it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Julio/Agosto 2021 - nº 43

Las estrellas del ransomware

‘La ciberseguridad se está convirtiendo en una utility. O la tienes o no eres nadie’ (Consuelo Fernández, Grupo Tecnatom)

“El endpoint siempre ha sido muy importante, pero después de la pandemia, todavía más” (Miguel Carrero, WatchGuard Cytomic)

Qualys: Ya no solo somos un escáner de vulnerabilidades. El futuro está en el XDR

Commvault: Metallic ofrece la certeza absoluta de que la información está preservada

Revista IT Trends. Apps, datos y espacio de trabajo: siguiente ola de la transformación digital

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

it Digital Security

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

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

John McAfee, el inventor del antivirus que falleció en prisión

El pasado 23 de junio fallecía en una prisión de Barcelona John McAffee, a quien se le atribuye el haber inventado el antivirus y que vivió la vida intensamente.

Tras trabajar como programador en el Instituto de la NASA, en Univac como diseñador de software, en Xerox como arquitecto de sistema operativo y en Computer Sciences Corporation como consultor de software, fue en la década de 1980, cuando trabajaba en Lockheed cuando una copia del virus Brain le lleva a desarrollar un programa capaz de combatirlo.

Años más tarde renunciaría a su puesto en Lockheed y se centraría en McAfee Associates, que se convertiría en Network Associates, para, siete años después, llamarse McAfee y convertirse en una de las mayores compañías de ciberseguridad del mundo, con una fuerte presencia tanto en el mundo del consumo como en el empresarial. Dimitiría de la compañía en 1994 y terminaría mudándose a Belize, después de que los cien millones de su fortuna se redujeran a cuatro debido a una serie de malas inversiones.

Fue en Belize, y en 2012, donde tuvo uno de sus mayores conflictos con las autoridades después del asesinato a tiros de un vecino, Gregory Faull, un contratista de 52 años y nativo de Florida. La casa de McAfee en la isla de Ambergris Caye fue registrada y la policía dijo que querían interrogarlo como parte de una investigación por asesinato, pero McAfee solicitó asilo en Guatemala alegando que no estaba huyendo de las autoridades de Belice y haciendo uso de las redes sociales y las entrevistas públicas para salvar su reputación

Pasó un tiempo en Guatemala y luego se mudó a Montreal, Canadá, donde trabajó en un documental sobre su vida. Se postuló para presidente de Estados Unidos en 2016 y en 2017 se subió al tren de Bitcoin y criptomonedas para terminar siendo acusado de evasión fiscal. En octubre de 2020, McAfee fue detenido en España y encarcelado en una prisión de Barcelona, donde fallecería tras haberse confirmado su extradición a Estados Unidos. Tenía 75 años.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

itds

Sumario

En Portada

Las estrellas del Ransomware

Actualidad

Qualys:
Ya no solo somos un escáner de vulnerabilidades. El futuro está en el XDR

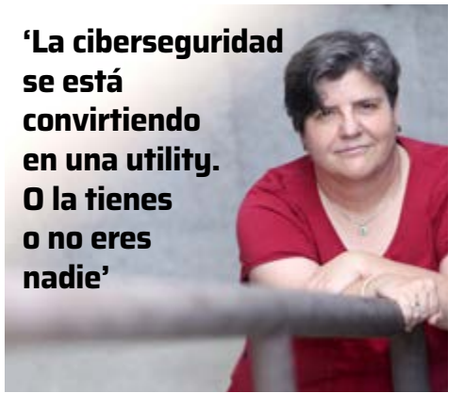
Commvault:
Metallic ofrece la certeza absoluta de que la información está preservada

Zscaler:
Hay que invertir en arquitecturas Zero Trust modernas

Revista IT Trends

Apps, datos y espacio de trabajo: siguiente ola de la transformación digital

Entrevistas



‘La ciberseguridad se está convirtiendo en una utility. O la tienes o no eres nadie’

Consuelo Fernández, Grupo Tecnatom

‘Las compañías necesitan seguridad ligada al desarrollo de nuevas aplicaciones’

Tony Hadzima, Palo Alto Networks

No solo IT

¿Preparados para la transformación digital?

Quitar al cliente de centro de la organización

Índice de anunciantes

‘El endpoint siempre ha sido muy importante, pero después de la pandemia, todavía más’

Miguel Carrero, WatchGuard Cytomic

‘Los clientes quieren sacar partido a todas sus inversiones de seguridad’

Ángel Ortiz, Cisco

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
RESPUESTA	**DETECCIÓN**

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Qualys: Ya no solo somos un escáner de vulnerabilidades. El futuro está en XDR

Experto durante años en el mercado de gestión de vulnerabilidades, hace unos cuantos que Qualys decidió salir de su zona de confort para adentrarse en el mundo de la seguridad endpoint, cloud e IoT con nuevas capacidades que giran en torno a la gestión de activos, y la protección, detección y prevención de amenazas que le permiten competir no sólo con sus rivales tradicionales (Tenable o Rapid7) sino con jóvenes actores como Crowdstrike, SentinelOne o Cybereason.

Qualys no solo está siendo capaz de llevar más soluciones al mercado y ampliar la penetración en sus clientes, sino posicionarse en una de las tendencias de mercado que más están calando en las empresas: XDR (Extended, Detection and Response).

Tres años después de fichar por Qualys, Sergio Pedroche se ha convertido, hace apenas unos meses, en el responsable de la compañía para España y Portugal, donde en los últimos meses también se ha conseguido alcanzar una entidad propia en EMEA; “antes no teníamos ese estatus sino que dependíamos de otros países, y el cambio es una apuesta clara de la compañía por España, por Portugal y por el potencial de crecimiento que tenemos. Actualmente somos 5 personas en el equipo y estamos pendiente de incorporar durante este año una persona más”, asegura Sergio Pedroche.

Trabajo, empatía y experiencia es lo que quiere aportar Sergio Pedroche a su nuevo cargo. No sólo acumula más de quince años de experiencia en el

"Simplificar en un momento en el que las empresas gestionan más de 50 herramientas de seguridad diferentes es vital"

Sergio pedroche, director general de Qualys Iberia

sector, sino tres y medio en Qualys, donde ha ocupado diferentes roles.

Sobre el producto que más se vende en España, menciona el VMDR, o Vulnerability Management, Detection, and Response, con el que se pretende "dar un servicio más global, más enfocado al riesgo" y que ayude a mejorar la presencia en el cliente "y poder crecer con ellos". Asegura Sergio Pedroche que el mercado demanda respuesta, poder remediar en entornos cloud, en entornos de contenedores, que cada vez se utilizan más y son muy cambiantes".

Asegurando que el típico servicio de gestión de vulnerabilidades tenía las horas contadas, el director general de Qualys en Iberia dice que VMDR es un cambio total que ha permitido a la compañía centrarse en el pilar básico: el inventario. No se puede proteger lo que no se sabe que existe y por tanto el primer paso es saber lo que se tiene y dónde se tiene, que no es otra cosa que la famosa visibilidad con la que los responsables de IT se pelean desde que la movilidad, el cloud y el as-a-service irrumpieron en el mercado.

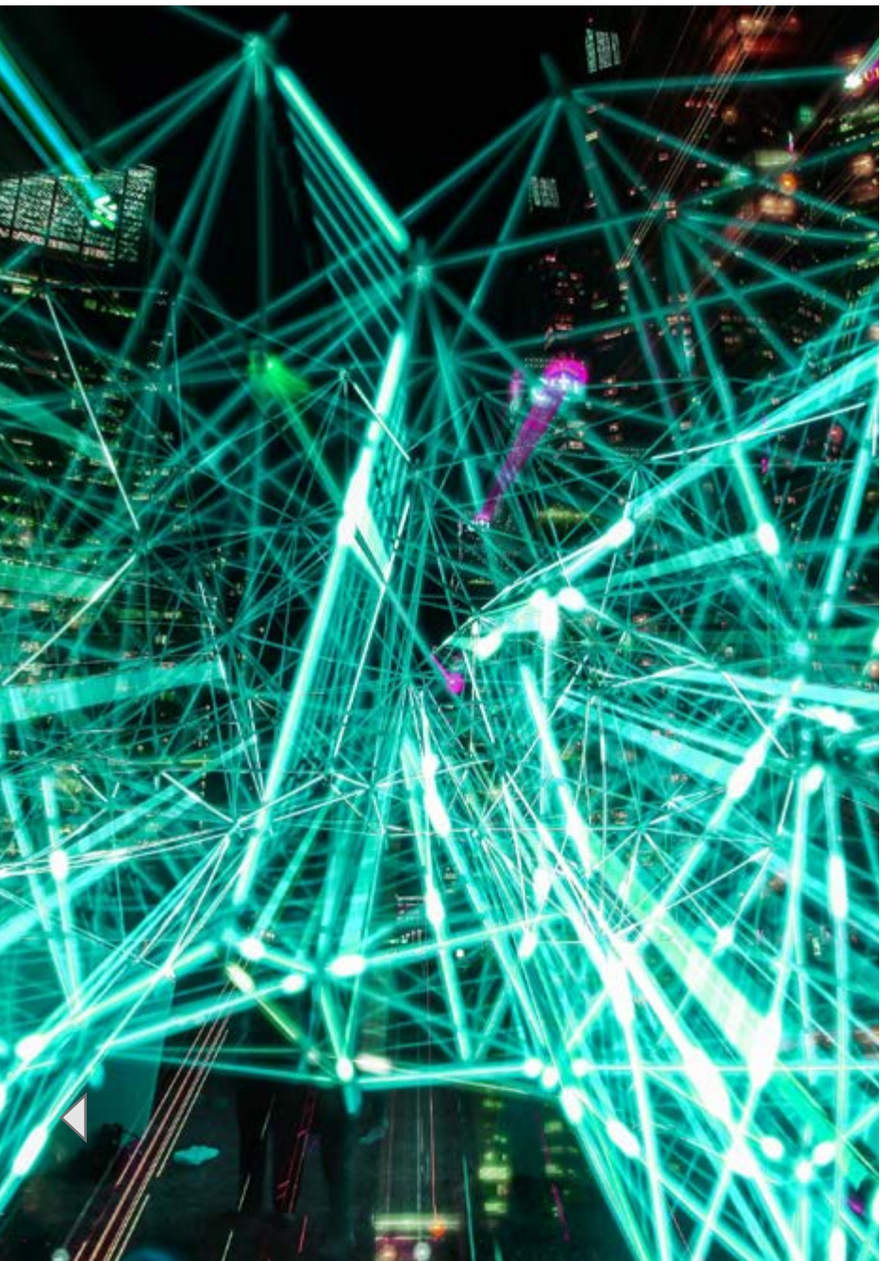
"El primer paso saber lo que tienes, un inventario, tener visibilidad en cualquier tipo de entorno", asegura Sergio Pedroche, añadiendo que además no sólo se necesitan ver las vulnerabilidades, sino también cuáles son las configuraciones incorrectas. Por otra parte, destaca que la clave de VMDR es la priorización; "es decir, dentro de todo lo malo que tengo, ¿qué remediación es más urgente para mi negocio?".

Avanzando hacia EDR

"Para empezar Qualys no es una herramienta, sino que es un servicio que nació en la cloud hace bastantes años y consolida todo en una única consola y con un mismo agente", responde Sergio Pedroche cuando le preguntamos por el diferencial de Qualys.

Simplificar en un momento en el que las empresas gestionan, según distintos estudios, más de 50

No solo se necesitan ver las vulnerabilidades, sino también cuáles son las configuraciones incorrectas



herramientas de seguridad diferentes, es vital. No sólo porque aumentar la complejidad significa aumentar el coste, sino porque el tiempo de más que requiere la gestión de tanta herramienta hace que la detección y respuesta a los ataques también lleve más tiempo, “y el enfoque de Qualys es intentar simplificar todo esto”.

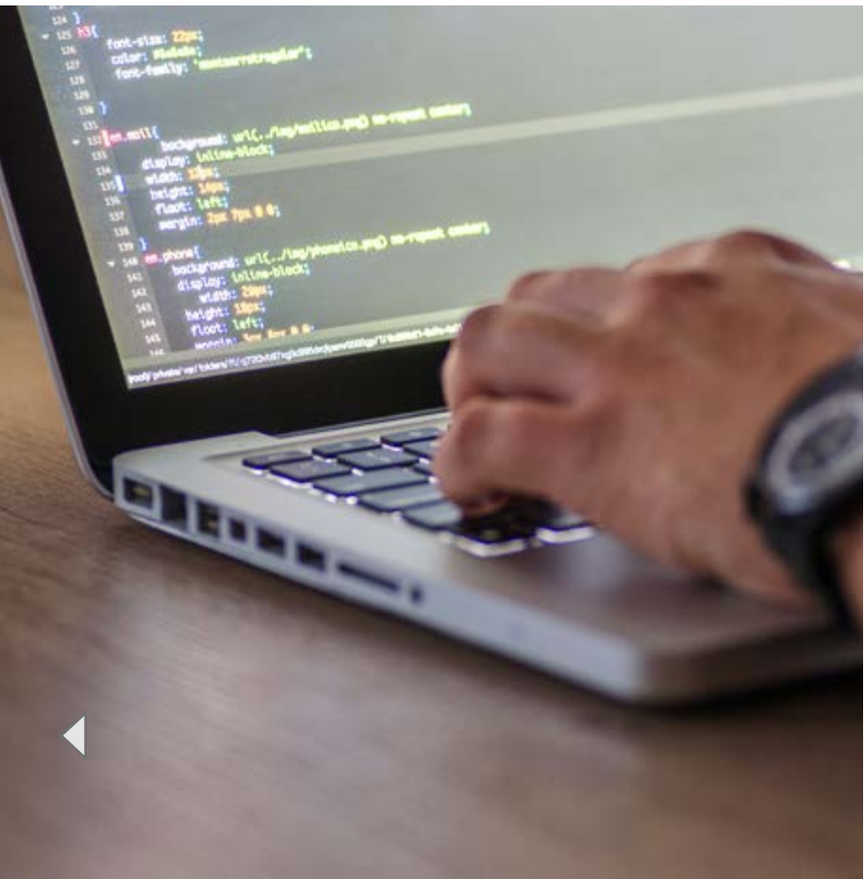
El razonamiento, explica el directivo de Qualys, es que si una empresa tiene debilidades y conoce las amenazas “le demos las herramientas para intentar corregirlas. Y si además de corregirlas podemos aprender, intentar prevenir, mejor. Esta es la estrategia de desarrollo de Qualys” que, como decíamos al principio, ha invertido en

Philippe Courtot, el CEO que llevó a Qualys al siguiente nivel

El pasado 5 de junio y con 76 años fallecía Philippe Courtot, CEO de Qualys durante 20 años.
Además de sus dos décadas al frente de Qualys, Courtot era conocido por fundar cc:Mail en 1988. Cuando a principios de la década de 1990, cc:Mail se convirtió en una de las plataformas líderes de correo electrónico para PC, Courtot se la vendió a Lotus.
CEO de Verity y de Signio, que ayudó a vender a VeriSign, Philippe Courtot fue uno de los inversores originales en Qualys, que lo nombró su CEO en 2001. Además de liderar la OPI de la empresa en 2012, bajo su supervisión, Qualys se convirtió en uno de los primeros proveedores de gestión de vulnerabilidades.
A principios de este año, Courtot tomó una baja médica y renunció como CEO poco después. En abril, Qualys nombró a Sumedh Thakar para asumir el cargo de presidente y director ejecutivo. Thakar, un veterano de Qualys, fue director de producto, responsable de la creación de Qualys Cloud Platform, dijo la compañía. Thakar lamentó el fallecimiento de Courtot en un comunicado en el que aseguró que siempre le estarían agradecidos por su liderazgo, su visión y gran pasión por ayudar a los clientes empresariales con soluciones prácticas para abordar los mayores desafíos relacionados con la seguridad.

Trabajo, empatía y experiencia es lo que quiere aportar Sergio Pedroche a su nuevo cargo

nuevas capacidades para impulsar su crecimiento. La mayoría de las capacidades de la nueva plataforma giran en torno a la gestión de activos, la protección, detección y prevención de amenazas para terminales y entornos de nube. Esto no solo incluye la mencionada plataforma VMDR sino otras capacidades de diferenciación de productos, incluido Multi-Vector EDR y la oferta de XDR (extended, detection and response) para correlacionar los conocimientos de varios sistemas. Multi-Vector EDR implementa un solo agente para la administración de inventario de activos, VMDR, cumplimiento, monitorización de integridad de archivos y administración de parches. El agente se puede implementar para monitorizar servidores, instancias en la nube y endpoint. Otras capacidades para diferenciar su plataforma incluyen SaaSDR, FIM (administración de integridad de archivos) y administración de parches.



Asegurando que “el inventario es la clave”, menciona también Sergio Pedroche la solución Qualys CSAM (CyberSecurity Asset Management) “que es la evolución de nuestro inventario” para dar respuesta a preguntas tan sencillas como qué máquinas están autorizadas, en qué equipos tengo software que no tengo actualizado o si tengo instalados todos los agentes de seguridad que debo tener en todas las máquinas. “Esas preguntas no se las suele hacer seguridad porque no tienen las herramientas para ello, pero si las tuvieran sería genial”, asegura el directivo.

Enlaces de interés...

- Qualys anuncia su solución de inventario de activos de ciberseguridad
- Qualys anuncia más capacidades a su solución de protección de los endpoints
- Sergio Pedroche dirigirá Qualys en España y Portugal

La hoja de ruta

Cuando le preguntamos por el futuro próximo, explica el responsable de Qualys en España que el IoT está en la hoja de ruta, y que la seguridad del IoT todavía está por explorar, que es un campo que, al igual que ocurre con los móviles, no se está securizando como se debe.

“El futuro está en el XDR”, asegura Sergio Pedroche añadiendo que para Qualys el XDR es la consolidación de “toda la información que se pueda, no sólo la nuestra, sino de terceros, y aplicar la inteligencia artificial y automatización”. La estrategia de Qualys pasa por dar respuesta a cuantas más cosas mejor, “pero el siguiente paso es dar la respuesta automáticamente”.

Compartir en RRSS

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com

Commvault:
Metallic ofrece la certeza absoluta de que la información está preservada

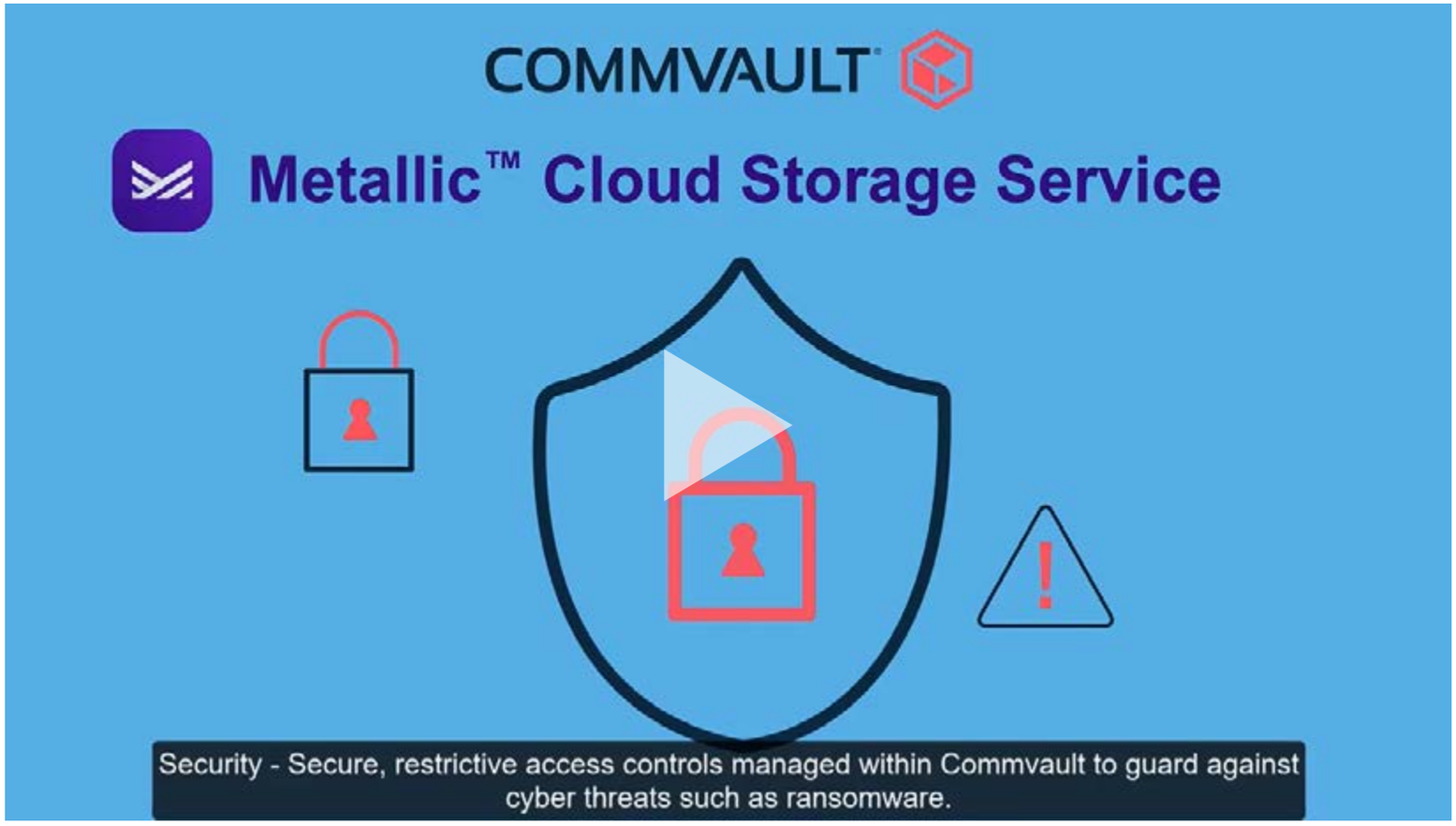
Fue hace algo menos de dos años, durante su evento anual Commvault GO 2019 cuando se anunciaba Metallic. La oferta de backup como servicio de la compañía, que en España está disponible desde primeros de año, lo hacía en un momento en que las organizaciones de TI mueven su infraestructura a modelos híbridos y multicloud, cuando Commvault transiciona hacia una compañía SaaS, cuando la mentalidad de la isla prevalece porque hay pocos estándares comunes que permitan que las aplicaciones y sus datos interactúen fácilmente entre plataformas.

