye varias soluciones, que van desde una solución de pago por uso de 2 TB (la más pequeña) hasta un modelo de suscripción de hasta 368 TB (la más grande).

NETAPP
Calle Rosario Pino, números 14-16. Planta 17
28020 Madrid
Teléfono: 91 571 42 02
Web: www.netapp.com/es
Precio: consultar

Oracle Content and Experience Cloud

Plataforma nativa de la nube para la producción, gestión y entrega de contenido en todas las líneas de negocio, ofreciendo capacidades para atender una amplia variedad de necesidades comerciales.

La multinacional norteamericana ha escogido para participar en este artículo su solución Content and Experiencie Cloud. Se trata de un hub (o concentrador) de contenido basado en la nube informática que permite activar la gestión de contenido omnicanal y optimizar la experiencia del usuario con independencia del momento y el lugar en el que se encuentre. A este respecto, Content and Experience Cloud permanece integrada en Oracle Cloud Platform lo que permite, precisamente, mantener disponibles todos sus archivos ya se encuentre el usuario en casa, en la oficina, en el aeropuerto o en un hotel de cualquier país del mundo (lo hace combinando la plataforma como servicio PaaS de Oracle con su infraestructura en la nube)

En un momento en el que el contenido es el corazón de todos los esfuerzos de marketing y ventas, esta herramienta permite compartir, colaborar, procesar y también administrar todo este material, ayudando a las organizaciones a desarrollar, usar y distribuirlo para ofrecer experiencias contextualizadas; mejorar la fidelidad del cliente; y crear prescriptores de la marca. Y es que, de hecho, esta solución de colaboración gestiona el flujo de trabajo de modo que agiliza la creación y entrega de esos contenidos, mejorando la productividad de los empleados y la experiencia del cliente. En este sentido, puede abordar las necesidades de los usuarios de negocios y de TI, lo que les permite trabajar juntos para brindar experiencias digitales modernas y atractivas (DX).

Oracle Content and Experience Cloud ofrece, por otro lado, una única plataforma nativa de la nube para la producción, la gestión y la entrega de contenido en todas las líneas de negocio, proporcionando capacidades para atender una amplia variedad de necesidades comerciales, cubriendo la parte que va desde la participación de los empleados y de los clientes hasta la habilitación de ventas y desarrollo comercial.

Estas capacidades clave incluyen, por un lado, la colaboración de contenido, colaborando en el contenido internamente y con equipos externos mediante acceso móvil; y, por otro, un concentrador centralizado de contenido que facilita el uso de un centro de contenido único para crear, compartir, administrar y publicar contenido en cualquier canal, incluidos documentos comerciales, activos digitales, contenido generado por el usuario y contenido web.

Asimismo, hay espacio para una experiencia omnicanal constante a favor de experiencias que resulten atractivas en todos los canales y administrando el contenido desde las propias aplicaciones empresariales.

La plataforma se integra con Oracle Customer Experience Cloud Suite, un paquete de aplicaciones en la nube que permite a las organizaciones adoptar un enfoque más inteligente para la gestión de la experiencia del cliente y las iniciativas de transformación empresarial. También se integra –como mencionábamos al comienzo- con una serie de servicios de Oracle Cloud Platform, incluidos Oracle Process Cloud (gestiona el ciclo de vida de los procesos de negocio); Oracle Mobile Cloud (despliegue de aplicaciones móviles integradas con una infraestructura cloud de back-end robusta y de nivel empresarial) y Oracle Integration Cloud, que simplifica la integración entre la nube y aplicaciones on-premises tanto de Oracle como de terceras partes.

Oracle
Calle José Echegaray, 6B.
28230 Las Rozas (Madrid)
Teléfono: 91 603 61 88
Web: www.oracle.com/es
Precio: consultar

Sarenet Plataforma Cloud

Su ventana de cliente ayuda a gestionar los recursos de que se dispone de una forma sencilla, monitorizando el rendimiento de la red y modificando aquellos parámetros que fuesen necesarios.

Madrid, Barcelona y Bilbao son las ciudades elegidas por Sarenet para desplegar sus seis datacenters con vigilancia y mantenimiento 24 x 7 a cargo de técnicos especializados.
A este respecto, pone a disposición de los usuarios una amplia gama de soluciones en la nube de forma totalmente personalizada, soluciones flexibles que facilitan ampliar recursos de manera inmediata para necesidades puntuales que puedan surgir en la empresa.
Además, permite soluciones híbridas a diferentes niveles para –de esta manera- convertirse en una extensión más de la infraestructura del cliente.
En esta línea, Sarenet ha adaptado su infraestructura para que los clientes que utilizan Veeam back-up, una de las soluciones más extendidas en entornos VMWare, puedan utilizarles de forma transparente, bien como repositorio de las copias que se realizan o como un centro de procesamiento de datos alternativo, formando parte del plan de recuperación ante desastres de la organización. Así, el cambio de roles ante la caída parcial de las máquinas en casa del cliente resulta un proceso también transparente y totalmente integrado gracias a la tecnología presente con esta solución que tuneliza y extiende la red de los servidores en casa del cliente hasta los albergados en la cloud del proveedor.

> La solución de Sarenet ofrece la posibilidad de que una compañía puede conectarse a sus equipos sin intermediarios

Otra de las ventajas de esta propuesta es la posibilidad de que una compañía puede conectarse a sus equipos sin intermediarios, ya que Sarenet combina distintas clases de tecnologías (por ejemplo fibra, cobre, radio…) y a muy bajas latencias ya que la última milla es propia. De igual forma, hay espacio para enlaces redundantes tanto a nivel nacional como internacional, conexiones directas de operadores de tránsito y con extensión de red hasta hosters de terceros y sus plataformas.
La seguridad también es importantes y, en este sentido, la plataforma provee de cortafuegos de aplicaciones, sistemas de mitigación de ataques DDoS y caminos redundados.
Además, con la ventana de cliente las organizaciones podrán gestionar los recursos disponibles de una manera sencilla, monitorizando el rendimiento de la red y modificando los parámetros que fuesen necesarios como los referidos a la memoria, la configuración de alertas o las ampliaciones de CPUs, entre otros.
En el caso de tener que solucionar de manera rápida cualquier incidencia o necesidad, el proveedor dispone de un soporte técnico cualificado propio.

Sarenet
Calle Arturo Soria número 201. 1ª planta
28043 Madrid
Teléfono: 91 515 51 23
Web: www.sarenet.es
Precio: Consultar

VMware vSan

Está basado en componentes y servidores x86 estándar que ayudan a reducir el coste total de propiedad (TCO) en hasta un 50 % en comparación con el almacenamiento tradicional, según indica el propio fabricante.

En estos momentos, toda iniciativa empresarial implica un proyecto de TI y muy probablemente varios proyectos. Así, y como consecuencia de esta transformación digital constante, los departamentos de TI necesitan un enfoque sencillo y rentable para la infraestructura del centro de datos; un enfoque que no requiera conocimientos ni formación completamente nuevos.

Es en este escenario donde hace su aparición VMware vSan, una plataforma de almacenamiento definida por software nativo que ha desarrollado este fabricante para ayudar a los clientes a evolucionar hacia una infraestructura hiperconvergente (HCI) sin riesgos, a la vez que reduce los costes de TI y proporciona una solución ágil lista para el hardware del futuro, así como para los cambios en el cloud y las aplicaciones.

vSan proporciona almacenamiento seguro y optimizado para flash, y crea depósitos de almacenamiento conectado a un servidor con el que se brinda un almacén de datos compartido altamente flexible y adecuado para cualquier carga de trabajo virtualizada, incluidas las aplicaciones esenciales, los escritorios virtuales, los servicios de TI remotos, la recuperación ante desastres y la infraestructura de la práctica de ingeniería de software DevOps. Asimismo, ayuda en la evolución del centro de datos sin riesgos, además de controlar los costes de TI y responder a las necesidades empresariales de ampliación del futuro. Basado en componentes y servidores x86 estándar que ayudan a reducir el coste total de propiedad (TCO) en hasta un 50 % en comparación con el almacenamiento tradicional, ofrece la agilidad necesaria como para ampliar fácilmente el entorno de TI y cifrado HCI nativo.

Entre sus ventajas, vSan permite extender de manera uniforme la virtualización al almacenamiento con una solución hiperconvergente integrada y segura que, básicamente, funciona con el entorno general de VMware.

Asimismo, se perfila como una plataforma diseñada para la era multicloud y creada para aplicaciones empresariales modernas y contenedores. A este respecto, la infraestructura definida por software sobre la que se asienta utiliza las últimas tecnologías de hardware y también admite aplicaciones de nueva generación, por lo que los negocios interesados pueden adentrarse en la cloud. Otra característica a indicar es la opción de implementar clústeres flexibles y robustos para una protección asequible del sitio.

VMware
Calle Rafael Botí, número 26. 2ª planta.
28023Madrid
Teléfono: 91 412 50 00
Web: www.wmware.com/e
Precio: consultar

Todo realizado con los mejores productos de:

www.mkm-pi.com

Información a medida

Los nuevos retos de la ciberseguridad

La ciberseguridad cobra cada vez más importancia en un mundo hiperconectado. Por primera vez en la historia, la práctica totalidad de las empresas, independientemente de su tamaño y del sector al que pertenezcan ponen a la seguridad entre sus prioridades.

Por Manuel Navarro

Hay algo que ha cambiado. El año 2017 y los ataques sufridos por grandes empresas y Administraciones Públicas hicieron saltar las alarmas a todos. Se pasó del "eso a mi no me pasa" a una psicosis por asegurar cualquier cosa. Así que, algo bueno ha tenido Ransomware. Lo que no ha logrado la formación, lo ha conseguido un malware. No hay mal que por bien no venga que dice el refrán y en este caso es más cierto que nunca.

Los retos que se tienen por delante son numerosos. Para Miguel López, Country Manager de Barracuda, "el primero y más importante es, probablemente, concienciar a usuarios, directivos, y gobiernos de que la Seguridad de los activos informáticos es, actualmente, el punto más débil de prácticamente todas nuestras estructuras productivas y de servicios. A medida que nuestra sociedad es cada día más dependiente de la conexión e intercambio de datos entre usuarios, dispositivos y máquinas los ataques contra cualquier elemento conectado serán cada vez más dañinos y con mayor potencial de causar graves perjuicios tanto desde el punto de vista económico como desde la perspectiva de la seguridad de las personas e infraestructuras. Existe actualmente un grave desfase entre el daño potencial que representa un ataque y los recursos que se invierten en defenderse del mismo y eso es algo que la industria del cibercrimen conoce bien y explota cada día".

Los avances tecnológicos están revolucionando la forma en la que trabajamos y vivimos. Sin embargo, este adelanto va acompañado de un aumento de las ciberamenazas. Los ataques tendrán un amplio alcance y el cibercrimen continuará profesionalizándose, pues cada vez está más organizado. De hecho, los ciberdelincuentes se asocian para conseguir el máximo beneficio con cada uno de sus ataques. Por eso, Alfonso Ramírez, director general de Kaspersky cree que "se hace necesario proteger la infraestructura corporativa ya que cualquier empresa puede ser víctima de un ataque. Para ello, es necesario contar con una solución de seguridad fuerte y robusta, capaz de predecir, detectar, prevenir y dar respuestas a las amenazas. El cibercrimen nunca duerme. De hecho, según investigaciones de Kaspersky Lab, en 2016 el 32% de las empresas españolas reconoció ser víctima de una ciberamenaza. Por ello, es importante que las empresas, independientemente de su tamaño, cuenten con una buena solución de ciberseguridad para evitar ser alcanzados por las actividades delictivas de los grupos cibercriminales".

Como decíamos, el año 2017 fue extremadamente convulso en materia de seguridad, en 2018 nos enfrentamos a varios retos. Los nuevos vectores de ataque van creciendo paulatinamente estos años. El número de incidentes de seguridad va creciendo año tras año de forma alarmante. En este sentido, podemos asegurar que las amenazas en materia de seguridad afectan ya, tanto a particulares como a pymes y grandes empresas.

Para Alejandro Cadarso, Business Development for Wireless & IT Security Solutions en EinzelNet, "Hay que prestar especial atención también a nuevas fórmulas de ataque dirigidas a los dispositivos móviles, especialmente Android, y destinadas a rootear el dis-

positivo de forma que sea casi imposible combatirlo desde un antivirus, a no ser que esté instalado de serie. De igual modo, a los ataques a través de técnicas de rootkit, que permiten a los hackers ocultarse de la vista del sistema operativo y de las soluciones de seguridad. Por otro lado, tanto Internet de las Cosas como el pago por móvil, con cada vez más dispositivos conectados a Internet ofrecen brechas de seguridad que son y van a ser continuamente atacadas".

