it TRENDS

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

El futuro digital empieza hoy

DICIEMBRE 2018

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

Director Juan Ramón Melara
juanramon.melara@itdmgroup.es
Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales Eva Herrero
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de IT User
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora de medios on-line
Bárbara Madariaga barbara.madariaga@itdmgroup.es

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

Nace IT Trends:

¿qué tendencias tecnológicas cambiarán los modelos de las empresas?

En los últimos años, el ritmo de innovación tecnológica se ha acelerado y han sido muchas las empresas pioneras que se han subido a esa ola para transformar sus modelos de negocio. Muchas otras se encuentran en pleno proceso o dando sus primeros pasos, pero todas pueden aprovechar las más recientes propuestas del mercado para idear su concepto de empresa con nuevos modelos basados en datos, nuevas infraestructuras ágiles, nuevos métodos de trabajo auspiciados por soluciones tecnológicas... El resultado es una empresa que empieza a definirse como digital.

La digitalización es un proceso constante porque así lo es la industria que la alimenta. En IT Digital Media Group queremos desgranar cómo está siendo ese proceso de transformación digital de las organizaciones españolas y cómo el mercado tecnológico está apoyando dicho cambio con sus soluciones. Por esta razón, hemos lanzado IT Trends, un proyecto que aglutina productos meramente editoriales, como una web, revistas digitales y #DiálogosIT con las principales empresas del sector, junto a otras iniciativas como los Encuentros IT Trends para conocer las tendencias que van a definir 2019 en la industria TI, y un estudio de mercado publicado en forma de Documento Ejecutivo que nos ayudará a descubrir la realidad de la empresa española en cifras, en lo que a la adopción y evolución de las TI se refiere. Los resultados los puedes leer aquí.

Visita IT Trends en www.ittrends.es o síguenos en Twitter en @ITTrends_ITDM y conoce cómo están calando en las empresas las últimas propuestas tecnológicas para construir el nuevo entorno digital.

Gracias a nuestros compañeros de viaje **F5**, **DXC Technology**, **Sophos**, **GMV**, **Kaspersky Lab**, **Sonicwall**, **D-Link** y **Equinix** por su interés en este tipo de iniciativas novedosas y por querer conocer la realidad del ecosistema en el que todos habitados...

Felices #ITTrends

Juan Ramón Melara
Director General IT Digital Media Group

IT Trends: Así es la realidad digital de la empresa española

2019 será un año prometedor en lo que a tecnologías de la información se refiere. Nuevas propuestas tecnológicas se irán adentrando en las empresas a medida que se encuentre aplicación a las mismas en el negocio, y aquellas que ya están asentadas, vivirán también algunos cambios.

¿En qué estado se encuentran las iniciativas tecnológicas en la empresa española? ¿Cómo invertirá en 2019 y cuáles serán sus prioridades? ¿Cómo valora la llegada de nuevas propuestas tecnológicas y ve su posible aplicación al negocio?

Con el propósito de averiguar cuál es el estado digital de la empresa en España, IT Research realizó durante los meses de septiembre a noviembre una encuesta para ahondar en las prioridades tecnológicas de las organizaciones. Los resultados de este trabajo de campo, se reflejan ahora en un Documento Ejecutivo IT Research (que puedes descargar aquí) y arrojan una posición asentada en las organizaciones de los proyectos de transformación digital, adopción de cloud o modernización del puesto de trabajo, así como una excepcional preocupación por la seguridad, si bien revela también que aún queda un largo camino por hacer en áreas como Big Data, IoT, Blockchain o Inteligencia Artificial.

El documento contempla también la percepción de las empresas respecto a asuntos como los retos en ciberseguridad o retención de talento, dos cuestiones fundamentales para las organizaciones en 2019.

Esta primera edición del Documento Ejecutivo recoge ahora el estado de las iniciativas tecnológicas en las empresas españolas y la intención que tienen de cara al próximo ejercicio. Y en enero, esta información se complementará con datos sobre la intención de inversión de las organizaciones en TI a lo largo del año, su percepción sobre los presupuestos de TI disponibles en 2019 y objetivos del presupuesto. Descarga ahora este primer capítulo y te avisaremos de la disponibilidad de esta nueva información en enero. “Para IT Digital Media Group, un proyecto como IT Trends y un Documento ejecutivo como el que hemos generado ha sido un reto maravilloso. Normalmente, las editoriales de tecnología nos dedicamos a suministrar información a nuestros lectores de cómo evoluciona el mercado, las principales novedades o las estrategias de negocio y era un reto conseguir que nuestros lectores profesionales nos ayudaran a conocer, de primera mano, la realidad tecnológica de la empresa española. Gracias a todos los que lo habéis hecho posible. Los resultados son prometedores en cuanto a la alineación de la empresa española con el resto de países de nuestro entorno utilizando la tecnología como elemento disruptivo”, afirma Juan Ramón Melara, Director General de IT Digital Media Group.

Descarga aquí este Documento Ejecutivo y descubre aquí cómo es la realidad digital de la empresa española. ■

TODOS LOS DATOS DE LA **REALIDAD DIGITAL** DE LA EMPRESA ESPAÑOLA

Descarga este **documento ejecutivo** de itRESEARCH

it TRENDS

Tendencias TI para no perder el tren de la Transformación Digital en 2019

Todo apunta a que 2019 será el año en el que la transformación digital se convierta en una realidad en las empresas. Las organizaciones han estudiado este año la lección y el próximo se acelerará la digitalización de las organizaciones. Además de cloud, que se presupone se irá convirtiendo en un estándar de un modo u otro, irá cogiendo mayor tracción la aplicación de tecnologías emergentes como blockchain y la inteligencia artificial, esperamos la llegada de 5G y las empresas tendrán que repensar sus modelos de negocio para dar cabida al mayor protagonismo que cobra el cliente y aprovechar la información que le puedan dar los datos.

Las cifras de IDC

El gasto mundial en Transformación Digital llegará a los 59.000 millones de dólares entre 2018 y 2021.

Y en estos momentos en los que terminal el año, las consultoras tecnológicas y de negocio realizan sus predicciones para el ejercicio siguiente. ¿Qué veremos en 2019? A continuación, podrás leer las principales tendencias auguradas por estos observadores del mercado para el siguiente año, tanto desde el punto de vista de negocio como tecnológico. Y no te pierdas algunos datos destacados de cómo marchará el mercado TI en este próximo 2019.

GARTNER: 10 TENDENCIAS TECNOLÓGICAS ESTRATÉGICAS PARA 2019

La consultora define como tendencia tecnológica estratégica aquella que tiene un potencial disruptor y que está empezando a salir de un estado emergente para tener un uso e impacto mayor, o aquellas que están teniendo un rápido crecimiento y marcarán un punto de inflexión en los próximos 5 años. Las tendencias tecnológicas que propone para este 2019 casan con lo que ha definido como una estrategia ContinuousNEXT, y que incluye estos cinco aspectos: privacidad, inteligencia aumentada, cultura, gestión de producto y gemelos digitales. Así pues, estas son las tecnologías que posibilitarán el próximo año la creación de dicha estrategia:

1 Dispositivos autónomos. Vehículos autónomos, robots, o drones utilizan la inteligencia artificial para realizar funciones que antes hacía el hombre. Su automatización va más allá de la proporcionada por rígidos modelos de programación y explotan la IA para ofrecer comportamientos avanzados que interactúen de una forma más natural con el entorno y las personas. Según Gartner, en 2021, el 10% de los vehículos serán autónomos.

2 Analítica aumentada. La analítica aumentada se centra en áreas específicas de la inteligencia aumentada, utilizando aprendizaje automático para transformar cómo el contenido analítico se crea, consume y comparte. La consultora cree que en 2019 habrá una serie de instrumentos para analizar los datos que permitirán a las personas ajenas al campo de la analítica, extraer información, convirtiéndose en "ciudadanos científicos de datos". Los datos, pero sobre todo las informaciones obtenida gracias a éstos, se integrarán cada vez más en aplicaciones empresariales, en los departamentos, por ejemplo, de recursos humanos, marketing, ventas, asistencia al cliente y finanzas.

3 Desarrollo basado en Inteligencia Artificial. La inteligencia artificial podrá ser usada para desarrollar aplicaciones para automatizar procesos de análisis o pruebas de datos. Según Gartner, para 2022, habrá co-desarrolladores de inteligencia artificial en los equipos de al menos el 40% de los nuevos proyectos de desarrollo de aplicaciones.

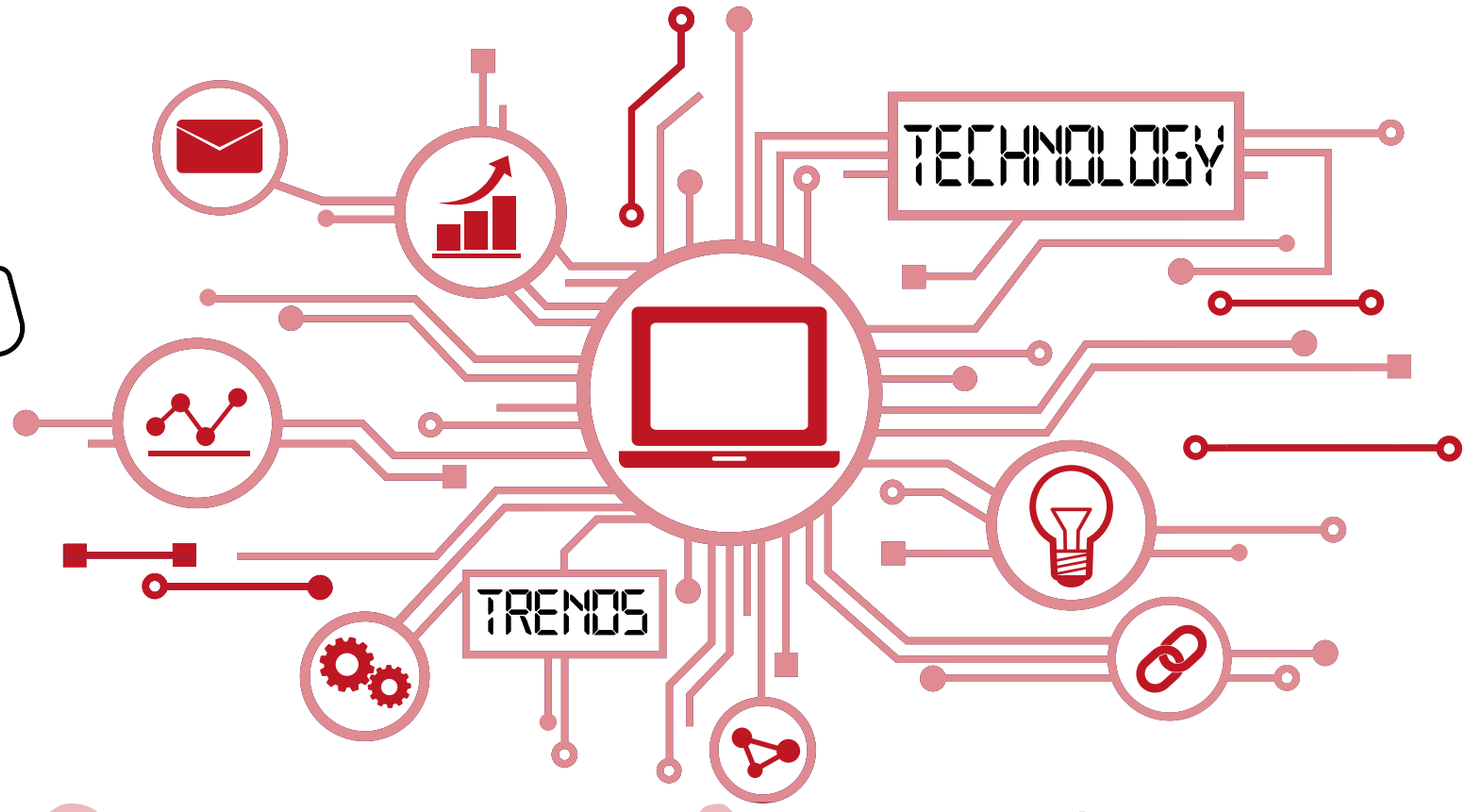
4 Gemelos digitales. Son una representación digital de un objeto físico, con vida propia y que interactúan entre sí en el mundo digital. Para 2021, los gemelos digitales serán utilizados por la mitad de las grandes empresas para lograr una mejora de la ventaja competitiva y la eficiencia del 10%.