No desvelamos ningún misterio al decir que los datos son el corazón de cualquier negocio y que han pasado de vivir protegidos por un perímetro de seguridad ya disuelto a estar distribuidos entre nubes y entornos. La protección de datos en forma de copia de seguridad / restauración es un servicio esencial para cualquier empresa, que ahora se enfrenta al reto de tener esos datos distribuidos.

Elisa Martínez es la directora de desarrollo de negocio de Metallic en España, Portugal e Italia desde primeros de año, tras pasar más de dos en Hitachi Vantara y acumular experiencia en el negocio de big data de Micro Focus. Asegura que Commvault es una empresa que ha estado por delante de las peticiones de los clientes y de las necesidades del mercado y que “Metallic supone un reto tecnológico

"Con Metallic tengo la certeza absoluta de que mi información está preservada, porque mis datos están aislados y son inmutables"

Elisa Martínez, directora de desarrollo de negocio de Metallic en España, Portugal e Italia



COMMVAULT Y METALLIC

CLICAR PARA VER EL VÍDEO

al llevar, gradualmente, todas las capacidades de la plataforma tradicional de Commvault a un sistema as-a-service". Explica que la importancia de Metallic va más allá de ser un producto Commvault desplegado en la nube y que ha supuesto "una apuesta y una revolución" dentro de la compañía "para adelantarnos a las necesidades que el mercado estaba empezando a apuntar".

La situación del mercado muestra que el 50% de las empresas que tienen brechas de seguridad no las han detectado, que las ciberamenazas son más y más sofisticadas y que la pandemia ha dado más sentido a la palabra ciberresiliencia, a la capacidad de recuperarse de forma rápida de un desastre, incluido un ciberataque. Y para ello "lo primero que se necesita es un plan de prevención, tener una monitorización constante de nuestro entorno para detectar anomalías, incluir tecnologías que tengan esas capacidades de machine learning, de inteligencia artificial para ayudarnos en esa prevención", dice

Elisa Martínez, añadiendo que, además, no hay que olvidarse de contar con un sistema de backup y recuperación que nos permite recuperarnos de forma rápida de los ciberataques o de errores internos de personas.

El cliente y el ransomware

"Metallic está dirigido a las empresas e instituciones que son conscientes de que el valor de su negocio está en su información, en sus datos y están interesados en mantener la continuidad de su actividad y de su negocio ante cualquier circunstancia adversa, sea externa o interna", asegura Elisa Martínez, añadiendo que no sólo las grandes empresas pueden ser clientes de Metallic y mencionando sectores como el sanitario, despachos de abogados o arquitectos, etc.

Respecto a si es una solución asequible para esas empresas no tan grandes, dice la responsable de Metallic en España, Portugal e Italia que "tenemos formas y fórmulas de calcular el TCO de una solución como la nuestra", disponible en suscripciones anuales y con una flexibilidad que, "donde tiene más sentido es las pequeñas empresas".

Hablemos del ransomware. Se ha convertido en una de las mayores amenazas de seguridad, en el arma preferida para los ciberdelincuentes, que mejoran sus creaciones no sólo haciéndolas más dirigidas, sino dando una vuelta de tuerca a la extorsión planteada: si no pagas, publico los datos, con lo que no sólo se violan legislaciones como

Metallic es la oferta de backup como servicio de Commvault

GDPR, sino que se hace pública información financiera o relativa a la innovación, lo cual tiene un impacto enorme y puede llevar a una empresa a su extinción.

Con una solución como Metallic "puedo tener mis copias totalmente aisladas, con capacidad de poder recuperar la información en el momento en el que estaba antes de producirse un ataque, ya sea, insisto, externo o un error humano. Con Metallic tengo la certeza absoluta de que mi información está preservada, porque mis copias son inmutables, porque están aisladas y porque sé en el momento exacto en el que se ha producido el ataque de Ransomware y voy a poder ir a un momento anterior a ese ataque para recuperarme".

¿El imparable crecimiento y éxito del ransomware nos tienta a volver a la cinta? Responde Elisa Martínez con otra pregunta: ¿deberíamos volver a la tracción animal porque hay accidentes de coches". Obviamente la respuesta es no, la respuesta al ransomware pasa por "proveernos de más seguridad, tener planes de prevención, que la ciberresiliencia

"Somos la única compañía que tenemos capacidad de hacer conversiones entre prácticamente todas las nubes que hay en el mercado"

Elisa Martínez, directora de desarrollo de negocio de Metallic en España, Portugal e Italia

esté en nuestro día a día, e identificar al partner tecnológico que simplifique nuestro día a día".
Apunta por otra parte que si realmente la idea que extraemos de la de las cintas es el aislamiento, "las técnicas de air-gapping de Metallic y Commvault es lo que garantizan: copias totalmente aisladas e inmutables".

El valor de Metallic

Metallic es Commvault desplegado en la plataforma Azure, "es tecnología Commvault con más de 25 años de experiencia en el mercado de backup. No somos una empresa de nicho, ni se ha realizado una compra para dar respuesta a las necesidades as-a-service", afirma Elisa Martínez cuando le preguntamos por el valor de la propuesta de Metallic. La descripción le lleva a asegurar: "No tenemos competidores en el mercado".

La propuesta de la compañía gestiona cargas de Office 365, Salesforce, bases de datos de SAP HANA, Oracle, máquinas virtuales, Dynamics 365… "cada vez añadimos más cargas al portfolio y el

Enlaces de interés...

- Commvault presenta Metallic, su propia plataforma SaaS de protección de datos
- Metallic Salesforce Backup
- La gestión de los datos está en el corazón de la seguridad en la nube
- Las empresas priorizarán la protección las cargas de trabajo en la nube en 2021

Metallic es Commvault desplegado en plataforma Azure

espíritu de Metallic es ir añadiendo cada vez más cargas al servicio". Para Elisa Martínez, la capacidad de simplicidad y automatización de Metallic son "una demostración de la solvencia" de la propuesta.

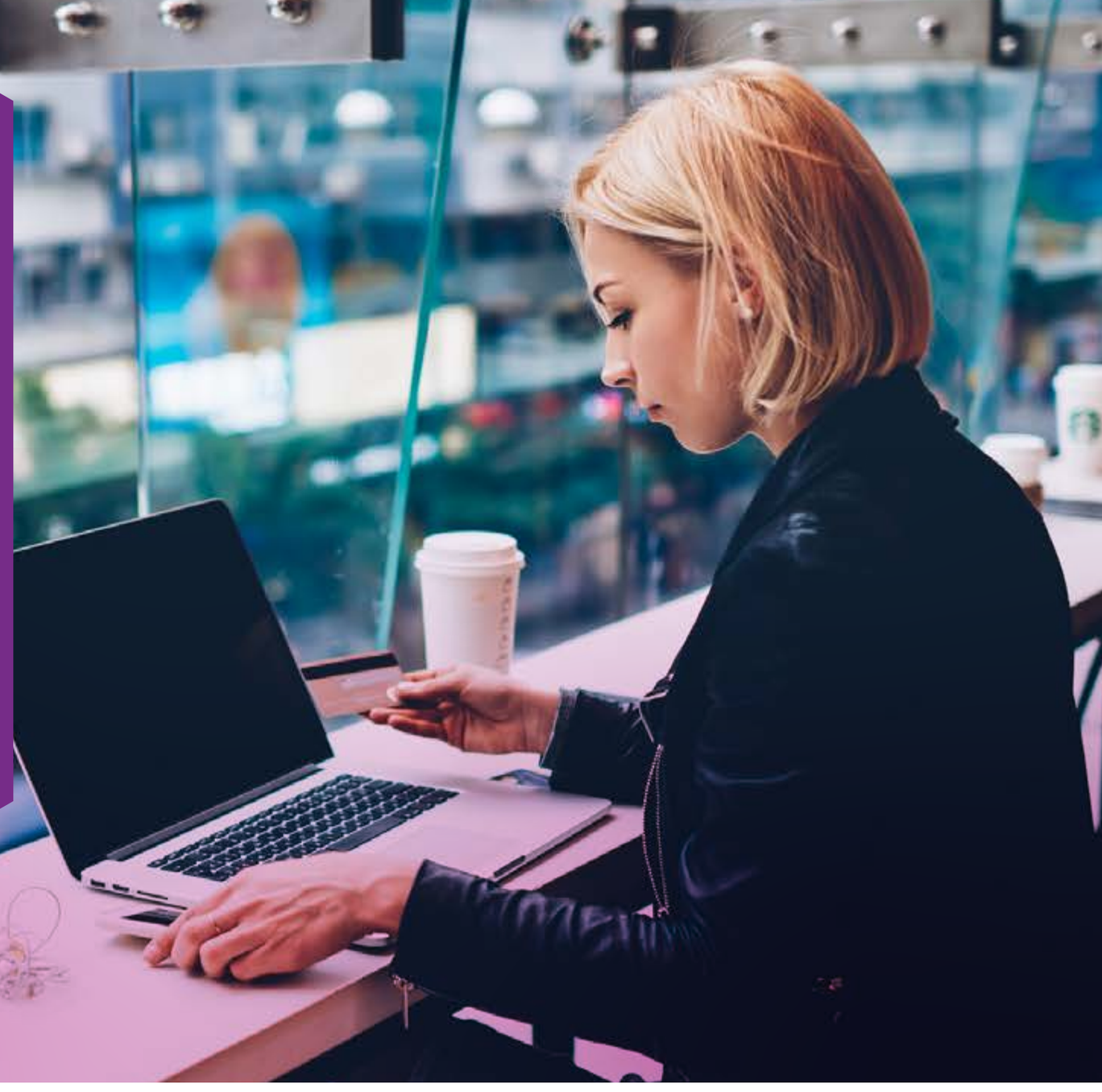
El mundo híbrido y multicloud en el que nos movemos permite a las empresas elegir libremente dónde colocan sus cargas de trabajo en función de los requisitos de cumplimientos de auditorías, de política o de seguridad. Esto, explica la directiva, genera arquitecturas independientes que llevan a la necesidad de tener productos y sistemas de software diversos con proveedores diversos. El uso de contenedores y de la APIs es una de las maneras de afrontar esta complejidad en un despliegue multicloud, "y en este sentido Metallic da cobertura a Kubernetes y todas las APIs que puedan ser necesarias dentro de una empresa".

Pero lo más importante, "es que con Metallic garantizamos la capacidad de no tener dependencias de terceros. Somos la única compañía que tenemos capacidad de hacer conversiones entre prácticamente todas las nubes que hay en el mercado. Eso quiere decir que, por ejemplo, podemos hacer llevar una copia de una máquina virtual de Azure a Amazon o a Google sencillamente con un proceso de backup y restore, sin ninguna herramienta externa y sin necesidad de ninguna tecnología de terceros".

Finaliza Elisa Martínez diciendo que se están cumpliendo todas las expectativas, "e incluso un poco más" que la compañía tenía para Metallic, "que ha sido muy bien recibido por nuestros partners, que lo ven como una gran oportunidad porque pueden aportar mucho más valor". it

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN



ENTRUST

Zscaler: Hay que invertir en arquitecturas Zero Trust modernas

Hace unas semanas se celebraba el evento Zenith Live 2021, el cuarto evento anual de Zscaler que este año, también en formato virtual, llevaba por título Full Cloud Ahead y que se ha convertido, según la compañía "en el destino de los profesionales de TI para aprender e intercambiar ideas sobre el futuro de la seguridad, las redes y el cloud".

Ya que todas las amenazas llegan a través de Internet, si el tráfico se redirige y analiza en Zscaler Trust Exchange, incluido el tráfico cifrado, se eliminan las amenazas

Lo decía Jay Chaudhry, CEO, presidente y fundador de Zscaler, encargado de inaugurar el evento hablando del enfoque único en la nube de Zscaler para la ciberseguridad, que, según él, ofrece un mejor rendimiento, visibilidad, y prevención y gestión de amenazas. La adopción masiva de la digitalización durante la pandemia aumentó una superficie que los ciberdelincuentes aprovecharon para aumentar sus ataques, aseguraba Jay Chaudhry, mencionando no sólo el de SolarWinds –que se estima que ha afectado a 18.000 empresas de todo el mundo, sino el de Microsoft Exchange, el de Colonial Pipeline, UBS… Los ciberdelincuentes "se están moviendo más rápido que nunca" decía el directivo, añadiendo que "si seguimos gastando la mayor parte de nuestros presupuestos de seguridad en defensas perimetrales, como los firewalls, seguiremos siendo vulnerables a este tipo de ataques".

Aboga el CEO de Zscaler por optimizar las inversiones de seguridad "en una arquitectura Zero Trust moderna capaz de conectar de forma segura al usuario adecuado con la aplicación adecuada, independientemente de la ubicación", un modelo que permite una adopción del cloud sin fisuras y que la compañía impulsa con su Zscaler Trust Exchange. La propuesta busca ofrecer confianza cero "a través de una nube especialmente diseñada que utiliza el contexto para hacer cumplir las políticas", y se basa en tres principios: Zero Trust Network Access, que busca no conectar a los usuarios con las redes, sino con las aplicaciones; Zero Attack Surface, que busca hacer que las aplicaciones sean invisibles –lo que no se puede ver, no se puede atacar; y Zero Passthrough Connections, una arquitectura proxy que mejora la seguridad y la protección de los datos.

Los beneficios de la arquitectura Zscaler Trust Exchange es garantizar que el cloud es un lugar seguro para hacer negocios y acelerar la transformación digital

"Los beneficios de la arquitectura Zscaler Trust Exchange es garantizar que el cloud es un lugar seguro para hacer negocios y acelerar la transformación digital", aseguraba Chaudhry para añadir después que las soluciones de la compañía ayudaban a los clientes en tres áreas clave: la modernización del puesto de trabajo, la transformación de la seguridad y la transformación de la red.

Explicaba el directivo que Zscaler habilita el trabajo seguro desde cualquier lugar mediante un agente instalado en el endpoint que hace que el tráfico vaya a través de Zero Trust Exchange aplicando las mismas políticas y protecciones sin importar dónde está el usuario, y ofreciendo una gran experiencia para todos los usuarios y todas las aplicaciones, "ayudando a identificar y resolver de forma proactiva problemas de rendimiento", porque, aseguraba el directivo, con un acceso directo a las aplicaciones, a veces puede haber algún problema con el portátil, la red WiFi local, la latencia… y los clientes de la compañía resuelven el problema con Zscaler ZDX.

Seguía el CEO de Zscaler adelante con su discurso asegurando que también ayudan a los clientes en lo que a la transformación de la seguridad se refiere "para reducir los riesgos del negocio" protegiéndolo no solo contra las ciberamenazas sino contra la pérdida de datos. Explicaba que ya que todas las amenazas llegan a través de Internet, si el tráfico se redirige y analiza en Zscaler Trust Exchange, incluido el tráfico cifrado, se eliminan las amenazas. Además, eliminar los movimientos laterales, utilizados en muchas cadenas de ataques, pasa por hacer una segmentación de cargas de trabajo, una capacidad que se ha mejorado gracias a la compra de SmokeScreen.

También busca Zscaler impedir la pérdida de datos y financiera con una solución de DLP que detecta y bloquea cualquier intento de robar los datos; un

"Si seguimos gastando la mayor parte de nuestros presupuestos de seguridad en defensas perimetrales, como los firewalls, seguiremos siendo vulnerables a los ciberataques"

Jay Chaudhry, CEO, Zscaler

servicio CASB que protege los datos de las aplicaciones SaaS; y una solución de CSPM (Cloud Security Posture Management) que protege los datos en la nube pública.

Las mejoras llegan en torno a lo que Gartner denomina CIEM, o Cloud Infraestructure Entitlements Management. Para mejorar la plataforma de la compañía en esta área se ha comprado Trustdome, que gestiona las reglas y permisos para que los usuarios sólo accedan a la carga de trabajo correcta; "integrando la oferta CSPM y CIEM ofrecemos a nuestros clientes una mejor postura de seguridad y remediación de seguridad de la carga de trabajo", aseguraba el directivo.

Por último se adentraba Jay Chaudhry en el tercer aspecto en el que la compañía está ayudando a los clientes, que no es otro que la transformación de la red para la adopción hacia un mundo cloud. Mencionaba el directivo el uso de la plataforma Zscaler Trust Exchange para la conectividad en la nube, como el elemento capaz de conectar de forma segura las cargas de trabajo entre múltiples nubes y centros de datos y anunciaba un servicio de comunicación de cargas de trabajo a cualquier nube "que elimina la complejidad de las redes y dispositivos heredados, incluidos los appliances virtuales, firewalls, routers y gateways".

Terminaba asegurando el directivo que la compañía trabaja de cerca con un amplio ecosistema de partners y aliados "para realizar una integración y validación basada en API para garantizar implementaciones más simples". it

Enlaces de interés...

- 'En la práctica, la microsegmentación permite frustrar prácticamente cualquier cadena de ataque' (Alberto Cita, Zscaler) - 08 JUN 2021
- Zscaler refuerza sus capacidades de defensa activa con la compra de Smokescreen
- Zscaler compra Trustdome para un mayor control de los accesos al cloud

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

‘La ciberseguridad se está convirtiendo en una utility. O la tienes o no eres nadie’

(Consuelo Fernández, Grupo Tecnatom)

Con más de 30 años de experiencia en el sector, Consuelo Fernández es la CISO del Grupo Tecnatom. Dice que hace unos años valía con tener un firewall, pero que ahora la seguridad perimetral es lo que menos importa; que saber escoger la mejor solución de ciberseguridad pasa por tener muy claros cuáles son los beneficios que se quieren conseguir; que un buen CISO tiene que hablar un lenguaje que se entienda; que las herramientas en torno a la detección temprana de incidentes y basadas en IA serán imprescindibles, y que por pedir, pediría un sistema de detección de incidentes que no diera falsos positivos.

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

Tecnatom es una empresa de ingeniería que presta sus servicios en el sector nuclear desde su creación en el año 1957 y en la última década ha diversificado sus servicios y productos en el mercado internacional y en otros sectores industriales como el aeronáutico, ferroviario, petroquímico, etc. Suministra servicios y productos con altos contenidos tecnológicos los cuales mejora continuamente para adaptarse a las necesidades y requisitos de los diversos clientes y mercados. La seguridad de la información del Grupo Tecnatom es responsabilidad de Consuelo Fernández, su CISO, con quien hemos tenido la oportunidad de hablar.

Cuando le preguntamos cuáles cree que son las grandes cualidades que tiene que tener un CISO empieza diciendo que siempre se ha pensado que un buen responsable de ciberseguridad tiene que tener un perfil técnico, pero que en realidad eso no es verdad; “ahora mismo el CISO tiene que ser un convencedor en toda la organización, tiene que hablar un lenguaje que se entienda, saber comunicar cuáles son los auténticos riesgos y entender el negocio para saber cuáles son las limitaciones que puede haber, además de buscar un equilibrio entre la seguridad y el trabajo de todos los empleados”.

Al hablar de la evolución de la figura del CISO dice Consuelo Fernández que la legislación le está dando un puesto que antes, considerados unos frikis que estaban todo el día hackeando cosas, no

"Hace unos años valía con tener un firewall, y ahora la seguridad perimetral es lo que menos importa"

tenían. Al margen de que la nueva legislación sobre ciberseguridad en servicios digitales e infraestructuras críticas ha dado más protagonismo al CISO, "yo creo que realmente la evolución del CISO ha venido en consonancia con la evolución de los ciberdelincuentes". Añade que las empresas han debido evolucionar porque los ciberdelincuentes "son cada vez más inteligentes y van siempre por delante, lo que te obliga a cambiar constantemente tus estrategias de seguridad. Hace unos años valía con tener un firewall, y ahora la seguridad perimetral es lo que menos importa".

Sobre si el peso del CISO seguirá aumentando dentro de las compañías, dice Consuelo Fernández que dependerá del tipo de empresa. La CISO de Tecnatom depende organizativamente del CIO y asegura que "no hace falta tener un puesto de relevancia para asegurar que la seguridad se realiza dentro de la empresa realmente". Añade además que "te tienes que ganar que la gente te haga caso, no porque tengas un cargo, sino porque lo que estás haciendo has sido capaz de explicarlo bien". Dice también Consuelo Fernández que un CISO va a ser muy necesario siempre, sobre todo desde el punto de vista de "tener a alguien que lleve la gestión de los riesgos de ciberseguridad que hay".

La empresa española avanza lento a la hora de considerar la seguridad como una prioridad. Falta un impulso, dice Consuelo Fernández, y ese impulso vendrá por la obligación, una obligación que comenzó el año pasado con la pandemia, que no sólo ha impuesto el teletrabajo, sino que ha incrementado el perímetro de seguridad. El número de ataques ha crecido "y deberíamos ir un poco más deprisa".

Mercado

El de la seguridad es uno de los mercados más fragmentados. El número de empresas se cuentan por decenas por cada tecnología, sumando miles, y si bien el proceso de consolidación se ha acelerado en los últimos años, hay un boom en cuando a nacimiento de empresas con bellos ideales y tecnologías avanzadas. La evolución ha hecho, además, que se haya alcanzado un mínimo

tecnológico en las propuestas que llegan al mercado. ¿Cómo escoger entre, literalmente, decenas de propuestas? Explica Consuelo Fernández que cada empresa tiene que escoger aquella solución que más se ajusta a sus necesidades desde el punto de vista de la funcionalidad, de la facilidad de implantación, y también desde el punto de vista de los costes de la propia solución. “Nosotros básicamente nos basamos en los grandes gurús” para el proceso de selección de una solución, y después pedimos a diferentes fabricantes una prueba de concepto “teniendo siempre muy claro cuáles son los beneficios que al final queremos conseguir con la solución”.