Otros retos se van a encontrar en las plataformas de pago en el móvil y los sistemas de cobro son objetivo prioritario de los ciberdelincuentes. En este sentido, es conveniente estar atentos al cumplimiento y certificación que deben cumplir grandes y medianas empresas para cubrir su riesgo.

"El reto para muchas empresas, independientemente de su tamaño, es blindarse ante las amenazas que pueden dañar seriamente su imagen y sus finanzas. En este sentido, el objetivo de muchos ataques será acceder a la información confidencial de la compañía (datos financieros, planes estratégicos, etc.), así como a datos de sus clientes. Será importante contar con una buena consultoría en el cumplimiento de la nueva normativa europea en GDPR", concluye Cadarso.

Las ciberamenazas son múltiples y cada vez crecen más. En este sentido, José de la Cruz, director técnico de Trend Micro, asegura que "por ello, es necesario controlar todos los posibles vectores de entrada de amenazas. Hoy en día el perímetro se ha difuminado y nos encontramos con que los usuarios interactúan desde dentro y fuera de las redes corporativas y pueden almacenar e intercambiar información con sistemas alojados fuera o dentro de

APLICACIONES DE ALMACENAMIENTO CLOUD SEGURAS

Alain Karioty, Director Regional de Ventas de Netskope

El entorno profesional moderno está inundado de aplicaciones cloud orientadas a la empresa; empleados y organizaciones las demandan para hacer la jornada laboral más productiva. A este respecto, el último informe Netskope Cloud desvela que, de media, en cada organización se utilizan más de 1.000 aplicaciones cloud. Sin embargo, ¿son conscientes las empresas del número total de aplicaciones utilizadas por sus empleados? Ciertamente, las aplicaciones en la nube son una forma rentable de aumentar la productividad, pero su uso creciente, especialmente de las no autorizadas, puede poner en peligro los datos.

Entonces, ¿cómo pueden las empresas aprovechar ambos mundos? A continuación cinco pasos prácticos

Las empresas que buscan habilitar de forma segura las aplicaciones de almacenamiento cloud pueden seguir cinco medidas prácticas que les ayudarán en este cometido. Así, como punto de partida, es esencial proteger los datos corporativos confidenciales que se almacenan en la nube. El almacenamiento en la nube es la segunda categoría de aplicaciones cloud más popular, justo por detrás de las de marketing. Muchas organizaciones eligen una solución como Google Drive, Egnyte, Dropbox, Box o Microsoft OneDrive para unificar sus datos. Como primera medida, estas empresas deberían comenzar por establecer qué datos importantes se encuentran almacenados en este tipo de apps (según Netskope, el 8% de los archivos recogidos en aplicaciones corporativas de almacenamiento cloud violan alguna política de control de fuga de datos por contener información sensible) para protegerlos. De igual modo, si una empresa no utiliza una única solución de almacenamiento cloud como las mencionadas anteriormente, es aconsejable que, cuanto menos, se decante por una única solución (o las menos posibles) acorde con las opiniones de los empleados y los requisitos de la organización. Es recomendable también formar a los empleados en la aplicación seleccionada para garantizar su aceptación total y su uso continuo.

Además de determinar qué aplicaciones utilizan los empleados, las organizaciones deben supervisar la actividad de las aplicaciones (cargas, descargas, recursos compartidos...) para desarrollar una visión de los riesgos planteados. También es importante monitorizar cualquier actividad arriesgada o inusual, dado que es casi imposible detectar una acción anómala. Por otro lado, el acceso a la aplicación por aquellos empleados cuyas credenciales se han visto comprometidas en una violación de datos, puede suponer un riesgo. Es difícil saber si quien accede a la aplicación es realmente el empleado y no un hacker.

Por su lado, el ecosistema de aplicaciones que se integra en el conjunto de aplicaciones corporativas de almacenamiento cloud también debe ser controlado. Existen decenas de aplicaciones cloud que ayudan a que la empresa funcione con mayor fluidez, sin embargo, algunas probablemente carezcan de seguridad a nivel empresarial. Si las aplicaciones no han sido facilitadas por el departamento de TI, administrarlas o aplicar políticas para controlar su uso puede convertirse en una tarea ardua.

Desafortunadamente muchos empleados no muestra mucho interés en la seguridad. Por ello, las empresas pueden optar por permitir que los empleados trabajen libremente, mientras las decisiones de seguridad se lideran desde el departamento de TI. En la práctica, esto significa que una vez que la empresa haya seleccionado una aplicación de almacenamiento cloud, TI establecerá y aplicará políticas granulares para garantizar que se utiliza de forma segura. Un ejemplo sería bloquear la carga de archivos que contienen ciertos tipos de datos, como nombres y direcciones de clientes.

La RGPD es un recordatorio oportuno para que las empresas controlen sus datos. Garantizar que el uso de la aplicación de almacenamiento en la nube esté habilitado de manera segura es una buena forma de comenzar, y puede evitar multas considerables en el futuro.

las mismas. Esto requiere implementar sistemas de protección flexibles y que sean capaces de cubrir todos esos vectores".

RIESGOS

Sin embargo, muchas veces las empresas, sobre todo las pequeñas y medianas están asumiendo riesgos innecesarios, aunque de forma inconsciente. Para Alf Melin, Security Operations Centre Manager de Getronics, "es muy raro que las empresas tomen riesgos innecesarios. Normalmente, cuando se asumen riesgos, estos son sopesados para que en el cómputo de beneficio/perjuicio el resultado sea positivo. Hoy en día parece imprescindible para una empresa el hecho de estar conectada a Internet (pedidos, publicidad, incidencias, …), con lo que no es factible huir de la red para evitar el peligro. Lo mismo es aplicable a la infraestructura de cada empresa: el mundo on-line aumenta el vector de exposición de los componentes de la infraestructura corporativa. Pero esta exposición debe asumirse debido a que la apertura a Internet cambia el paradigma de ciertas tareas que no sería posible realizar de otra manera o sería mucho más ineficiente repercutiendo en el beneficio". No están muy de acuerdo en CA Technologies. Jacinto Grijalba, Security Solution Account Manager, cree que el problema radica en la versión clásica que se tiene en muchas empresas de la seguridad: "esta visión clásica de la seguridad se ha demostrado obsoleta y de alto riesgo si pensamos en el alcance masivo de los ataques de los últimos años, que han conseguido de forma ilícita millones de datos de usuarios en todo el mundo. Muchos de estos ataques han sido perpetrados con credenciales de acceso de usuarios reales obtenidas de forma fraudulenta mediante robo o ataque de fuerza bruta al ser demasiado débiles. El nuevo perímetro de seguridad es la identidad y la forma de gobernar su acceso a los datos de una organización. Las identidades y sus accesos deben poder gestionarse en cual-

quier tipo de entorno, sea cual sea los sistemas de información que se utilicen y sin importar si ésta reside en el perímetro de la organización o fuera de ella, como sería el caso de aplicaciones ofrecidas en la nube". Lo mismo opina Alberto Rodas Sales Engineer de Sophos: "los riesgos que corren las empresas es la creencia de que con su solución de seguridad tradicional es suficiente. Lamentablemente, nos encontramos con este escenario más veces de las deseadas y no es hasta que tienen un incidente grave de seguridad, que en verdad se dan cuenta de lo desprotegidos que estaban, por desgracia, ya tarde". Finalmente, Manuel Cubero, Director Técnico de Exclusive Networks asegura que "ninguna empresa quiere tomar riesgos innecesarios, nadie busca meterse en problemas de forma gratuita. En cambio, la velocidad que el negocio obliga a imprimir en la evolución tecnológica de las compañías hace que sea más probable caer en riesgos innecesarios. Como ejemplos, hablar de trabajar con aplicaciones en la nube sin evaluar bien a fondo sus implicaciones y cómo integrarlas adecuadamente en materia de seguridad. También la implementación de dispositivos IoT que manejan y que suben datos a la nube sin un estudio previo de las implicaciones que pueden llevar a cabo, sin olvidar las colaboraciones de última hora con empresas de terceros en las cuales se cedan datos, que ahora estarán más fuertemente regulados por la ley de GDPR, sin una buena gestión de los riesgos".

Una de las técnicas que están empezando a tomar impulso son la inteligencia artificial y machine learning. Ésta última, además está teniendo especial incidencia entre todos los fabricantes y desarrolladores de soluciones de seguridad

NUEVAS TÉCNICAS

Ante los nuevos retos y desafíos aparecen nuevas formas de defensa. Una de las técnicas que están empezando a tomar impulso son la

inteligencia artificial y machine learning. Ésta última, además está teniendo especial incidencia entre todos los fabricantes y desarrolladores de soluciones de seguridad que ven en ella una técnica efectiva para anticiparse a nuevos ataques. Desde hace ya algún tiempo esta nueva tecnología se está usando en diversos productos de seguridad y está facilitando la evolución y eficiencia de los mismos. Prácticamente, todos los productos de seguridad más punteros basan parte de sus análisis en motores de Machine Learning o se apoyan en estas técnicas para complementar lo que ya tenían. En este sentido, Borja Pérez, country manager de Stormshield afirma que "machine learning es una capa más de seguridad. Ayuda, y lo hará más en un futuro cuando se comparta más información entre distintos actores en el mundo de seguridad. Ahora bien, hay entornos no conectados donde machine learning no ayuda tanto. En infraestructuras críticas o industria, debemos ofrecer soluciones que sean capaces de actuar sin depender de inteligencia externa". Desde la multinacional germana G Data creen que Machine Learning es una técnica muy interesante. En esta firma afirman que las empresas de ciberseguridad nos apoyamos en innovaciones para mejorar nuestras soluciones y adaptarlas a las nuevas amenazas. Pero no podemos perder la perspectiva ni dejar de ver la realidad cotidiana que viven nuestras empresas y que nos dice que muchas de ellas se convierten en víctimas por hacer doble clic en un correo electrónico malicioso y porque todos los empleados, desde el recepcionista hasta el director general, son usuarios con los mismos privilegios y los mismos derechos de administración. Lo cierto es que Machine Learning se está incorporando cada vez a un mayor número de soluciones y es que tal y como afirma Manuel Cubero de Exclusive Networks, "Desde hace ya algún tiempo esta nueva tecnología se está usando en diversos productos de seguridad y está facilitando la evolución y eficiencia de los mismos. Prácticamente, todos los productos de seguridad más punteros basan parte de sus análisis en motores de Machine Learning o se apoyan en estas técnicas para complementar lo que ya tenían". No obstante, no hay que centrarse en el Machine Learning como una solución única para resolver los problemas de seguridad. Tal y como afirma el Miguel López de Barracuda, "es un termino de moda del que probablemente se está abusando en muchos departamentos de marketing. No obstante, es cierto que todos los fabricantes punteros de soluciones de seguridad venimos haciendo uso, desde hace tiempo, de este tipo de tecnologías en diversos modos con el objeto de mejorar nuestro nivel de respuesta frente a los cada vez más sofisticados ataques. Machine Learning nos permite, por ejemplo, hacer frente a nuevos ataques e identificar nuevos tipos de malware basándonos únicamente en su comporta-

LOS MEJORES HÁBITOS DE SEGURIDAD

Por Watchguard

2018 ya está en marcha y, en este momento, los propósitos de Año Nuevo pueden ser un recuerdo lejano para algunos. Sin embargo, en WatchGuard creemos que nunca es demasiado tarde para comenzar a construir buenos hábitos de seguridad o para romper los negativos. Por ello, nuestro equipo de investigación ha recopilado una serie de acciones con aquello que se debe y no se debe hacer para ayudar a que se mantengan seguros online tanto los administradores de redes como los usuarios.

Si es administrador de red y está preocupado por la seguridad, a continuación encontrará algunas maneras de mejorarla. Si por el contrario, usted es solo un usuario que está preocupado por todas las noticias de hackeos (robo de bitcoins, chips de Intel con fallos, espionaje de Estados-nación…) siga leyendo para conocer unos simples pasos que puede seguir para mejorar de manera significativa su seguridad digital y que no tenga impacto en su vida diaria.