Encuentros it TRENDS

Las tendencias TIC para la empresa digital
de la mano de los líderes del sector

SEGURIDAD

PLATAFORMA



NEGOCIOS DIGITALES

5 Empoderamiento del extremo de la red. El término edge computing indica "la elaboración de informaciones al borde de la red, donde se producen los datos". De acuerdo con Gartner, muy pronto el edge computing y el cloud computing serán modelos complementarios, por lo que los servicios cloud podrán ser distribuidos como servicios centralizados también en los servidores distribuidos. En los próximos cinco años, los chips de Inteligencia Artificial especializado, junto con una mayor potencia de procesamiento, almacenamiento y otras capacidades avanzadas, se incorporarán a un amplio abanico de dispositivos en el extremo de la red.

6 Experiencias inmersivas. Las empresas, tanto B2C como B2B, están experimentando con tecnologías cada vez más inmersivas. En 2020, según Gartner, éstas serán experimentadas por el 70% de las empresas, pero solo el 25% de estas aplicaciones se lanzará en producción.

7 Blockchain. Las cadenas de bloques podrán cambiar la realidad industrial haciéndola más transparente, bajando costes, reduciendo los tiempos de transacción y eliminando las autoridades centrales que subyacen en el modelo actual. Aunque Gartner lista esta tecnología en sus recomendaciones para 2019, no será hasta 2030 cuando se perciba su impacto: para entonces habrá generado 3.100 millones de dólares en valor comercial.

8 Espacios inteligentes. Son entornos físicos o digitales en los que interactúan personas y tecnología. Se caracterizan por una creciente autonomía, inteligencia y conexión. Siguen el ejemplo de las ciudades inteligentes y, según Gartner, son cada vez más importantes convirtiéndose en parte integral de nuestra vida diaria. Los espacios inteligentes podrían ayudar en temas como la reducción del calentamiento global.

9 Privacidad y ética. Individuos, gobiernos, y organizaciones están cada vez más preocupados por el uso de sus datos. Por eso , se están enfrentando cada vez más a este problema – como ya estamos viendo con el RGPD. Gartner prevé que para 2021, las organizaciones que han subestimado las medidas adecuadas de privacidad pagarán un 100% más de los costes de conformidad respecto a competidores que no han subestimado el problema.

RPA: BENEFICIOS Y RETOS DE LA AUTOMATIZACIÓN DE PROCESOS BASADOS EN ROBÓTICA

10 **Computación cuántica.** Si hoy solo el 1% de las organizaciones mundiales asigna presupuesto a la computación cuántica, para 2023 la tendencia cambiará: las inversiones procederán del 20% de las organizaciones. Los ordenadores cuánticos permiten la resolución de problemas difíciles de resolver a través de un enfoque tradicional o que requieren largos tiempos de resolución con un algoritmo tradicional. Encajan perfectamente en las industrias militar, automovilística, aseguradora, financiera y farmacéutica, donde el control de calidad es esencial.

Más sobre las principales tecnologías propuestas por Gartner para 2019 aquí.

Las cifras de Gartner

El 47% de los CIO de EMEA afirma que sus organizaciones ya han cambiado los modelos de negocios o están en proceso de hacerlo.

IDC: EL FUTURO ES MULTICLOUD

La transformación digital de las empresas avanza a diferentes ritmos en cada país, pero los líderes de TI que han apostado por este proceso en los últimos años ya han adoptado las estrategias que marcarán el camino para los rezagados. Según IDC, ya se encuentran en condiciones de pasar a la segunda fase, impulsados por los avances realizados en la inteligencia de datos y por su actual capacidad para desarrollar nuevas aplicaciones y servicios digitales que les permitirán avanzar junto con sus clientes.

En una reciente publicación de la consultora, Frank Gens, vicepresidente y director de análisis de IDC, dijo que: "a medida que las industrias, y la economía global, se reajustan y consolidan rápidamente en torno a la innovación digital, los CXO deben competir para reinventar sus organizaciones para el acelerado mundo de la innovación multiplicada. Esto significa reinventar la TI en una infraestructura de nube distribuida, pilas de software de nube pública, desarrollo e implementación de aplicaciones ágiles y nativas de la nube, AI como la nueva interfaz de usuario y nuevos enfoques generalizados de seguridad y confianza a escala".

Para dar una medida de hacia dónde se encaminará la industria de las tecnologías de la información, IDC ha publicado una lista con las diez principales predicciones TI:

❖ Para 2022, más del 60% del PIB mundial estará digitalizado, y el crecimiento en todas las industrias estará impulsado por las ofertas mejoradas digitalmente.

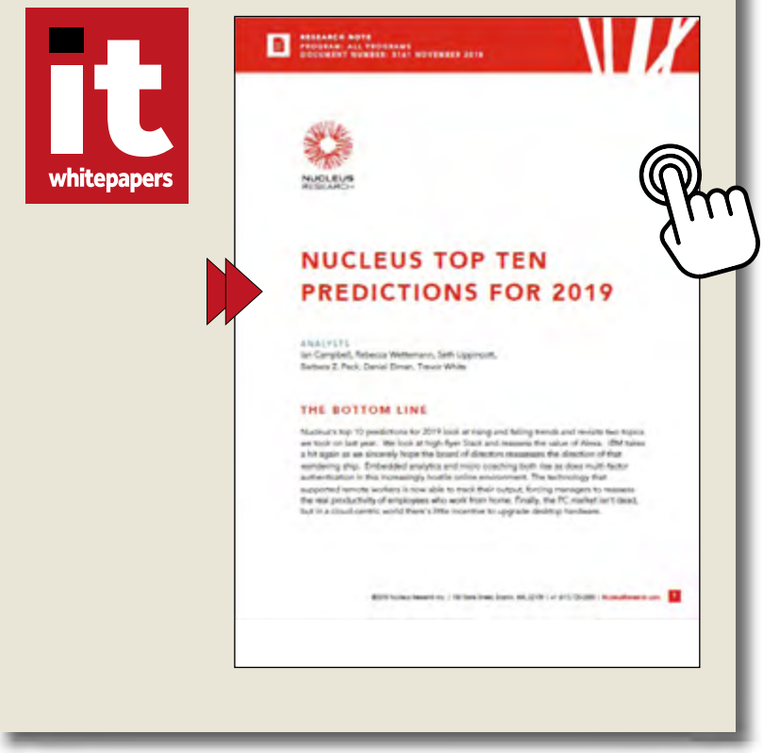
❖ De cara a 2023, más del 75% de todo el gasto en TI se destinará a tecnologías de la llamada "tercera plataforma", y más del 90% de las empresas crearán entornos digitales de TI nativos para competir en la economía digital.

❖ En 2022, más del 40% de los despliegues en la nube de las organizaciones incluirán la computación EDGE, mientras que un 25% de los sistemas y dispositivos de punto final ejecutarán algoritmos de inteligencia artificial.

❖ Para 2022, el 90% de todas las aplicaciones tendrá una arquitectura de microservicios que mejorará la capacidad de diseñar, depurar, actualizar y aprovechar el código de terceros. Y el 35% de todas las aplicaciones de producción serán nativas de la nube.

❖ En 2024, una nueva clase de desarrolladores profesionales producirán código sin scripts personalizados, lo que permitirá ampliar el nú-

10 PREDICCIONES SOBRE LA INDUSTRIA TECNOLÓGICA PARA 2019, SEGÚN NUCLEUS RESEARCH



TECHNOLOGY YOU NEED. NOT TECHNOLOGY WE MAKE.

INTRODUCING DXC TECHNOLOGY.

A new kind of partner, tempered by experience, fiercely independent and ready to help you grab all the opportunities digital transformation has to offer.

www.dxc.technology/GetItDone

DXC.technology | THRIVE ON CHANGE.

mero de desarrolladores un 30% y acelerará la transformación digital.

❖ Entre 2018 y 2023, estas nuevas herramientas y el mayor número de desarrolladores permitirá crear más de 500 millones de nuevas aplicaciones lógicas. Esto igualará la cantidad creada en los últimos 40 años.

❖ De cara a 2022, el 25% de la nube pública se basará en procesadores que no sean x86 (incluyendo procesadores cuánticos), y las organizaciones gastarán más en aplicaciones de tipo SaaS verticales en vez de en horizontales.

❖ Para 2024, las interfaces de usuario basadas en inteligencia artificial y la automatiza-

Las cifras de Forrester

Las empresas gastarán 4.349 millones de dólares en el diseño, planificación, construcción y ejecución de soluciones de IoT para 2023, frente a los 1.861 millones de dólares empleados en 2017.

Así debe ser la agenda del CIO en 2019

Las organizaciones están adentrándose en la tercera era de la TI, que se produce una vez que las empresas pasan de una etapa de experimentación digital a su aplicación masiva.

Para Gartner, la empresa digital ha alcanzado este año un punto de inflexión al detectar, tras una encuesta mundial, que el 45% de los CIO han cambiado ya sus modelos de negocio o están haciéndolo. La necesidad de abordar la digitalización del negocio ha calado y ya se está aplicando de forma masiva, lo que está conduciendo a una nueva era tecnológica en la que el CIO debe estar atento a los rápidos incrementos en el escalado del negocio digital.

La encuesta de Gartner revela que el 33% de los participantes ha evolucionado en sus esfuerzos de digitalización para escalar, frente al 17% del año pasado, y esto es achacable a la necesidad de conectar más con el cliente a través de los canales digitales. Esa capacidad de escala se está viendo en volumen, alcance y agilidad, y esto se refleja en más servicios y acciones digitales, más interacciones, mayor afinidad con el cliente y unos costes menores del servicio.

La transformación hacia empresas digitales está siendo respaldada por un crecimiento constante de los presupuestos de TI que, en 2019, en opinión de los CIO, será del 2,9%. Este porcentaje es un promedio, ya que los encuestados de EMEA creen que se producirá un aumento del 3,3%; los de Asia Pacífico del 3,5%, los de Norteamérica del 2,4%; y los de Latinoamérica del 2%.

Por otro lado, las tecnologías emergentes disruptivas jugarán un gran papel en los cambios que se están produciendo. La más mencionada es la inteligencia artificial, seguida de analítica.

Gartner también detecta un elevado interés por la ciberseguridad como base del negocio digital. Está también en la agenda de los CIO de la mayoría de las empresas, aunque creen que la organización de TI sola ya no puede proporcionar más seguridad.