Proveedores de soluciones para el sector industrial, dice la CISO de Tecnatom que, si bien en el mundo industrial la cultura de seguridad es algo fundamental, la parte ciber, como no podía ser de otra manera, se está considerando cada vez más y ahora la ciberseguridad se considera por nuestros clientes en los procesos de adjudicación de ofertas”.

"Tenemos más capacidad de saber dónde están los incidentes y menos capacidad de poder dedicarle el tiempo que necesita todo eso"

"Cada empresa tiene que escoger aquella solución que más se ajusta a sus necesidades desde el punto de vista de la funcionalidad, de la facilidad de implantación, y también desde el punto de vista de los costes de la propia solución"

Insiste la CISO en que la ciberseguridad es una obligación, y asegura que un hacker no puede tirar abajo un avión o parar un oleoducto. La ciberseguridad se está convirtiendo en una utility. O lo tienes o no eres nadie.

Servicios gestionados

Sobre el papel que juegan los servicios gestionados de seguridad, casi imprescindibles para las empresas, nos cuenta Consuelo Fernández que cada vez se tienen más herramientas de detección; "tenemos más capacidad de saber dónde están los incidentes y menos capacidad de poder dedicarle el tiempo que necesita todo eso", y añade que en su empresa están convencidos de que "hay que tener ayuda externa con un servicio gestionado para que el personal interno se dedique a aquellas cosas que realmente dan valor al negocio".

El siguiente paso es cómo seleccionar al mejor proveedor de servicios gestionados. Al respecto, dice Consuelo Fernández que "los proveedores necesitarían escuchar un poco más a sus clientes y ver qué necesitan realmente porque hay muchos tipos de clientes. Ahora mismo la selección de un buen proveedor de servicios gestionados es complicado".

Tecnologías imprescindibles

Ya no vale con tener seguridad perimetral, ya no vale con tener un firewall, dice Consuelo Fernández cuando le preguntamos qué tecnologías de seguridad considera imprescindibles dentro de una

"Los proveedores necesitarían escuchar un poco más a sus clientes y ver qué necesitan realmente"

empresa. Dice que ahora hay que preocuparse por defender la identidad (más allá de usuario y contraseña), así como la defensa del endpoint y del dato, que ahora está en cualquier sitio y requiere sistemas de cifrado, tanto en tránsito como en reposo, así como un IRM; añade que los permisos de acceso son importantes, por lo que además habría que contar con tecnologías de doble factor de autenticación para proteger usuarios.

También le preguntamos a la CISO de Tecnatom por las tecnologías que considera que serán necesarias en un futuro. Dice que habrá que tener herramientas en torno a la detección temprana de incidentes "donde la inteligencia artificial nos va a poder ayudar mucho", aunque, añade, por el momento el coste es demasiado alto.

Lo ideal, asegura, sería contar con sistemas de detección que en tiempo real y a través de inteligencia artificial dijeran qué tipo de amenazas y qué tipo de intentos de intrusión está teniendo una empresa, incluido si está habiendo alguna fuga de información, si hay datos que se han llevado a un cloud y no deberían estar allí… ". Es decir, todo tipo de información y todo tipo de avisos, pero sin tener que dedicar horas a analizarlos". ¿Qué te gustaría tener? "Un sistema que no diera falsos positivos", responde rotunda, aclarando que montar un SIEM o un entorno de monitorización no cuesta tanto, pero "dedicarle tiempo para enseñarle y ver todos los avisos que te está enviando para saber si es positivo o no es lo que más cuesta".

¿Después de más de un año de pandemia, este 2021 es diferente en lo que respecta a la ciberseguridad? En la parte positiva dice la CISO de Tecnatom que se está viendo una mayor concienciación por parte de la alta dirección de las empresas, "con lo cual el trabajo de un CISO se hace más sencillo". En la parte negativa "los malos no van a parar, y cuando cierras una puerta llegarán con una ganzúa diferente. Cuando se dice que la seguridad al 100% no existe, es verdad".

Enlaces de interés…

- 'No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla' (Alejandro Sánchez es el CISO de SEAT)
- 'Los CISOs nos hemos dado cuenta de que la preparación al final del día compensa' (Fermín Serna, Citrix)
- 'No estamos en el momento de que sólo contratando tecnología podamos estar protegidos' (Judit Closa, habitissimo)
- 'El cloud no se hace responsable de la seguridad' (Toni García, LETI Pharma)
- 'Si puedo envenenar un data lake o hacer que un algoritmo funcione mal, tendré más influencia para la extorsión' (Rik Ferguson, Trend Micro)
- 'Ha habido estafas millonarias con un phishing básico' (Forensics&Security)

Compartir en RRSS

Proteja su experiencia en la nube de Azure.

Soluciones para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad »

Más información:
iberia_team@barracuda.com
barracuda.com

Barracuda Microsoft

STRENGTH IN SECURITY™

‘Las compañías necesitan seguridad ligada al desarrollo de nuevas aplicaciones’

(Tony Hadzima, Palo Alto Networks)

Rosalía Arroyo

Fundada en 2005 por Nir Zuk, antiguo ingeniero de Check Point y NetScreen Technologies, y principal desarrollador del primer firewall y el primer sistema de prevención de intrusiones (IPS), Palo Alto ha evolucionado enormemente en estos 16 años. En 2007, buscando dar respuesta a que los empleados pudieran utilizar aplicaciones modernas de forma segura, lo que implicaba el desarrollo de un firewall capaz de identificar y proporcionar información detallada y control de aplicaciones, lanzó al mercado su primer producto, considerado el primer NGFW (Next Generation Firewall)

La compañía debutó en la Bolsa de Nueva York el 20 de julio de 2012, recaudando 260 millones de dólares con su oferta pública inicial, después de ser incluida durante años en los cuadrantes de Gartner relacionados con la seguridad de red. Dos años después fundó la Cyber Threat Alliance con Fortinet, McAfee y Symantec, una organización sin fines de lucro con el objetivo de mejorar la ciberseguridad mediante el fomento de la colaboración entre organizaciones de ciberseguridad compartiendo la inteligencia de las amenazas.

A lo largo de los años Palo Alto ha evolucionado su oferta adentrándose en otros segmentos del mercado y más allá del firewall. Así, la compañía compite en el de seguridad endpoint con su propuesta Cortex XDR [evolución de Traps], o en el de la seguridad de la nube con Prisma Cloud. El siguiente caballo de batalla es el del desarrollo de aplicaciones, el mundo del DevSecOps, de la Shift-Left Security.

Llegar hasta aquí no ha sido fácil. Desde 2014 Palo Alto acumula 16 adquisiciones, empezando por la de Morta Security en enero de 2014 y

"Las empresas necesitan transformar su arquitectura de red de acceso remoto, con lo cual vemos también apuestas muy grandes en toda la parte de SASE"

terminando con la de Bridgecrew en febrero de 2021.

Tony Hadzima es el responsable de Palo Alto Networks en España y Portugal desde que la compañía abriera sus oficinas en la región hace más de once años. Con él hablamos de evolución, de impactos y de futuro

¿Cuál ha sido la evolución de Palo Alto? ¿en qué segmento de mercado la colocarías ahora?
Llegamos con el objetivo de simplificar la vida de los responsables de seguridad hace catorce años y vimos varios capítulos pendientes. Uno de los capítulos pendientes sería cómo simplificar la operación y la gestión de tantos elementos de ciberseguridad, porque hablamos de un mercado hiper fragmentado.

Y entonces la evolución de Palo Alto ha sido ver consolidación en el mercado, ver la necesidad de interconectar esas piezas, tener una buena integración y una buena automatización. Porque si analizamos un poco el panorama de los ciberatacantes, los cibercriminales utilizan muchas técnicas de automatización, de machine learning, para buscar los agujeros en las compañías. Y vemos que, desde el punto de vista de ciberseguridad, las ciber defensas deberían también implementar esas mismas tecnologías: no sólo proteger la parte de red o la seguridad perimetral, sino también la parte de nube, la parte de acceso roto y la parte del endpoint. Y si todos esos elementos comparten información, inteligencia, pues la respuesta es mucha más automatizada y tiene mucho más sentido.

Y lo que intentamos hacer básicamente es reducir lo máximo posible el tiempo medio para detectar un ataque. Y si por algún motivo entra, tener los sistemas preparados para responder, mejor automáticamente, o si no, pues acortar el tiempo de reaccionar con una intervención manual o humana.

¿Por dónde está creciendo más Palo Alto?
El crecimiento de lo que nosotros llamamos las nuevas tecnologías, las next generation, es muy

Cortex XDR es uno de los lanzamientos más disruptivos de la compañía

muy elevado. La parte del negocio más tradicional, más consolidado, mantiene un crecimiento por encima de la competencia.

Palo Alto ha realizado un total de 16 adquisiciones, ¿cuáles crees que han tenido más impacto en la evolución de la compañía?
Identificaría tres. La compra de Cybera en 2014, que nos permitió entrar en el mercado de endpoint. Fuimos el primer fabricante de seguridad de red que se metía en la parte de endpoint, lo cual fue bastante disruptivo. También fue importante la compra de RedLock, una compañía de seguridad cloud sobre todo en entornos multi cloud para hacer evaluaciones de la postura de ciberseguridad a través de múltiples configuraciones y la detección de comportamiento. Y la tercera gran adquisición es la de Demisto, con la que entramos en el mercado SOAR para la orquestación y automatización de la respuesta, y que nos permitió integrar los diferentes componentes de nuestra oferta.

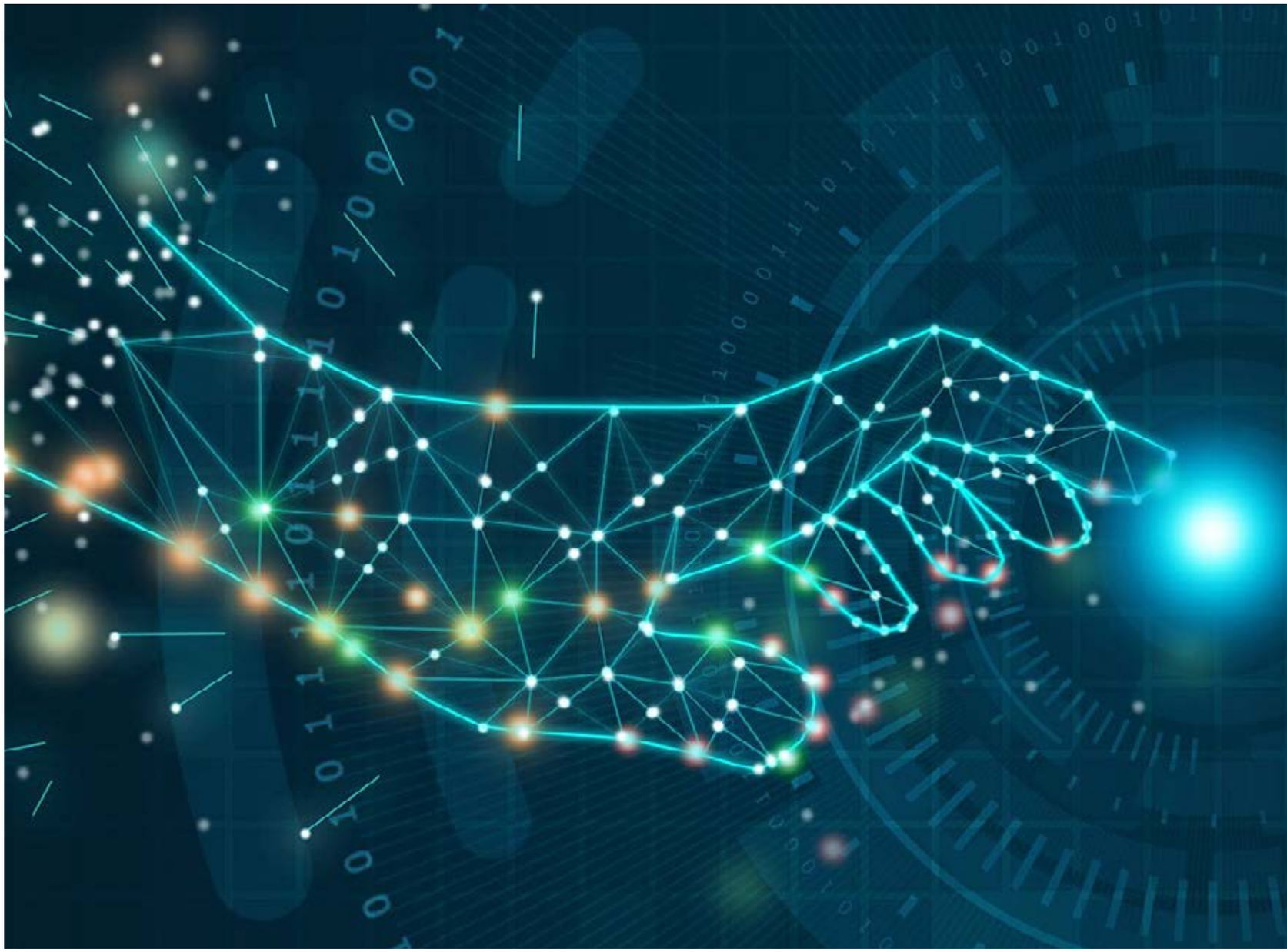
A nivel de lanzamientos, ¿cuál crees que ha sido el más disruptivo?
Cortex, porque ha sido la evolución de Traps. Cortex XDR ha sido la redefinición del mercado de

EDR. EDR es la detección y la respuesta de endpoint y con XDR volvemos a la red, conectamos la nube y volvemos a conectar con terceros; es decir, incorporamos la inteligencia de red no sólo de Palo Alto sino de otros fabricantes a nivel de firewall, lo que simplifica la vida de los CISOs y de los CIOs, que buscan esa reducción de complejidad porque tiene mucho más sentido tener todo integrado, automatizado y consolidado.

¿Qué es lo que puede aportar Palo Alto en el mundo del DevSecOps?

La misión de un responsable de seguridad es frenar los ataques, y un departamento de desarrollo de aplicaciones tienen que cumplir con unas fechas, sacar el producto, tiene su ciclo continuo de desarrollo, adaptarse a la velocidad de los clientes o del uso interno de las aplicaciones, y la seguridad tiene que formar parte de todo eso. A través de la adquisición de RedLock ofrecemos una tecnología API que monitorizar constantemente las configuraciones y comportamientos, para que todo vaya totalmente alineado con la velocidad de desarrollo.

Por otra parte, también adquirimos una compañía llamada Twistlock para la seguridad de contenedores, y PureSec que es para la parte de serverless. Y todo ello está incorporado en la suite de Prisma Cloud con el fin de ofrecer una seguridad 360, a nivel de múltiples nubes, de contenedores, a nivel de Zero Trust y luego tener esa integración o facilidad con los otros componentes de la red o de endpoint



"La tercera gran adquisición es la de Demisto, con la que entramos en el mercado SOAR para la orquestación y automatización de la respuesta"

"Lo que intentamos hacer básicamente es reducir lo máximo posible el tiempo medio para detectar un ataque"

y tener pues herramientas un poco más sencillas para para los clientes.

Por último, la compra de Bridgecrew expande las capacidades de la compañía en el mercado de DevSecOps

¿Cuál es la situación de Palo Alto en España?
Vamos a ser línea con la Corporación. Estoy encantado con el equipo que tenemos, con la demanda del mercado y con los éxitos que tenemos.

¿Hacia dónde mira Palo Alto? ¿Qué es lo que podemos esperar en los próximos años de una empresa que se está reinventando constantemente?
Las grandes apuestas a futuro están en la parte de cloud, donde además se han realizado las últimas adquisiciones. También vemos que las compañías necesitan seguridad ligada al desarrollo de nuevas aplicaciones, que los equipos de DevOps, de SecOps quieren que la seguridad forme parte del proceso de desarrollo.

Además, con la pandemia hemos visto esa aceleración de transformación digital, esa aceleración de compañías que necesitan ir a la nube, esas compañías que necesitan transformar su arquitectura de red de acceso remoto, con lo cual vemos también apuestas muy grandes en toda la parte de SASE.

Y la tercera gran apuesta sería lo que nosotros definimos dentro de Cortex como SOC de futuro, SOC autónomo, utilizando Cortex Data Lake para incorporar todos los datos de diferentes fuentes, bien de Palo Alto o de terceros y tener esa capacidad de automatizar los procesos mediante el SOAR, que antes era Demisto y ahora es Cortex XSOAR. La filosofía de SOC autónomo encaja en la filosofía de dar a los clientes esas herramientas y capacidades para transformar su sus defensas actuales.

Enlaces de interés...

- Palo Alto Networks actualiza Prima Cloud
- Palo Alto Networks simplifica la adopción de una seguridad de red Zero Trust
- Palo Alto Networks refuerza su equipo de investigación de amenazas con consultoría de ciberseguridad

Compartir en RRSS

X-Ray Vision for Malware

VMRAY

vmray.com

Quiere eliminar incertidumbre y rumores, formar un buen equipo, hacer crecer el negocio a nivel internacional e impulsar el concepto de XDR. Dice que el talón de Aquiles de la seguridad es la complejidad; que uno de los retos del Threat Hunting, y del mercado de seguridad en general es el déficit endémico de personal en cualquier parte del mundo; y que es una obligación dar a los proveedores de servicios, partners y grandes clientes una seguridad eficiente y más sencilla de comprar, de consumir y de utilizar. Hablamos con Miguel Carrero, responsable desde hace unos meses de WatchGuard Cytomic.

‘El endpoint siempre ha sido muy importante, pero después de la pandemia, todavía más’

(Miguel Carrero, WatchGuard Cytomic)

Rosalía Arroyo

"Cuando WatchGuard me llamó para esta aventura hubo muchas cosas que me interesaron. Una de las cosas que me gusta mucho de Watch-Guard es que conozco a los inverso-res, conozco a la compañía y me gusta mucho su estrategia”. Quien lo dice no es otro que Miguel Carrero, Vice President, Strategic Accounts & Security Service Providers Cytomic, a WatchGuard Brand, desde hace unos meses.

El nombramiento le hace dejar atrás Estados Unidos, donde llegó en 2006 “para vivir la aven-tura americana durante un par de añitos”, que se convirtieron en 15 trabajando para empresas tan grandes como HP, probando en el mundo de los

emprendedores con Siemplify o adentrándose en el de la detección y respuesta de red (NDR) en WireX Sytems.

Sobre la estrategia de WatchGuard dice que coincide con la aproximación de tener carriles independientes para cada uno de los vectores de seguridad: las redes, el endpoint, la identidad, las aplicaciones, los datos… "WatchGuard ya tenía la parte de red, había hecho una inversión importante en la parte de identidad multifactor, también en la parte del WiFi seguro, y faltaba esa parte del endpoint; porque el endpoint siempre ha sido muy importante, pero después de la pandemia todavía más", asegura Miguel Carrero, quien añade que la estrategia de tener "distintos elementos de seguridad en un portafolio integrado como un servicio de cloud a través de proveedores de servicios de seguridad, me encajaba muy bien" a la hora de aceptar el proyecto.

Sobre Cytomic, la unidad de negocio creada por Panda Security para ofrecer servicios avanzados al mercado enterprise, y de la que ahora se ha hecho cargo Miguel Carrero, dice el directivo que "tenemos la oportunidad de empujar esa aproximación que María Campos y el equipo empezaron con muchísimo talento y buenos resultados en España, el portafolio de WatchGuard y llevar la unidad de negocio a nivel mundial".

La Cytomic de Panda Security, comprada por WatchGuard hace más de un año, es ahora WatchGuard Cytomic. Sobre la marca explica Carrero que Cytomic "estaba consiguiendo buenos resultados a nivel nacional y queremos utilizarlo y tener

"Nuestra obligación como WatchGuard es darles a nuestros proveedores de servicios, partners y grandes clientes una seguridad eficiente y más sencilla de comprar, de consumir y de utilizar"

"Queremos seguir dando soluciones de seguridad a nuestros partners y a nuestros clientes, y seguir siendo un punto referente para nuestro equipo de producto"

esa noción de foco en el proveedor de servicios y la gran empresa", pero que no hay que olvidar que WatchGuard "es una marca internacional con presencia en Singapur, China, Australia y Latinoamérica…".

La nueva Cytomic bajo el paraguas de WatchGuard amplía su alcance; ya no se asocia a una empresa de seguridad endpoint, sino de firewall, de seguridad de red, de doble factor de autenticación.

Explica Miguel Carrero que se tiende hacia la XDR (Extended, Detection and Response), "a ese elemento de seguridad interconectada con telemetría de distintos elementos. A eso es a lo que va la seguridad, eso es lo que necesitan nuestros clientes y eso es lo que Watchguard Cytomic tiene", asegura.

Explica que el gran cambio es pasar de tener una aproximación para empresa y proveedores de servicios en el EDR "para serlo en el XDR, en un elemento de seguridad más completo. No sólo nos permite darles mayor elección a los clientes, sino hacerlo con mayor sencillez. Porque si me apuras el talón de Aquiles de la seguridad es la complejidad, y no todas las empresas tienen la capacidad de gestionar esa complejidad. Nuestra obligación como WatchGuard es darles a nuestros proveedores de servicios, partners y grandes clientes una seguridad eficiente y más sencilla de comprar, de consumir y de utilizar".

¿Preparados para el Threat Hunting?