Para administradores de red:

1. Implemente la autentificación multifactor en toda la empresa (MFA).

2. Cree y pruebe un plan de Continuidad de Negocio y Recuperación de Desastres (BC/DR).

3. Ofrezca con regularidad formación en materia de seguridad.

4. Involúcrese en la legislación cibernética. La ciberlegislación se ha convertido en información importante.

5. No planifique su estrategia de seguridad de forma unilateral.

6. No se centre exclusivamente en la tecnología de seguridad preventiva.

7. No se vuelva complaciente o se desanime.

Para los consumidores:

1. Utilice autenticaciones de doble factor gratuitas (2FA) siempre que estén disponibles.

2. Utilice un administrador de contraseñas.

3. Invierta en hardware o software de seguridad sin importar qué plataforma use.

4. ¡Haga copias de seguridad!

5. Aplique los parches con regularidad.

6. No envíe pagos basados solamente en textos o emails.

7. No haga click con facilidad.

8. No se una a redes públicas o abiertas sin protección.

9. No crea que las cosas buenas llegan gratuitamente.

10. No deje abierto su ordenador en público.

Recuerde, tanto para las empresas como para los usuarios, la buena seguridad se basa a menudo en conductas mantenidas en el día a día, más que en cualquier otro error o decisión. Si se compromete a cumplir con esta serie de prácticas y revisarlas de vez en cuando, estará en camino de tener un año más seguro.

ASEGURAR LAS TRES FAMILIAS DEL IOT

WILLIAM MALIK, CISA VP INFRASTRUCTURE STRATEGIES, TREND MICRO

Asegurar Internet de las Cosas (IoT) es difícil. Una de las razones es que Internet de las Cosas está compuesto por tres grupos de tecnología distintos. Cada uno de estos grupos cuenta con una arquitectura de restricción completamente diferente. Para asegurar los tres grupos se requiere un enfoque distinto en cada uno de ellos.

IoT 0.9 - El grupo originario contiene toda la Tecnología Operativa (OT) heredada y los Sistemas de Control Industrial (ICS) que hacen uso de algún tipo de red, pero no el modelo OSI. Estas herramientas emplean protocolos simples porque no tienen ni mucha potencia, ni memoria, ni ancho de banda, ni CPU disponibles. Los dispositivos ICS tradicionales tienen una vida útil de 15 a 25 años. Pueden encontrarse en lugares remotos o inaccesibles.

¿Cómo de remoto? La nave espacial Voyager 1 cuenta con poco menos de 70K de almacenamiento, tres procesadores con una capacidad de procesamiento agregado de 130.000 instrucciones por segundo y un transmisor de radio de 22,4 vatios. Los 249 vatios de potencia restantes (frente a los 470 en el lanzamiento) proceden de tres generadores termoeléctricos de isótopos propulsados con plutonio. Consulte https://voyager.jpl.nasa.gov/ para obtener más información sobre este dispositivo remoto ICS.

Asegurar los dispositivos IoT 09 es una tarea complicada. Pocas personas tienen la combinación de habilidades necesarias para hacer este trabajo. Requiere profundos conocimientos de ingeniería del diseño del dispositivo y sus limitaciones operativas, y de las capacidades y limitaciones de los protocolos de red para construir una red de información y protección basada en el dispositivo. Las limitaciones de procesamiento prohíben cualquier autentificación, autorización, cifrado o capacidad de firma digital convencional a bordo. Los proveedores tradicionales de ICS no tienen equipos de seguridad de la información integrados. Los clientes de ICS pueden tener un equipo de seguridad de la información, pero ellos entienden las arquitecturas de seguridad TI convencionales, no las limitaciones de arquitecturas ICS.

La manera más efectiva de asegurar los dispositivos IoT 0.9 es el aislamiento: colocar los dispositivos en una red segmentada, no vinculada a la red corporativa. Esta táctica va en contra de la unidad de red, provocando que el estado del dispositivo esté casi en tiempo real disponible para toda la organización. Si bien el enfoque respalda el deseo de la dirección de "obtener más y mejor información", establece una red plana sin protección y abierta a atacar. Actuar como cortafuegos fuera de IoT 0.9 o ejecutarlo por completo en una red separada proporcionará, al menos, aislamiento. Los sensores fuera de banda en la red aislada pueden detectar e informar del tráfico sospechoso sin impedir la capacidad de respuesta o seguridad del dispositivo.

IoT 1.0 - Llamaremos al grupo intermedio IoT 1.0. Estos híbridos consisten en dispositivos que se conectan en red utilizando parte de la pila OSI. Estos híbridos presentan un gran problema. Cumplen bien con sus requisitos OT, y es que su arquitectura fundamental lo garantiza. Sin embargo, generalmente no incorporan capacidades de seguridad de red en sus diseños. Su arquitectura no dirige la seguridad de la información.

Los híbridos están restringidos. Los dispositivos IoT 1.0 tienen un ancho de banda limitado, una escasa potencia de procesamiento, una vida útil de la batería baja y poca memoria. Hacen uso de estos recursos con los que cuentan para proporcionar capacidad de respuesta en tiempo real y una gran disponibilidad, no para cifrar datos, autenticar mensajes entrantes, validar solicitudes de control de acceso, descargar archivos de firmas o escanear malware.

Los híbridos en red son fáciles de descubrir usando Shodan o Censys, ya que carecen de firewall o filtrado. Responden a los requerimientos de la red de forma eficiente, rápida e ingenua. Estos primeros dispositivos asumen la integridad y la privacidad de la red en la que se encuentran. Asumen también que cualquier señal entrante es correcta y está destinada a ellos. El modelo subyacente es mecánico: si presiono el freno, el vehículo debería reducir la velocidad. Si aprieto el interruptor, la luz debería encenderse. La autentificación lleva tiempo y puede retrasar una corrección crítica. Al igual que con IoT 0.9, la segmentación de la red, el aislamiento y la monitorización fuera de banda pueden mitigar algunos riesgos.

IoT 2.0 - Describe dispositivos IoT contemporáneos construidos desde cero, con capacidades completas de Internet. Estos son los que más se pueden proteger, si la seguridad es un criterio de diseño evidente. Los dispositivos IoT 2.0 pueden ser mucho menos restringidos. Las mejoras en las capacidades de la batería, las técnicas de recarga, las operaciones de bajo consumo, el diseño eficiente del procesador, las arquitecturas de red avanzadas, el diseño mejorado de la antena y la amplia memoria dan a IoT 2.0 una arquitectura de sistema más similar a la TI. Estos dispositivos se están acercando a los convencionales que pueden usar tecnologías contemporáneas de seguridad de la información, con algunas adaptaciones. El registro en un canal o dispositivo de almacenamiento no crítico, por ejemplo, puede ser posible sin comprometer la fiabilidad, la capacidad de respuesta y los objetivos de seguridad. Diseñar seguridad de la información en IoT 2.0 es posible.

miento y sin necesidad de tener que recurrir en todos los casos a tecnologías de análisis en profundidad y "sandboxing". Todo ello redunda en una gran mejora de la fiabilidad y velocidad en la de detección de nuevas amenazas. El problema aquí es que éste es un arma de doble filo y empezamos a ver tentativas de usar este tipo de tecnologías también por parte de los cibercriminales, lo cuál es ciertamente preocupante por el alcance que puede llegar a tener".

EL PAPEL DEL CISO

El responsable de seguridad de una empresa adquiere cada vez un papel más importante dentro de la estrategia de la compañía. De hecho, es un cargo que no era importante hasta hace unos pocos años. Josep Albors, responsable de investigación y concienciación de ESET asegura que "a día de hoy el CISO debería jugar un papel vital en cualquier empresa de un tamaño respetable ya que es la persona encargada de diseñar y aplicar los esquemas de seguridad que van a proteger activos muy importantes. Sin embargo, demasiadas veces se encuentran incapaces de acometer esta tarea por restricciones que les impiden contar con los recursos necesarios. Por eso es importante que se sepa trasladar la importancia de invertir (que no gastar) en seguridad a los altos directivos, para evitar tener que lamentarse ante un ataque dirigido a la empresa que tenga éxito".

El CISO además de velar por la seguridad de su compañía, tiene que reportar directamente al consejo de administración. El problema que nos encontramos en algunas compañías es que el CIO ejerce el papel de CISO. Este es un verdadero problema ya que adicionalmente en muchos casos también adoptará el papel de DPO o DPD. Como asegura el portavoz de EinzelNet, "el enfoque o estrategia en materia de seguridad de una empresa se ha convertido ya en una de las principales tareas a definir; liderar desde el Top Management de la compañía: es el elemento fundamental para acometer nuevos enfoques y cambios. El CEO tiene ya que ponerse al frente de la ciberseguridad de su empresa y trasladar a todos las decisiones y estrategias adoptadas. Por supuesto, el CISO seguirá jugando un papel fundamental, pero todos los actores (con el Comité de Dirección al frente) deben cambiar su rol y asumir el principio del principio de "Accountability" o "Responsabilidad Proactiva" que viene regulado en la GDPR". Para Miguel López, "el papel del CISO es un rol extraordinariamente complejo ya que debe definir y ejecutar la estrategia de ciberseguridad de la empresa… la cuál afecta a todos los departamentos de la misma y será percibida en muchas ocasiones como un impedimento al funcionamiento "normal" hasta la fecha de cada área y recurso. El gran reto del CISO (entre otros) es, probablemente, ser capaz de sumar a todos los diferentes líderes

de la empresa a la estrategia de seguridad e integrar de forma efectiva y funcional dicha estrategia con el funcionamiento correcto y eficiente de cada departamento. El otro gran reto es el de conseguir los recursos económicos necesarios para ejecutar dicha estrategia". Finalmente el director general de Kasperrsky afirma que "Los CISOs, además de implementar una estrategia de ciberseguridad y de conseguir un presupuesto para ello, tienen que encargarse de establecer una cultura corporativa en relación con la seguridad. Desde el administrativo al director general. Cualquier trabajador de la compañía debe conocer cuál es la conducta adecuada".