10 PREDICCIONES PARA EL CIO

IDC coincide con Gartner y Forrester al señalar que el CIO tiene que reinventarse. La consultora arroja para esta figura directiva las siguientes predicciones. La primera es que para 2021, el 70% de los CIOs ofrecerán "conectividad ágil" a través de APIs y arquitecturas que interconecten las soluciones digitales de proveedores de nube, desarrolladores de sistemas, nuevas empresas y otros. Esta tendencia vendrá impulsada por las necesidades de las líneas de negocio, dice IDC.

En segundo lugar, en esa misma fecha, obligados a seguir reduciendo el gasto tecnológico, mejorar la agilidad de las TI y acelerar la innovación, el 70% de los directores de TI aplicarán la analítica de datos y la inteligencia artificial a los procesos, herramientas y operaciones de TI.

>> Continúa

ción de procesos reemplazará a una tercera parte de las aplicaciones basadas en pantalla actuales. Mientras tanto, para 2022 el 30% de las empresas utilizará tecnología conversacional para fidelizar a los clientes.

❖ En 2024, el 50% de todos los servidores podrá encriptar los datos en reposo y en movimiento, más de la mitad de las alertas serán gestionadas por automatismos basados en IA y 150 millones de personas tendrán identidades digitalizadas basadas en blockchain.

❖ En el año 2022, las cuatro mega plataformas cloud más importantes acapararán el 80% de todos los despliegues IaaS y PaaS, pero en 2024 el 90% de las organizaciones G1000 adoptarán tecnologías y herramientas de nube híbrida y multicloud que podrían desbloquear este oligopolio.

Más sobre las predicciones de IDC aquí.

FORRESTER: LA TRANSFORMACIÓN SE VOLVERÁ PRAGMÁTICA

Forrester dice de 2019 que representa un año en el que las ambiciones estratégicas se traduci-

>> Continuación Así debe ser la agenda del CIO en 2019

Dice la tercera predicción que, en 2022, el 65% de las empresas encargará a los CIOs que transformen y modernicen las políticas de gobernanza para aprovechar las oportunidades y los nuevos riesgos que plantean las tecnologías de inteligencia artificial, machine learning, así como las cuestiones éticas y las relacionadas con la privacidad de datos.

El cuarto pronóstico es que, en los próximos cuatro años, el 75% de las estrategias digitales de éxito se llevará a cabo mediante una organización de TI transformada, esto es, con infraestructuras, aplicaciones y arquitecturas de datos modernizadas y racionalizadas.

La siguiente señala que, en solo dos años, para 2020, el 80% de los ejecutivos de TI será compensado basándose en indicadores de rendimiento de negocio y en métricas que miden la eficacia de TI para impulsar el desarrollo y el crecimiento del negocio.

En 2020, también apunta IDC que el 60% de los CIO optarán por una infraestructura de confianza digital que vaya más allá de la prevención de ciberataques y que permita a las organizaciones recuperarse de situaciones adversas, incidencias y efectos adversos.

En su séptima predicción, señala que el 75% de los CIO que no preparen a sus equipos de TI para facilitar la innovación, la disrupción y el escalado habrán fallado en sus funciones.

Además, hasta 2022, el talento formado en tecnologías emergentes no será suficiente y faltarán por cubrir al menos el 30% de las posiciones que se demanden a escala global. Por tanto, vislumbra IDC que las empresas tendrán que optar por estrategias diferenciadoras en desarrollo y retención del talento con estas habilidades.

La penúltima sostiene que, para 2021, el 65% de los CIO extenderá las prácticas de agile/DevOps en la empresa para conseguir la velocidad necesaria de innovación, ejecución y cambio. Y, la décima y última, es que el 70% de los directores de TI que no puedan gestionar que la gobernanza, la estrategia y las operaciones de TI se dividan en edge computing, tecnología operacional y TI, habrán fallado profesionalmente. Este pronóstico es para 2023.

EL CIO EN 2018, SEGÚN KPMG

SOPHOS

INTERCEPT X

VER EL FUTURO ES EL FUTURO DE LA CIBERSEGURIDAD.

- Protección Anti-Ransomware
- Protección Anti-Exploit
- Protección Predictiva Deep Learning
- Remediación y Limpieza Avanzados

Más información y pruebas gratuitas en:

www.sophos.com/es-es

rán en esfuerzos pragmáticos, ya que, en 2018, los líderes se pusieron como objetivo iniciativas a gran escala en materia de transformación digital y experiencia del cliente, pero se enfrentaron a la dura realidad de que estas estrategias son difíciles, costosas y desafían cómo dirigen sus negocios. La consultora dice también que los líderes empresariales tendrán que tomar duras decisiones sobre qué es o no verdaderamente estratégicos y cuál es la base para sus estrategias en 2020, mientras se preparan para una posible recesión económica.

Entre las predicciones de la consultora, señala que la experiencia del cliente sigue siendo dudosa; las marcas abandonarán iniciativas estratégicas de experiencia del cliente y recurrirán a métodos tradicionales para obtener ganancias a corto plazo. Asimismo, apunta que las iniciativas de transformación digital se abordarán desde un punto de vista más pragmático. Respecto a los CIO, señala que el 25% de ellos ampliará sus límites y recuperará sus competencias para crear modelos que traduzcan innovación liderada por tecnología para dar valor al cliente, pero el resto, se volverá un simple operador.

Las cifras de Gartner

Para 2023, Alibaba y Amazon habrán capturado el 40% del mercado del comercio minorista online global.

Asimismo, Forrester recoge que la Inteligencia Artificial sentará sus bases y que las empresas adoptarán más componentes para beneficiarse de la promesa de la IA. Además, la automatización de procesos robotizados (RPA) y la IA crearán trabajadores digitales para más del 40% de las empresas En este sentido, otra de sus predicciones asegura que los robots reinventarán la gestión de talento.

Respecto a blockchain, asegura que las cadenas de bloques permitirán a los publicistas ver dónde hay pérdidas y abuso de la publicidad, y cómo se gasta su dinero en la cadena de suministro de compra de medios de comunicación. Finalmente, avanza que el Internet de las cosas (IoT) se pondrá a trabajar y que despegará en el espacio B2B, mientras que en el B2C seguirá intentando entrar.

Más sobre las predicciones de Forrester en este informe. ■

MÁS INFORMACIÓN

- 8 predicciones tecnológicas para 2019 - IDC
- El gasto mundial en TI aumentará un 3,2% el próximo año, según Gartner
- Los retailers aumentan su inversión en nuevas capacidades digitales
- Agenda del CIO para 2019 según Gartner
- Agenda del CIO para 2019 según IDC
- Seis predicciones para la industria tecnológica en 2019 y más allá (Financial Times)
- El CIO en 2018, según KPMG
- La realidad digital de la empresa española en datos

Las cifras de IDC

Para 2022, más del 60% del PIB mundial estará digitalizado

Si te ha gustado este artículo, compártelo

itTRENDS

Las tendencias tecnológicas
que marcan el ritmo de la Transformación Digital, vistas por sus protagonistas

Son varias las tendencias TIC que impulsan a las empresas hacia la Economía Digital. Algunas están ya más avanzadas que otras en su despliegue, pero todas serán los mimbres que redefinan la economía, los negocios y la relación de las empresas con su entorno, sus clientes y sus trabajadores. Pero ¿cuáles son estas tendencias? Los principales jugadores del mercado nos dan su opinión.

ENTORNOS MULTI-CLOUD MÁS SEGUROS

Lo primero que quisimos saber es cuáles son estas tendencias que marcarán la evolución de las TIC en este 2019.

En este sentido, Juan Rodríguez, director general de F5 Networks, apunta "que 2019 será el año del multi-cloud. Cada vez más empresas moverán sus operaciones a entornos de nubes múltiples, asignando cargas de trabajo al modelo de nube que sea más adecuado en cada caso para alcanzar los objetivos de velocidad, agilidad y seguridad que hoy en día ne-

“2019 estará marcado por 5G, arquitecturas de Inteligencia Artificial distribuidas, blockchain, mini-clouds y la interconexión”

IGNACIO VELILLA, MANAGING DIRECTOR DE EQUINIX ESPAÑA

“EL TRÁFICO DE INTERCONEXIÓN CRECERÁ 10 VECES MÁS QUE EL TRÁFICO POR INTERNET” (IGNACIO VELILLA, EQUINIX)

cesita cualquier tipo de negocio para seguir siendo relevante para sus clientes. Como parte de este cambio, tecnologías como IA y Machine Learning serán fundamentales a la hora de impulsar niveles más altos de automatización y conseguir que desaparezcan las reticencias que aún puedan existir con respecto al multi-cloud. Para ello, una de las claves va a ser garantizar la seguridad de este entorno. En este sentido, la implementación de un ecosistema sólido que integre soluciones de seguridad y cloud ayudará a crear servicios de TI de extremo a extremo que proporcionen un mayor contexto, control y visibilidad sobre el panorama de amenazas actual, además de la confianza necesaria para eliminar al máximo la complejidad”.

Por otra parte, “durante el próximo año va a continuar el crecimiento exponencial de dispositivos conectados (IoT). En muchos casos, estos dispositivos carecen de una gestión remota eficaz, por lo que, con toda certeza, van a ser el origen de múltiples incidentes de seguridad. Nuestra división especializada en seguridad, F5 Labs, señala que los thingbots, construidos exclusivamente con dispositivos IoT ya se están convirtiendo en uno de los sistemas preferidos por los ciberdelincuentes”.

“Este 2019”, finaliza, “será también el año del inicio de la era Super-NetOps, es decir del nacimiento de una nueva generación de profesionales de TI capaz de terminar con los silos provocados por la desconexión que ha venido existiendo entre los equipos NetOps, SecOps y DevOps de las organizaciones actuales”.

ALINEAR LAS COMPAÑÍAS CON EL NEGOCIO DIGITAL

En opinión de Juan Parra, general manager, Iberia, DXC Technology, son seis las tendencias que impactarán el viaje hacia la Transformación Digital de las empresas en 2019. Tal y como nos explica, “innovación digital, aplicaciones de TI, o

Kaspersky for Business

KASPERSKY lab

938 ataques al minuto.
7 niveles de protección.
1 solución.

Proteja su empresa con cifrado de datos y sistemas de gestión más avanzados

Pruebe gratis Kaspersky Endpoint security for Business ADVANCED

Kaspersky® Endpoint Security for Business

Advanced

“EL COMPONENTE MÁS IMPORTANTE EN LA CIBERSEGURIDAD SON LAS PERSONAS” (RICARDO MATÉ, SOPHOS)

“En 2019 veremos que se seguirá incrementando el número de ataques de ransomware dirigido”

ALBERTO RUIZ, PRESALES ENGINEER, SPAIN AND PORTUGAL, SOPHOS

nuevas plataformas de IoT son algunos puntos que arrojan luz sobre las tendencias digitales que veremos en 2019. La transformación empresarial se está acelerando a medida que las compañías hacen grandes apuestas por su estrategia digital para conseguir mayor eficiencia operacional, introducirse en nuevos mercados, rediseñar las experiencias de usuario para sus clientes y lograr ahorros significativos que se puedan reinvertir para financiar el futuro digital de la compañía”.