Tiene claro Miguel Carrero que una de las cosas que la pandemia puso de manifiesto, "y que WatchGuard ya había visto, es la relevancia del endpoint". Asegura también que ahora tenemos que ser más capaces de provisionar, gestionar, hacer nuestro trabajo, distribuirlo… de una forma remota, y que eso implica "la necesidad de poder gestionar esa seguridad de una manera más sencilla".

Sobre si el mercado, las empresas, están preparadas para hacer Threat Hunting, una de las propuestas estrella de WatchGuard Cytomic, dice el directivo que sí, y que el gran reto del Threat Hunting ha sido la intersección de dos vectores novedosos y complicados: explotación de Big Data y seguridad en un momento en que había expertos de uno y otro, pero no de ambos. "Pero ahora las cosas han cambiado, "las tecnologías se están haciendo más intuitivas y nuestra plataforma Orion es muy sencilla de utilizar", tanto que no tienes que ser un experto de big data o de las últimas tecnologías de machine learning para hacer uso del Threat hunting. "No hay que ser un experto en la tecnología, sino en la utilización de la tecnología", asegura Miguel Carrero.

Un segundo reto del Threat Hunting, y del mercado de seguridad en general "es el déficit endémico de personal en cualquier parte del mundo", lo que incide en que las herramientas tienen que ser sencillas de utilizar, que es lo que ocurre con Orion sobre

la que asegura: “estamos muy ilusionados con esta plataforma y los clientes también; los clientes la van usando más, les gusta y le van sacando cada vez más partido”.

EDR, XDR, MDR

Nacido en el mercado de antivirus, Panda Security evolucionó su producto hasta meterse de lleno en el mercado de EDR (Endpoint Detection and Response), que es lo que se está implementando como solución de seguridad para puntos finales. Pero el mercado sigue avanzando y del EDR pasamos al mencionado XDR que lo que hace es recoger y analizar más telemetría, entre otros sitios de la red, que es donde WatchGuard, como fabricante de firewalls, tiene mucho que aportar. La situación en todo caso es complicada: por un lado para los fabricantes de seguridad endpoint que no están evolucionando sus productos correctamente y con la velocidad requerida y terminarán quedándose fuera del mercado;

"Estamos muy ilusionados con la plataforma Orion, y los clientes también"

UNA ESTRATEGIA GLOBAL ÚNICA Y GRANDES OPORTUNIDADES PARA PARTNERS Y CLIENTES, ASÍ QUEDA WATCHGUARD

En marzo de 2020 se anunciaba la compra de Panda Security por parte de WatchGuard. El acuerdo, cerrado en junio, crea una empresa de seguridad con una oferta para la red, el cloud, el endpoint y los accesos que, bien asentada en el midmarket, busca sumar nuevas oportunidades en la parte alta del mercado. Apostando por el canal y una oferta gestionada centralmente a través de la plataforma WatchGuard Cloud, la compañía afronta un año lleno de oportunidades para los clientes y el canal de distribución.

por otra parte para los clientes, que ven avanzar las tecnologías con demasiada rapidez.

Dice Miguel Carrero que los adversarios son gente muy lista, preparada, que combinan tecnologías, tienen un marketplace donde comparten expertise y tecnología, y que si nada más les pones un vector de protección, detección y respuesta, lo terminan evitando. "Cuando lo haces multi-dimensional es mucho más complicado porque tienen que evitar todo lo que ven en el endpoint, pero ahora también tienen que evitar que no les detecte la red, y que no les detecte la identificación… ahí es donde realmente se lo pones complicado".

Sobre las propuestas de MDR (Managed Detection and Response) que están llegando al mercado, asegura Miguel Carrero que es el proveedor de servicios gestionados, el MSSP quien tiene que darlo. "Nosotros seguimos muy comprometidos con nuestro canal, con el actual, con el futuro y con todas estas compañías capaces de ofrecer servicios de MSSP y MDR y a las que queremos darle las tecnologías, pero dejarles hueco para ofrecer su valor. Creemos que es la manera correcta de crecer, y crecer de una forma muy colaborativa con nuestros partners".

¿Qué previsiones tiene Miguel Carrero para WatchGuard Cytomic? "Por una parte eliminar las incertidumbres y rumores", asegura el directivo explicando que "lo que queremos es que el equipo que tenemos siga creciendo, y formar un equipo muy bueno, que trabaje muy bien junto y que trabaje muy bien con nuestros partners".

Por otra parte, se potenciarán dos vectores de crecimiento, por un lado el portfolio de WatchGuard, y por otro el crecimiento geográfico, "que WatchGuard Cytomic no sólo esté en España sino que vaya más lejos". Añade el directivo que "queremos seguir dando soluciones de seguridad a nuestros partners y a nuestros clientes, y seguir siendo un punto referente para nuestro equipo de producto, que es excepcional tanto en la parte de España, de Panda Cytomic, como internacional. Esa es la visión que tenemos". it

Enlaces de interés...

- 'Nos sentimos orgullosos del pasado que hemos heredado de Panda Security' (WatchGuard) - 30 MAR 2021
- Cytomic, tu arma de caza contra el cibercrimen
- Cytomic ayuda a las organizaciones con una promoción de sus servicios MDR
- Cytomic Orion permite la creación de reglas de hunting propias

Compartir en RRSS

Síguenos en:

CIFRADO HARDWARE
EN EL ÁMBITO FINANCIERO

cryptosec LAN

realsec
La clave para proteger su negocio

www.realsec.com

HSM con el mayor rendimiento transaccional del mercado

- Incluidos todos los algoritmos de cifrado simétricos y asimétricos **(sin costes adicionales ocultos).**
- Autenticación de doble factor para cumplimiento PSD2 e integración con soluciones de Blockchain.
- Certificación FIPS 140-2 level 3 del NIST y la Certificación PCI PTS HSM v2.0. del PCI Security Standards Council.

‘Los clientes quieren sacar partido a todas sus inversiones de seguridad’

(Ángel Ortiz, Cisco)

Cuando hace años Cisco, un grande entre los grandes en el mundo de las redes y la conectividad, decidió apostar por el mercado de seguridad, sabía que le iría bien, aunque quizá no tanto. La unidad de negocio genera más de 3.000 millones de dólares anuales de ingresos, ya se le considera un jugador en el mercado de seguridad, algo que, al menos en España, costó algunos años, y ha desarrollado una de las redes privadas de ciberinteligencia más grandes del mundo. Llegar hasta aquí no ha sido fácil, ni barato.

Rosalía Arroyo

Detrás están años de desarrollo y una inversión de 6.000 millones de dólares en compras en los últimos seis años. La última, Kenna Security, experta en gestión de vulnerabilidades, se produjo el pasado mes de mayo, después de la de Portshift, centrada en la creación de soluciones de seguridad de aplicaciones el año pasado.

Hace unos meses Ángel Ortiz se convertía en el director de ciber-seguridad en Cisco España, haciéndose cargo del negocio de ciberseguridad de la compañía. Atrás dejaba seis años en McAfee y experiencia acumulada en Acuntia, Nortel o Telindus. Hablamos con él sobre la situación de Cisco Seguridad en España, qué demandan las empresas o algunas tendencias que ganan peso en el mercado.

"Creemos que la aproximación del Zero Trust debe ser completa y securizar lo que llamamos las tres 'W': el Workforce, el Workplace y los Workloads"

¿En qué segmento del mercado de ciberseguridad colocarías a Cisco?
Cisco tiene un portfolio de extremo a extremo que cubre todos los vectores de ataque, desde el endpoint, el correo electrónico, la red, la navegación y ahora la nube. Somos una de las empresas con el portfolio más amplio, más completo y más de aproximación a plataforma.

Cisco ofrece una plataforma unificada pero a la vez abierta para los clientes que ayuda a simplificar esa complejidad a la que muchas veces se enfrentan los CISOs por tener múltiples soluciones de diferentes fabricantes y que luego en la práctica resulta difícil y complicado de operar, de gestionar y de encontrar las amenazas cuando se producen.

¿Qué es lo que os están demandando los clientes?
Mayor simplicidad. Ayudarles a hacer su vida más sencilla y más simple. El mercado de la seguridad está tremendamente atomizado; hablamos de unos 3.500 fabricantes de seguridad a nivel mundial, algo que no es demasiado sostenible en el largo plazo. Los clientes quieren tener una visión unificada, poder consolidar alertas y poder sacar partido a todas sus inversiones de seguridad.

Además, en los tiempos de pandemia lo que han demandado ha sido facilitar una adopción segura de la nube, del teletrabajo y de todo el proceso de transformación digital, lo cual marca otra de las tendencias que vamos a ver: cada vez más los proyectos seguridad van a estar vinculados a proyectos de transformación digital dentro de las compañías.

Cada vez se invierte más en seguridad y cada vez hay más amenazas, más problemas de seguridad. ¿Hacia dónde nos lleva eso?
Efectivamente, algo tenemos que hacer de forma distinta. La tendencia en el mercado ha sido que

Simple, inteligente y en todas partes. Así debe ser la seguridad para Cisco

"La seguridad debe estar en el centro de todo en el nuevo mundo en el que vivimos. Creemos que debe hacerse con un enfoque de plataforma que sea simple, integral y basado en la inteligencia", dijo Chuck Robbins, CEO de Cisco hace unas semanas, durante la celebración de la RSA Conference. Aseguraba además el directivo que ya no hay ningún perímetro en la empresa que defender, que necesitamos visibilidad en todos los puntos finales, usuarios y aplicaciones, así como asegurar los puntos de control críticos con autenticación continua sin contraseña.

Durante la conferencia la compañía dio a conocer sus últimas innovaciones en materia de seguridad:

• **Mejora de la visibilidad y simplificación de la detección y respuesta extendidas (XDR).** Asegurando que las organizaciones que no priorizan las soluciones integradas tienen casi el doble de probabilidades de haber sufrido un evento de seguridad importante, Cisco continúa expandiendo sus capacidades XDR, integrando múltiples puntos de control de seguridad y aplicando análisis y automatización para reducir el tiempo de detección y respuesta de los clientes.

• **Cumplir con una visión SASE con seguridad en la nube mejorada.** La arquitectura SASE de Cisco integra múltiples funciones de red y seguridad en una única oferta de conectividad segura. Esto simplifica significativamente la seguridad y reduce el coste, el tiempo y los recursos que antes se requerían para la implementación, la configuración y la integración.

• **Redefiniendo y simplificando la seguridad de la red.** Los entornos de aplicaciones en constante cambio hacen que la seguridad de la red sea más compleja. Las aplicaciones modernas de integración continua y entrega continua (CI/CD) necesitan una coordinación más estrecha entre los desarrolladores, los equipos de seguridad y de red para garantizar que los entornos de aplicaciones y las cargas de trabajo sean seguros, que los firewalls estén configurados adecuadamente y las políticas estén integradas. De lo contrario, las vulnerabilidades y las configuraciones incorrectas en estos entornos en constante cambio dejan las puertas abiertas para los posibles actores de amenazas.

cada vez que aparece un tipo de amenaza, un tipo de ataque, lanzamos un producto para cubrir esa nueva vulnerabilidad, pero al final estamos incorporando una solución más que gestionar y que añade complejidad en el entorno global.

No necesariamente hay que tener más seguridad entendida como más soluciones de seguridad en nuestro entorno, sino que hay que conseguir que las que tenemos trabajen de forma orquestada y tengan sentido dentro de nuestro ecosistema. Que

"Hemos visto claramente una preocupación por adoptar la nube de forma segura, y todo como servicio en la medida de lo posible"

esa ciberinteligencia, esa información que tenemos sea información útil y que nos permita sacar partido, y no estar sumergidos en un mar de alertas que al final no sirven para nada.

¿Qué opinas de tendencias como SASE (Secure Access Service Edge)?
El paradigma SASE propone el ser capaces de conectarnos de forma segura en nuestras aplicaciones corporativas, desde cualquier dispositivo y desde cualquier lugar. La persona que antes trabajaba en una oficina de 9 a 6 tenía una conexión de alta velocidad que posiblemente permitía voz y datos, tenía un perímetro dentro de nuestra compañía que lo protegía y que aplicaba contramedidas de seguridad para controlar el acceso a ese perímetro y cómo estaba dentro de ese perímetro, y normalmente las aplicaciones también estaban en el datacenter, y ahora lo que tenemos que hacer es facilitar eso y que al usuario se le entregue la conectividad y la seguridad de una forma segura desde la nube. Eso es lo que en definitiva es SASE.

Pero no todas las propuestas SASE son iguales. Cada cual la está adaptando como quiere...
Cuando hablamos de SASE hablamos de seguridad y hablamos de conectividad. La definición de Gartner respecto a SASE habla de una serie de servicios de seguridad que además son varios: el proxy cloud, el firewall-as-a-service, el zero trust en el acceso a la red para comprobar que efectivamente el usuario es el que debe ser, la parte de CASB para controlar la actividad que hacen mis usuarios en la nube… pero también es la parte de SD-WAN y de conectividad, y al final cada fabricante ha acabado cogiendo lo que le interesa de ese mensaje de Gartner ofreciendo visiones muy parciales.

"Cisco ofrece una plataforma unificada pero a la vez abierta para los clientes que ayuda a simplificar esa complejidad a la que muchas veces se enfrentan los CISOs"

En ese sentido, Cisco sí que tiene las cosas claras y ofrece un SASE de verdad, tanto desde el punto de vista de la seguridad como de la conectividad. Se ha trabajado en que las soluciones de SD-WAN que tiene Cisco (Vitela y Meraki) estén muy integradas con su solución de Umbrella, que es la que lleva a cabo la seguridad en la nube, y que juntas conforman la propuesta SASE de Cisco. Se trata de una visión conjunta y global de lo que es SASE y no una visión parcial que acabará llevando a niveles de adopción diferentes por parte de las empresas.

¿Y qué opinas del modelo Zero Trust?
Creemos que la aproximación del Zero Trust debe ser completa y securizar lo que llamamos las tres 'W': el Workforce o usuarios, el Workplace o puesto de trabajo y los Workloads, o las cargas de trabajo que tenemos en la nube o en nuestros datacenter híbridos.

Con el Zero Trust, al final o bien se hacen aproximaciones muy parciales centrados en la parte de ZTNA (Zero Trsut Network Access) o de una autenticación fuerte para mis usuarios, pero Zero Trust, al igual que SASE, es también una filosofía en la que debemos asumir que se ha podido producir un ataque y comprobar a cada paso que des que estás autorizado a darlo y que es legítimo. Y eso es mucho más que comprarme una solución puntual, sino que debe ser una estrategia que deben seguir las compañías.

Seguimos con las tendencias. Parece que ahora se nos queda corto el EDR y nos vamos hacia el XDR, ¿crees que tiene sentido correr tanto?
Es verdad que el mercado avanza de forma vertiginosa y que muchas veces pasamos de estar hablando de una solución a otra casi sin tener un nivel de adopción suficiente de la primera. Pero también es verdad que también los ataques evolucionan a una velocidad que es vertiginosa y tenemos que adaptarnos. Yo creo que el XDR tiene mucho sentido, precisamente por

Enlaces de interés...

- Las grandes adquisiciones de Cisco
- Cisco amplía su oferta de seguridad en torno a la plataforma Cisco SecureX
- Un futuro sin contraseñas ¿cada vez más cerca?

esta aproximación de plataforma de la que te he hablado, de conseguir que nuestras soluciones operen de forma orquestada. Además, Cisco aquí tiene mucho que decir porque está presente en las redes de muchos de nuestros clientes y podemos potenciar la solución endpoint aprovechando la inteligencia que podemos recopilar de todos los elementos de red que tenemos.

Un año después de la pandemia, ¿qué cambio estáis observando en el mercado? ¿Han cambiado los hábitos de inversión de las empresas?

Creo que se ha dado más importancia a la ciberseguridad con el aumento del número de ataques que hemos tenido. Sí que hemos visto claramente una preocupación por adoptar la nube de forma segura, y todo como servicio en la medida de lo posible, incluso en entornos de administración pública que antes eran más reacios.

¿Qué puede aportar Ángel Ortiz al Cisco Seguridad?

He estado mucho tiempo en uno de los principales integradores de Cisco y de otros fabricantes a nivel de comunicaciones y conozco bien el mundo de las comunicaciones y del IT general. Además en los últimos años he estado en McAfee, que es una empresa del entorno puro de ciberseguridad, lo cual me permite tener el conocimiento de ambos mundos y ver, por ejemplo, la importancia de que la parte SD-WAN tiene que estar bien imbricada con la parte de cloud security.

Esa visión de conocer bien los dos mundos, tanto el mundo de las comunicaciones que puede representar el negocio más tradicional de Cisco, como el puro de la ciberseguridad y lo que éste demanda "es algo que puedo aportar. Y espero hacerlo en los próximos meses". it

Compartir en RRSS

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

Los **equipos de investigación de amenazas de SonicWall Capture Labs** proporcionan a las empresas, pymes, agencias gubernamentales y otras organizaciones inteligencia de ciberamenazas existentes para proteger a su personal distribuido contra una superficie de ataque en continua expansión.

Al proporcionar una visión completa de estos datos, el ***Informe de Ciberamenazas 2021 de SonicWall*** muestra cómo piensan y operan los cibercriminales, ayudando a las organizaciones a prepararse mejor para las amenazas del futuro.

OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

▼ 43%

EL MALWARE CAE AL NIVEL MÁS BAJO DESDE 2014

+ 1 días

IDENTIFICACIÓN MÁS RÁPIDA DE MALWARE "NUNCA ANTES VISTO"

▲ 62%

EL RANSOMWARE ALCANZA UNA CIFRA RÉCORD

▲ 74%

INSPECCIÓN DE MEMORIA PROFUNDA MEJOR QUE NUNCA

▲ Máx. 3 años

EL CRYPTOJACKING HA VUELTO

▲ 66% IOT

EL MALWARE DE IOT AUMENTA UN 66%

▲ 20%

INTENTOS DE INTRUSIÓN EN CONSTANTE CRECIMIENTO

itTRENDS

JULIO 2021

Apps, datos y espacio de trabajo: siguiente ola de la transformación digital

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Directora de IT Digital Security
Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Director de IT User e IT Reseller
Pablo García pablo.garcia@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es
Redacción y colaboradores Ricardo Gómez, Alberto Varet, Hilda Gómez, Arantxa Herranz, Reyes Alonso
Diseño revistas digitales Eva Herrero
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska
Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

El IBEX-35, ejemplo de transformación digital

Un reciente estudio de Adigital y Opinno señala que el 95% de las empresas del IBEX 35 tiene ya una estrategia digital definida y está trabajando para ponerla en marcha. No sorprende que esto sea y deba ser así, ya que las grandes empresas han sido las primeras conscientes de los beneficios que la digitalización aporta a las organizaciones y a la economía de los países.

El informe señala muchos puntos de avance entre estas organizaciones: el 47% ha establecido objetivos digitales entre sus directivos para impulsar la transformación; el 79% están incorporando metodologías Agile; 3 de cada 4 empresas ya dispone de aplicaciones y datos integrados en la nube; y el mismo porcentaje ha digitalizado su logística, utilizando sistemas de control y rastreo de productos, soluciones de inteligencia artificial para la gestión de inventario y otros tipos de software para la optimización de procesos.

Con todo, también pone de manifiesto también algunas asignaturas pendientes tales como el desconocimiento de las habilidades digitales de los empleados (63%) o la necesidad de crear una estrategia de venta omnicanal.

El camino de la digitalización supone una constante evolución y para seguir avanzando hay que revisar continuamente tecnologías y procesos. Eso es lo que nos hemos propuesto este trimestre en IT Trends: hacer una revisión de las últimas tendencias en tres áreas clave para continuar en la senda de la transformación digital: aplicaciones, puesto de trabajo y datos.

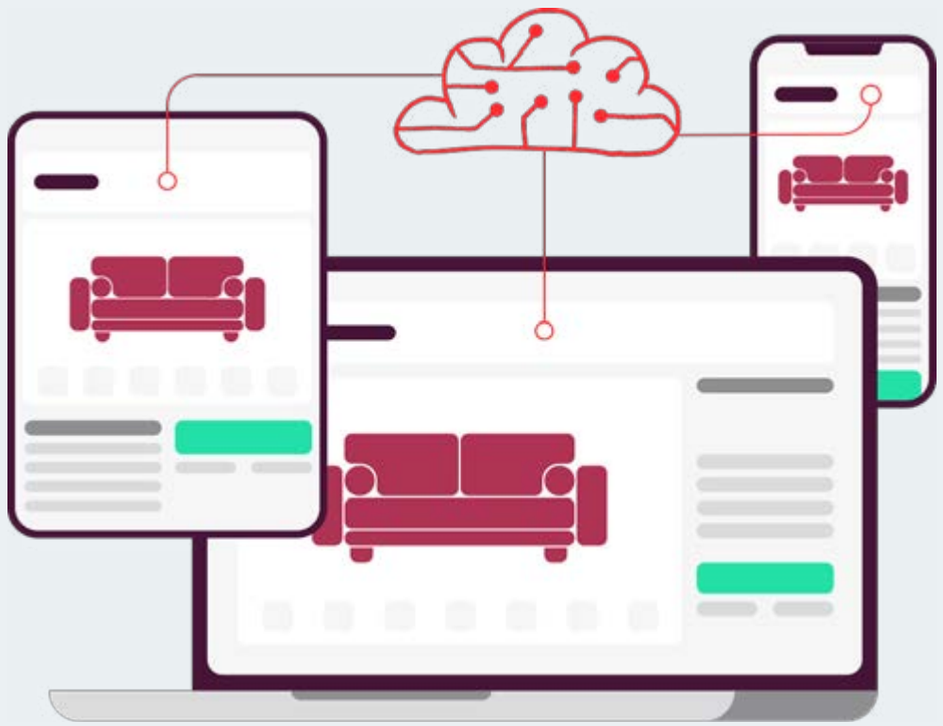
Para ello, puedes repasar los Encuentros IT Trends que hemos celebrado: Aplicaciones, ¿cómo desarrollo, entrego y gestiono mi software?; Mejorando la experiencia del trabajador remoto y Entendiendo la Era del dato: tecnologías y propuestas para gestionar la "datificación" En estas sesiones hemos buscado la opinión del mundo académico, empresarial y tecnológico a la hora de analizar las últimas tendencias en estas áreas. Te invito a leer en las próximas páginas las conclusiones de estos tres encuentros y a ver (y profundizar tanto como quieras) el conocimiento que todos los expertos han compartido con nosotros tanto en las mesas redondas como en las píldoras informativas.