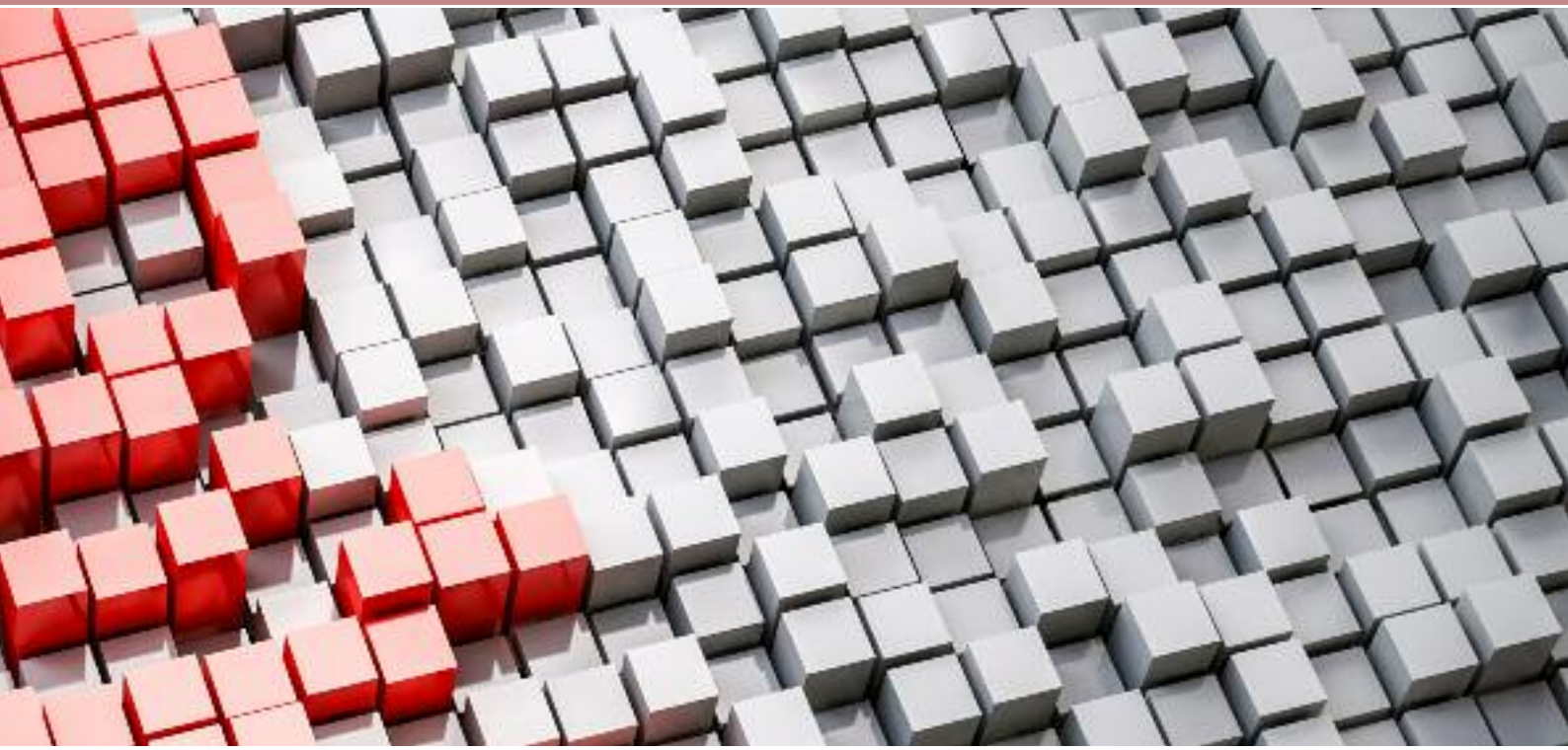
NORMAS A ADOPTAR

Los ataques como tal son un riesgo que no se puede prevenir. Se suele se mitigar poniendo controles para minimizar el impacto de dichos ataques. Desde Getronics dan una serie de pautas para que las medidas de seguridad seab efectivas y el negocio no se vea afectado:
i) Un punto único de entrada y salida de la información corporativa que cumpla con los patrones establecidos de tráfico de red necesarios. ii) La oportuna protección de cada dispositivo (ordenadores de usuario, servidores, dispositivos de red…) y mantenimiento del servicio mediante antivirus, actualizaciones de sistema operativo, programas (navegadores, Flash, Java…), balanceadores de carga, restricción de los permisos de usuario únicamente a los que necesita para su trabajo,
iii) Restricción de unidades de disco extraíbles a la mínima expresión
Desde EinzelNet afirman que "lo principal es poner barreras pero con una estrategia de seguridad efectiva, ya que el exceso de medidas de seguridad puede afectar a la productividad y, por ende, al rendimiento económico del negocio. Nosotros abogamos por soluciones de seguridad multicapa, con herramientas de protección que permitan asegurar la infraestructura TI de forma ubicua, desde el endpoint hasta la Red y el Centro de Datos para reducir el tiempo de detección y reacción, proporcionando así una protección escalable frente a un mayor abanico de vectores y durante todas las etapas de los ataques". No obstante, esto no quiere decir que la empresa no vaya a sufrir un incidente de seguridad. Recordemos que también tenemos que protegernos desde el interior que es donde principalmente tenemos fuga de datos. Por lo tanto, por este orden aconsejaríamos: protegerte, detectar, mitigar y recuperar.

> Lo principal es poner barreras pero con una estrategia de seguridad efectiva, ya que el exceso de medidas de seguridad puede afectar a la productividad

EL USUARIO COMO EL ESLABÓN DÉBIL

Pero el mayor riesgo de todos viene por parte del usuario. La mayoría de los ataques vienen porque el usuario se confía. Desde Fortinet, José Luis Laguna, su responsable técnico, afirma que "las personas seguimos siendo el eslabón más débil de la cadena, en muchas ocasiones por el desconocimiento generalizado sobre ciberseguridad, los peligros que entraña y las graves consecuencias que puede acarrear al negocio. La concienciación sigue siendo prioritaria para tratar de evi-



tar, en la medida de lo posible, que se produzcan brechas de seguridad provocadas por el personal de la compañía. Al margen de ello no todos los problemas de seguridad se producen por desconocimiento de los usuarios y por este motivo es también imprescindible contar con soluciones de seguridad que ofrezcan una protección adaptada al contexto actual, donde el perímetro de la red se ha extendido con el uso de tecnologías como Cloud e IoT, pero además, que estas soluciones faciliten la gestión, ofrezcan visibilidad de los eventos de la red y permitan identificar y eliminar el malware antes de que se extienda por toda la red. En definitiva, se requiere más inversión a nivel económico y humano para hacer frente a los retos que plantea el actual panorama de amenazas".

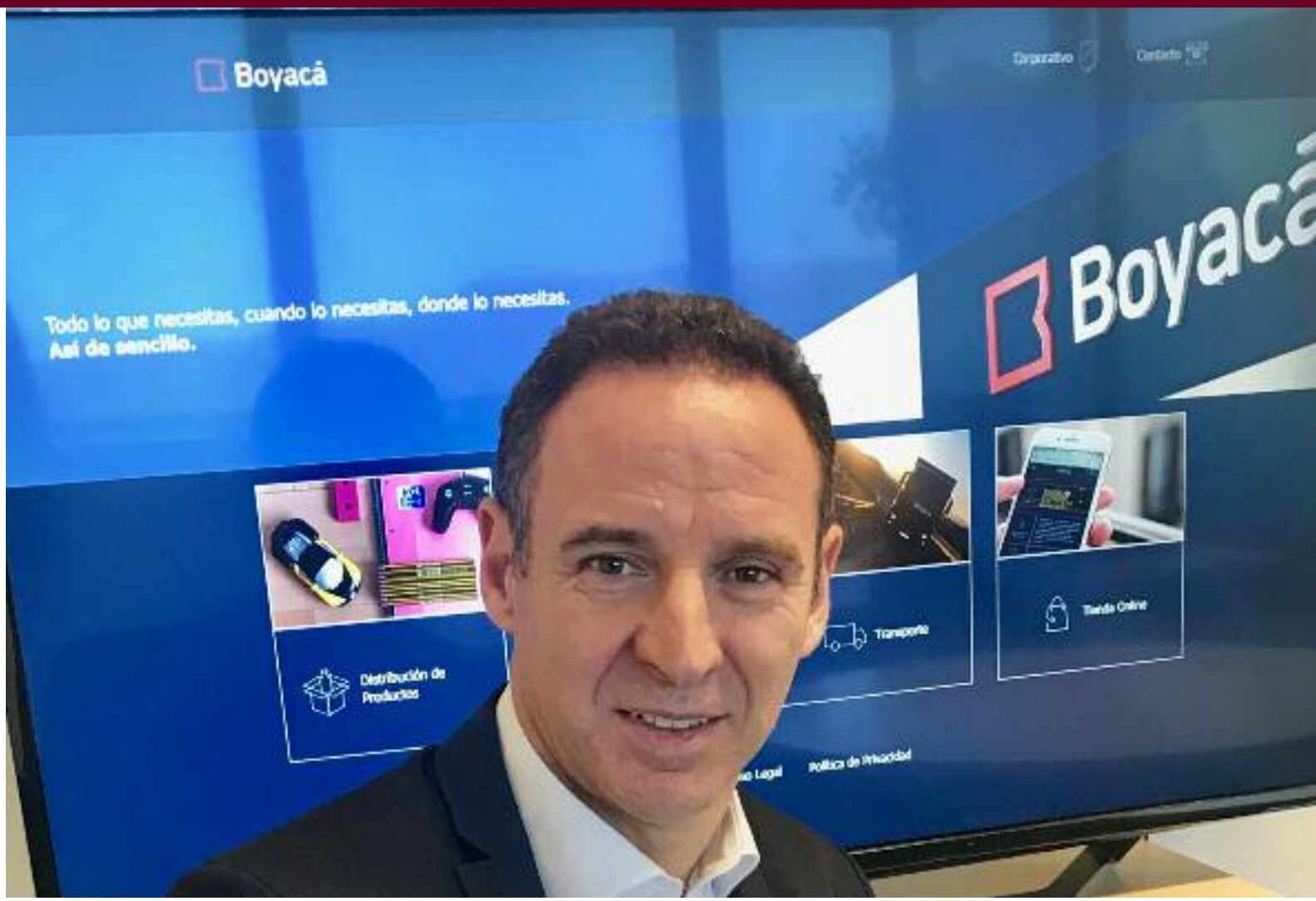
Según el informe de Kaspersky Lab y B2B International "El factor humano en la seguridad TI: los empleados hacen vulnerables a las empresas", el 46% de las empresas españolas admiten que sus empleados son su principal debilidad en la seguridad TI. De hecho, los empleados suelen ocultar los incidentes de seguridad en el 40% de las empresas españolas.

Empleados poco cuidadosos o desinformados son una de las principales causas tras de los incidentes de ciberseguridad. Mientras que el malware es cada vez más sofisticado, la rea lidad es que el factor humano puede suponer un peligro cada vez mayor.En concreto, los empleados descuidados son una de las principales brechas dentro de la ciberseguridad corporativa en lo referente a ataques dirigidos. Mientras que los cibercriminales más expertos pueden utilizar un malware hecho a medida y unas técnicas de alta tecnología, al final suelen aprovechar el punto de acceso más sencillo: la naturaleza humana.

Los cibercriminales suelen utilizar a los empleados como punto de acceso a la infraestructura corporativa. Correos phishing, contraseñas débiles, llamadas falsas de soporte técnico… Incluso un USB perdido u olvidado, puede llegar a comprometer a toda la empresa.

Por todo ello, la necesidad de implementar medidas dirigidas al personal es cada vez más evidente: el 22% de las empresas en nuestro país están analizando cómo mejorar la seguridad mediante la formación, haciendo que este sea el tercer método de ciberdefensa más popular, después de la implementación de un software más sofisticado (40%) y la incorporación de más personal de seguridad TI (31,6%)

La mejor manera de proteger a las organizaciones frente a las ciberamenazas relacionadas con las personas es combinar las herramientas adecuadas con las prácticas adecuadas. Se debe incluir también a RRHH y a la alta dirección para motivar y animar a los empleados a que sean diligentes y soliciten ayuda en el caso de incidentes. La formación sobre seguridad a los empleados, aportando unas claras instrucciones en lugar de unos documentos voluminosos, la construcción de habilidades y la motivación junto con la creación de la atmósfera adecuada, son los primeros pasos que toda organización debe tomar. Samuel Najar, Inside Sales para Europa del Sur e Israel de Netskope, asegura que "El usuario puede estar entrenado. Sin embargo, está demostrado que es mucho más eficiente implantar medidas que permitan reducir el riesgo mientras se realiza un "coaching" sobre el usuario en el momento de realizar las acciones no deseadas, ya que esta en contexto". Finalmente, el portavoz de Trend Micro considera que "El usuario es el último eslabón en la cadena que representa la estrategia de ciberseguridad de una compañía. La formación/concienciación juegan un papel importante, pero, obviamente, no podemos basar nuestra estrategia de ciberdefensa en ella. En este sentido el endpoint, dispositivo donde el usuario interactúa con otros sistemas y redes, cobra una gran importancia y debe ser protegido frente a la diversidad de amenazas existentes implementando mecanismos que proporcionen seguridad sin impactar en el rendimiento del mismo".



"Es cuestión de tiempo que los camiones sean autónomos"

¿A qué se dedica la parte principal del presupuesto de TI de la empresa?

Mantenimiento y Desarrollo de Software a medida.

¿En qué área se está invirtiendo más este año?

Migración de infraestructuras a la nube y mejora de las comunicaciones.

¿Qué proyecto es del que está más satisfecho?

Desarrollo de un sistema nuevo para la distribución y gestión integral del transporte, incluyendo los sistemas embarcados en vehículos.

Si le pusieran todos los beneficios de la empresa a cargo del departamento de TI, ¿qué le gustaría implementar?

Me gustaría seguir desarrollando nuestro sistema integral de transporte, dotándole de todos los medios técnicos que permita atender las peticiones de nuestros clientes dinámicamente. El nuevo reto sería mejorar la interacción con clientes y proveedoresde forma que permita una mayor satisfacción y control de los procesos logísticos por parte del cliente.

¿La seguridad es un problema?

No tiene porque serlo si se atiende convenientemente con los recursos necesarios para ello. Las inversiones en seguridad tienen que ser contempladas y priorizadas como parte de un plan estratégico de la compañía. La seguridad es algo que tiene que ser continuamente estimado y revisado en consonancia con los riesgos y probabilidades que se quieren evitar. Ningún proyecto dentro de la compañía, por pequeño que sea, debe obviar este apartado.

Cuando habla de necesidades tecnológicas al resto de directivos, ¿le entien-

den? ¿Qué es lo que más cuesta explicarles?

Parte de nuestro trabajo es hacer entender nuestras complejidades técnicas, traduciendo estas a conceptos empresariales con relaciones causa-efecto. No siempre conseguimos que nos entiendan en toda la amplitud pero si en lo básico y necesario. Lo que más cuesta explicar son siempre aquellas propuestas más innovadoras y en donde a veces las ventajas no son medibles o comparables de una forma directa con la alternativa actual.