Las tendencias que estiman que impactarán en el mercado desde DXC apuntan que “las empresas tomarán decisiones de ejecución más alineadas en apostar en el negocio digital de la compañía. Se verán nuevos modelos de negocio y tecnologías construidas desde lo digital. Una estrategia digital unificada entre el negocio y la TI es la única forma de disminuir las carencias técnicas que impiden que las empresas experimenten la innovación digital. Asimismo, las empresas adoptarán plataformas de nueva generación de IoT. A medida que las empresas van adaptándose al entorno digital, las pequeñas “cosas” se convierten en una fuerza impulsora para adoptar plataformas de nueva generación en 2019. También hay que atender a la innovación en la nube. La industria de TI continúa desarrollando la infraestructura de TI inteligente y generalizada que va más allá de la nube para incluir edge computing, plataformas IoT, inteligencia de máquinas, realidad aumentada/realidad virtual, blockchain... Las compañías desarrollarán formas completamente nuevas

“En la Infraestructura como servicio la tendencia será la gestión de redes desde la nube, incluso para las pymes”

Anselmo Trejo, marketing and communications manager de D-Link España y Portugal

“SEGURIDAD, MEJORA DEL RENDIMIENTO Y MOVILIDAD MARCARÁN EL FUTURO DE LA RED” (ANTONIO NAVARRO, D-LINK)

para aprovecharlo, como las aplicaciones descentralizadas (DApps)”.

La cuarta de estas tendencias indica que “las empresas entran en la era de la Tecnología de la Información. El aprovechamiento de la información se convertirá en una competencia central en 2019. Junto con esto, las compañías rediseñan sus experiencias de usuario en medio de medidas de protección de datos y privacidad más estrictas. Proteger los datos personales de los clientes obligará a las compañías a pensar en su estrategia digital teniendo en cuenta la GDPR establecida. Y, por último, las empresas comienzan a cerrar sus centros de datos. El centro de datos de las compañías se está volviendo menos relevante a medida que los datos y el procesamiento del negocio están en la nube. Por ello, para operar de manera más eficiente y obtener más valor de sus datos, las empresas están cambiando las cargas de trabajo de sus principales proveedores de nubes públicas, que tienen un ancho de banda masivo y centros de datos ubicados estratégicamente. Esta tendencia se desarrollará entre los tres a cinco próximos años, ya que la migración a la nube da paso a los reemplazos creados para la nube”.

NUEVAS Y MÁS PELIGROSAS AMENAZAS

En palabras de Alberto Ruiz, presales engineer for Spain and Portugal, Sophos, “desde el punto de

DETECTE MÁS AMENAZAS CON
ANTIVIRUS DE PRÓXIMA GENERACIÓN

Comparando Q1 2018 y Q1 2017, el cliente promedio de SonicWall enfrentó un aumento de...

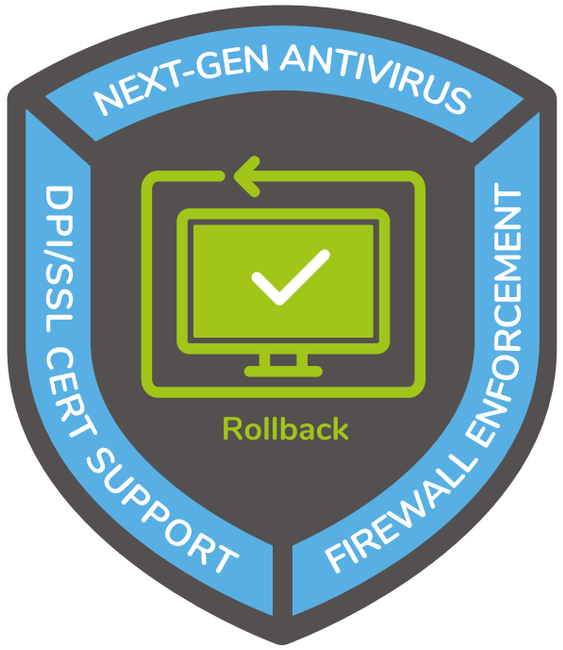
15% en ataques de phishing

400% en ataques encriptados

151% en ataques de malware

226% en ataques de ransomware

CON CAPTURE CLIENT PUEDE



- Controlar continuamente su sistema en busca de comportamiento malicioso
- Hacer rollback de un ataque de ransomware
- Usar el aprendizaje automático para detener los ataques antes de que sucedan
- Sinergizar con los firewalls de SonicWall para protección en capas
- Permitir la inspección del tráfico cifrado por el firewall sin advertencia del navegador

ADEMÁS, CAPTURE CLIENT ESTÁ CERTIFICADO PARA USO CORPORATIVO

Más información en: **SonicWall.com/Capture-Client**

SONICWALL®

spain@SonicWall.com
935 480 400

“2019 será el año de multi-cloud, y la clave va a ser garantizar la seguridad de este entorno”

JUAN RODRÍGUEZ,
DIRECTOR GENERAL DE F5 NETWORKS

vista de la ciberseguridad y tal y como señalamos en el último, Informe de Ciberamenazas 2019, realizado por Sophos, durante el próximo año 3 áreas destacarán entre las más vulnerables en este sentido: aumento de ataques de ransomware dirigido, aumento de amenazas de malware en IoT y aumento de app maliciosas”.

A lo largo de este año, continúa, “hemos detectado que los cibercriminales han variado su modus operandi y han renunciado a los grandes ataques masivos por ataques mucho más rentables. Durante el próximo año 2019 veremos cómo se seguirá incrementando el número de ataques de ransomware dirigido, mucho más sigilosos, más sofisticados e infinitamente más peligrosos en comparación con los grandes ataques masivos de ransomware. Asimismo, los dispositivos IoT, tanto en las empresas como en los hogares se están presentando como las nuevas puertas de entrada para los cibercriminales. Las insuficientes medidas de seguridad en estos dispositivos están facilitando que los criminales los utilicen como puntos de acceso a redes empresariales, por ejemplo”.

“CÓMO SECURIZAR LOS ENTORNOS MULTICLOUD SERÁ CLAVE EN 2019” (JUAN RODRÍGUEZ, F5 NETWORKS)

“Por último”, añade, “no podemos olvidarnos de los dispositivos móviles. Los ciberdelincuentes harán uso de apps teóricamente legítimas para redireccionar al usuario a sitios web de phishing e infectar los dispositivos. Durante el 2019 aumentarán este tipo de aplicaciones en tiendas oficiales como Google Play o Apple Store, ya que son capaces de sortear los controles de seguridad basados en el análisis del código fuente”.

EL CIBERCRIMEN NO DESCANSA

También apunta hacia un incremento de las amenazas Alfonso Ramírez, director general de Kaspersky Lab, que lo resumen en una frase: “el cibercrimen nunca duerme y 2019, al igual que el año que dejamos, seguirá siendo muy intenso en materia de ciberseguridad”.

Para este responsable, seis son los puntos a tener en cuenta en materia de seguridad de cara a 2019. “Aunque la industria de la ciberseguridad

"HAY QUE INCLUIR LAS CAPACIDADES DIGITALES EN LOS PROCESOS DE NEGOCIO" (JUAN PARRA, DXC TECHNOLOGY)

ha descubierto sistemáticamente operaciones muy sofisticadas patrocinadas por gobiernos", explica, "los actores de las amenazas pasarán a la clandestinidad y a un segundo plano para evitar la publicidad y la probabilidad de ser "descubiertos". Con recursos suficientes, podrán diversificar los conjuntos de herramientas y las prácticas, lo que dificultará enormemente la detección y la atribución. Los ataques a las cadenas de suministro serán más frecuentes. Este es uno de los vectores de ataque más preocupantes que se ha explotado con éxito en los últimos dos años. Asimismo, muchos cibercriminales contarán con un componente móvil en sus campañas con el fin de ampliar la lista de víctimas potenciales. Aunque no habrá un gran brote de malware dirigido a móviles, veremos una actividad continua y nuevas formas para que los atacantes tengan acceso a los dispositivos de las víctimas. Además, las redes de bots de Internet of Things (IoT) seguirán

"La transformación se está acelerando según las compañías apuestan por su estrategia digital"

Juan Parra, general manager, Iberia, DXC Technology

creciendo a un ritmo imparable, algo que hemos visto ya en los últimos años, y el Spear-phishing será aún más importante en un futuro próximo. Los datos obtenidos de diferentes ataques a gigantes de las redes sociales como Facebook e Instagram, y LinkedIn o Twitter, ya están disponibles en el mercado para que cualquiera los adquiera. Las recientes filtraciones de datos a gran escala de diferentes plataformas de medios sociales podrían ayudar a los atacantes a mejorar el éxito de este vector de infección. Por último, llegarán nuevos APT a escena, y los actores más avanzados aparentemente desaparecerán del radar".

MÁS INTELIGENCIA PARA EL NEGOCIO Y PARA LA PROTECCIÓN

Sergio Martínez, country manager de Sonicwall en Iberia, se muestra positivo al apuntar que en 2019 "continuará construyéndose la digitalización de todo, con más dispositivos inteligentes, recogiendo datos de todo tipo, algoritmos de IA analizándolos, y, por supuesto, un incremento exponencial de las violaciones de la privacidad y ataques a las empresas con muy diversos fines. Por tanto, se acelerará la carrera por el mundo conec-

D-Link®
FOR BUSINESS

SWITCHES SMART CON GESTIÓN AVANZADA L2 Y L3 STATIC ROUTING

GARANTÍA DE POR VIDA

D-Link DGS-1210

Smart Gigabit Managed Switches

Por fin la gestión de red Enterprise al alcance de la PYME

Interfaz CLI Compacto y Web Gui | PoE, PoE+ hasta 370W Power Budget | Dual image | LACP

Un Switch para cada necesidad
Amplia variedad de modelos con diferentes densidades de puertos Gigabit

Uplinks Fibra Óptica
Aseguran rendimiento y escalabilidad en despliegues de larga distancia

“En 2019 destacarán la hiperconectividad, ciberseguridad y la Inteligencia Artificial necesaria para gestionar todo esto”

Sergio Martínez, country manager de Sonicwall en Iberia

“LAS PROTECCIONES HAN DE SER INTELIGENTES, EVOLUTIVAS Y AUTOMÁTICAS” (LUIS FISAS, SONICWALL)

tado, y eso implica la necesidad de invertir mucho más en ciberseguridad. También vemos un crecimiento acelerado en la construcción de redes inalámbricas y de dotar de conectividad a todo. Así, hiperconectividad, ciberseguridad y la Inteligencia Artificial necesaria para gestionar todo esto”.

MÁS CAPACIDAD E IMPORTANCIA DE LA NUBE

En opinión de Anselmo Trejo, Marketing and Communications manager de D-Link España y Portugal, “en redes y comunicaciones, en la IaaS o Infraestructura como servicio, la tendencia será la gestión de redes desde la nube, incluso para las pymes. Con ello, tanto las redes de datos como el acceso a Internet, piezas claves en cualquier modelo de negocio y a cualquier escala empresarial, aumentarán su rendimiento, fiabilidad y seguridad. Y todo ello con un ahorro considerable en costes de despliegues y administración IT. En cuanto a tecnología hardware, en los entornos corporativos debe darse una profunda transición tecnológica tanto a las redes 10 Gigabit en cuanto a switching, mientras que en entornos WiFi hay que potenciar la migración al protocolo AC Wave 2 con MU-MIMO para aumentar el rendimiento en entornos de alta densidad de usuarios al habilitar el envío simultáneo a múltiples dispositivos,

“El cibercrimen nunca duerme y 2019 seguirá siendo muy intenso en materia de ciberseguridad”

Alfonso Ramírez,
director general de Kaspersky Lab

en lugar del secuencial estándar hasta ahora con WiFi N y AC Wave 1”.