De cara a este periodo estival, no te pierdas la lectura de nuestro nuevo informe: Tendencias tecnológicas de alto impacto para tu negocio, en el que hemos recogido las principales observaciones del mercado tecnológico y cómo impactará en las organizaciones.

Agradecemos a todos los patrocinadores y socios que este trimestre han apoyado nuestras actividades y a ti, lector, te deseamos un ¡feliz verano! ■

Arancha Asenjo
Directora IT Trends

fastly



Las experiencias de compra más rápidas, personalizadas y seguras se encuentran en el edge

Fastly ayuda a las empresas minoristas online más seguras —como Shopify, Ticketmaster y Etsy— a superar las expectativas de los clientes ofreciéndoles experiencias digitales seguras y de alto rendimiento a escala.

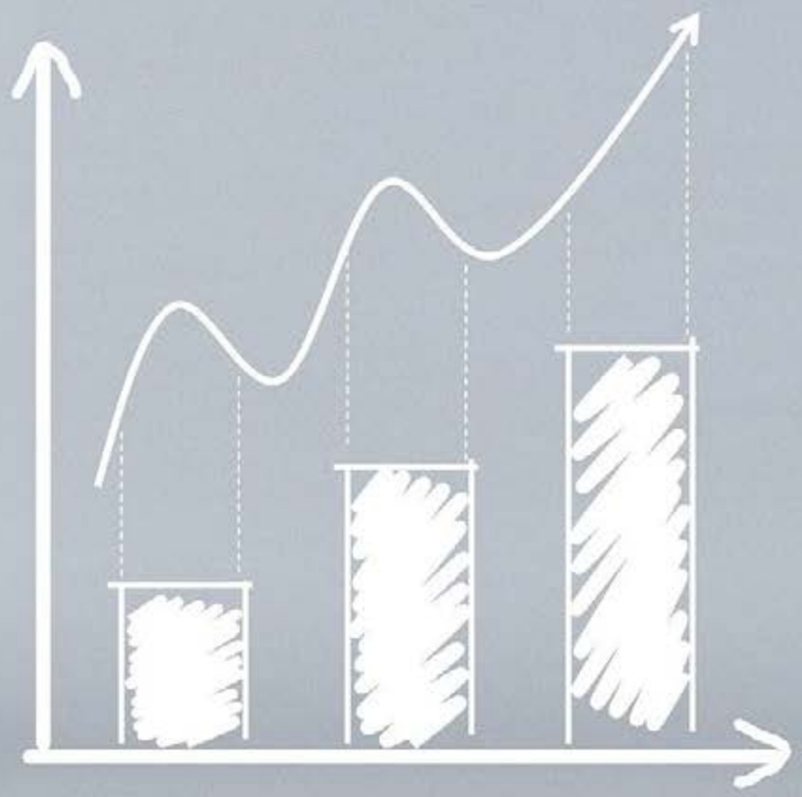
Descubre más en:

fastly.com/es/solutions/retail/

itTRENDS

Cuatro puntos clave en la transformación digital financiera

La digitalización viene acompañada de muchos cambios en las organizaciones, y algunos departamentos como el financiero están adaptándose con mucha lentitud a esta nueva realidad. Por ello, los expertos de Gartner han elaborado una lista con las cuatro iniciativas de digitalización más importantes que deberían llevar a cabo los directores financieros. Éstas abordan cuestiones clave para lograr el éxito en un futuro en el que las finanzas estarán ligadas más que nunca a la tecnología y a los datos, un campo de juego para el que no todos están preparados.



A medida que las organizaciones progresan en la transformación digital de sus negocios, la tecnología se infiltra cada vez más en todos los procesos, y un área clave que debería estar al día es la de las finanzas. Ante esta realidad, los directores financieros se encuentran con numerosas dificultades y con muchos caminos posibles a seguir, pero no todos llevan al éxito. Para arrojar algo de luz, los analistas de Gartner han elaborado una lista con las cuatro áreas que consideran más importantes para el desarrollo de planes de transformación digital de las finanzas empresariales. Su idea es recalcar aquellos puntos que los líderes de finanzas deberían abordar de forma más directa para poder alcanzar los objetivos financieros.

En palabras de Peter Nagy, investigador vicepresidente de la práctica de Gartner Finance, "muchas actividades comerciales que eran competencia tradicional de los departamentos financieros, como la gobernanza de datos centralizada, se están democratizando en toda la empresa, o ya no son diferenciadores importantes en el valor que los equipos financieros pueden ofrecer a la empresa. Para cumplir con la visión de un departamento de finanzas más ágil y digital para 2025, los directores financieros deben duplicar las cosas que las finanzas pueden hacer mejor que nadie".

LAS FINANZAS NECESITAN REPLANTEAR SUS PLANES DE DIGITALIZACIÓN

Como explican en su informe, las iniciativas de transformación digital de los departamentos financieros han sido hasta ahora muy pobres y de muy poca profundidad, y solo un 39% de los directores financieros que los han llevado a cabo creen que han proporcionado beneficios tangibles al departamento, y mucho menos a la organización en su conjunto. Pero el terreno de juego está cambiando, y ahora la digitalización de las finanzas empresariales es uno de los pasos clave para todo el proceso de transformación digital de los negocios. Y, por ello, los directores financieros deben cambiar el chip y buscar nuevas formas de añadir valor a las operaciones, apoyándose en la tecnología.

Según Nagy, el cambio que se ha producido en los últimos años es notable y ahora "los datos, el análisis y las soluciones tecnológicas sofisticadas se han democratizado cada vez más en toda la organización, con muchas funciones y tomadores de decisiones mejor posicionados para analizar y actuar en base a sus propios datos". En este contexto, no puede ser que los departamentos financieros sigan al margen del cambio, y es preciso no solo que sigan esta corriente, sino que los CFO sean capaces de liderar una transformación que siente las bases de cómo se llevarán a cabo las operaciones financieras de la organización en el futuro.

Nagy señala que, "en un entorno de creciente complejidad organizacional, que hace más difícil para las organizaciones financieras adaptar el soporte, los planes de transformación deben organizarse en torno a las áreas donde más destacan los puntos fuertes de las finanzas". En su opinión, estas son el mantenimiento de estándares de calidad, la experiencia en diseño de procesos de extremo a extremo y el apoyo a la toma de decisiones a nivel de cartera y balance". Por ello, este informe destaca que los líderes de los departamentos financieros deberían centrarse en estas cuatro áreas clave a la hora de diseñar sus nuevos planes de transformación digital.

❖ **Garantizar la calidad de los datos**

Los datos que manejan las organizaciones se generan cada vez más rápido y en mayor cantidad y variedad y, para aprovecharlos, es vital separar el grano de la paja y hacerlo bien. En una era en la que los responsables de la toma de decisiones se basan en información de calidad los líderes financieros deben garantizar que siguen proporcionando datos fiables y adecuados a las necesidades de cada departamento. Por ello, las finanzas deberían centrarse en guiar la gobernanza de los datos hacia un cambio de modelo, en el que no exista una "única fuente de verdad", sino un enfoque basado en "versiones suficientes de la verdad". Esto supone centrarse en la preparación para la toma de decisiones, en vez de en la precisión de los informes, ya que cada área del negocio puede tener una visión diferente, que requiera información tratada de una forma concreta. Por ello, proporcionar datos generales, por muy precisos que sean, no ayuda a la toma de decisiones, sino que la complica, y los departamentos financieros deberán alinearse más con las necesidades de cada área para ofrecer datos que les ayuden de verdad.

❖ **Visión del soporte a nivel de cartera**

Los departamentos financieros se han centrado durante mucho tiempo en adaptar su soporte a las decisiones específicas de la unidad de negocio. Pero la complejidad de la organización aumenta y este modelo no se adapta a una mayor escala, no proporciona el necesario apoyo a la toma de decisiones y presenta riesgos de duplicación y de dejar áreas oscuras en la financiación, que pueden causar problemas al negocio. Para romper con esta ineficacia los expertos de Gartner recomiendan a los directores finan-

La tecnología se infiltra cada vez más en todos los procesos, y un área clave que debería estar al día es la de las finanzas

cieros centrarse en proporcionar apoyo a nivel de cartera, con expertos especializados que se centren en áreas como la optimización de costos, el inventario y las mejoras de los productos y servicios. Y afirman que este enfoque mejora en 2,5 veces la solidez financiera de las decisiones operativas, algo que se debería tener uy en cuenta a la hora de establecer una estrategia de cara al futuro.

❖ **Experiencia en balances**

El uso cada vez mayor de tecnologías basadas en datos permite a las unidades de negocio llevar a cabo sus propios análisis de pérdidas y ganancias, sin necesidad de recurrir constantemente al departamento financiero para obtener información. La investigación de Gartner revela que un 67% de los responsables de la toma de decisiones sí agradecerían que el departamento financiero les proporcionase un mayor apoyo en relación al balance, pero actualmente el 87% del soporte financiero está centrado todavía en el apoyo de pérdidas y ganancias. Por ello, los analistas recomiendan a los departamentos de finanzas que incorporen a más expertos capaces de proporcionar apoyo a la toma de decisiones en el balance de la tesorería y la contabilidad, y para ayudar en el cumplimiento de los objetivos de análisis y planificación financiera (FR&A). Y también que recurran a socios comerciales de finanzas integradas para las solicitudes de apoyo a las decisiones comerciales.

❖ **Experiencia en diseño de procesos de extremo a extremo**

Para los expertos de Gartner, las organizaciones cada vez dependen menos del departamento financiero para la síntesis y el análisis de datos del negocio. Pero consideran que todavía hay margen para que las finanzas proporcionen más valor a través de su experiencia en el diseño de procesos de extremo a extremo, algo que llevan haciendo mucho tiempo. Esto se lograría siendo cada vez más críticos a medida que se van interrumpiendo más procesos por la automatización digital, por lo que recomiendan aprovechar esta dilatada experiencia para acelerar nuevos procesos. Por ejemplo, la tendencia hacia la hiper-automatización que se está expandiendo en las empresas más innovadoras de la propia industria financiera.

Este es un cambio muy radical, que implica a muchas áreas del negocio, y que debe planificarse de extremo a extremo. Por ahora, la mayoría de los equipos financieros solo está

Los directores financieros se encuentran con numerosas dificultades y con muchos caminos posibles a seguir, pero no todos llevan al éxito

en el escalón de la automatización tradicional, que se basa en ir eliminando trabajo manual con aplicaciones como RPA. Pero en los próximos años esto va a escalar, afectando a cadenas de proceso más largas en muchas empresas, y aquí los departamentos financieros pueden proporcionar mucho apoyo gracias a su experiencia en evaluar procesos que afectan a múltiples niveles dentro de la organización.

MUCHO CAMINO POR DELANTE

Esta investigación de Gartner revela que el 93% de los líderes de departamentos financieros comparten una visión muy similar de cómo será su futuro. Su enfoque se basa en priorizar lo digital para proporcionar datos bajo demanda, con una estructura financiera a gran escala y una mayor diversidad de habilidades entre los miembros de sus equipos. Pero también muestra que las iniciativas de los directores financieros no están alcanzando sus objetivos.

Por ahora, solo un 15% de los líderes encuestados está contento con el progreso de sus iniciativas de automatización, solo un 23% con las capacidades de análisis comercial en tiempo real y un 12% con el progreso de tecnologías digitales, en general. Esto pone de relieve que los planes de transformación digital de los departamentos financieros están mal enfocados, no cuentan con el apoyo necesario y probablemente no logren sus objetivos al mismo ritmo que la digitalización de otras áreas del negocio.

Esto es un problema grave, que los expertos recomiendan atajar lo antes posible, algo que se puede lograr si se centran las estrategias en estas cuatro áreas clave. Pero también hay otros problemas que se deben resolver, como la escasez de habilidades digitales entre los empleados, que dificulta el trabajo con las nuevas tecnologías. O la falta de una cultura de transformación e innovación constante en los departamentos de finanzas, que genera resistencia y desconfianza por parte de los trabajadores y de los propios líderes, minando cualquier intento de cambiar a mejor.

Estos y otros problemas deben estar muy presentes en la agenda de los directores financieros para los próximos años. Teniendo en cuenta la aceleración que se está produciendo en la transformación digital y en la automatización de procesos dentro de las organizaciones, los departamentos de finanzas podrían quedar rezagados en una modernización que se está volviendo imparable. En esta nueva era los datos financieros y su análisis serán fundamentales, pero no de la forma tradicional, y se deberán reforzar las capacidades en tiempo real y la integración con otros departamentos de nuevas maneras que sean más ventajosas para el negocio. ■

MÁS INFORMACIÓN

- Áreas clave en los procesos de transformación digital de los departamentos financieros
- Futuro digital de las finanzas
- Los CFO necesitan acelerar la adopción de la IA
- Los departamentos financieros se vuelvan con la digitalización
- Los CFO aceleran la transformación digital
- Entendiendo la era del dato
- La tecnología RPA genera nuevos retos para los CFO

Si te ha gustado este artículo, compártelo

SYSDEV KALIPSO
mobile application generator

iOS

GENERADOR LOW CODE DE APPS MÓVILES

Utiliza tecnologías emergentes y desarrolla las mejores aplicaciones con Kalipso Studio.

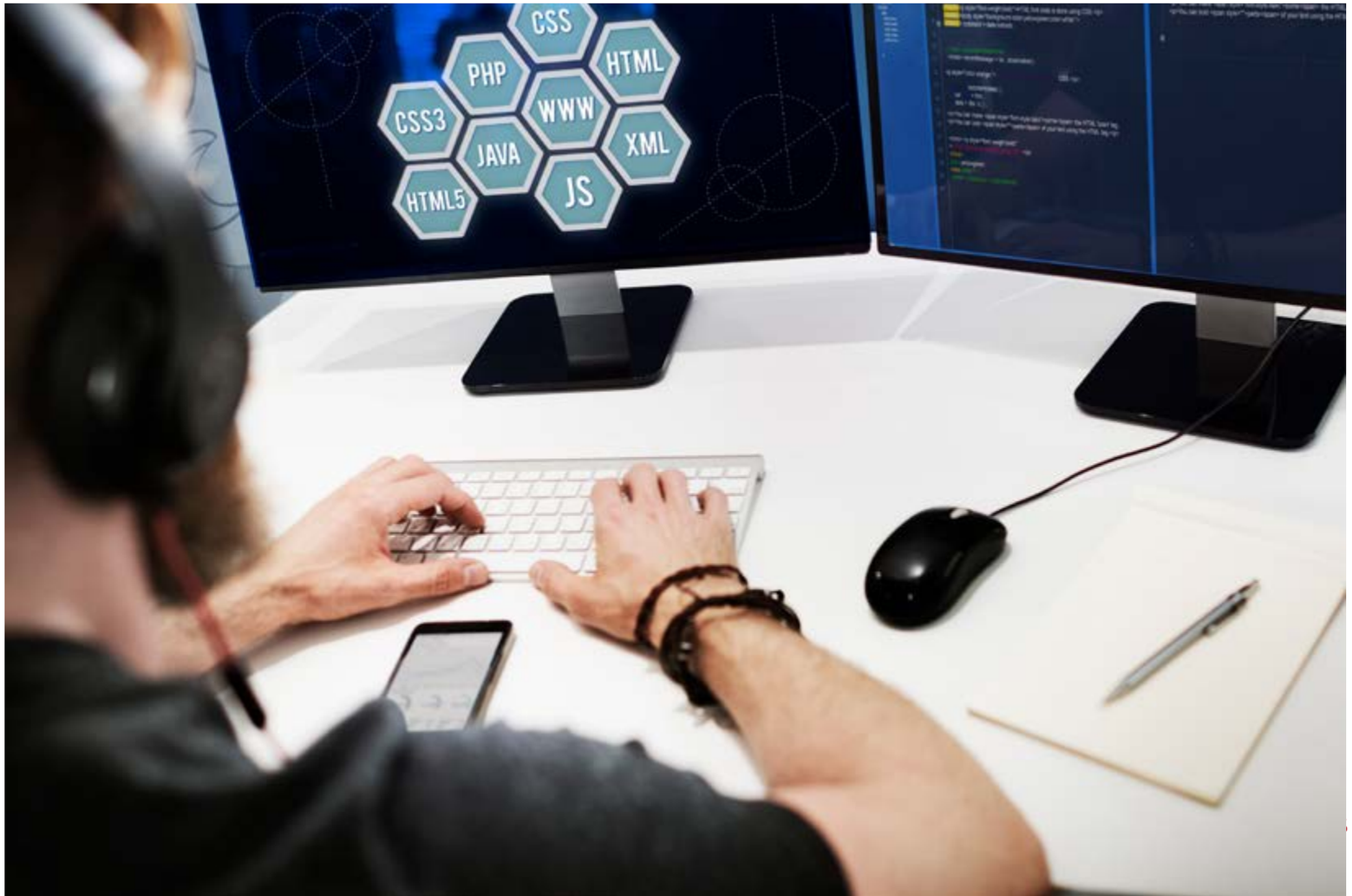
- Aplicaciónes Nativas
- Multi OS Deploy
- Conexión Base de Datos Online/Offline
- Código de Barras
- NFC, RFID
- Impresión

La digitalización industrial se apoya en el software de ingeniería moderno

En la próxima década se va a producir un avance significativo de la digitalización en el sector industrial, lo que va a beneficiar al mercado mundial de software de ingeniería. Según los expertos, en este tiempo se expandirá el uso de software especializado para el diseño, la simulación y la fabricación inteligente, incrementando el valor de este mercado en un 13% hasta el año 2030.

La transformación digital del sector industrial va a acelerarse en la próxima década, cuando se esperan grandes avances en la automatización de las fábricas, a medida que las empresas adopten tecnologías para la fabricación inteligente, siguiendo los preceptos de la industria 4.0. Esto transformará profundamente la industria, y tendrá un impacto positivo en muchos mercados tecnológicos asociados a la actividad industrial, como el de software de ingeniería. En esta categoría se encuentran varias categorías de aplicaciones que apoyan la fabricación, como CAD (Diseño Asistido por Ordenador), CAM (Fabricación Asistida por Ordenador) y CAE (Ingeniería Asistida por Ordenador).

El software de estas categorías se está convirtiendo en un apoyo fundamental para los diseñadores de producto y fabricantes, pro-



porcionando herramientas que ayudan a las empresas de construcción y de fabricación a reducir los costos relacionados con el desarrollo y la fabricación. Según una investigación publicada por Transparency Market Research, la automatización dentro del proceso de desarrollo de producto está impulsando la demanda de software de ingeniería avanzado, un mercado que crecerá con solidez en los próximos años. Este estudio pronostica que los ingresos crecerán a una tasa interanual compuesta (CAGR) del 13% hasta el año 2030.

Como explican los expertos, este tipo de software permite a los usuarios visualizar, diseñar y controlar un objeto, entorno o cualquier elemento gráfico dentro de un entorno virtual, así como ejecutar simulaciones complejas y cada vez más realistas, en unos casos para mejorar el diseño de productos, y en otros para diseñar posibles modificaciones en los procesos de las fábricas. Esto permite acelerar y optimizar el desarrollo de productos, reduciendo los costes y complementando las estrategias de automatización en otras áreas. Especialmente en las industrias manufacturera y de construcción, que son los dos principales clientes del mercado de software de ingeniería.

Así, la próxima década será clave para el mercado de software CAD, CAM y CAE, gracias al avance de la automatización en estas industrias y a nuevos enfoques como el de software de ingeniería basado en la nube. Cada vez hay más ofertas de este tipo, que están ganando peso en el mercado gracias a que permiten ahorrar tiempos de implementación, espacio en el disco duro del cliente y permiten el trabajo remoto y colaborativo, incrementando la flexibilidad y reduciendo los costos operativos. Por ello, los expertos esperan que el segmento de soluciones en la nube continuará creciendo rápidamente en los próximos 10 años.

Para los investigadores, Norteamérica será uno de los principales mercados de software de ingeniería, especialmente por la importante presencia de este tipo de soluciones en el sector de la construcción, Y se espera que la tasa de adopción de este tipo de soluciones siga aumentando en la próxima década, gracias a que en este tiempo se van a llevar a cabo grandes proyectos de infraestructura, tanto en Estados Unidos como en otros importantes mercados mundiales. Por ejemplo, en Europa, otros de los grandes mercados de este tipo de software, pero en este caso también hay una gran vinculación con el sector industrial, por ejemplo, en la fabricación de automóviles.