¿Se puede trabajar desde casa?

Sí, hace años que esta cuestión no plantea dificultades técnicas. La dificultad actualmente consiste en que cada manager cambie de una cultura presencialista a una cultura basada en objetivos, adaptando como quiere que trabaje su equipo. Personalmente no soy partidario de forzar una forma de trabajo u otra.

¿Qué modelo de smartphone utiliza? ¿Lo tiene asegurado?

He utilizado tanto Iphone como Android en los últimos años. Ahora mismo uso Android y no lo tengo asegurado.

¿Cuál es la herramienta que realmente le cambió la vida?

Los smartphones, empezando por esas robustas Blackberries de primeros de los 2000s.

A la empresa española, tecnológicamente, le falta….

Invertir más en I+D+i y tener una clara visión y confianza en que dichas inversiones son rentables.

¿Harto de solucionar los problemas tecnológicos de la familia y amigos? ¿Qué le suelen pedir?

No, para nada. Siempre es un placer intentar ayudar. Lo único que ha cambiado es que antes solía ser yo mismo el que solucionaba gran parte de lo que me pedían y ahora les remito a algún profesional más especializado .

¿Tiene cuenta en redes sociales? ¿En cuáles?

Si. Linkedin, Instagram y totalmente en des-uso Facebook.

¿Cree que las empresas deben tener perfil en redes sociales?:

Si, totalmente. Las empresas deben de comunicar allí donde estén sus potenciales clientes, proveedores, competidores, empleados…

¿Qué es eso de la transformación digital? ¿Slogan o necesidad?

En mi opinión es algo que tiene que ocurrir o está ocurriendo en aquellas empresas que busquen perpetuarse, es una necesidad vital de las empresas. Todo está cambiando, los mercados, los procesos, la forma de interactuar con clientes y terceros. El modo genérico en que la empresa tiene que adaptarse a esos nuevos cambios es lo que en general llamamos "Transforamción Digital", no es un eslogan, es una realidad, es una metamorfosis de todas las áreas de la empresa.

¿En la nube u on-premise?

En la nube claramente, en mi opinión los modelos on-premise solo están justificados cuando la escala es muy muy grande o bajo especificidades muy concretas.

¿Hay mucho talento en su empresa?

Si, como en la mayoría de empresas de este país, el talento de las personas es un gran activo.

¿Piensa en la distribución con drones?

Creo que está aún lejos, pero ¿por qué no?. Las empresas debemos de estar preparadas para esa mentalidad innovadora, la historia nos ha enseñado que a veces ciertos descubrimientos hacen que se acelere un notable salto en la tecnología.

¿Los camiones de la distribución serán autónomos?

Si, esta cuestión no es ya, si lo serán o no, ahora la incógnita es saber cuanto tardarán. Como todas las tecnologías, esta seguirá una curva de adopción en S y tendremos que ver cuán rápido se consumen las etapas iniciales hasta la madurez.

José María Castillo

Information Systems Director de Boyacá

Fecha de nacimiento: 3/11/1966
Estado Civil: Casado.
Hijos: Dos.
Deportes: Running, padel, ciclismo, futbol
Hobbies: Motociclismo, robótica, bricolaje.
Estudios: Ingeniero Informático UPM, Executive MBA por IE
Antigüedad en la empresa: 3 años
Personas a su cargo: 40
Trabajos anteriores: Consultor estratégico de Sistemas , IT Manager y Director de sistemas para diversas compañías multinacionales de sectores como Telecomunicaciones, Farmacia o Gran Distribución.

ECIJA

Los peligros de Whatsapp

Javier López,
ECIJA Abogados

El escándalo generado en noviembre de 2017 por los mensajes realizados en el chat de Whatsapp de la policía municipal de Madrid, donde se habría insultado y amenazado a la Alcaldesa Manuela Carmena y otras personas y colectivos, devolvió a la actualidad el riesgo que puede conllevar el uso de los sistemas de mensajería y las redes sociales. En este caso, se trataba de un chat en el que participaban unas ciento cincuenta personas, lo que hace que la difusión sea mucho mayor, por lo que resulta aconsejable extremar las cautelas ante el gran número de destinatarios de los mensajes.

Y es que estos comentarios podrían ser constitutivos de delitos de odio (penado con prisión de 1 a 4 años y multa de 6 a 12 meses por el art. 510-1 del código penal), de vejaciones (penado con prisión de 6 meses a 2 años y multa de 6 a 12 meses por el art. 510-2 del código penal), de amenazas (penado con prisión de 6 meses a 2 años por el art. 169-2 del código penal) o de calumnias (penado con prisión de 6 meses a 2 años o multa de 12 a 24 meses por el art. 206 del código penal). Respecto de este último, la Sentencia de la Audiencia Provincial de Pontevedra de 22 de noviembre de 2017 establece que se produce el delito cuando concurren los siguientes elementos: a) expresiones objetivamente ofensivas y suficientemente graves para considerar menoscabada la dignidad y el honor de la víctima; b) claridad de las expresiones que excluye la posibilidad de que la acusada no fuera consciente de su significado; c) contexto en que se profieren; d) falta de rectificación tanto en el propio Whatsapp, como en la conciliación y juicio; e) ausencia de interés en la comprobación de la verdad (exceptio veritatis); f) inexistencia de prueba de las imputaciones y g) falta de indicio, careciendo de base objetiva o indiciaria la imputación.

Dicho esto, se plantea la cuestión de si dichos comentarios estarían amparados por la libertad de expresión establecida en el art. 20 de la Constitución. Para ello sería necesario analizar cada uno de ellos para comprobar si han sobrepasado los límites del derecho constitucional y han incurrido en el delito, toda vez que, según tiene establecido el Tribunal Constitucional, el derecho fundamental a expresar juicios personales y subjetivos, creencias, pensamientos y opiniones, incluida la crítica de la conducta de otro, aun cuando sea desabrida y pueda molestar, inquietar o disgustar no ampara las frases y expresiones decididamente injuriosas, ultrajantes u ofensivas que carecen de relación con las ideas u opiniones que se exponen y, por tanto, son innecesarias a este propósito (SSTC 49/2001, 204/2001, 20/2002, 99/2002, 160/2003, entre otras).

Por otro lado, también habría que considerar si se trata de conversaciones privadas protegidas por el derecho a la intimidad regulado en el art. 18 de la Constitución y en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen; o si esto no sería óbice para que se considere que se ha cometido un delito a la luz de la doctrina jurisprudencial que establece que la extensión actual de las nuevas tecnologías al servicio de la comunicación intensifica de forma exponencial el daño de afirmaciones o mensajes que, en otro momento, podían haber limitado sus perniciosos efectos a un reducido y seleccionado grupo de destinatarios, de forma que quien hoy incita a la violencia en una red social sabe que su mensaje se incorpora a las redes telemáticas con vocación de perpetuidad y carece de control sobre su zigzagueante difusión, pues desde que ese mensaje llega a manos de su destinatario éste puede multiplicar su impacto mediante sucesivos y renovados actos de transmisión (STS de 18 de enero de 2017).

Y, es que no conviene olvidar que, caso de serlo, los delitos siguen siendo delitos con independencia del medio a través del cual se lleven a cabo, con el agravante de que los realizados en el ciberespacio (Whatsapp, Line, Facebook, Twitter, Instagram, YouTube, etc.) dejan un rastro que puede ser seguido por las fuerzas policiales para acreditar que se han producido, así como el autor de los mismos. Recientemente, han sido sonados los casos de los polémicos tuits del exconcejal Guillermo Zapata o Cassandra Vera, cuyos comentarios difícilmente habrían podido ser perseguidos si no se hubieran hecho a través de las redes sociales.

Los delitos son delitos con independencia del

medio a través del cual se lleven a cabo, con el agravante de que los realizados en el ciberespacio como Whatsapp dejan un rastro
Pero estos no son los únicos contratiempos que pueden generarse con el uso del Whatsapp. Es habitual que se utilicen los sistemas de mensajería para enviar fotografías y videos a otros usuarios, por ejemplo, de menores. En este punto hay que ser especialmente cuidadoso y no enviarlo a nadie que no sea de estricta confianza, ya que podrían reenviarse a otros destinatarios no deseados, con la consecuencia de que la imagen de los menores se vería difundida indebidamente.
En este sentido, la Instrucción 2/2006 sobre el Fiscal y la protección del Derecho al Honor, Intimidad y Propia Imagen de los menores recuerda que el principio general de protección reforzada de los derechos a la intimidad y a la propia Imagen de los menores.
Iguales precauciones deben adoptarse con las fotografías que se ponen en el perfil del usuario, ya que cualquiera que disponga de nuestro número de teléfono podría bajarse la fotografía sin la menor dificultad. No obstante, esta imagen no podría difundirse sin el consentimiento de la persona afectada en atención a la doctrina del Tribunal Supremo que establece que publicar la fotografía de una persona sacada de su cuenta de Facebook (o de otra red social) exige su consentimiento expreso, ya que lo contrario supone una intromisión ilegítima en su derecho a la propia imagen (STS 91/2017).
Pero, ¿cómo se puede entender prestado este consentimiento cuando se trata de un menor? Según establece la jurisprudencia, sin perjuicio de que debe evitarse, en interés del menor, una sobreexposición en estos ámbitos, en el caso de menores, siempre que no medie el consentimiento de sus padres o representantes legales con la ausencia del Ministerio Fiscal (art. 3 de la citada Ley Orgánica 1/1982), la difusión de cualquier imagen de éstos ha de ser reputada contraria al ordenamiento jurídico. Y en el supuesto de que los padres estén divorciados o separados, la decisión de publicar una fotografía del hijo en una red social pertenece a la esfera de la responsabilidad parental compartida por ambos progenitores y no a la guarda, de forma que, siendo los dos progenitores titulares de la patria potestad es necesario el acuerdo de ambos para poder publicar imágenes del hijo en redes sociales. (SAP Barcelona de 25 de abril de 2017).
Asimismo, en el plano profesional, no es extraño que muchas comunicaciones con clientes y proveedores se realicen por Whatsapp por la facilidad, rapidez e inmediatez que supone este sistema. Pues bien, aquí también es necesario tomar precauciones para no difundir datos o información que pudieran estar protegidos por el deber de confidencialidad o por la normativa sobre protección de datos, en especial, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
Por último, respecto al uso de aplicaciones utilizadas para monitorear los mensajes de Whatsapp por padres a sus hijos, empresarios a sus empleados, etc., si se hace sin el consentimiento de estos, podría constituir un delito de vulneración del derecho a la intimidad y el descubrimiento y revelación de secretos, sancionado con las penas de prisión de 1 a 4 años y multa de 12 a 24 meses (art. 197-1 del código penal). En el caso de que se utilice para vigilar, sin su autorización, a la pareja o expareja, también se produciría un delito de "stalking" (acoso), castigado con la pena de prisión de 3 meses a 2 años o multa de 6 a 24 meses (art. 172 ter-1-1º del código penal).

La transformación digital de Nationale-Nederlanden

Después de separarse del Grupo ING, Nationale-Nederlanden, una de las mayores aseguradoras a nivel mundial, tuvo que afrontar un importante proceso de renovación, que incluía la parte tecnológica. Jordi Bueno, CIO de Nationale-Nederlanden ha contado a BYTE TI cómo se ha llevado a cabo dicho proceso de transformación digital. ***Manuel Navarro***

Poniendo el foco en el cliente como principal elemento de la estrategia de transformación que iba a llevar a cabo Nationale-Nederlanden, los responsables de la compañía vieron que la separación de ING iba a suponer una magnifica oportunidad para reinventarse. Jordi Bueno, cuenta cómo ha sido todo el proceso.

¿Cuándo comienzan a realizar el proceso de transformación digital?

Puede decirse que 2015 marcó un antes y un después para Nationale-Nederlanden. En ese año, culminamos nuestro proceso de separación del Grupo ING y volvimos a convertirnos en una empresa totalmente independiente. El cambio de marca lo recibimos con los brazos abiertos y además, desde el principio, lo vimos como una oportunidad para reinventarnos. Puede decirse que vivimos una auténtica revolución y que la transformación digital fue una de las protagonistas pero no la única. Lo que sí es cierto es que, desde entonces, la innovación se convirtió en una de nuestras abanderadas.

¿Cuáles eran las necesidades que querían cubrir?