MÚLTIPLES TENDENCIAS CONVERGENTES

Para Ignacio Velilla, managing director de Equinix España, nuestros veinte años de experiencia ayudando a empresas a aprovechar los beneficios de su plataforma global de interconexión, nos posiciona como una empresa con una visión especial a la hora de detectar tendencias. Y este 2019 estará marcado por el 5G, el boom de las arquitecturas de Inteligencia Artificial distribuidas, el desarrollo de múltiples redes de blockchain, la implementación de mini-clouds en diversas regiones para cumplir con los requisitos de protección de datos y la interconexión como aliado perfecto de las empresas en la creación de nuevos servicios digitales y en la migración al cloud y a entornos híbridos”.

RETOS PARA LAS EMPRESAS

El desarrollo de estas tendencias implicará una serie de retos para las empresas. En este sentido, Desde F5, Juan Rodríguez, “está claro que las aplicaciones son la base de cualquier tipo de negocio en el nuevo entorno digital, sin embargo, en muchas ocasiones, se produce un canto de sirena que reduce el concepto de transformación digital a “si desarrollas una aplicación, los clientes llegarán”. Es decir, se tiende a simplificar y a trasmi-

tir una imagen colorida de la realidad, con miles de clientes potenciales acudiendo alegremente a la llamada. Pero la realidad no es tan sencilla. El nuevo escenario requiere la adopción de unos procesos y una base digital sobre la que operar. Lo mismo está pasando con otro aspecto clave, como es el de la seguridad. Sorprendentemente, las organizaciones todavía destinan la mayor parte de sus presupuestos de seguridad a proteger todo excepto las identidades de los usuarios y las aplicaciones vitales para el negocio, siguiendo una inercia que fue válida en el pasado, pero que ya no lo es. Asimismo, la nube ya se ha convertido en la gran aliada de las organizaciones europeas a la hora de superar los retos del negocio en el nuevo escenario digital, sin embargo, estas mismas organizaciones muestran aún poca confianza en sí mismas si se trata de resistir un posible ataque en un entorno multi-cloud, debido a su falta de conocimientos y experiencia con todo lo relacionado con la seguridad de las aplicaciones desplegadas en nubes públicas".

Para Alberto Ruiz, de Sophos, "vemos dos retos claros: uno, aumentar y mejorar los niveles de control de los dispositivos que manejen, no solamente los endpoints, sino los dispositivos móviles y los servidores de su red. La mayoría de los movimientos laterales que realizan los cibercriminales en sus ataques, se producen en los endpoints y recurren a técnicas maliciosas para avanzar por el sistema y aumentar sus privilegios. Es importante contar con medidas de seguridad, que permite compartir la información entre los endpoints y los firewalls para poder detectar y automáticamente aislar un sistema que sea vulnerable a una posible infección, antes de que se extienda por todo el sistema. El segundo reto será conseguir concienciar y formar a los usuarios para conseguir minimizar los riesgos. El phishing es un gran negocio. Durante los últimos años, los ataques han registrado unos niveles de crecimiento récord, y un sólido programa de concienciación sobre la seguridad es un componente fundamental en cualquier estrategia de defensa exhaustiva".

¿Quieres saber más?

Para la elaboración de este reportaje hemos contado con las opiniones de jugadores principales del mercado TI en nuestro país. Puedes leer el contenido íntegro de estas entrevistas en este enlace

Anselmo Trejo, de D-Link, nos comenta que "el reto será una mayor inversión inicial en equipos y soluciones. Pero, aunque pueda parecer que el coste es mayor en todas las tecnologías comentadas (PoE, 10 GbE, administración de red desde la nube, gestión de red), incluso en el corto y medio plazo los beneficios en rendimiento, fiabilidad y ahorro de costes de instalación deben decantar la balanza a la hora de definir cada proyecto".

En Equinix estiman, y así nos lo comenta Ignacio Velilla, que "las compañías se enfrentarán en 2019 a retos que irán ligados a la inversión en infraestructuras móviles para la poder aprovechar las ventajas del 5G, la distribución de arquitecturas de Inteligencia Artificial para aproximarlas al Edge, el despliegue de nuevos puntos de interconexión que permitan el desarrollo de múltiples redes blockchain, la implementación de mini-clouds que cumplan con el GDPR y la adopción de soluciones de interconexión que permitan a las empresas beneficiarse de las ventajas de los entornos híbridos y multicloud".

Desde la perspectiva de Sonicwall, que no explica Sergio Martínez, "la hiperconectividad, el trabajo en cualquier lugar, el acceso a todas las aplicaciones corporativas, con cualquier dispositivo de empresa o particular, el crecimiento exponencial del malware, el cifrado (SSL) del tráfico en internet que convierte a los cortafuegos en convidados de piedra, la complejidad de los sistemas... O se construye una defensa en profundidad para prevenir, detectar y reacción en tiempo real de forma automatizada, o vamos camino de muchos problemas".

EFECTOS DE LA INNOVACIÓN

Y no queríamos terminar este repaso sin comentar los efectos que verán las empresas a raíz de estas tendencias y su implantación. Los resume Juan Rodríguez diciendo que "se convertirán en organizaciones más veloces, ágiles y seguras. Todo ello hará que sus propuestas sigan siendo relevantes para sus clientes".

Para Sergio Martínez, "la ciberseguridad es el suelo sobre el que se construye la confianza. Sin ella, no hay empresas, no hay negocio. Y hoy en día, un problema de seguridad compromete la confianza de los clientes en las organizaciones,

EQUINIX

Descubre más sobre nuestro servicio ECX Fabric™

DESCUBRE MÁS

poniéndolas en riesgo de desaparición. Esto no había ocurrido nunca, y ahora, es perfectamente posible. No podemos jugar con nuestra seguridad y nuestra reputación".

En palabras de Ignacio Velilla, "las nuevas tendencias tecnológicas, aunque en muchos casos conllevan una serie de retos en cuanto a inversión, cambios, y apuestas de futuro, buscan una optimización en los procesos de negocio de las empresas, la agilidad de sus servicios o su escalabilidad. El desarrollo de nuevas tecnologías cuenta con el potencial de incrementar, de manera espectacular, el rendimiento empresarial a largo plazo. En la actual era digital, donde cada vez más empresas compiten por los mismos nichos de negocio, la integración de estas tendencias y la conexión eficiente y en tiempo real con partners y clientes son dos imperativos que deben afrontar las organizaciones. Ahora, más que nunca, la inversión en tecnología es vital".

Y finaliza Anselmo Trejo indicando que, "en el caso del PoE, un significativo ahorro en costes de despliegue y mantenimiento de la red de datos, al prescindir de las tomas eléctricas para cada punto de acceso, cámaras o telefonía IP. Y en redes Switching 10 GbE y Wireless con AC Wave 2 será el rendimiento y la escalabilidad los mayores beneficios. Respecto a la gestión de red con servicios en la Nube, ahorrará costes en los departamentos de administración IT o en las empresas instaladoras o de servicios de soporte IT, al evitar los desplazamientos de técnicos in-situ en muchas de las incidencias, incluso también habrá un descenso significativo en horas de soporte técnico telefónico, ya que al gestionarse la red en remoto como si el técnico estuviera en la propia sede o empresa". ■

Doce meses, una tendencia TI

Como hemos visto, son múltiples y variadas las tendencias que convergen en este 2019, pero ¿cuál creen nuestros interlocutores que es la tendencia, la principal en este año nuevo?

Para Sergio Martínez, "sin duda la ciberseguridad. Necesitamos proteger nuestros datos, nuestra privacidad, nuestros negocios, en este mundo hiperconectado. La concienciación es necesaria pero ya no es suficiente. Hay que hacer los deberes y dotar de seguridad a aquello que, por diseño, no lo tiene".

Sigue esta línea Alfonso Ramírez, que indica que "en 2018 los actores de amenazas han llevado a nuevos paradigmas, produciéndose un cambio en el panorama actual pues los sofisticados actores de las amenazas buscan el silencio para sus ataques con el fin de aumentar las probabilidades de éxito. Este cambio hace muy improbable el hallazgo de nuevas operaciones a gran escala y sofisticadas, y definitivamente, llevará el desarrollo de la detección y atribución al siguiente nivel".

Más concreto se muestra Alberto Ruiz al apuntar que, "desde luego, el ransomware dirigido es la tendencia más peligrosa y a la que debemos prestar más atención durante el próximo año".

Por su parte, Juan Rodríguez estima que, "sin duda, el concepto multi-cloud. A la hora de abordar sus procesos de transformación, los responsables de TI buscan, fundamentalmente tres beneficios: La optimización de sus tecnologías, el incremento de la competitividad y una mayor eficacia de las operaciones comerciales de sus organizaciones".

Para Anselmo Trejo, "la gestión de red en la nube tanto en entornos híbridos como multi-nube debe estar en el horizonte de cualquier proyecto a medio o largo plazo".

Según Ignacio Velilla, "no podemos prever con seguridad qué tendencia será la protagonista del próximo 2019, pero podemos definir la interconexión como una tendencia en alza en los próximos años".

Por último, en opinión de Juan Parra, se seguirá avanzando en "una estrategia digital unificada entre el negocio y la TI, que es la única manera de disminuir las carencias técnicas que impiden que las empresas aprovechen todas las posibilidades que ofrece la innovación digital".

it TRENDS

El futuro será Multi-Cloud

VINCENT LAVERGNE,
vicepresidente regional de Ingeniería de Sistemas en F5 Networks

La capacidad para seguir el ritmo del cambio tecnológico y la evolución de la demanda de los consumidores empujará a muchas empresas a un punto de inflexión en los próximos cinco años. En este escenario, los nuevos entornos multi-cloud representan una gran oportunidad para innovar y mantenerse a la vanguardia de cada sector. Sin embargo, también son un desafío estratégico importante.

La tecnología multi-cloud no solo supone un cambio de juego, también es el principal camino hacia la transformación digital. La adopción de una estrategia basada en múltiples nubes servirá para sentar las bases de una innovación sin precedentes, al alinear la labor de los arquitectos cloud con la de los equipos DevOps, NetOps y SecOps, y promoviendo nuevos servicios que las infraestructuras tradicionales no son capaces de ofrecer.

Aunque aún hoy existen desafíos relacionados con el coste, las capacidades de los profesionales, las restricciones legales y las configuraciones de infraestructura heredadas, las perspectivas para la adopción de modelos multi-cloud son propicias. Las tecnologías como la inteligencia artificial y el aprendizaje automático serán fundamentales para impulsar niveles más altos de automatización, dejando atrás los obstáculos que impiden aprovechar todo el potencial de la computación en nube en todas sus formas y configuraciones.

AGILIDAD, EFICIENCIA Y AHORRO DE COSTES SIN PRECEDENTES

El progreso tecnológico continúa imparable y aprender a moverse en la nube ya se está convirtiendo en una obligación para todo tipo de organizaciones. La complejidad y el coste aparecen como los grandes impedimentos a la hora de optar por un entorno de múltiples nubes, sin embargo, esto está cambiando rápidamente. Las oportunidades de crecimiento y de excelencia en el servicio que ofrecen los entornos multi-cloud harán que en un plazo no mayor de cinco años las actuales preocupaciones sean historia. Eso sí, los beneficios, tanto económicos como en innovación, que traen consigo los procesos de transformación solo se producirán si se suceden con una fluidez y seguridad ininterrumpidas.