Por otro lado, los expertos del International Research Journal of Engineering and Technology creen que en este tiempo es muy probable que el 22% de los trabajadores altamente cualificados del sector de la fabricación (unos 2,7 millones) se jubilen. A pesar del avance de la automatización, esto obligaría a las fábricas a contratar a otros 700.000 trabajadores, pero se estima que en los próximos 10 años la escasez de mano de obra en las fábricas podría supera los 8 millones de personas, lo que resultará en una pérdida de ingresos estimada en 607.000 millones de dólares. Esto supone una importante crisis de talento que las industrias esperan superar empleando nuevas tecnologías y un menor porcentaje de trabajadores humanos, pero que deberán ser formados para trabajar en entornos con mayores requisitos técnicos en materia digital. ■

MÁS INFORMACIÓN

- Los fabricantes aumentan el gasto en software PLM
- Más empresas se alían para refundar las bases del desarrollo de software
- El mercado de tecnologías de desarrollo low code crecerá un 23% en 2021

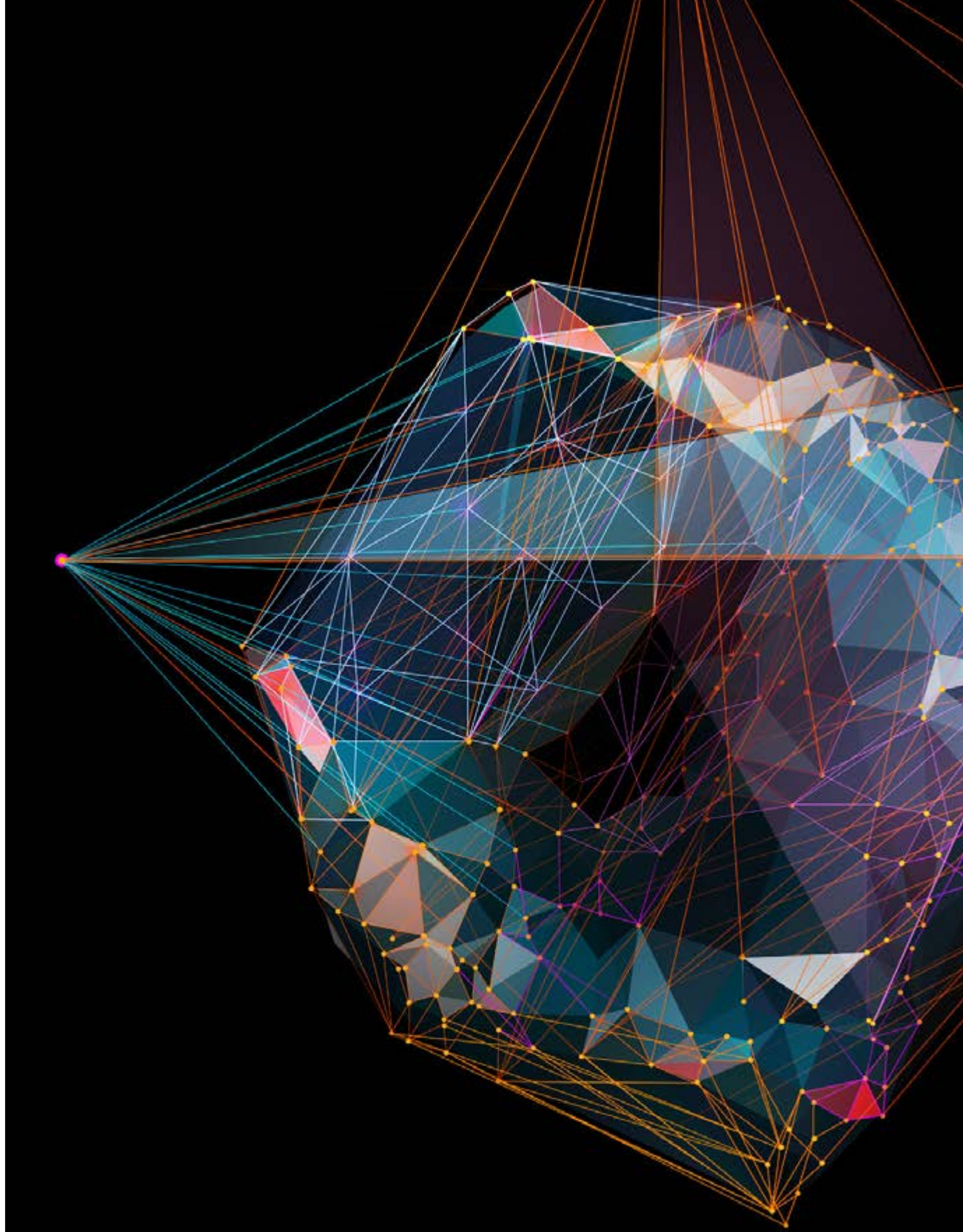
Si te ha gustado este artículo, compártelo

Insight Empowered

Know your data, empower your people, drive your future.

Protect, manage, archive, and gain strategic insight from your data, while driving employee empowerment and efficiency to support rapid digital change.

Learn more ›



#ENCUENTROSITTRENDS

Aplicaciones, ¿cómo desarrollo, entrego y gestiono mi software?

Aplicaciones móviles, tiendas online, redes sociales, aplicaciones para gestionar los clientes, colaborar y ser productivos... se han convertido en herramientas imprescindibles para comprar, vender, ofrecer nuevos productos, conocer al cliente, gestionar la empresa, mejorar el rendimiento... En definitiva, innovar para hacer crecer al negocio.

Para ello, estas aplicaciones necesitan recopilar información de los usuarios (y responderles según su comportamiento), de la empresa, de las cosas que se conectan a Internet... Deben manejar datos de diversa naturaleza, que se alojan en diferentes ubicaciones y plataformas; y saber quién tiene derecho de acceso. Así mismo, las aplicaciones están cada vez más automatizadas, exigen un desarrollo continuo, ser seguras, estar monitorizadas y ofrecer un óptimo rendimiento, adaptarse a cualquier tipo de plataforma, y gestionarse correctamente dentro de la pila de software con la que se trabaja en la empresa.

Para conocer de primera mano las principales tendencias en el mundo del desarrollo de aplicaciones, celebramos, dentro del ciclo de Encuentros IT Trends, una sesión online en la que se abordaron estas cuestiones tanto desde el punto de vista académico como empresarial. Para la ocasión reunimos a Susana Ladra González, vicepresidenta del CPEIG (Colegio Profesional de Enxeñaría Informática de Galicia) y directora del Campus Innova de la Universidad de A Coruña; José Jesús García Rueda, profesor en el Grado en Ingeniería del Software en el Centro Universitario U-tad; Miguel Ángel García Cumbreras, subdirector de la Escuela Politécnica de la UJA y coordinador de los títulos de ingeniería informática y director del Máster de Ciberseguridad de la misma Universidad; Raúl de La Fuente Lopes, solutions engineer de Couchbase; Luis Colino, director preventa de Micro Focus; y Arsénio Gil, CEO de SysDev.

Puedes ver la sesión clicando en la imagen y leer sus principales conclusiones en las siguientes páginas.

#ENCUENTROSITTRENDS

Desarrollo de aplicaciones: el software sigue de moda

Las aplicaciones son una pieza imprescindible para manejar equipos, redes y negocios. La cara más visible hoy en día del software son esas aplicaciones que usamos a diario para manejar todo lo que nos rodea, nuestro trabajo, nuestras compras, las redes sociales, las finanzas de una empresa, las relaciones con los clientes…

Estas aplicaciones tienen que responder de una manera rápida, ser seguras, tienen que integrarse con el resto de las aplicaciones de la empresa que, en algunos casos, son antiguas, y tienen que desarrollarse de una forma ágil. El desarrollo de software es un campo cambiante, con nuevos lenguajes de programación, nuevas arquitecturas,

(De arriba hacia abajo) Susana Ladra González (Colegio Profesional de Enxeñaría Informática de Galicia), José Jesús García Rueda, (Centro Universitario U-tad) y Miguel Ángel García Cumbreras (Escuela Politécnica de la UJA). Clica en la imagen para ver el vídeo.

“DevOps ha sido adaptado de forma importante en las empresas, y algunos informes estiman en un 40% el aumento de este tipo de profesionales”

SUSANA LADRA GONZÁLEZ, COLEGIO PROFESIONAL DE ENXEÑARÍA INFORMÁTICA DE GALICIA

nuevas metodologías... Descubrir qué tendencias se están imponiendo en este mundo de las aplicaciones y cómo las aprecian quienes están enseñando estos lenguajes y metodologías de desarrollo fue el objetivo de la primera mesa redonda de este Encuentro IT Trends titulado Aplicaciones, ¿cómo desarrollo, entrego y gestiono mi software?, en la que participaron Susana Ladra González, vicepresidenta del CPEIG (Colegio Profesional de Enxeñaría Informática de Galicia) y directora del Campus Innova de la Universidad de A Coruña; José Jesús García Rueda, profesor en el Grado en Ingeniería del Software en el Centro Universitario U-tad; y Miguel Ángel García Cumbreras, subdirector de la Escuela Politécnica de la UJA y coordinador de los títulos de ingeniería informática y director del Máster de Ciberseguridad de la misma Universidad.

Es evidente que vivimos en el mundo de las apps, y lo primero que quisimos saber es cómo ha evolucionado este segmento en los últimos años. En palabras de Susana Ladra González, “las apps han evolucionado de la mano del cambio de nuestra propia sociedad. Los dispositivos móviles están en alza y son los preferidos por los usuarios para tener todo al alcance de la mano. Han relegado claramente a los ordenadores de sobremesa, y destaca el crecimiento de aplicaciones para las empresas, pero también otras de propósito específico, como son las de salud, entretenimiento, compras... El año 2020 ha acelerado la Transformación Digital y ha marcado el mercado de las aplicaciones. Vemos una adopción generalizada por los servicios cloud e incorporación de la IA en muchas de estas aplicaciones, así como un incremento de apps de soporte de dispositivos interconectados, ya sea IoT o en el

“Simplemente hablar de experiencia de usuario ha colocado el foco sobre ello y es una oportunidad de seguir creciendo en este sentido”

JOSÉ JESÚS GARCÍA RUEDA, CENTRO UNIVERSITARIO U-TAD

hogar. Otras aplicaciones que vienen creciendo son las de RV o RA”.

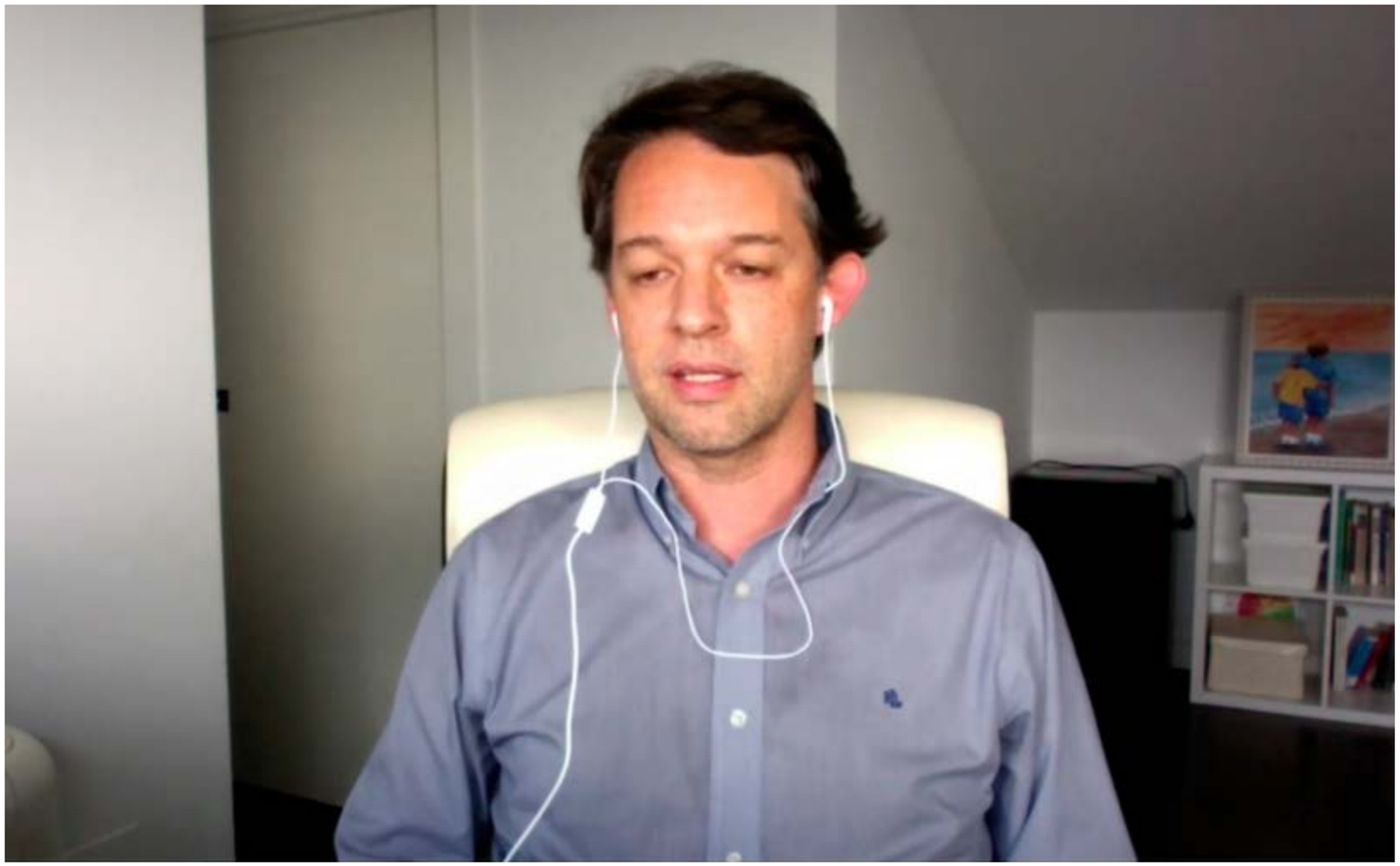
La experiencia de usuario se ha convertido en un asunto de primer orden con estas aplicaciones. Para José Jesús García Rueda, “es un reto y una oportunidad, porque hasta hace poco tiempo la usabilidad parecía algo secundario, pero simplemente hablar de experiencia de usuario ha colocado el foco sobre ello y es una oportunidad de seguir creciendo en este sentido. Igual que hemos acuñado el término, hemos creado al profesional, y de nuestras aulas salen especialistas capaces de diseñar la interacción con este tipo de aplicaciones, que conocen las técnicas, metodologías y conceptos que tienen que aplicar para mejorar esta experiencia, haciéndola no solo más amigable, sino también más sencilla, accesible y con experiencias adaptadas al tipo de app con la que tratemos en cada momento. Probablemente, incluir en nuestro equipo un profesional para el diseño de la interacción es la mejor forma de afrontar este reto”.

Un elemento esencial en el desarrollo es el lenguaje de programación. Hablando de los más utilizados a día de hoy, Miguel Ángel García Cumbreras señaló que “estamos en una revolución tecnológica continua. Esto, a nivel académico, en cuanto a lenguajes de programación, es difícilmente abordable, porque los planes de estudio no están preparados para soportar estas diversas olas de desarrollo que están llegando. Estudiamos algunos lenguajes de programación, pero lo importante, a nivel académico, es preparar a los alumnos para que puedan abordar cualquier tipo de lenguaje. Les damos los fundamentos para que puedan afrontar cualquier reto que se plantee en la empresa. Pero centrándonos en los lenguajes, para apps móviles se siguen usando mucho los lenguajes propios de los grandes fabricantes, mientras que en desarrollo web se siguen separando los lenguajes del front-end

y del back-end, pero son lenguajes muy declarativos, con una curva de aprendizaje bastante simple y buen rendimiento. Sin duda, tenemos un gran reto por delante para adaptarnos a las necesidades del mercado".

AGILIDAD DE DESARROLLO Y DESPLIEGUE

Si una cosa es demandada en este momento a nivel de desarrollo es la agilidad, y de ahí han surgido plataformas no-code o low-code. Según apuntó Susana Ladra González, "tradicionalmente eran necesarios grandes equipos de profesionales de desarrollo, algo con alto coste, y el objetivo era reducir estos costes optimizando y automatizando parte del código gracias al modelado. Las aproximaciones low-code son un reflejo de esa tendencia. Busca reducir la cantidad de código a escribir. La mayor parte del código se generaría de forma automática gracias a los modelos y solo hay que completar algunas partes que son más específicas o complejas. La idea es que los profesionales puedan centrarse en las partes de mayor complejidad o en las especificidades de los clientes, evitando las más rutinarias. Tienen un potencial increíble para revolucionar el mercado del software, porque podrían evitar mucho trabajo manual, creando aplicaciones con menores inversiones de dinero, tiempo y riesgos para los clientes". Otra cosa es el desarrollo no-code, apunta Ladra, "que permiten el desarrollo de apps simples en base a plantillas



"Estamos sacando al mundo laboral muy buenos ingenieros, pero el tiempo académico es finito, y hay que seguir formándose porque la seguridad y el desarrollo tienen un potencial muy importante y el papel de los profesionales va a ser fundamental"

MIGUEL ÁNGEL GARCÍA CUMBRERAS, ESCUELA POLITÉCNICA DE LA UJA

predefinidas, pero que generan aplicaciones con mucha menor flexibilidad".

Si ponemos el foco en el desarrollo de aplicaciones para empresas, y hablamos de nuevas tendencias y plataformas, José Jesús García Rueda comentó que "si hablábamos de la multitud de lenguajes, estas plataformas recogen el testigo y lo amplifican. Depende mucho del lenguaje elegido y del tipo de producto a desarrollar. Hablamos de decenas de frameworks diferentes que podemos utilizar. Cada vez van a ser más importantes las plataformas que permiten a las empresas desarrollar más allá de sus equipos específicos de programación, pero todavía queda terreno por avanzar en este sentido. A la hora de elegir entre la gran cantidad de plataformas hay que tener en cuenta también las necesidades del cliente y el conocimiento del equipo de desarrollo, porque uno de los riesgos es incluir en el proyecto tecnologías novedosas que nuestro equipo de desarrollo no haya probado nunca. Por la propia evolución, es algo que nos vemos obligados a hacer, pero no deja de ser un riesgo. Un equipo trabajando con herramientas que no conoce, va a aumentar de forma impredecible los tiempos de desarrollo y va a aumentar el número de errores en el código".

Otro elemento fundamental es la nube. Cuando hablamos del desarrollo y entrega de software, explicó Miguel Ángel García Cumbreras, "la nube se ha abierto ahora a todos los públicos. Se ha generalizado con unos servicios muy adaptados al uso, lo que permite dimensionar la estructura de cualquier proyecto sin una inversión importante. A eso se une el desarrollo ágil, con entregas parciales y constantes al cliente. La nube es fundamental para esto. Junto con esto, la normativa en cuanto al uso de la nube también ha acompañado, proporcionando seguridad en el despliegue y funcionamiento".

DEVOPS Y DEVSECOPS

DevOps y DevSecOps son otras dos tendencias claras de los últimos años. Para Susana Ladra, "hemos detectado demanda de expertos en estos enfoques. Las metodologías ágiles se han adoptado de forma masiva en el sector, y los equipos de trabajo necesitan una buena comunicación entre ellos en todas las fases. DevOps ha sido adoptado de forma importante en las empresas, y algunos informes estiman en un 40% el aumento de este tipo de profesionales. En el caso de DevSecOps, también es necesario, porque la seguridad es una prioridad, e integrar la seguridad desde el inicio es un enfoque diferente y cada día aumenta la demanda de estos profesionales, tanto en la parte más técnica como en la parte más cultural, porque estas metodologías requieren un cambio en la empresa".

En este sentido, cabe preguntar por el rol de las tecnologías de pentesting para poner a prueba las aplicaciones. En opinión de José Jesús García, "necesitamos fomentar el cambio de mentalidad y contar con la seguridad desde el primer minuto. Las tecnologías de pentesting nos permiten probar la seguridad una vez que el proyecto está armado, para asegurarnos de que todo está perfectamente protegido. Pero esto no sustituye, sino que complementa, la apuesta por la seguridad desde el inicio, pensando, incluso, en cómo se va a integrar en un sistema más grande".

Como conclusión sobre el futuro de los desarrolladores, Miguel Ángel García apuntó que desde el terreno académico "estamos sacando al mundo laboral muy buenos ingenieros, muy preparados, pero el tiempo académico es finito, y hay que seguir formándose porque la seguridad y el desarrollo tienen un potencial muy importante y el papel de los profesionales va a ser fundamental. La titulación más especializada de un ingeniero en seguridad de las aplicaciones va a tener su espacio propio, y las empresas deben entender que no todo el software lo pueden desarrollar los mismos perfiles, y el nivel de seguridad dependerá del nivel de capacitación de los equipos de trabajo". ■

#ENCUENTROSITTRENDS

Mejores prácticas para el desarrollo y gestión de aplicaciones

Toda la tecnología está cambiando rápidamente, pero si hay un área que lo está haciendo todavía más es el mundo del software, las aplicaciones, tanto a nivel de desarrollo como de entrega de las mismas, con cambios significativos que están teniendo un gran impacto en las empresas y los negocios. Conocer las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlos en producción y administrarlos, fue el objetivo de la segunda mesa redonda de este Encuentro IT Trends titulado Aplicaciones, ¿cómo desarrollo, entrego y gestiono mi software?, en la que contamos con la participación de Raúl de La Fuente Lopes, solutions engineer de Couchbase; Luis Colino, director preventa de Micro Focus; y Arsénio Gil, CEO de SysDev.

Tal y como explicaba Luis Colino, "desde hace dos o tres años estamos viendo

De arriba hacia abajo) Raúl de La Fuente Lopes (Couchbase), Luis Colino (Micro Focus), y Arsenio Gil (SysDev). Clica en la imagen para ver el vídeo.

“Hay que mantener la apuesta por estándares abiertos para no caer en errores del pasado”

RAÚL DE LA FUENTE LOPES, COUCHBASE

la evolución de todo lo que tiene que ver con el desarrollo de aplicaciones hacia el mundo Agile, y en este último período, provocado por la pandemia, ha habido cierta deslocalización de los equipos de desarrollo que ha impactado en este mundo Agile, que, normalmente, se apoya en equipos pequeños y concentrados con un gran nivel de colaboración. Todo esto ha tenido que pasar a un plano totalmente virtual, adoptando diferentes marcos de trabajo y escalando a toda la empresa, a la vez que se permite la convivencia con los aplicativos que no pueden moverse a este mundo ágil. El software legacy de las empresas es una realidad, y hay que hacer convivir ambos mundos”.