En lo que se refiere al punto de partida no había negociación posible: el cliente era el centro de la estrategia y, a partir de ahí, empezamos a construir. Pensar por y para las personas hace que, en primer lugar, tengas que adaptarte a las necesidades y peticiones de los nuevos tiempos en los que la digitalización de procesos resulta imprescindible. Muy pocos pueden imaginarse su día a día sin recurrir a Tablets, smartphones, smart-TV's, etc. y nosotros, como compañía que presta servicios, tenemos la obligación de facilitar el acceso a la información de manera inmediata, con procesos sencillos y directos, cumpliendo con las medidas de seguridad más exigentes y mejorando la eficiencia en costes operativos. Empezamos dotando a nuestra red comercial con más de 1.000 Tablets para desarrollar de forma digital una relación con el cliente y contratación de productos. Un proceso que permite realizar un completo análisis de las necesidades de las personas (AdN) en pro de ayudarles a construir su futuro financiero y que ha reducido los tiempos de emisión de pólizas de 25 días a apenas unas horas.

¿En qué consistió la fase de estudio?

Inicialmente, revisamos de arriba abajo todos los aplicativos de negocio y sobre que tecnologías estaban construidos. El ejercicio comenzó con un proceso clave: la ayuda en la planificación del futuro financiero y la contratación de pólizas. Entonces, vimos una clara oportunidad de digitalización; simplificando, optimizando los procesos y eliminando el papel a la vez que consolidábamos y reducíamos el número de aplicaciones que teníamos disponibles para la pre-venta y venta. En paralelo, también pusimos el foco en implantar un modelo que favoreciera la movilidad y que nos permitiera tener oficinas más flexibles y más presencia de agentes en movilidad cubriendo el territorio español. A continuación, vimos como continuar con la digitalización acometiendo los procesos de post-venta. De primeras, el cambio propuesto, provocó rechazo e ilusión a partes iguales. Al final, es lógico aferrarse a lo establecido y seguir confiando en aquello que funciona. Podemos tener muy buenas ideas e intentar ver cómo adaptarlas a las necesidades de la gente real pero sin una buena estrategia de comunicación y orientación el cambio es muy difícil. En nuestro caso, la fase de estudio estuvo marcada por hacer ver el sentido de urgencia que tomaba la transformación, echar un vistazo a lo que estaba haciendo la competencia, analizar los motivos por los que debíamos hacer cambios, y probar qué tecnologías nos eran más favorables.

¿Cuáles son los pasos que se dieron??

Jordi Bueno es el CIO de Nationale-Nederlanden

Aunque el momento más importante del proceso de transformación fue el año 2015, lo cierto es que comenzamos a desarrollar propuestas en esa línea dos años antes. En 2013, lanzamos una nueva web de clientes, una plataforma intuitiva, sencilla y personalizada que nació con el propósito de ofrecer el mejor servicio a nuestros clientes a partir de sus necesidades.

El segundo hito fue la completa digitalización del proceso de venta llevada a cabo al año siguiente. Primero comenzamos con un piloto y, meses después, todos nuestros agentes podían llevar a cabo el estudio de las necesidades del cliente, prepararse la entrevista, realizar una fotografía de su DNI, rellenar la solicitud y formalizar el contrato obteniendo la firma digital y biométrica del cliente de forma inmediata estuvieran dónde estuvieran a través de una Tablet. Ya en el año 2015, todo nuestro portfolio de soluciones estaba disponible en la aplicación de venta y fue entonces cuando acometimos el proyecto de formalización online. Además, nuestra herramienta AdN experimentó una actualización completa a lo que hay que sumar el inicio del proceso de registro automático de pólizas que perseguía reducir los tiempos de emisión y eliminar fallos. A estos proyectos, le siguieron mejoras continuas en la web encaminadas a lograr una mayor autonomía del cliente en sus gestiones así como la digitalización de todas las transacciones post venta.

¿Qué premisas fueron las que se abordaron?

La premisa inicial era conseguir ser punteros dentro del sector a partir de aplicaciones y desarrollos dirigidos a adaptarse a las necesidades de los clientes. La experiencia nos dice que, a partir de la situación vivida en los últimos años, las personas reclaman más transparencia y capacidad de respuesta y nuestro objetivo era y es satisfacer a nuestros clientes independientemente del canal que procedan (red comercial, empresas, online, etc.) y dónde o cuándo quieran establecer una relación con nosotros. Obviamente, a nadie se le escapa que la tecnología, además, puede ayudar a optimizar procesos y costes. En este sentido, por ejemplo, convertirnos en compañía con filosofía "papel 0" ha hecho que lleguemos a ahorrarnos 1,8 millones de euros en un ejercicio.

¿Tuvieron que pasar por periodos de formación los empleados?

Si hay algo que nos distingue de la competencia es el equipo humano que no solo aceptó el reto del cambio si no que instauró la innovación en su propio ADN y confió en la transformación para conseguirlo. Desde el inicio hasta ahora, hemos dado muchos y variados pasos, algo que ha hecho necesario incorporar nuevos perfiles digitales –como especialistas en datos, desarrolladores web y movilidad, expertos en cloud, en marketing digital, etc. – que a priori puede parecer que no encajan con el negocio de una aseguradora tradicional pero es que ya no lo somos. Además, muchos de los que formábamos parte de la compañía hemos tenido que reciclarnos y abrir la mente a nuevas alternativas en un mundo que gira muy deprisa.

¿Qué ventajas ha reportado a los clientes este nuevo modelo?

La transformación se desató para ellos y, por tanto, su opinión siempre ha sido un factor clave a la hora de tomar decisiones y pensar y definir nuevos proyectos. El modelo con el que actualmente operamos, y que se sustenta en la tecnología en gran parte, ha reducido los tiempos, agilizado la comunicación, simplificando procesos, etc. Prueba de ello es el reciente lanzamiento de nuestro Canal Directo, una plataforma de venta online que permite contratar un producto de ahorro e inversión desde casa utilizando la tecnología más puntera como, por ejemplo, el reconocimiento facial a la vez que se cumplen los estándares de seguridad más altos.

Big Data, Dark Data… ¿dinero que las empresas tiran?

No hace falta decirlo: vivimos en la Era de la Tecnología. Esto tiene múltiples consecuencias…

Pepe Varela

Entre las cuales no es la menos importante (precisamente) que las empresas disponen de una gran cantidad de datos (sobre sus clientes, la competencia, el mercado) que no siempre son capaces de analizar y aprovechar en su totalidad.
Bernardo Posada (@bernardoposada) comunicador, experto en el seguimiento de medios e innovador del análisis informativo a través de la Inteligencia Artificial, es Director General de Eprensa y socio fundador de Puntonews.com. En su opinión "para las empresas se ha convertido en una necesidad (imperiosa) disponer de las herramientas y capacidad suficientes para sacar provecho a su Big Data. Esto es lo que se llama aplicar el Business Intelligence (BI) a la empresa".
Una vez que la empresa ha asumido que no tiene otra que que gestionar, del mejor modo posible, el caudal de datos del que dispone, surge la necesidad de buscar herramientas eficaces que le permitan recopilar y analizar todo ese Big Data. Según explica el CEO de Puntonews.com "un ejemplo de BI, habitual en cualquier empresa, es la recolección de información detallada sobre sus clientes para, posteriormente, predecir comportamientos, hacer proyecciones de ventas o identificar patrones de consumo".
Precisamente Puntonews acaba de lanzar Hallon Reports 2.0, un servicio de análisis y métrica que permite el seguimiento de la aparición en medios de comunicación.
Bernardo explica que "la herramienta permite la creación de gráficos de manera flexible, incluso con datos de diferente origen, lo cual aporta una visión mucho más global al análisis. Los nuevos gráficos son diagramas de barras, circulares, tartas, series temporales y mapas de presencia y dispersión geográfica, tanto de España como de cualquier país en el que se está realizando el seguimiento".

LOS DARK DATA

¿A qué nos referimos los tecnólogos cuando hablamos de Dark Data y cuál es su diferencia con otros tipos de datos generados en el uso de dispositivos electrónicos, en las redes o en los procesos industriales? ¿Cómo puedo explotar mejor estos "datos ocultos" en la actividad diaria de mi empresa y qué beneficio tiene su análisis? Mauricio Marchant (@mmarchant_ec), Director de proyectos, especialista en marketing digital y optimización SEM, además de growth hacker y data scientist con experiencia en grandes multinacionales, da respuesta a estas preguntas.
Para él "lo primero que hay que señalar es que, si BI son los datos que la empresa utiliza en su operativa diaria, Dark Data son los datos que resultan del uso de las infraestructuras de telecomunicación, redes, navegación, y procesos industriales y que hasta hace poco, ni se coleccionaban, ni se almacenaban ni explotaban".
Ejemplos de Dark Data son los datos de registro de un TPV de un comercio, los datos de repetición de una antena de telecomunicación, la localización por GPS de un transporte, o las señales de los sensores de una máquina industrial o de un aparato de salud. Según un estudio reciente de IBM el 80% de los datos generados son Dark Data o datos desestructurados y esta cifra llegará al 93% en 2020. IBM también estima que el 60% de los datos pierden su valor si no se utilizan dentro de una ventana temporal adecuada.

TRANSFORMAR LOS DATOS EN INFORMACIÓN… Y EN DINERO

Para Bernardo Posada "ésta es, quizás, la propiedad más importante de BI, tener la capacidad de convertir los datos en información y ésta en conocimiento". ¿El objetivo final? El fundador de Puntonews.com lo

tiene claro "optimizar la toma de decisiones en la empresa, tales como reducción de costes, proyecciones financieras, planificación de ventas, eficiencia en la producción, gestión de inventarios…" Juan José Gilsanz (@gilsanzjj) es director general de MBIT. Para él, y sobre la opinión de Bernardo Posada "la clave para que una empresa pueda alcanzar todos estos objetivos está en contar con analistas especializados tanto en Big Data como en Data Science como en el uso de las herramientas y metodologías adecuadas. Esto es casi obligatorio, puesto que con las herramientas y tecnologías convencionales resultaría prácticamente imposible capturar, gestionar, procesar y analizar tanta información disponible".

2018, año clave para BI

Esto es lo que opina Juan Luis Peñaloza Figueroa (jluispf@emp.ucm.es). Para este profesor, de Analítica Web y Big Data en la escuela de negocios Spain Business School "2018 será un año de generalización y consolidación del sistema Big Data donde, de hecho, los datos gobiernan gran parte de nuestras vidas. Esto es posible, precisamente, gracias al trabajo de unos analistas que tienen los conocimientos necesarios para explotar estos datos y transformarlos en valor". En palabras del profesor Peñaloza, "las soluciones Big Data, penetrarán, cada vez más, en todos los sectores productivos y económicos. Esto abarca desde la venta al por menor hasta la Administración Pública, la vida diaria de las personas y, en general, toda actividad económica y social".

DE LA GRAN EMPRESA A LA PYME

Este será, según diversos expertos, otro de los grandes pasos que dará la implantación de BI para este 2018. Para Elena Díaz de Liaño, consultora de transformación digital "lo primero que deben hacer las pymes es tener un plan para saber si son digitales. Muchos pueden creer que son digitales por el simple hecho de tener una agenda con los datos de sus clientes. Esto es un error bastante común. Además, hay que tener paciencia. Siempre hay proyectos fallidos. El que diga que todo sale bien a la primera, sencillamente miente". Sobre como del Big Data surgió el Business Intelligence, como análisis de la empresa y sus clientes, Díaz de Liaño recordó que "todo comenzó con Jeff Bezos (el fundador de Amazon), quien a comienzos del año 2000 utilizó BI para relanzar su empresa". La verdad es que 2018 promete ser un año para recordar en el entorno Big Data y BI. Lo veremos.

Ejemplos de Dark Data son los datos de registro de un TPV de un comercio, los datos de repetición de una antena de telecomunicación, la localización por GPS de un transporte, o las señales de los sensores de una máquina industrial

El despertar de la Inteligencia Artificial

El crecimiento de la Inteligencia Artificial acapara muchas de las noticias tecnológicas: desde algoritmos que aprenden cómo jugar sin intervención humana (el caso de Go), pasando por Elon Musk y Mark Zuckerberg profundizando en los riesgos y los beneficios de la IA para la humanidad, hasta Rusia y China, que han declarado la inteligencia artificial como una prioridad de investigación. El Deep learning, uno de los subcampos más importantes de la investigación en inteligencia artificial, será especialmente prometedor.

Filip Pieczynski, Director de desarrollo de negocio de RTB House

En términos generales, el objetivo de la inteligencia artificial es hacer que los ordenadores sean igual de inteligentes, o incluso más, que los seres humanos, dándoles habilidades de razonamiento y pensamiento similares. Entre las muchas formas de lograr esto, el machine learning o aprendizaje automático es la tecnología de referencia, utilizada ampliamente en todas las industrias.