SUPERANDO LA BRECHA DEL TALENTO

Vivimos en un mundo de múltiples nubes, basado en las aplicaciones y preocupado por la seguridad. Todo ello hace que se incremente la demanda de profesionales capaces de dominar las tecnologías más avanzadas y de proporcionar valor estratégico a las organizaciones a través de ellas. Se ha hablado mucho últimamente sobre la escasez de talento, pero es hora de abandonar el mito de que este problema no tiene solución. Hay que impulsar el potencial caleidoscópico de los profesionales más jóvenes y lograr que las nuevas tendencias tecnológicas generen oportunidades de carrera atractivas y liberen a las fuerzas de trabajo existentes para destinarlas a labores más estratégicas y gratificantes.

ASEGURAR EL FUTURO Y GENERAR CONFIANZA

Los hackers han sido capaces de dejar de actuar como unos aficionados románticos para convertirse en representantes de una nueva actividad económica que puede llegar a tener más recursos que los destinados a la innovación empresarial.

Aunque existen desafíos relacionados con el coste, las capacidades de los profesionales, las restricciones legales y las configuraciones de infraestructura heredadas, las perspectivas para la adopción de modelos multi-cloud son propicias

El radio de acción de la ciberdelincuencia es también cada vez mayor. La capacidad de desarrollar e implementar rápidamente aplicaciones y servicios escalables en cualquier lugar y en cualquier plataforma es vital para satisfacer la demanda de los clientes y seguir siendo competitivos. Por ello, la implementación de un ecosistema sólido que integre soluciones de seguridad y cloud ayudará a crear servicios de TI de extremo a extremo que proporcionen un mayor contexto, control y visibilidad sobre el panorama de amenazas, además de la confianza necesaria para eliminar al máximo la complejidad.

CUMPLIR CON LA LEGISLACIÓN

El Reglamento General de Protección de Datos de la UE (GDPR) es la legislación más completa y de mayor alcance de su clase, sin embargo, no es suficiente. En un plazo de cinco años será necesario disponer de un estándar global para la protección de datos. Regular un mundo de múltiples nubes digitales sin fronteras es uno de los mayores desafíos al que se enfrentan los gobiernos de todo el mundo. Necesitamos encontrar fórmulas de colaboración que funcionen con agilidad. Mientras tanto, las empresas deben cumplir con la legislación existente, que se hace cada vez más compleja por la creciente influencia de la computación en la nube.

UNA ÚNICA NUBE NO ES SUFICIENTE

En un futuro próximo, las empresas y organismos públicos van a tener que afrontar grandes desafíos, que tienen que ver con nuevas amenazas de seguridad, escasez de talento o infraestructuras de TI deficientes, algo que puede frenar su acceso a la innovación. La automatización, la orquestación y la optimización son ahora el nuevo mantra y los entornos multi-cloud surgen como respuesta a todo ello. Tal es así, que en poco tiempo, contar con conocimientos suficientes sobre el funcionamiento de los entornos multi-cloud será un requisito para el cumplimiento con la legislación, la seguridad de la corporación, el servicio al cliente y la supervivencia en el mercado. Esta va a ser, sin duda, una de las claves que marcará el futuro. ■

it TRENDS

Enfoque para el cambio a digital en 2019

JUAN JUAN,
CTO, Sur de Europa,
DXC Technology

En el 2019 organizaciones y empresas emprenderán objetivos digitales ambiciosos (Digital business moonshots).

Si las empresas tradicionales desean crecer hacia el negocio digital necesariamente deberán apostar y comprometerse con una estrategia digital unificada, lejos de estrategias "bimodales" que no garantizan convergencia y generan competencia por los escasos recursos con talento para la necesaria transformación digital.

En el 2019 las empresas, las grandes en particular, tomaran mayor número de decisiones en la línea de una estrategia digital unificada. Podemos esperar una avalancha de innovación en negocio, por la tecnología aplicada a nuevos negocios y a existentes, arriesgando nuevos modelos acordes con la necesidad digital del negocio. Sin embargo, es posible que el grado de madurez de la infraestructura – necesaria para soportar determinadas innovaciones de negocio – no sea suficiente y por un mal resultado inicial pueda pensarse que la decisión sobre la iniciativa fue errónea.

Es relevante, además de identificar la innovación, asegurar el tiempo de puesta en producción coordinado con la madurez de los fundamentos tecnológicos necesarios en cada organización. Es importante la disciplina en la formulación y prueba de los nuevos modelos de negocio, así como la capacidad de contar con los factores cruciales en el éxito de todo negocio – el talento adecuado, el presupuesto, el liderazgo, la capacidad de ejecución, la cultura de cambio y la gestión constante de expectativas.

Estos factores, que han existido siempre y que a menudo se han minusvalorado en empresas tradicionales, ahora cobran una relevancia extrema y obligan a decisiones críticas:

- ¿Cuál es el margen de seguridad apropiado para tomar una decisión de riesgo sobre una iniciativa con nueva tecnología, considerando todas las variables anteriores junto el nivel de exposición al fracaso?
- ¿Es posible abordar una iniciativa con solvencia?

Con la manera de pensar convencional será muy difícil no quedar bloqueado ante las preguntas anteriores y, la proposición bimodal no aportará soluciones correctas ya que la decisión deberá contemplar el todo de la organización.

La valentía, que no la irresponsabilidad, de tomar decisiones contemplando el resultado a largo plazo, aun cuando pueda haber disrupciones en el negocio a corto plazo, marcará la diferencia de la verdadera transformación hacia el negocio digital de una empresa. Sobre todo, porque esa valentía se pone a prueba en cómo se comunica la decisión, cómo se gestiona el cambio en los afectados por la decisión y en cómo se flexibilizan de manera ágil las subsecuentes decisiones alineadas con la obtención del resultado ambicionado. La toma de la decisión y la elaboración de la estrategia con su dificultad es tal vez la parte más fácil del proceso.

Si las empresas tradicionales desean crecer hacia el negocio digital necesariamente deberán apostar y comprometerse con una estrategia digital unificada

El factor más relevante en una organización para gestionar el cambio es convertirse en una "organización que aprende" (learning organization). Una "learning organization" es una organización hábil en crear, adquirir y transferir conocimiento, en modificar su comportamiento en respuesta al conocimiento adquirido y sus implicaciones.

En la situación de la economía actual, con el alto grado de interdependencia por la abundancia informativa, que elimina las fronteras entre competidores, no queda alternativa, las empresas deben aprender lo que digital significa para la velocidad del cambio y a reformular, cuando no abandonar, viejos, aunque exitosos, modelos de negocio.

Siempre sin perder de vista las respuestas a tres preguntas sobre cualquier iniciativa de aprendizaje y cambio continuo: ¿Para qué cambiamos? ¿Cómo gestionaremos el cambio? ¿Cómo mediremos el resultado?

"Learning organizations" cultivan cinco actividades cuidadosamente: sistemática en la solución de problemas, experimentación de nuevos enfoques, incorporación de lo aprendido, emulación de las buenas prácticas y rápida y eficiente transmisión del conocimiento a toda la organización.

Transformarse a digital implica poner soluciones tecnológicas a las cinco actividades anteriores y forzar la adopción de esas soluciones.

- Desde cualquier dispositivo (IoT) y las plataformas necesarias para concentrar y actuar sobre los datos que esos dispositivos generan.
- Por la necesidad de procesar en local y en la nube los datos para la toma de decisiones descentralizada pero coordinada.
- Concediendo la garantía de privacidad y derechos necesaria en la transparencia al compartir conocimiento que, en su contexto, lleva la esencia intelectual y de identidad de los actores que lo producen.
- Permitiendo a las empresas prescindir progresivamente de la acumulación de información en centros de datos propios por las garantías necesarias y suficientes que proporcionan los sistemas de nube pública de proceso.
- Alcanzando el éxito por la Inteligencia Artificial en obtener claridad en el tratamiento de la información y la creación de conocimiento.

Estas soluciones y convertirse en una "learning organization" serán las tendencias principales para el 2019. ■

APLICACIONES ÁGILES Y EXPERIENCIAS DIGITALES

En la economía actual, el software rápidamente muestra su edad a la hora de realizar relaciones comerciales basadas en el compromiso, pues las aplicaciones heredadas son frágiles y monolíticas y no fácilmente proporcionan agilidad. Una plataforma de aplicaciones moderna, basada en el negocio, puede llevar a las organizaciones a generar nuevos servicios para los clientes, extraer datos de aplicaciones más antiguas y con ellos crear la base de un núcleo digital que soporte la continua transformación del negocio y dé resultados medibles.

it TRENDS

5 razones por las que necesita un EDR

RICARDO MATÉ,
country manager
Iberia Sophos

Las herramientas Endpoint Detection and Response (EDR) están diseñadas para complementar la seguridad de los endpoints con mayores capacidades de detección, investigación y respuesta. Sin embargo, el alboroto que rodea a las herramientas EDR puede dificultar la comprensión de cómo se pueden utilizar exactamente y por qué son necesarias. Para empeorar las cosas, las soluciones actuales pueden ser complicadas de utilizar, carecen de suficientes capacidades de protección y consumen muchos recursos. A continuación, algunos puntos a tener en cuenta para considerar una solución EDR realmente efectiva y sencilla:

INFORMACIÓN CON CONFIANZA SOBRE SU SITUACIÓN DE SEGURIDAD EN CUALQUIER MOMENTO

Los equipos de TI y seguridad a menudo están motivados por métricas de ataque y defensa, sin embargo, la pregunta más difícil de responder para la mayoría es "¿estamos seguros en este momento? Esto se debe a que, la mayor parte de las redes, tienen puntos ciegos considerables que hacen que los equipos de TI y seguridad tengan dificultades para ver lo que sucede en sus entornos. La falta de visibilidad es la razón principal por la que las organizaciones luchan por entender el alcance y el impacto de los ataques. Esto se manifiesta frecuentemente cuando ocurre un incidente y el equipo asume que están a salvo porque ese incidente fue detectado. Una solución EDR ha de proporcionar información adicional que determine si otras máquinas fueron impactadas. El hecho de poder ver las otras ubicaciones donde existen amenazas, permitirá al equipo de seguridad priorizar los incidentes para una investigación adicional y una posible reparación. Generar una visión clara de la postura de seguridad de una organización también proporciona la ventaja de poder informar sobre el estado de cumplimiento. Esta información ayudará a identificar las áreas que pueden ser vulnerables a los ataques. También permitirá a los administradores determinar si el alcance de un ataque ha impactado en las áreas donde se almacenan los datos confidenciales.

DETECTAR ATAQUES QUE HAN PASADO DESAPERCIBIDOS

Cuando se trata de ciberseguridad, incluso las herramientas más avanzadas pueden ser derrotadas con tiempo y recursos suficientes, lo que dificulta la comprensión real de cuándo se producen los ataques. Las organizaciones a menudo dependen únicamente de la prevención para mantenerse protegidas, y aunque la prevención es crítica, EDR ofrece otra capa de capacidades de detección para encontrar potencialmente incidentes que han pasado desapercibidos. Las organizaciones pueden utilizar EDR para detectar ataques buscando indicadores de compromiso (IOCs). Esta es una manera rápida y directa de cazar ataques que podrían haber sido pasados por alto. Las búsquedas de amenazas se inician con frecuencia después de una notificación de inteligencia de amenazas de terceros: por ejemplo, una agencia gubernamental (como US-CERT, CERT-UK o CCN-Cert) puede informar a una organización de que hay actividad sospechosa en su red. La notificación puede ir acompañada de una lista de CPIs, que puede utilizarse como punto de partida para determinar lo que está sucediendo. Una buena solución EDR proporcionará una lista de los principales eventos sospechosos, para que los analistas sepan exactamente qué deben investigar. Esto facilitará a los analistas el priorizar sus cargas de trabajo y centrarse en los eventos más importantes.