Para Raúl de la Fuente, “la creación de equipos multidisciplinares es una tendencia en los entornos Agile. La pandemia lo ha cambiado todo, incluso cómo nos relacionamos con el mundo, por lo que es posible que alguna de las aplicaciones, que fueron creadas para un propósito, no se puedan adaptar a la forma de interrelacionarnos que tenemos actualmente. Por eso, muchos de los planes de modernización de las organizaciones se han acelerado, y vemos ejemplos como el mundo contactless o la economía hogareña”.

En palabras de Arsénio Gil, “existe en este momento una necesidad brutal de las compañías para sobrevivir en este mercado. Ya no tenemos visibilidad de pedidos de clientes a dos o tres años, sino que tienes pedidos para meses o semanas. Los márgenes son más bajos, y tienes que reinventar cada día, y para eso necesitas información en tiempo real y fidedigna. La única solución es digitalizar tus procesos. Por eso, las aplicaciones son cada vez más fundamentales, el software es vital. Esta información correcta es lo que te va a ayudar a decidir, y las decisiones estarán muy marcadas por la calidad de esta información. Además, las fuentes de información son muy diferentes, y si ésta no está integrada para consultarla de forma

¿QUÉ BASE DE DATOS OFRECE MAYOR RENDIMIENTO EN ENTORNOS CLOUD?

Para este informe, Altoros utilizó el benchmark YCSB para comparar el rendimiento de tres productos populares de DBaaS NoSQL: Couchbase Cloud, MongoDB Atlas y Amazon DynamoDB. El informe mide su rendimiento relativo en términos de latencia y rendimiento para tres configuraciones de clúster diferentes y bajo cuatro cargas de trabajo distintas. A la vista de este documento, Couchbase Cloud tuvo un mejor rendimiento en todas las cargas de trabajo evaluadas, soporta operaciones de agregación, filtrado y JOIN en grandes conjuntos de datos sin modelar los datos para cada consulta, y garantiza la escalabilidad necesaria a medida que los clústeres y los conjuntos de datos aumentan de tamaño.

“Más allá de la adaptación de nuevos desarrollos, la mayoría de las organizaciones no han nacido en un entorno digital y no pueden comenzar el desarrollo desde cero en metodologías ágiles”

LUIS COLINO, MICRO FOCUS

fácil, será más complicado competir con quién sí cuenta con ello. Por tanto, es algo en lo que las empresas deben invertir”.

PAUTAS PARA DESARROLLAR UN BUEN SOFTWARE

Ante este panorama, apuntaba Luis Colino, “cuando entramos en un proceso de digitalización de las aplicaciones, la automatización de los procesos es clave, y todas las fases del desarrollo, el testeo, el despliegue… tiene que vivir en un mundo muy acelerado. Más allá de la adaptación de nuevos desarrollos, la mayoría de las organizaciones no han nacido en un entorno digital y no pueden comenzar el desarrollo desde cero en metodologías ágiles. Precisamente, donde mayor necesidad estamos detectando es en digitalizar lo que ya existía, en transformar a la nueva era lo que tenían estas organizaciones. Ahí detectamos problemas a la hora de recopilar y visualizar toda la información, sobre todo en proyectos mixtos donde no todo es Agile. Hay que dar una prioridad máxima a los objetivos del negocio, cada euro de gasto tiene que estar relacionado con un objetivo de negocio claro. En resumen, aceleración máxima ayudando a las organizaciones a transformarse desde su tecnología anterior”.

Algunos expertos indican que no se trata de adoptar tecnología por adoptarla, y, en este sentido, señalaba Raúl de la Fuente que “hay que tener cuidado con las palabras de moda, porque simplemente por el hecho de mover datos o aplicaciones de sistemas legacy a la nube ya siento que me estoy modernizando, pero los problemas que tenía los sigo teniendo. Hay que ver cómo reducir complejidades, aumentar rentabilidades. Hay que buscar la simplicidad operacional, contando con software más rápido que implique menos soporte y me permita centrarme en mi negocio”.

Pero la pregunta es si todo esto ayuda a reducir el impacto de la falta de recursos. Para

“La única solución de las empresas para adaptarse al mercado es digitalizar tus procesos, y por eso las aplicaciones son cada vez más fundamentales”

ARSÉNIO GIL, SYSDEV

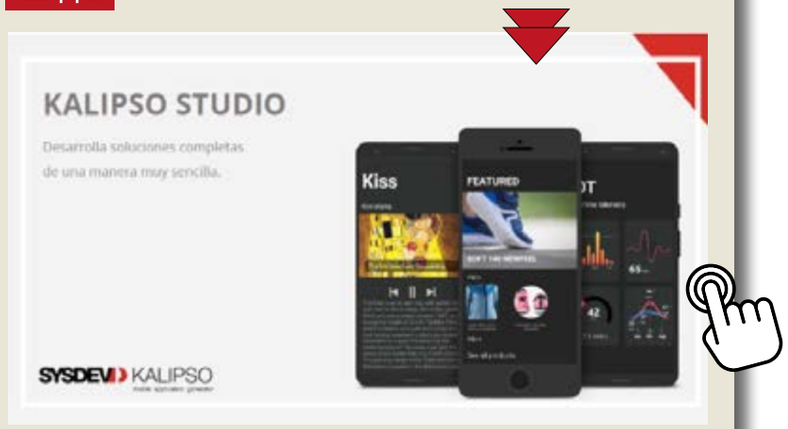
Arsénio Gil, “éste es un problema que viene desde hace tiempo y que se está agudizando. Las metodologías de low-code pueden ayudar a reducir este problema, porque aceleran los ciclos de desarrollo reduciendo los errores, pero, además, puedes reciclar recursos humanos de otras áreas para ayudar en estas tareas. Asimismo, puede ayudar a resolver también el problema de la retención de talento, sobre todo en las economías más pequeñas. Estas plataformas permiten tener más recursos disponibles y ayudar mucho a desarrollar soluciones para los clientes”.

CONVIVENCIA DE APLICACIONES ÁGILES Y SOFTWARE HEREDADO

Evidentemente, es una realidad en las empresas la convivencia del software Agile con el software legacy. Para Luis Colino, “si lo que tienes es válido para tu objetivo, es mejor no cambiarlo. En la complejidad del mundo híbrido no hay blancos y negros, hay muchos grises. Podemos cubrir necesidades específicas para mejorar la calidad de los datos o el resultado sin necesidad de remplazarlo todo porque es más moderno. Primero, analiza la función de una solución y nosotros te ayudamos a mejorarlo. Esto ayuda mucho en la transformación digital. Otra cosa es si necesitamos mejorar el proceso o el software, no se trata de cambiarlo porque sí, sino de mejorarlo en función de lo que necesitemos”.

Para Raúl de la Fuente, “quizá hay que decidir qué va a pasar con estas aplicaciones. Hemos de tener clara la evolución de estas aplicaciones y la gestión del dato antes de tomar una decisión sobre ello”. Pero sí es necesario integrarse con otras piezas de las TI de la empresa. “Es imprescindible que la tecnología interactúe bien con el resto de elementos de las TI. La

¿QUÉ ES KALIPSO STUDIO?



Kalipso Studio es un generador de aplicaciones móviles que permite el desarrollo sin necesidad de programación compleja. Con una interfaz sencilla, permite a sus usuarios desarrollar proyectos móviles para Windows Android e iOS. Entre las principales características de esta herramienta destacan la capacidad para el desarrollo de aplicaciones nativas en un entorno multi OS y multi lenguaje con conexión de Base de Datos Online/Offline, control de lector de código de barras para las principales marcas de hardware y sistemas RFID/NFC.

forma de convivir también es importante. Por ejemplo, si hablamos de bases de datos, Couchbase puede convivir con una base de datos tradicional manteniendo la correlación de los datos, lo que nos permite aliviar las cargas en los procesos de migración", continuó.

Hemos visto que otra tendencia es el desarrollo con plataformas low-code. Pero ¿cómo está impactando en las organizaciones? En opinión de Arsénio Gil, "el objetivo de estas plataformas es hacer más en menos tiempo, y en un mercado tan competitivo es importante que las empresas dibujen estrategias para incorporar clientes, pero también para mantenerlos. Por esto es necesario digitalizar los procesos de manera rápida para no perder oportunidades. Además, las nuevas tendencias tecnológicas son cada vez más necesarias en la creación de procesos de interacción con los usuarios, y este tipo de plataformas te pueden ayudar mucho utilizando lo que ya está modelizado. Por tanto, las compañías van a seguir integrando estas plataformas en las empresas".

Cambios a tener en cuenta

El mundo de las TI es cada día más híbrido y multicloud, y esto impacta también en el desarrollo de aplicaciones. Para Raúl de la Fuente, "es una tendencia obvia para dar más libertad y flexibilidad al cliente. Nosotros apostamos por ser lo más abiertos posibles, pudiendo desplegar Couchbase en la propia red privada virtual del cliente, lo que nos permite no tener que redefinir políticas de seguridad o de interconexión. Además, tenemos una única consola para administrar todos los elementos dentro de la infraestructura del cliente".

Y para Luis Colino, la experiencia del cliente es esencial. "Una de las partes principales del uso de las aplicaciones es la usabilidad para el usuario. Desde el punto de vista del desarrollador, nos estamos centrando mucho en la Inteligencia Artificial a la hora de definir una estrategia de pruebas. Además, esta IA nos permite que un script sea omnicanal, que nos permita ser independiente de plataforma, además de automatizar y a agilizar los test de las aplicaciones".

También tiene un gran impacto en esta experiencia del usuario la seguridad. Para Arsénio Gil, "el coste de no tener seguridad o tener una seguridad baja, va a ser mayor que el de apostar por la seguridad desde el principio. Tenemos que estar seguros al cien por cien, porque si te equivocas vas a poner a tu compañía en riesgo. No es una opción, es una obligación".

CONVIENE NO OLVIDAR

En opinión de Raúl de la Fuente, "hay que mantener la apuesta por estándares abiertos para no caer en errores del pasado".

Por su parte, Luis Colino reconocía que "en alguna ocasión vamos a tener un problema de seguridad, pero lo importante es estar preparado para ello, incluyendo la seguridad en todos los pasos del camino, y ser capaces de reaccionar de manera rápida, ágil y efectiva".

Finalizaba Arsénio Gil apuntando que "es básico que hagamos un análisis en profundidad de lo que queremos y necesitamos antes de escribir una línea de código. Es algo esencial, pero no todo el mundo lo hace. Además, hay que tener plataformas de testeo a todos los niveles. Y, sobre todo, no dejar de lado la experiencia del usuario. Es algo fundamental". ■

MÁS INFORMACIÓN

- Cómo elegir una base de datos para tus aplicaciones móviles
- Cómo elegir una plataforma de Enterprise Agile
- Kalipso Studio: Características

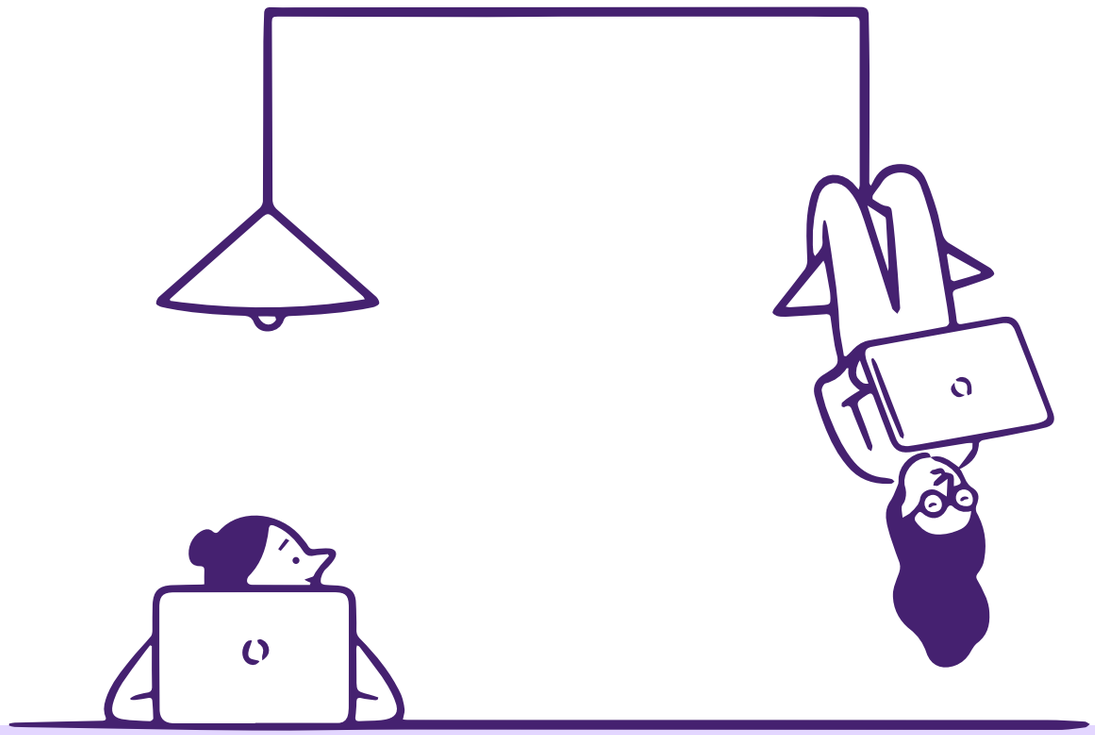
Mejores prácticas para el desarrollo y gestión de aplicaciones

“Todas las organizaciones tienen un valor basado en el cuidado de sus aplicaciones” (Couchbase)

“Nos anticipamos para adaptarnos a la necesidad real de una aplicación o servicio” (Micro Focus)

“Kalipso Studio crea soluciones complejas de forma sencilla con tecnología Low Code” (SysDev)

Tus empleados
se merecen una
tecnología tan
única como ellos.



citrix™

it TRENDS

Pros y contras de los futuros modelos de trabajo remoto e híbrido

En el último año, los beneficios que aporta el teletrabajo han salido a la luz, y muchas empresas antes reticentes se han planteado adoptar modalidades de trabajo remoto o híbrido para cuando la pandemia se haya estabilizado. Pero los trabajadores no solo han percibido ventajas por trabajar desde casa, ya que la falta de planificación y otros problemas organizativos les ha generado altos niveles de estrés y ansiedad, lo que afecta al rendimiento. Y ahora están preocupados porque las empresas no están teniendo en cuenta este factor ni sus comentarios al respecto a la hora de diseñar el puesto de trabajo del futuro, y por la falta de información al respecto.

Para muchas organizaciones la imposición del teletrabajo durante la pandemia ha sido un gran descubrimiento, ya que antes no creían que se pudiese implantar con éxito a esta escala, o ni siquiera se lo planteaban. Pero a lo largo de este año muchas han comprobado que el rendimiento se ha mantenido o, incluso, ha aumentado. Por ello, ahora se plantean un esquema organizativo basado en el teletrabajo o en modalidades híbridas, que combinan horarios o etapas presenciales con el puesto laboral remoto.

La percepción de los trabajadores es bien distinta, porque en muchos casos la orquestación de esta modalidad laboral no ha sido adecuada, y también les ha perjudicado de cierta forma. Según los estudios más recientes, un elevado porcentaje de personas se han encontrado teletrabajando fuera de horas, ya sea atendiendo llamadas, emails o realizando sus labores más allá de la jornada normal. Y se ha detectado un gran aumento de los niveles de ansiedad, estrés y agotamiento, algo que está aumentando a medida que se acercan los cambios que redefinirán el modelo laboral en su empresa.

Según una reciente investigación realizada por McKinsey, los empleados necesitan tener más certeza sobre la forma en que se conformará el puesto de trabajo híbrido y remoto del futuro. Cada vez más voces se alzan solicitando más claridad a este respecto, y que se atiendan sus peticiones y opiniones a la hora de diseñar cómo se trabajará en el futuro. Porque consideran que esta presión acaba minando las fuerzas de los trabajadores, que se sienten cada vez más insatisfechos, y esto acaba afectando a las relaciones interpersonales con los compañeros de trabajo, a su vida personal y también a la productividad laboral.

La encuesta realizada por esta consultora revela que la principal fuente de ansiedad de los trabajadores proviene de que los empleados todavía no han sido debidamente informados sobre cómo va a organizar su empresa el modelo de trabajo. Porque, aunque muchas han comunicado su intención de adoptar el trabajo virtual híbrido o el teletrabajo, pocas han explicado cuáles serán las pautas, políticas, expectativas y enfoques que seguirán con el suficiente grado de detalle.

Esto suscita muchas dudas entre los empleados, que demandan una mejor comunicación por parte de los líderes, incluso si todavía no han definido claramente los cambios que van

Los empleados que reciben una comunicación más detallada por parte de la empresa se sienten en general más integrados en la organización, y esto tiene un reflejo directo en la productividad

EL TRABAJADOR EXIGE MÁS CAPACIDADES DIGITALES Y APUESTA POR LOS ENTORNOS LABORALES HÍBRIDOS

a realizar. Y, según McKinsey, las empresas que han tenido esto en cuenta registran mayores niveles de satisfacción entre sus trabajadores, que se han traducido en una mayor productividad general y en un mayor bienestar personal. Para tener una idea más clara de la situación los responsables d esta encuesta han elaborado una lista con los factores que más preocupación y ansiedad causan entre los trabajadores.

SENTIMIENTO DE INCLUSIÓN

Los empleados que reciben una comunicación más detallada por parte de la empresa se sienten en general más integrados en la organización, y esto tiene un reflejo directo en la productividad. Según la encuesta, los empleados que se sienten más incluidos gracias a esta información tienen casi cinco veces más posibilidades de incrementar su rendimiento. Por ello, los expertos recomiendan incrementar la frecuencia y el grado de detalle de las comunicaciones, tanto para informar de qué decisiones se han tomado como para avanzar las opciones que se barajan de cara al futuro.

PROBLEMAS DE COMUNICACIÓN

Los resultados de esta investigación revelan que el 40% de los empleados aún no ha sido informado sobre la visión que tiene la organización de cara al futuro de su puesto de trabajo, y un 28% afirma que la información que le ha llegado es insuficiente. Esto es un factor generador de estrés que afecta negativamente al compromiso del trabajador con la organización.

ANSIEDAD EN EL PUESTO DE TRABAJO

Directamente relacionado con el punto anterior, las empresas que apenas se comunican con los trabajadores sobre cómo será el trabajo tras la pandemia, o que no lo hacen, están elevando el malestar entre sus empleados. Esto se traduce en ansiedad, estrés y problemas con sus colegas, entre otras consecuencias, y en una consiguiente pérdida de rendimiento. Esto supone pérdidas económicas que McKinsey cifra en hasta un trillón de dólares al año a nivel mundial.

TRABAJADORES "QUEMADOS"

El efecto "burn-out es un viejo enemigo de muchos trabajos en los que las personas deben dar el máximo, siguiendo un ritmo que no se puede soportar de forma indefinida. Pero este fenómeno de desgaste se está expandiendo a medida que aumenta la ansiedad y el estrés de los trabajadores, en puestos en los que antes no era tan común. Esta encuesta revela que casi la mitad de los empleados sienten síntomas de agotamiento excesivo en el trabajo, y los expertos afirman que este es uno de los problemas que más efecto tienen en el rendimiento laboral. Además, alerta de que estas cifras podrían se mucho peores, ya que quienes se encuentran en este estado tiene

menos probabilidad de responder a encuestas como esta, por lo que hay una gran bolsa potencial de trabajadores quemados que no aparecen aquí. Asimismo, destaca que muchas de las personas que han llegado a este punto probablemente ya hayan abandonado su trabajo a consecuencia del alto nivel de exigencia.

COMPARTIR INFORMACIÓN

Según McKinsey, la falta de comunicación organizacional hace que los empleados que no reciben suficiente información tienen casi tres veces más probabilidades de acabar quemados que quienes sí la reciben. Por ello, los expertos instan a las empresas a que mejoren e incrementen sus comunicaciones con la fuerza laboral, compartiendo información sobre sus intenciones en materia laboral, incluso si no están seguros de cómo van a diseñar el futuro puesto de trabajo.

MÁS FLEXIBILIDAD

Más de la mitad de los empleados encuestados para realizar esta investigación afirman que les gustaría que su organización adoptara modelos híbridos de trabajo virtual que fuesen flexibles, en los que los empleados puedan combinar mejor la presencia física con el teletrabajo. Y los expertos afirman que atendiendo y evaluando cuidadosamente estas peticiones, las empresas pueden diseñar mejor el modelo de organización laboral que adoptarán tras la pandemia, lo que mejorará la cultura empresarial, la vinculación de los trabajadores con la organización y los resultados a todos los niveles.

RIESGO DE FUGA DE TALENTO

Más de una cuarta parte de los encuestados dice que se plantearía cambiar de empresa si ésta decide volver al modelo de trabajo 100% presencial anterior a la crisis. Aunque esto depende de las políticas que acaben adoptando las empresas, de la disponibilidad de otros empleos con condiciones y salarios iguales o mejores, y del papel que adopte la automatización en el rediseño del puesto de trabajo del futuro.

4 RECOMENDACIONES PARA IMPLEMENTAR UN MODELO DE TRABAJO HÍBRIDO

Más de la mitad de los empleados encuestados afirman que les gustaría que su organización adoptara modelos híbridos de trabajo virtual que fuesen flexibles

PREDOMINIO DEL TELETRABAJO

Para más de la mitad de los trabajadores gubernamentales y corporativos entrevistados el teletrabajo debería ser la fórmula dominante en el modelo de trabajo híbrido ideal, combinando al menos tres días a la semana de trabajo remoto con uno o dos días a la semana de modalidad presencial, como mucho. Y los investigadores destacan las respuestas en este sentido de los empleados de Estados Unidos, donde casi un tercio de la fuerza laboral preferiría teletrabajar a tiempo completo.