La influencia de la IA se puede apreciar especialmente en el Deep learning, una rama innovadora de la Inteligencia Artificial que imita el trabajo del cerebro humano en el procesamiento de datos y la creación de patrones en la toma de decisiones. Este año se ha convertido en una tecnología imprescindible en muchas áreas (como la asistencia sanitaria o la automatización de automóviles). Además, el Deep learning también ha tenido en 2017 un gran impacto en toda la industria publicitaria.

Inspirado por las neuronas biológicas en nuestros cerebros, el Deep learning ha hecho posible obtener descripciones del usuario más fiables, más ricas e interpretables por una máquina, del potencial de compra del cliente sin ningún conocimiento humano. Por ejemplo, RTB House, empresa global que ofrece tecnología de retargeting, ha analizado conjuntos de datos masivos para mostrar que un enfoque basado en la inteligencia artificial puede conducir a una tasa de conversión un 35% mayor que la acción del ser humano. Pero los algoritmos de Deep learning pueden lograr resultados todavía mejores. Esta tecnología puede predecir los hábitos y deseos únicos de un usuario para la industria publicitaria. Simplifica la experiencia cotidiana de usuario al ofrecer anuncios profundamente orientados que contienen no solo los productos que tenemos más probabilidades de comprar, sino también aquellos que no hemos visto o productos que ni siquiera hemos pensado.

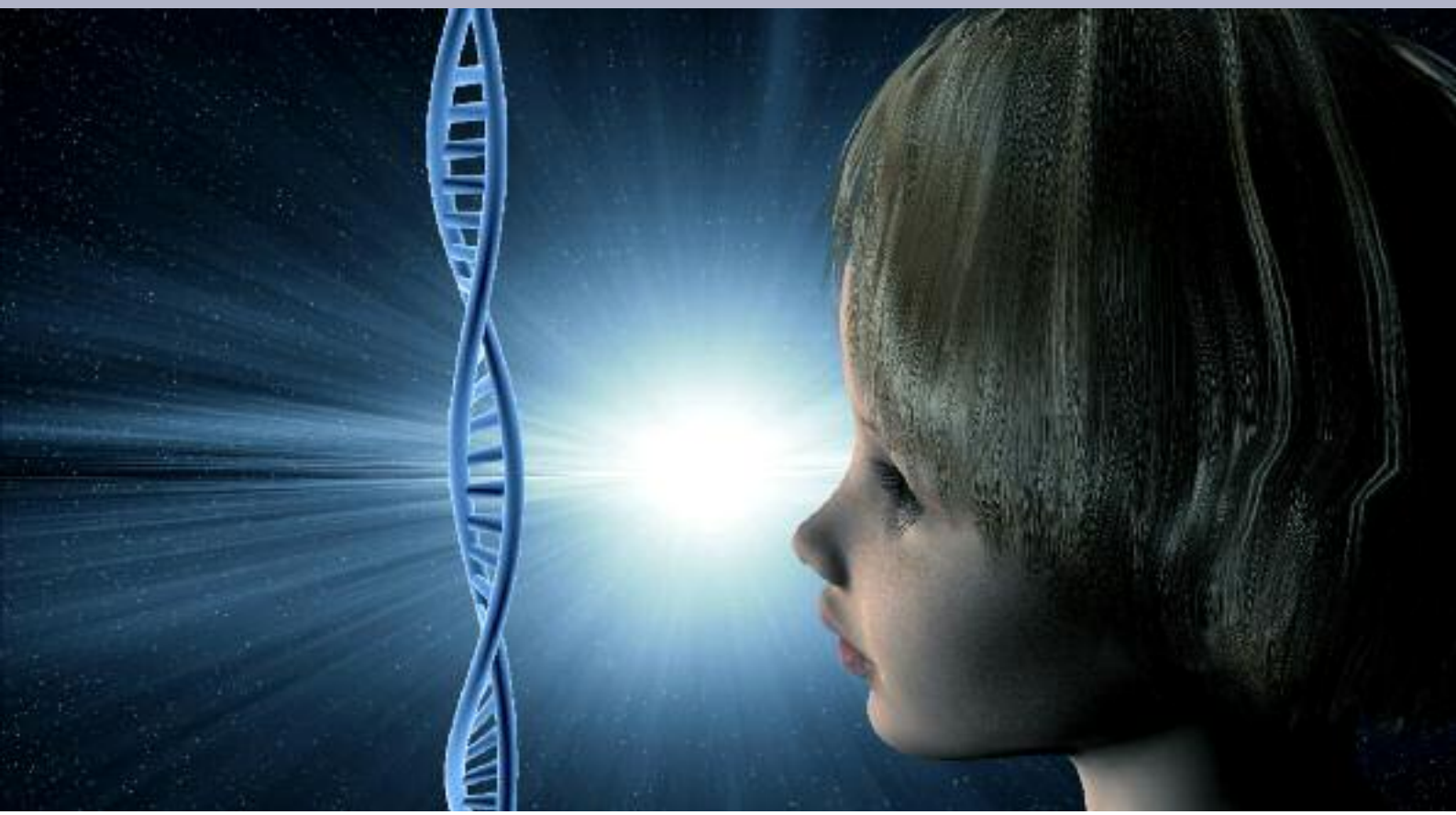
Muchas marcas ven el beneficio de implementar la IA y las soluciones de Deep Learning en sus productos o herramientas. En 2018, esperamos ver empresas líderes enfocadas en desarrollar más y mejores aplicaciones con Inteligencia Artificial.

Del aprendizaje supervisado a nuevas áreas

En 2017 vimos una desviación del llamado "aprendizaje supervisado", un enfoque estándar utilizado por el machine learning. Su premisa se basa en las instrucciones que ofrece una persona a un ordenador para que aprenda, teniendo en cuenta patrones de ejemplos, conjuntos de datos y respuestas preexistentes.

En 2018, en la investigación de IA se profundizará en áreas más sofisticadas, como el 'transfer learning'. Esta es una forma de Deep Learning en la que la enseñanza de una máquina se basa en varias simulaciones. La máquina aprende a tomar decisiones utilizando el conocimiento obtenido de muchas simulaciones, en lugar de datos objetivos de la realidad. Esto hace que el proceso sea mucho más fácil, rápido y económico. Usando este método, una máquina aprende a tomar decisiones con conclusiones lógicas o deducciones a las que llega por sí misma.

El segundo enfoque se conoce como "aprendizaje reforzado". Su objetivo es que la máquina tome las mejores decisiones en función de los comentarios que recibe del entorno y las consecuencias de sus propias acciones. Por ejemplo, en la industria publicitaria, se aplica a los anunciantes cuando



hacen una oferta para comprar anuncios. Los sistemas de subastas son tan complejos que incluso los especialistas del sector a tienen problemas para determinar la tasa óptima que les permita alcanzar los resultados deseados al menor coste. Una máquina también se encontrará con problemas. Sin embargo, a diferencia de un ser humano, puede progresar y hacer ofertas las 24 horas del día en un entorno de simulación. También puede aprender mucho más rápido que un humano. En función de los resultados de sus simulaciones de subastas, puede aprender cómo pujar de la manera más efectiva y, por lo tanto, cómo ganar las subastas.

NUEVOS TRABAJOS

Por supuesto, los algoritmos de Deep Learning aprenden de la misma forma que las personas. Pero su principal diferencia, como hemos dicho, es que la máquina aprende incomparablemente más rápido y puede analizar cantidades inimaginables de datos. Tampoco tienen que dormir y no cometen muchos errores. Aquí es donde el factor de rendimiento súper humano entra en juego. De una manera muy simple, la IA intentará superar a las personas en todas las áreas posibles. Hoy en día, los algoritmos de aprendizaje son capaces de reconocer mejor las imágenes que el ser humano.

¿Significa que las máquinas que superan a los humanos también ocuparán sus puestos de trabajo? No exactamente. Según el Foro Económico Mundial, el 65% de los niños que acceden hoy en día a las escuelas de primaria terminarán en trabajos que actualmente no existen. La tasa actual de desarrollo de inteligencia artificial permite que más compañías busquen más especialistas en IT, analistas de datos y programadores. En 2018 probablemente vivamos un boom de nuevas ofertas de trabajo para científicos de datos, una posición que hasta ahora no ha sido muy popular.

El objetivo final para el Deep Learning es hacer nuestras vidas más fáciles y nuestro trabajo más efectivo. Por lo tanto, el uso de IA ya no es un estándar, sino una necesidad para las empresas que desean ser competitivas en un mercado global. No se trata de la capacidad de personalizar o mejorar las capacidades de un producto final, sino también de una gama de otras actividades indirectas de productos, como la recopilación y el análisis de datos. Las empresas ahora tienen una cantidad tan grande de datos para analizar que no se mantienen al día con el procesamiento. Esto afecta directamente las decisiones tomadas por sus empleados y, en consecuencia, los resultados financieros.

Las empresas especializadas en la recopilación y análisis de datos para diversos negocios tendrán un papel cada vez más importante. Las compañías con presupuestos más grandes usarán a su vez IA para sugerir qué ofrecer a los clientes, recomendar términos para darles a los proveedores e instruir a los empleados sobre qué decir y qué hacer, en tiempo real. También pronto surgirán muchas nuevas empresas, ofreciendo soluciones basadas en algoritmos de aprendizaje, ya que esta tecnología se va a seguir desarrollando.

La inteligencia artificial en 2017 se ha convertido en parte de nuestra vida cotidiana y en parte de la opinión pública. Los próximos años se centrarán en el desarrollo de tecnologías basadas en la IA que reemplazarán a los seres humanos en muchas tareas difíciles, en última instancia, haciendo nuestras vidas mucho más fáciles. Pero aún nos queda mucho trabajo por delante.

Preparación del CRM para análisis predictivo

Las barbacoas en el jardín son un clásico del verano. Uno de los ingredientes clave para una buena comida al aire libre es el tiempo. Hay quien ve un cielo despejado y enseguida prepara la barbacoa. Otros, por su parte, creen que el dolor de articulaciones es una señal de lluvia. Gracias a los avances en meteorología, la mayoría de la gente abre su app de pronóstico del tiempo para asegurarse de que la previsión no sea de lluvia a la vez que prepara la carne. Todos estamos más contentos cuando nos aseguran un resultado positivo de nuestro esfuerzo.

Imad Alabed, director senior, Pivotal & Knova

Antiguamente, muchas empresas se basaban en su instinto y su experiencia pasada; pero ahora el mercado exige que las decisiones empresariales se basen en hechos y cifras; no en corazonadas. En una encuesta reciente de Aberdeen Group sobre análisis e inteligencia empresarial, el 46 % de los encuestados indicaron que las presiones competitivas les exigen estar orientados a los datos. La capacidad de convertir las tendencias históricas y los datos en tiempo real en información que les permita pasar a la acción allana el camino para lograr mejoras de rendimiento.

ATENCIÓN AL FUTURO

El acceso a los datos no es suficiente para que una empresa mantenga su ventaja competitiva. Los empleados de cualquier nivel de responsabilidad deben poder tomar medidas basadas en la información disponible. Aberdeen define el análisis predictivo como una tecnología que permite que las empresas analicen datos estructurados y no estructurados para revelar tendencias y correlaciones, además de predecir la probabilidad de que se den ciertos comportamientos de los clientes. Las soluciones de gestión de la relación con el cliente (CRM) son el complemento idóneo para el análisis predictivo, ya que la empresa puede maximizar las oportunidades de venta y mejorar la productividad de sus directores de cuentas.
Tomar la decisión errónea en el momento equivocado puede resultar caro; se necesita tener la capacidad de predecir "qué" y "dónde".
Además de mejorar las relaciones comerciales y garantizar la prestación de un servicio de alta calidad, las empresas deben conocer a sus clientes y contar con datos históricos de los compradores para formarse una visión clara del verdadero interés del cliente. La combinación de análisis predictivo y CRM social ofrece un potencial aún mayor para conocer a los clientes actuales y potenciales. La información de perfiles, publicaciones e historiales de clics se puede usar para crear perfiles de clientes más completos, obteniendo así análisis más precisos. Un conocimiento mayor y más profundo de las tendencias de consumo en constante cambio permite a las empresas enriquecer el conocimiento del mercado y lograr mayor satisfacción del cliente final. En definitiva, un ciclo de realimentación positivo que proporciona una ventaja competitiva a las empresas.