RESPONDER MÁS RÁPIDO A POTENCIALES INCIDENTES

Una vez que se detectan los incidentes, los equipos de TI y de seguridad generalmente se esfuerzan por remediarlos lo más rápido posible para reducir el riesgo de que los ataques se propaguen y para limitar cualquier daño potencial. Naturalmente, la pregunta más pertinente es cómo deshacerse de cada amenaza. En promedio, los equipos de seguridad y de TI dedican más de tres horas a tratar de remediar cada incidente. EDR puede acelerar esto significativamente.

El primer paso que un analista podría dar durante el proceso de respuesta a incidentes sería detener la propagación de un ataque. Aislar los endpoints bajo demanda es un paso clave para evitar que una amenaza se extienda por todo el entorno. Los analistas a menudo hacen esto antes de investigar, ganando tiempo mientras determinan el mejor curso de acción. El proceso de investigación puede ser lento y doloroso. Esto, por supuesto, supone que se lleva a cabo una investigación. La respuesta a los incidentes depende tradicionalmente en gran medida de personal altamente cualificado. La mayoría de las herramientas EDR también dependen de los analistas para saber qué preguntas hacer y cómo interpretar las respuestas. Nuestra solución EDR ideal hará que los equipos de seguridad de todos los niveles puedan responder rápidamente a los incidentes de seguridad gracias a las investigaciones guiadas que ofrezcan sugerencias sobre los siguientes pasos, representaciones de ataques visuales claras y experiencia integrada.

AÑADIR EXPERIENCIA SIN AÑADIR PERSONAL

Por un amplio margen, las organizaciones que buscan añadir capacidades de detección y respuesta de endpoints citan el "conocimiento del personal" como el principal impedimento para la adopción de una solución EDR. Esto no debería ser una gran sorpresa, ya que la brecha de talento para encontrar profesionales cualificados en ciberseguridad ha sido ampliamente discutida durante varios años. Esta barrera es especialmente pronunciada en las organizaciones más pequeñas.

Para combatir la falta de conocimiento del personal, la solución EDR elegida ha de aprovechar el aprendizaje automático para integrar una visión profunda de la seguridad. Así, las capacidades inteligentes de EDR ayudarían a llenar los vacíos causados por la falta de conocimiento del personal, reproduciendo las funciones de varios tipos de analistas, como son los analistas de seguridad, analistas de malware y los de inteligencia de amenazas.

ENTENDER CÓMO OCURRIÓ UN ATAQUE Y CÓMO EVITAR QUE VUELVA A OCURRIR

Los analistas de seguridad tienen pesadillas recurrentes donde han sufrido un ataque: un ejecutivo grita: "¿Cómo ha ocurrido esto? La identificación y eliminación de archivos maliciosos resuelve el problema inmediato, pero no aclara cómo llegó allí en primer lugar ni qué hizo el atacante antes de que se cerrara el ataque. Una herramienta EDR ha de poner en relieve todos los eventos que condujeron a una detección, lo que facilitará la comprensión de los archivos, procesos y claves de registro que el malware tocó para determinar el impacto de un ataque, proporcionando así una representación visual de toda la cadena de ataque, lo que garantiza un informe seguro sobre cómo comenzó el ataque y hacia dónde se dirigió el atacante. Y lo que es más importante, al comprender la causa raíz de un ataque, es mucho más probable que el equipo de TI evite que vuelva a ocurrir. ■

itTRENDS

¿Cómo reconciliar las Smart Cities y la Seguridad?

ALFONSO RAMÍREZ,
director general de
Kaspersky Lab Iberia

Las Smart Cities o ciudades inteligentes llevan asociadas el compromiso de un urbanismo más sostenible, más económico, gracias a la digitalización. Estas ciudades recopilan y procesan datos para desarrollar y prestar servicios y optimizar su gestión; pero al mismo tiempo dejan las ciudades expuestas a más vulnerabilidades. Por lo tanto, la ciberamenazas pueden afectar a su infraestructura urbana, hospitales, transporte...

En Kaspersky Lab estamos especialmente comprometidos con los futuros retos del sector y trabajamos para asegurar la confidencialidad y la integridad de los datos. La implicación de la industria e instituciones públicas nos parece esencial, siempre a través de una dinámica de apertura, contraria a cualquier forma de balcanización de Internet. La Smart City debe convertirse en una "ciudad segura": éste es el significado de la iniciativa Securing Smart Cities en la que Kaspersky participa de forma activa.

No obstante, la fragmentación creciente del espacio digital por barreras geopolíticas y regulatorias y una interrupción de los proyectos de cooperación internacional puede dejar a cada país solo frente a las ciberamenazas globales.

Desde Kaspersky Lab abogamos por una mayor colaboración e intercambio de información. Este entorno abierto fomenta el dinamismo y la competencia en el sector de la ciberseguridad, lo que se traduce en tecnologías más eficientes.

¿CÓMO USAR LA TRANSPARENCIA PARA RESTAURAR LA CONFIANZA ENTRE LOS ACTORES?

La transparencia con respecto a nuestros clientes y partners no es solo una prioridad, es un sine qua non. Ése es el origen real de la Iniciativa de Transparencia Global. El objetivo de este proyecto, lanzado en 2017, es auditar el código fuente de nuestras soluciones para fortalecer la resistencia de nuestra infraestructura de TI ante cualquier riesgo que pueda comprometer la confianza.

El pistoletazo de salida ha sido la apertura del primer Centro de Transparencia de Kaspersky Lab en Zurich que permite a los partners autorizados, empresas y organismos acceder a revisiones del código de la compañía, actualiza-

ciones de software y de las reglas de detección de amenazas, junto con otras actividades. A través del Centro de Transparencia, Kaspersky Lab proporciona a Gobiernos, empresas y partners información sobre sus productos y su seguridad, incluida documentación técnica importante, esencial para una evaluación externa en un entorno seguro.

A este desarrollo principal le seguirá la reubicación del procesamiento de datos de otras regiones y el traslado a Zúrich del ensamblaje de software. En una segunda fase transferiremos nuestra cadena de compilación de software: nuestros productos antivirus y bases de datos serán compilados y firmados digitalmente en Suiza antes de ser distribuidos a nuestros usuarios.

Mientras tanto, un tercero independiente auditará nuestro almacenamiento y procesamiento de datos, los diferentes accesos que nuestros empleados tienen a los datos y compilaciones de software, así como nuestro código fuente. Esperamos que otros actores de la industria de la ciberseguridad se unan al movimiento.

Kaspersky Lab participa en esta iniciativa global sin ánimo de lucro (Securing Smart Cities) para abordar problemas de ciberseguridad en ciudades inteligentes.

Esto implica la colaboración entre diferentes partners: empresas, autoridades públicas, medios de comunicación, asociaciones y usuarios. ■

CIFRAS CLAVE DE LAS SMART CITIES

Según un estudio de KPMG y Siemens, los ayuntamientos españoles pueden llegar a ahorrar hasta un

60%

de su gasto con la tecnología digital y, aunque queda camino por delante, el 70% de los municipios ya están a medio camino de ser 4.0.

1,4

Billones de dólares en 2020 moverá el mercado global de Smart Cities

152,9

millones de euros, es el presupuesto del Plan Nacional de Ciudades Inteligentes que se ha creado en España

ESTADO DE LA CIBERSEGURIDAD INDUSTRIAL EN 2018

A medida que aumenta la conectividad en el mundo exterior, la seguridad se convierte en un asunto de máxima importancia en los entornos industriales. ¿Qué quieren las empresas? ¿Cuáles son sus prioridades y qué retos enfrentan? ¿Qué factores internos y externos impactan en la ciberseguridad industrial? ¿Qué estrategias y medidas se emplean?

Este informe busca dar respuesta a todas estas preguntas y analiza el estado de la ciberseguridad industrial a nivel mundial.

it TRENDS

El Día D y la defensa automatizada

SERGIO MARTÍNEZ,
country manager de
Sonicwall en Iberia

El 5 de junio de 1944, a las 21:45, la BBC de Londres transmitió, en su emisión continental, el mensaje con el que avisaba a la resistencia francesa, de la invasión aliada del día siguiente, el día "D". El famoso poema de Paul Verlaine "...Los largos sollozos de los violines de otoño, hieren mi corazón con monótona languidez..." era la señal que esperaban.

Erwin Rommel, comandante alemán del Muro del Atlántico, sabía que debía actuar muy rápido, casi de forma automática, ante cualquier intento de invasión aliada. Su estrategia era destruir al enemigo antes incluso de que pisara la arena de la playa en la que desembarcara... Y sabemos que no tuvo éxito en sus propósitos: la defensa alemana no estaba desplegada como pretendía Rommel, y la operación aliada del Día "D" triunfó.

Algo así pasa con nuestras defensas cibernéticas. Creemos estar preparados, y subestimamos a nuestros atacantes tanto o más como sobrevaloramos nuestras capacidades defensivas. Como ya sabemos, la desconfianza y la paranoia son buenos aliados del CISO, pero también un buen despliegue de nuestras defensas, tal y como pretendía Rommel. La defensa en profundidad que propugnamos en Sonicwall, preparada para prevenir, detectar amenazas de tipo desconocido, y reaccionar de forma automática, es una infraestructura hoy muy necesaria para prepararnos para este malware virulento y sofisticado en el que viviremos de ahora en adelante, probablemente sin ningún tipo de tregua ni cuartel.

Esta defensa en capas debe incluir varios elementos fundamentales para poder detectar y responder de forma adecuada a los peligros que nos acechan. El primero de ellos es una plataforma integrada Cloud, como punto único de gestión de la seguridad de la empresa. Un "single pane of glass", algo que nos permita gestionar de forma centralizada la infraestructura de seguridad y con visibilidad de todo lo que sucede en ésta. A continuación, una inteligencia artificial central, que aprenda de las amenazas y tome las medidas correctas en cada caso. Y no sólo basada en patrones, sino también en conducta, para poder detectar,

categorizar y aprender nuevo malware de carácter desconocido. Y este análisis del posible malware, no sólo debe realizarse de los ficheros, en estructuras “sandbox”, sino también de las piezas de software que se ejecutan en memoria, para descubrir y bloquear malware como Meltdown, Spectre y ForeShadow antes de su ejecución.

Otra pieza fundamental de esta arquitectura es el firewall, con su capacidad de análisis y localización de amenazas embebidas en el tráfico cifrado (ya más del 70% en internet). Sin esta funcionalidad desplegada, nuestro potente cortafuegos deja de tener sentido y se transforma en un convidado de piedra, sin poder hacer nada ante todo lo que pasa ante sus ojos.

La protección del endpoint o puesto de trabajo es otro de los elementos clave, sobre todo en estos tiempos en los que dicho endpoint se encuentra muchas veces fuera de la protección de la red interna, a merced de todo tipo de phishing y malware combinados en ataques muy efectivos (ransomware es un buen ejemplo). Los antivirus clásicos basados en modelos conocidos han perdido efectividad, más de 60 millones de virus catalogados tienen la culpa, hay que pasar a un modelo basado en comportamiento, ligero y efectivo.

Finalmente, otras piezas necesarias son también el Web Application Firewall (WAF), orientado a proteger aplicaciones de negocio críticas (y “legacy”) abiertas al exterior, y los CASB (Cloud Access Security Broker), para la protección de los usuarios y la información de la empresa residente en la nube.