PREPARACIÓN DE "LA BOLA DE CRISTAL"

La gran cantidad de información y la velocidad a la que circula son dos de los mayores retos a los que se enfrentan las empresas. Según la encuesta de Aberdeen, el 96 % de las empresas sufren un uso inefectivo de los datos. Uno de los aspectos del análisis predictivo que intimida a los usuarios potenciales es la precisión de los datos sobre los que se fundamentan las conclusiones. Para ofrecer el mejor análisis, los datos de trabajo deben estar preparados correctamente. Este paso es tan importante que algunos analistas dedican más de tres cuartas partes de su tiempo a preparar los datos para el análisis. La automatización de la preparación de los datos facilita que los usuarios mantengan el control de los mismos, reduciendo la carga informática. Los analistas de Gartner especializados en análisis predicti-

vo recomiendan que las empresas partan de datos limpios, precisos y completos en sus soluciones de automatización de las ventas antes de implementar una estrategia de análisis.

La inexactitud de los datos no es el único factor que puede estropear una previsión; en ocasiones, la información está desperdigada en tantas ubicaciones y en tantos formatos que no es posible consolidarla. Las empresas también deben integrar los datos en una vista unificada del cliente a través de todos los sistemas, para aumentar la precisión y la relevancia de los datos sujetos a análisis. Las empresas que utilizan cuadros de mandos analíticos tienen un 42 % más de probabilidades de tener los datos estandarizados procedentes de múltiples canales, lo que asegura una correcta integración del software. Además de datos "limpios", el análisis predictivo debe tener acceso a múltiples fuentes de datos, puesto que "aprende" con cada nuevo origen de datos. Al mismo tiempo, es importante evitar incorporar demasiadas fuentes con relativa rapidez. Un enfoque adecuado consiste en iniciar el proyecto con una cantidad menor de datos consolidados, lo que permite obtener un rendimiento rápido de la inversión, y posteriormente realizar un crecimiento tomando datos de nuevas fuentes. Esto asegura un crecimiento continuado de análisis predictivo.

CONCLUSIÓN

A pesar de que las soluciones CRM ya recopilan grandes cantidades de información, el análisis predictivo permite obtener datos a un nivel más profundo. Las soluciones CRM con análisis predictivo ofrecen información práctica en tiempo real que mejora las decisiones que deben tomar todos los días los equipos de ventas, operaciones, marketing y equipos ejecutivos.

La mayoría de sistemas CRM son extremadamente flexibles y ofrecen modelos de datos fáciles de modificar o ampliar. Esta flexibilidad garantiza que el CRM sea capaz de adaptarse a los requisitos cambiantes de los datos. Sin embargo, a lo largo de los años, muchas empresas no han prestado una adecuada atención al control de los datos. Prepare el camino al análisis predictivo iniciando una actividad de limpieza de los datos.

Prácticamente cualquier sector de actividad industrial puede beneficiarse, o acabará haciéndolo en breve, de la utilización de impresoras 3D

Enrique Ávila,

director del Centro Nacional de Excelencia en Ciberseguridad

"La estrategia española en ciberseguridad es buena pero faltan recursos"

Nacido en el año 2010, el Centro Nacional de Excelencia en Ciberseguridad (CNEC) es una institución que se crea ante el déficit de talento que existía entre las Fuerzas y Cuerpos de Seguridad del Estado en materia de Ciberseguridad. Forma parte de una red de centros europeos adscrito a la Universidad Autónoma de Madrid y Enrique Ávila, su director, mantuvo una charla con Byte TI, en la que analizó la situación de la ciberseguridad y ciberinteligencia en la actualidad.

Manuel Navarro

¿Cuáles son los objetivos del CNEC?

Nuestro objetivo es la formación avanzada de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado así como del mando conjunto de ciberdefensa. Ahora mismo tenemos un máster que es el el "Máster en análisis en evidencias digitales y lucha contra el cibercrimen" al que tienen acceso exclusivamente miembros de las Fuerzas y Cuerpos de Seguridad del Estado, aunque también ha accedido a él un diputado del Congreso. En estos momentos, hemos formado a más de 120 estudiantes. En definitiva, se trata de tener certificadas y formadas al mayor número de personas posibles para poder tirar del talento interno de la Administración Pública porque atraer al talento que hay en el mercado, es algo prohibitivo para la Administración, además de que la ley no lo admite.

¿Por qué no existe formación en España en materia de ciberseguridad?

Porque hemos confundido concienciación con formación. En España se han hecho campañas de concienciación pero no se han hecho campañas de formación. Hace dos años estuve impartiendo clase en la Escuela Superior de Guerra de Colombia. Allí tienen toda una planificación en materia de ciberdefensa y ciberseguridad. Por ejemplo, acaban de certificar a 100.000 ciudadanos como ciudadanos digitales. Es decir, tienen las competencias necesarias para ejercer sus derechos y sus responsabilidades de forma digital. Esto es muy importante, porque creo que los ciudadanos deberíamos tener la obligación de alfabetizarnos tecnológicamente. En España estamos haciendo uso de los medios y herramientas tecnológicas sin ningún tipo de formación previa y después intentamos alfabetizarnos y eso es una locura.

¿Qué es eso de la ciberreserva?

Somos un grupo de profesionales que hemos detectado una serie riesgos y amenazas que decimos que tenemos problemas para poder mitigar esas amenazas. Uno de esos problemas, por ejemplo es el talento. Hay más talento fuera de las Fuerzas Armadas que dentro. No digo que el talento de las Fuerzas Armadas sea malo, al contrario. Lo que sucede es que numéricamente, falta gente. Lo que vemos es que la Administración tiene muy difícil el acceso al talento, simplemente porque no puede pagarlo y porque estás compitiendo en un mercado global y el mejor talento, al final, se lo va a llevar Google. La única forma que se nos ha ocurrido de retener el talento es a través del voluntariado y que ese señor que trabaja en Google, colabore en la formación de otros durante por ejemplo, su tiempo de vacaciones.

Así que la ciberreserva es un cuerpo civil, que nunca tiene actividad operativa y que ofrece asesoramiento avanzado multidisciplinar. Y no estoy hablando de hackers: estoy hablando de psicólogos para acciones de contrainteligencia, de juristas para determinar que tipo de respuesta para actuar ante un ciberataque… Asi que proponemos crear capacidades transversales que además pueden generar muchas externalidades positivas.

El usuario representa el mayor riesgo de todos, ¿cómo se le educa?

La vida digital no hay que separarla de la vida analógica. Lo digital es una sobredimensión que nos ha sobrevenido. Hasta mediados del siglo XX, teníamos cuatro dimensiones. Ahora tenemos cinco. Y esta quinta dimensión tiene un problema añadido y es que es muy dinámica y muy rápida en el cambio. Además es aterritorial y es muy difícil aplicar las leyes en ella. Así que bajo estos parámetros hay que empezar a enseñar a la gente a que vive en esas cinco dimensiones. Esto se desarrolla educando a la gente en materia cibernética desde que son muy pequeños.

El concepto de ciudadano analógico no es el mismo que el concepto de ciudadano digital. Vamos a tener que desarrollar este último concepto. Además, vamos a tener que desarrollar el concepto de separación de poderes al ciberespacio. Tenemos que desarrollar estas nuevas áreas de conocimiento que son filosóficas, éticas y morales.

¿Los estados son seguros?

En España, los diferentes Gobiernos han hecho un esfuerzo importante para desarrollar una estructura de ciberseguridad y que es coherente y está bastante bien diseñada. Lo que nos faltan son los recursos. Ahora, además, esa estructura se va a ver reforzada por el Consejo Nacional de Ciberseguridad. Toda política pública tiene que ir acompañada de recursos, porque si no, es una simple entrada en el BOE. ¿Cómo se consiguen esos recursos? Dado que los recursos son limitados, se consiguen con un político que arriesga su capital político y que decide quitar esos recursos de una parte para destinarlos a ciberseguridad sabiendo de antemano que toda política pública genera incremento del gasto.

UN NUEVO TIPO DE CIENCIA

Por Miquel Barceló

Hace unos meses les hablaba de Origen, la última novela de Dan Brown. Pero en esa novela, de manera implícita, se aborda una cuestión que me pareció interesante: analizar hasta qué punto la computación, el uso de programas y modelos matemáticos, pueden también desencadenar nuevos procesos de pensamiento y aplicar los resultados de la computación a un nuevo tipo de aproximación al saber en diversas disciplinas.

Embarcado en una búsqueda de la posibilidad de todo ello acabé encontrando un libro que trata de algo parecido y que, aunque ha sido ampliamente criticado, no deja de sugerir nuevas ideas de cuya potencialidad sigo teniendo mis dudas pero que no dejan de tener su interés.

Se trata de A New Kind of Science (2002, Un nuevo tipo de ciencia) de Stephen Wolfram (científico británico conocido por su trabajo en ciencias de la computación, matemáticas y física teórica). En él, en grandes líneas, se aborda un estudio que pretende ser sistemático (aun siendo esencialmente empírico) de los sistemas computacionales y en especial de los autómatas celulares (cellular automata). El autor acaba recomendando el estudio metodológico de los que llama "programas simples" (programas pequeños y sencillos con ciertas características bien determinadas) y propone incluso extender ese tipo de estudio como base para otros campos de la ciencia e incluso de la filosofía.

Un programa simple o sencillo, siempre pequeño, vendría a estar caracterizado por cuatro rasgos muy determinados:

1 – su operativa puede ser completamente explicada con una ilustración gráfica sencilla

2 – su operativa puede ser completamente explicada en pocas sentencias de lenguaje humano

3 – puede ser implementado en un lenguaje de programación con sólo pocas líneas de código

4 – el número de variaciones posibles es tan pequeño que todas ellas pueden ser computadas.

Con todo ello, los programas simples de Wolfram suelen partir de un sencillo marco abstracto. Ejemplos lo serían diversos casos de simples autómatas celulares, máquinas de Turing y programas combinadores, mientras que autómatas celulares más complejos dejarían de serlo. Simplicidad es el rasgo dominante.

Para Wolfram lo importante de esos programas simples o sencillos es que la gran mayoría de los mismos son capaces de producir gran complejidad y por eso los recomienda como forma de estudio de sistemas complejos en un amplio conjunto de disciplinas, no sólo las informáticas. Wolfram sugiere que esos programas simples vendrían a ser la forma más sencilla de ciencia y una herramienta útil para el estudio de otros casos. Incluso sugiere que al igual que reconocemos como ciencias a la física y la química, dice que deberíamos reconocer una ciencia especial, propia y especifica centrada en ese estudio de los programas simples. La idea central es que el estudio de esos programas simples y su taxonomía permitiría suministrar un sistema coherente de ideas que permitirían incluso justificar la computación como un principio básico de organización de la ciencia, de cualquier ciencia...

De ahí a la hipótesis que usa Dan Brown en su novela Origen no hay más que un paso. Sofisticado pero posible.

Hasta aquí, la propuesta de Wolfram aunque no cabe olvidar que ha sido más bien criticada por pretenciosa (pretender que eso sea un nuevo tipo de ciencia y además una ciencia básica que ha de poder servir de base incluso para otras ciencias) y, también, otras muchas razones.

El libro fue un éxito de ventas y obtuvo diversos premios, aunque como libro científico ha sido criticado por aparecer directamente en forma de libro y no pasar por el sistema de revisión por pares tan típico de las revistas científicas. Ello permite, según algunos críticos, desautorizar el libro desde el punto de vista científico, aunque otras comentaristas se han sentido atraídos por la novedad de las ideas de Wolfram y ese intento de poner la computación (sencilla) en la base del conocimiento científico. Y Wolfram no es un cualquiera: en 2017 había sido citado ya en más de cincuenta mil publicaciones científicas...

Una gran mayoría de comentaristas están en una actitud de "wait and see" (esperar y ver) qué ocurre con todo ello en un futuro más o menos inmediato. Ya que hay pocas certezas y, tal vez, algunas intuiciones sugerentes.

Una gran mayoría de comentaristas están en una actitud de "wait and see" (esperar y ver) qué ocurre con todo ello en un futuro más o menos inmediato

¿Cómo serán tus experiencias en Nexica?

The Cloud Experience:

cloud pública, privada o híbrida,
en tu CPD o en el nuestro

nexica
digital dimension | economcom

NEXICA
C/ Acer, 30-32, 1º 4ª, 08038 Barcelona
C/ Dr. Zamenhof 36 bis, 1º A, 28027 Madrid
Contacta con nosotros: hola@nexica.com | **902 202 223**