Toda esta arquitectura ayuda a construir una defensa en profundidad en capas, orientada a proteger a todo tipo de organizaciones, grandes, medianas y pequeñas, proporcionando la capacidad estratégica que buscaba Erwin Rommel en ese lejano 1944 de reacción de forma inmediata y automática a cualquier amenaza, antes de que el desembarco se consolide y se constituya en un verdadero quebradero de cabeza.

Y es que ya lo aventuraba Linus Torvalds hace varios años, de forma profética: “el tiempo de las soluciones sencillas a problemas sencillos pasó, en tecnología y seguridad…”. ■

itTRENDS

Wi-Fi AC Wave 2,
la opción más equilibrada para entornos de alta densidad de usuarios

ANTONIO NAVARRO,
country manager
D-Link Iberia

En muchos aspectos, Wave 2 se basa en el éxito de su predecesor, al tiempo que aporta beneficios adicionales para las redes empresariales, en particular para las empresas que transfieren grandes volúmenes de datos en escenarios de alta densidad de usuarios, tanto corporativos, como públicos.

Dicho esto, el aumento de rendimiento de Wave 2 parece menos significativo en comparación con los del siguiente salto generacional: 802.11ax (11AX o WiFi6). Se espera que el WiFi6 muestre una mejora de rendimiento de cinco a diez veces superior a la de Wave 1, y cuatro veces más que Wave 2, lo que plantea la siguiente pregunta: ¿vale la pena la actualización a Wave 2 o hay que esperar a la implantación del 11AX? En D-Link pensamos que es hora de invertir en Wave 2 y no esperar a 11AX, porque estimamos que aún quedan dos años para 11AX sea un estándar con costes asequibles en grandes despliegues de puntos de acceso y, sobre todo, por la lenta llegada de dispositivos cliente compatibles; ya vimos con el estándar WiFi AC, lanzado en 2011, que no fue hasta 2015 que los móviles, portátiles o Smart TV empezaban a integrar tarjetas cliente compatibles, y todavía hay muchos dispositivos que sólo integran tarjetas WiFi N.

El protocolo WiFi 802.11ac Wave 2 es una evolución de la versión anterior, 802.11ac Wave 1, que fue lanzado por primera vez en 2011 y supuso grandes mejoras con respecto a 802.11n tanto para empresas como para consumidores. La gestión de energía mejorada, la mayor capacidad y la menor latencia brindaron una red inalámbrica de mayor rendimiento e hicieron de AC Wave 1 un estándar muy valorado hoy en día, consiguiendo además democratizar el acceso a la banda de frecuencia de 5 GHz.

Sin embargo, 802.11ac Wave 2 es ya una realidad al ser una evolución de WiFi AC y ofrece, con respecto a Wave 1, mayor velocidad, eficiencia y seguridad en entornos corporativos o públicos con alta densidad de usuarios, principalmente gracias al soporte de MU-MIMO, lo que permite a estos nuevos

Pensamos que es hora de invertir en Wave 2 y no esperar a 11AX, porque estimamos que aún quedan dos años para que 11AX sea un estándar con costes asequibles en grandes despliegues de puntos de acceso y, sobre todo, por la lenta llegada de dispositivos cliente compatibles

Puntos de Acceso enviar y recibir datos desde y hacia múltiples dispositivos simultáneamente en lugar del estándar secuencial de Wave 1 (y anteriores protocolos), lo que se traduce en un aumento muy significativo de la eficiencia en entornos de alta densidad de usuarios. En términos más simples, un solo Punto de Acceso Wave 2 actúa de la misma manera que si tuviéramos múltiples puntos de acceso Wave 1.

Como tal, MU-MIMO mejora la experiencia de conectividad general al distribuir datos de manera más eficiente, especialmente en entornos de alta densidad de usuarios. El uso simultáneo de smartphones, tabletas y portátiles ya es una realidad desde hace tiempo tanto en el lugar de trabajo moderno como en entornos públicos, por lo que esta capacidad adicional es una ventaja muy reseñable y que marca diferencias respecto a tecnologías anteriores.

Wave 2 aporta además Beamforming, que mejora el alcance y calidad de la conexión enfocando la señal Wi-Fi hacia cada cliente, emitiendo con mayor intensidad en dirección a los dispositivos conectados, y Band Steering, que consiste en conectar a cada dispositivo cliente a la banda más adecuada (2.4/5GHz) para optimizar el tráfico de red.

Si a esto le añadimos retrocompatibilidad con estándares anteriores (b/g/n/ac wave1), podemos afirmar que Wave 2 ha llegado para quedarse y consolidarse como el estándar de facto para las redes WiFi presentes y futuras, y con especial énfasis en proyectos para entornos de alta densidad de usuarios. ■

itTRENDS

Un 2019 marcado por 5G, Inteligencia Artificial, Blockchain y la interconexión

IGNACIO VELILLA,
managing director de
Equinix España

El desarrollo de nuevas tecnologías cuenta con el potencial de incrementar, de manera espectacular, el rendimiento empresarial a largo plazo, pero este proceso de innovación no está exento de complejidad. Aunque las posibilidades ofrecidas por las tendencias tecnológicas pueden ser infinitas, debemos tener en cuenta que las empresas están experimentando una situación complicada a la hora de afrontar su propia evolución digital.

Cada día, las empresas descubren nuevas soluciones digitales que necesitan integrarse perfectamente en sus infraestructuras TI con el objetivo de optimizar procesos de negocio, la agilidad de los servicios y su escalabilidad. Además, hacen frente a un número de dispositivos conectados que crece exponencialmente y que genera una cantidad ingente de datos. Esta realidad amplía las amenazas contra sus organizaciones, obligando a reforzar la seguridad de su información y el cumplimiento de las nuevas políticas de protección de datos.

En Equinix, tras 20 años de experiencia con empresas líderes mundiales, contamos con una perspectiva privilegiada a la hora de identificar las principales tendencias tecnológicas mientras desarrollamos soluciones a los retos que acompañan a estas innovaciones. Ayudamos a casi 10.000 empresas de todo el mundo a aprovechar el poder de nuestros ecosistemas empresariales y de interconexión y, cada año, aprovechamos nuestra visión única para mostrar las tendencias tecnológicas que protagonizarán la evolución de los negocios digitales.

De cara a 2019, en Equinix, hemos identificado las siguientes tendencias:

❖ El **5G** será la tecnología clave para encarar con garantía un nuevo escenario dominado por el Internet de las Cosas y la Inteligencia Artificial. Para aprovechar las capacidades del 5G, prevemos un incremento en las inversiones relacionadas con la construcción de infraestructuras móviles de vanguardia y la renovación de las ya existentes, así como la optimización del rendimiento y de los costes a través de hardware de vanguardia.

❖ En 2019, también seremos testigos del boom de las **arquitecturas de IA distribuidas**, que sustituirán a las arquitecturas centralizadas de primera generación. Este nuevo modelo permite aprovechar óptimamente las fuentes de origen de los datos manejados por las empresas que se encuentran en el edge local. Gracias a esta tendencia, las organizacio-

Cada día las empresas descubren nuevas soluciones digitales que necesitan integrarse perfectamente en sus infraestructuras TI con el objetivo de optimizar procesos de negocio, la agilidad de los servicios y su escalabilidad

nes podrán aprovechar la innovación de la IA en múltiples nubes públicas sin quedar atrapados en una sola nube, descentralizando aún más la arquitectura de la IA.

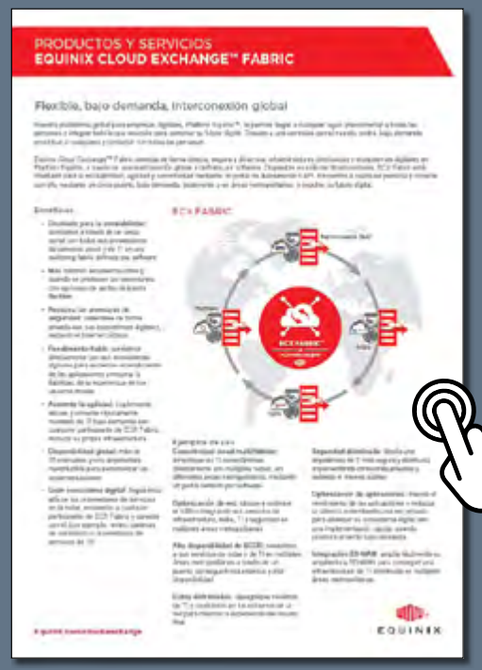
❖ Si hablamos sobre **blockchain**, la integración de esta tecnología en el día a día de las empresas requerirá del despliegue de puntos de interconexión para las organizaciones. En 2019, las empresas comenzarán a participar en múltiples redes de blockchain, formando una red de redes que permitirán interactuar con múltiples ecosistemas de negocio distintos. Por esta razón, el rendimiento de estas cadenas de bloques se convertirá en un requisito muy importante en el espacio empresarial para satisfacer aplicaciones de blockchain tan sensibles como la comunicación máquina a máquina (IoT) o la liquidación de divisas transfronteriza.

❖ Muchas empresas y proveedores SaaS están implementando **mini-clouds** en múltiples regiones para cumplir con los requisitos de cumplimiento y residencia de datos locales. Equinix también predice que, para prevenir brechas de datos, mantener su control y cumplir con las nuevas normativas como el GDPR, las compañías apostarán por nuevos modelos de gestión de información que se ajusten perfectamente al cifrado de datos. Además, las empresas usarán nuevas tecnologías de virtualización basadas en hardware para evitar que los proveedores de servicios supervisen los datos de sus clientes.

❖ La **interconexión** se mostrará como el aliado perfecto de las empresas en la creación de nuevos servicios digitales y en la migración de las cargas de trabajo existentes a plataformas de cloud de terceros, permitiendo a las organizaciones afrontar el siguiente nivel de desafíos asociados con los enfoques híbridos de cloud computing y multicloud. Los retos derivados de estos modelos dependen de capacidades como la seguridad, el análisis y el intercambio de datos, capacidades que pueden ser respaldadas por las nuevas soluciones de interconexión. Según el Índice Global de Interconexión, un estudio de mercado de Equinix, se prevé un crecimiento de ancho de banda de interconexión entre empresas y proveedores IT y cloud de un 98% anual hasta 2021. ■

it whitepapers ÍNDICE DE INTERCONEXIÓN GLOBAL

Este índice, publicado por Equinix, presenta nuevos datos sobre el enorme crecimiento del ancho de banda de la interconexión que está sosteniendo la interacción del negocio digital entre las empresas u organizaciones. El Índice prevé que el ancho de banda de la interconexión crezca hasta alcanzar más de 8.200 Terabits (Tbps) en 2021, un aumento drástico por encima de la previsión del año pasado. Descubre otros datos sorprendentes en el informe.



EQUINIX CLOUD EXCHANGE FABRIC

NETOPS CONOCE A DEVOPS. ESTADO DE LA AUTOMATIZACIÓN DE RED

RIESGOS Y RECOMPENSAS DE PROTEGER DATOS PERSONALES

SOPHOSLABS 2019 THREAT REPORT

DISEÑO Y PUESTA EN MARCHA DE UNA RED LAN CORPORATIVA DESDE CERO

MEJORES PRÁCTICAS PARA IMPLEMENTAR UNA PLATAFORMA ÁGIL

TODO LO QUE DEBERÍAS SABER SOBRE LAS AMENAZAS CIFRADAS

it whitepapers

it TRENDS