CONCILIACIÓN LABORAL Y FAMILIAR

El grupo de los trabajadores con hijos siempre ha sido el más proclive a aceptar e, incluso, solicitar un puesto de trabajo remoto, y tras este año de experiencia su preferencia ha ido cambiando hacia un modelo híbrido flexible, y solo un 8% ve con buenos ojos un trabajo completamente presencial. Por su parte, los trabajadores sin hijos menores de edad tienen casi tres veces más probabilidades de preferir esta fórmula, aunque la mayoría aún escogería un modelo flexible.

INQUIETUDES Y EXPECTATIVAS DE CARA AL FUTURO

Actualmente, los trabajadores están sometidos a mucho estrés por la incertidumbre que le genera la falta de comunicación sobre cómo cambiará, si lo hará, su puesto de trabajo. Entre tantas expectativas e inquietudes muchos están esperando que su organización opte por más flexibilidad, por reforzar las compensaciones competitivas y el bienestar de los empleados. Pero también les preocupa mucho cómo será su trabajo en el futuro, y cómo afectará a su vida en general la adopción de nuevas modalidades laborales que quizá no se ajusten a sus capacidades o esperanzas. Además, el temor físico por el riesgo sanitario también se ha convertido en un factor a destacar, y también el deterioro de las relaciones y la vinculación con los compañeros de trabajo, a causa de la distancia.

CUESTIÓN DE POLÍTICA

Por último, los expertos de McKinsey señalan que los empleados están muy preocupados por la forma que tomarán los acuerdos laborales y las políticas en este sentido, y temen que las nuevas fórmulas laborales no tengan en cuenta el bienestar de los trabajadores y la cohesión social, buscando más productividad con modalidades que acaben afectando negativamente a su trabajo y a su productividad. Así, más de un tercio de los entrevistados situaron entre las cinco políticas más importantes para ellos la claridad en los horarios y las expectativas de colaboración. Otras políticas de colaboración que consideran importantes son las que contemplan en uso de tecnologías para la preparación y organización de reuniones remotas desde las oficinas, y las pautas que se seguirán para el trabajo con documentación.

También han dado mucha importancia a las herramientas de colaboración y en la capacitación para trabajar con ellas, y en el reembolso de la inversión en dotarse a uno mismo de herramientas para trabajar en remoto, que en algunos casos ha supuesto inversiones elevadas. Y, para más de una cuarta parte de los encuestados, las principales políticas a tener en cuenta son las de microconectividad, tanto en eventos de equipos pequeños como en las estrategias de escucha y respuesta. ■

MÁS INFORMACIÓN

- Informe Empleos Emergentes 2020
- Mejorando la experiencia del trabajador remoto
- De vuelta a la oficina

COBRA TUS FACTURAS EN 24 HORAS

GRENKE
FAST // FORWARD // FINANCE

Y AYUDA A TUS CLIENTES CON SUS PROBLEMAS DE LIQUIDEZ

CONTACTA CON NOSOTROS
91 630 56 72 o
contigo@grenke.es

// VENTA POR CUOTAS

// RIESGO CERO DE IMPAGO

¿Alguna vez te has encontrado con clientes que necesitan tu tecnología, pero no tienen liquidez suficiente para pagarla? ¿Esto supone un problema a la hora de cerrar tus operaciones comerciales? Tus clientes necesitan la tecnología y el equipamiento más novedoso, pero esto resulta complicado de conseguir sin que comprometa la liquidez de su negocio. El renting tecnológico y de equipamiento de GRENKE es la solución perfecta, tus clientes pagan cómodas cuotas mensuales, mientras tú recibes el pago al contado del 100 % de tus ventas.

WWW.GRENKE.ES

#ENCUENTROSITTRENDS

Mejorando la experiencia del trabajador remoto

Para 2021, tres de cada diez empleados trabajarán desde sus casas. El teletrabajo se ha impuesto como una modalidad habitual de trabajo en todo tipo de organizaciones para aportar la flexibilidad que los empleados demandan, pero también para garantizar la continuidad de los negocios en caso de incidentes. Esté donde esté, el trabajador necesita acceder a todos los recursos empresariales, pero desde su casa, muchas veces con su propio equipo y casi siempre con su conexión a internet, lo que requiere aplicar tecnologías y modelos de seguridad específicos.

Trabajar en remoto también ha impuesto otra dinámica en las reuniones, ahora online y virtuales, necesarias para mantener la marcha de la empresas y los vínculos con la misma.

En IT Trends hemos reunido a diversos expertos para abordar los retos del teletrabajo y cómo avanzar en la productividad y el mejor desempeño de los empleados ahora que lo habitual es trabajar fuera de la oficina, en una sesión titulada Mejorando la experiencia del trabajador remoto, que constó de dos mesas de debate: la primera de ellas, con profesionales del mundo académico, técnico y de Recursos Humanos, y la segunda con especialistas en tecnologías de comunicaciones, seguridad, dispositivos o conexiones que involucran el trabajo remoto. ■

#ENCUENTROSITTRENDS

Nuevas modalidades de trabajo: el empleado remoto

Sonia Fernández Palma, consultora educativa y divulgadora en Ciberseguridad y Alfabetización Digital y miembro de Women4Cyber; Antonio Ramos, Vocal de la Junta Directiva de ISACA Madrid y Rafael Cubero Saiz, Head of People de Tecnatom Group, conversan sobre el impacto del teletrabajo en las empresas.

NUEVAS MODALIDADES DE TRABAJO: EL EMPLEADO REMOTO

Durante el Encuentro IT Trends titulado Mejorando la experiencia del trabajador remoto, tuvo lugar un primer debate cuyo objetivo fue examinar el teletrabajo y su impacto tanto en los empleados como en las empresas y departamentos de recursos humanos. Para ello se contó con la participación de So-

nia Fernández Palma, consultora educativa y divulgadora en Ciberseguridad y Alfabetización Digital y miembro de Women4Cyber; Antonio Ramos, Vocal de la Junta Directiva de ISACA Madrid; y Rafael Cubero Saiz, Head of People de Tecnatom Group.

Para Sonia Fernández Palma "lo que hemos vivido durante estos últimos meses ha sido y sigue siendo una situación excepcional que requería, sobre todo en el principio, de una actitud extraordinaria, tanto por parte de empresas como de personas de los trabajadores".

La respuesta de las organizaciones empresariales frente al cambio de modelo de negocio ha sido mixta, aseguró Antonio Ramos, quien añadió que muchas empresas afrontaron esta situación "con mucha premura, con mucha improvisación y corriendo muchos riesgos de seguridad". En todo caso, "el que más y el que menos ha sacado un gran aprendizaje. Creo que a partir de ahora podemos afrontar estas situaciones con mucha más experiencia, con mucho más conocimiento y sabiendo un poco mejor a qué nos enfrentamos".

En Tecnatom Group, "la situación se vivió como algo positivo porque lo que los empleados percibieron es que les estábamos cuidando", dijo Rafael Cubero, explicando que hubo un trabajo importante en el área de comunicación para que las relaciones entre las personas y con la empresa no se viesen perjudicadas. La empresa se apoyó en una red social empresarial creando grupos "para poder estar más unidos y no tener sentimientos de soledad", así como otras actividades, campañas y rutinas para mantener activas las relaciones entre empleados y con la empresa". Añadió que la clave fue una coordinación entre las áreas de IT, el área de recursos humanos y el área de servicio médico.

"Para mí, el gran secreto del teletrabajo es la formación"

SONIA FERNÁNDEZ PALMA, CONSULTORA EDUCATIVA Y DIVULGADORA EN CIBERSEGURIDAD Y ALFABETIZACIÓN DIGITAL Y MIEMBRO DE WOMEN4CYBER SPAIN

Asegurando que el principal activo de una empresa son las personas, y que es a las personas a las que hay que cuidar, dijo Sonia Fernández, que no sólo hay que darles herramientas a los empleados, sino formarles para saber utilizarlas. “Para mí el gran secreto es la formación”, aseguró esta consultora mencionando de manera específica la formación en habilidades digitales, muy especialmente en materia de seguridad, así como las habilidades sociales porque “no podemos pensar que como tenemos una pantalla delante, eso es una barrera”.

Además de las ventajas que aporta, como permitir la continuación del negocio, ¿qué retos está planteando este nuevo modo de trabajo? Para Antonio Ramos los retos son muchos “porque trabajar en este entorno digital hace que tengamos que cambiar a la forma en la que veníamos trabajando”, desde temas organizativos a temas técnicos, gestión del conocimiento y de seguridad.

“Lo principal es el negocio y ese es el punto de partida desde donde arrancamos”, dijo Rafael Cubero cuando se le plantea cómo se ha unido el área tecnología, negocio y recursos humanos en tiempos de pandemia. Explicó que algunos perfiles no podían dejar de ir a la oficina, pero que “trabajamos en crear el entorno más seguro posible”, mientras que a todas las personas que podían hacer el trabajo remoto se les dieron todas las posibilidades para hacerlo. En todo caso, en Tecnatom Group no se partía de cero, ya que se contaba con un sistema de trabajo a distancia que “ayudó a que la gente ya supiese a qué se enfrentaban”. Además, el departamento de sistemas tuvo varias tareas a realizar, desde asegurarse que todo el mundo tuviese un portátil para poderse llevar a casa, o una pantalla, reforzar las VPNs o “tareas de formación de todo el portfolio de herramientas de comunicación colaborativas que


Antonio Ramos, ISACA

“Trabajar en este entorno digital hace que tengamos que cambiar la forma en la que veníamos trabajando”

ANTONIO RAMOS, VOCAL DE LA JUNTA DIRECTIVA, ISACA MADRID

tenemos a nuestra disposición y que mucha gente no conocía".

Sobre cómo mejorar la experiencia del teletrabajo, apuntó Sonia Fernández que es importante que el teletrabajo tenga unas normas claras, "que se sepa a qué debemos atenernos". Añadió esta consultora y miembro de la asociación Women4Cyber Spain que es importante aceptar "que ya no vivimos en el mundo en el que vivíamos, sino que vivimos en otro con unas posibilidades infinitas y unos beneficios muy grandes, pero también con algunos inconvenientes y muchos retos por delante".

Respecto al modelo híbrido de trabajo dijo Antonio Ramos que hacer convivir el modelo tradicional asistencial con el remoto es un reto desde el punto de vista tecnológico. Aseguró que no está definida una situación en la que "tengo que ser capaz de hacer convivir un mundo en el que parte del tiempo se va a estar en la oficina y parte del tiempo fuera", algo que impacta a la hora de dimensionar tanto el tamaño de una oficina, las conexiones web, etc.

Para Rafael Cubero, una de las lecciones aprendidas de la explosión del teletrabajo es que el trabajo a distancia se va a quedar y "se ha convertido en un factor más de la propuesta de valor que todas las empresas ofrecen a sus empleados y que va a reforzar el sentimiento de pertenencia a las empresas que apuestan por ello". En cuanto a los planes de futuro en Tecnatom Group, estos pasan por establecer las reglas del trabajo a distancia, así como finalizar "un modelo conexión digital que favorezca la conciliación, pero con cuidado de que no se inmiscuya demasiado en nuestra vida personal". Apuntó también Rafael Cubero que se trabaja en la formación de todas herramien tas colaborativas, la reorganización de espacios en sede para crear unos espacios más amplios y más colaborativos o una mayor inversión en TI. ■


Rafael Cubero, Tecnatom Group

"El teletrabajo se ha convertido en un factor más de la propuesta de valor de las empresas"

RAFAEL CUBERO SAIZ, HEAD OF PEOPLE, TECNATOM GROUP

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

Los **equipos de investigación de amenazas de SonicWall Capture Labs** proporcionan a las empresas, pymes, agencias gubernamentales y otras organizaciones inteligencia de ciberamenazas existentes para proteger a su personal distribuido contra una superficie de ataque en continua expansión.

Al proporcionar una visión completa de estos datos, el Informe de Ciberamenazas 2021 de SonicWall muestra **cómo piensan y operan los cibercriminales**, ayudando a las organizaciones a prepararse mejor para las amenazas del futuro.

OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

▼ 43%

EL MALWARE CAE AL NIVEL MÁS BAJO DESDE 2014

+1 días

IDENTIFICACIÓN MÁS RÁPIDA DE MALWARE "NUNCA ANTES VISTO"

▲ 62%

EL RANSOMWARE ALCANZA UNA CIFRA RÉCORD

▲ 74%

INSPECCIÓN DE MEMORIA PROFUNDA MEJOR QUE NUNCA

▲ Máx. 3 años

EL CRYPTOJACKING HA VUELTO

▲ 66% IOT

EL MALWARE DE IOT AUMENTA UN 66%

▲ 20%

INTENTOS DE INTRUSIÓN EN CONSTANTE CRECIMIENTO

#ENCUENTROSITTRENDS

Cómo mejorar la experiencia del trabajador remoto gracias a la tecnología

Más de la mitad de los trabajadores apoya el teletrabajo. Es más, según una encuesta de la compañía de consultoría de gestión Korn Ferry, un 64% reconoce ser más productivo trabajando desde casa, además de valorar otros aspectos como el ahorro de tiempo en los desplazamientos y una mejor conciliación familiar y laboral.

Trabajar en remoto también ha impuesto otra dinámica en las reuniones, ahora online y virtuales, necesarias para mantener la marcha de las empresas y los vínculos con la misma, todos ellos temas tratados en el #EncuentroITTrends Mejorando la experiencia del trabajador remoto, en el que participaron Melchor Sanz, Direc-

Melchor Sanz (HP Inc.); Iván Rodríguez Santos (Citrix); Mª José Fernández (Granke); Agustín Sánchez Fonseca (NFON); Sergio Martínez (SonicWall); Iván Mateos Pascual (Sophos); y Guillermo Fernández (WatchGuard), durante el debate.

“Las pymes han recibido ayudas para hacer frente a esta digitalización y al teletrabajo”

Mª JOSÉ FERNÁNDEZ, BRANCH MANAGER, GRENKE

tor de Tecnología y Preventa de HP Inc.; Iván Rodriguez Santos, Lead Sales Engineer de Citrix Iberia; Mª José Fernández, Branch Manager de Grenke; Agustín Sánchez Fonseca, Responsable de desarrollo de negocio de NFON Iberia; Sergio Martínez, Iberia Regional Manager de SonicWall; Iván Mateos Pascual, Sales Engineer de Sophos; y Guillermo Fernández, Iberia Sales Engineer Manager de WatchGuard.

Lo primero que quedó claro durante el segundo encuentro de este evento online es que los empleados no estábamos preparados para teletrabajar. Lo aseguraba Melchor Sanz, Director de Tecnología y Preventa de HP Inc., afirmando que “estábamos preparados para teletrabajar un ratito, pero no ocho o nueve horas”. Mencionó el directivo que es la tecnología la que puede ayudar a que las empresas sean más eficientes y que los trabajadores estén trabajando de una manera más confortable desde cualquier ubicación, y que todo ello se haga sin que existan mayores riesgos de seguridad.

Más de un año después de la pandemia, cuando damos por hecho que el puesto de trabajo ya va a ser híbrido, ¿cómo será el puesto de trabajo del futuro? Para Iván Rodríguez Santos, Lead Sales Engineer de Citrix Iberia, la clave está en aplicaciones que sean capaces de conectar usuarios y datos a través de cualquier tipo de dispositivo y a través de cualquier ubicación. El éxito, asegura, llega “cuando somos capaces de brindar esta experiencia de usuario de forma consistente”.

Hablar de teletrabajo es hablar de digitalización, un proceso que, según Mª José Fernández, Branch Manager de Grenke, ya estaba en ciernes cuando llegó la pandemia. La crisis sanitaria llevó a las empresas a acelerar sus planes hasta el punto de que en estos meses se ha avanzado lo que se hubieran tardado diez años.

“No vale cualquier dispositivo para acceder a cualquier entorno”

MELCHOR SANZ, DIRECTOR DE TECNOLOGÍA Y PREVENTA, HP INC.

En lo que respecta a las herramientas de comunicación, que en realidad existen desde hace mucho tiempo, planteó Agustín Sánchez Fonseca, responsable de desarrollo de negocio de NFON Iberia, que no se les está sacando el máximo provecho por una cuestión cultural y por una falta de proceso a nivel de empresas; “al trabajador se le dan unas herramientas, pero hay que dotarles de objetivos y de procesos”. Aseguró también que, si antes se estaban infrautilizando, se ha pasado al extremo contrario y se utiliza

“La clave está en aplicaciones capaces de conectar usuarios y datos a través de cualquier tipo de dispositivo y ubicación”

IVÁN RODRIGUEZ SANTOS, LEAD SALES ENGINEER, CITRIX IBERIA

la videoconferencia para todo o el móvil demasiado cuando “no vale para un uso corporativo, ya que ni permite asegurar o dar la máxima calidad de atención, ni asegura la máxima disponibilidad”.

La digitalización acelerada y la falta de preparación para el teletrabajo han tenido un impacto en la seguridad de las empresas. El teletrabajo, explicó Sergio Martínez, director general de SonicWall Iberia, implica que accedemos a aplicaciones corporativas y a datos desde cualquier sitio, que el perímetro de seguridad ha desaparecido y que la superficie de exposición se ha incrementado. Ahora, aseguró el directivo “se hace necesaria una nueva seguridad”, que debe tener en cuenta cinco ideas sencillas: defensa por capas, visibilidad, ser capaces de detectar lo desconocido, realizar un acceso remoto seguro, y todo ello con un TCO y un coste disruptivo.

Desde Sophos Iberia, Iván Mateos, sales engineer de la compañía, apuntó que para que una solución funcione, para que algo se adapte y se pueda utilizar, tiene que ser fácil, tiene que ser “descomplicado”: “los usuarios tienen que poder trabajar desde casa como lo hacían desde la oficina y sin cargarles de responsabilidad”. Aseguró que muchas veces se tiende a echarle la culpa al usuario de lo que pasa y que, si bien el usuario tiene que saber hacer muchas cosas, hay otras muchas que no tiene por qué saber. “La solución es que no se tenga que preocupar por nada gracias a un ecosistema de ciberseguridad donde todo hable con todo y sea sencillo de administrar”.

¿Cómo podemos facilitarle la vida al empleado con un equilibrio entre la seguridad y su experiencia? Tiene claro Guillermo Fernández, Iberia Sales Engineer Manager de WatchGuard, que hay que encontrar la manera de ayudarles con herramientas que automaticen la parte de toda la problemática de seguridad sin abrumarles a alertas y a decisiones. Puso como ejemplo de equilibrio lo relativo a la gestión de contraseñas, que aseguró “sigue siendo un mal endémico que arrastramos de desde hace muchos años”.

“El principal inconveniente para no disfrutar de esta democratización de la tecnología es la cultura y el inmovilismo”

AGUSTÍN SÁNCHEZ FONSECA, RESPONSABLE DE DESARROLLO DE NEGOCIO, NFON IBERIA

Para Melchor Sanz, mejorar la experiencia del trabajador remoto pasa por “descomplicar”, y eso significa no sólo simplificar el acceso a la información, a una aplicación o a la red, sino hacerle la vida más fácil al empleado desde que pulsa el botón de su dispositivo. Añadió que “no vale cualquier dispositivo para acceder a cualquier entorno” y propuso una gestión moderna de los dispositivos que va desde la capa más física de seguridad a la capa de sistema operativo o la capa de aislamiento.

Asegurando que el trabajo remoto es sólo un marketing porque “al fin y al cabo todos los usuarios deberían trabajar allí donde estén”, mencionó Iván Rodríguez los servicios Workspace que permiten que el usuario acceda desde un único punto, allí donde esté, homogeneizando el acceso e incrementando la seguridad.

Lo habitual cuando se piensa en teletrabajo es asociarlo a grandes empresas, a multinacionales con empleados repartidos por todo el mundo. ¿Qué ocurre en el mundo pyme? Dijo Mª José Fernández que son las grandes compañías las que tienen más medios, y que las pymes se están digitalizando mucho más. Explicó que han recibido ayudas para hacer frente a esta digitalización a través de fondos ICO, ayudas que han llegado de Europa y propuestas como la de Grenke, que “permitimos que las empresas y las pymes puedan obtener todo el equipamiento de hardware, software, conexiones a Internet… y en general todo lo que necesiten para poder realizar el teletrabajo, agilizando todos los procesos y que los trabajadores estén cómodos y tranquilos”.

En este proceso de teletrabajo, ¿se ha conseguido unificar la experiencia del puesto de trabajo en la oficina y en casa? Dijo Agustín Sánchez Fonseca que el acceso a los datos desde la oficina ya estaba muy disgregado y que al irnos a casa no sólo ha generado un reto en cuanto a unificar la experiencia en casa y en la oficina como un único modelo de uso, “sino que tienes gente con perfiles diferentes, tienes millenials y tienes gente que se niega a dejar de usar el teléfono de sobremesa”. Explica que existe la oportunidad de unificar todas las comunicaciones en el menor número posible de dispositivos, y aun así po-

“Roto el perímetro, la única solución es poner diferentes medidas de seguridad”

SERGIO MARTÍNEZ, IBERIA REGIONAL MANAGER, SONICWALL

der tener esta herramienta en todos los dispositivos posibles, que es la manera de dar flexibilidad.

Roto el perímetro, “la única solución es poner diferentes medidas de seguridad”, dijo Sergio Martínez, añadiendo que la verdadera pandemia “es el robo de identidades para realizar luego ataques y movimientos laterales en las compañías”. Aseguró que los intentos de intrusión se dispararon gracias al robo de identidades y que el ransomware sigue siendo un grave problema. “Está muy claro que debemos desplegar más medidas de autenticación, que muchas aplicaciones se han migrado a la nube para facilitar su acceso desde fuera, que los ciberataques son más sofisticados… y que está claro que hay que aplicar y poner en marcha una nueva ciberseguridad basada en capas de extremo a extremo y de este a oeste”.

Para Iván Mateos hay un reto que tenemos que aplicar tanto al mundo de la ciberseguridad como a nuestra vida cotidiana: primero pensar y luego actuar; “si conseguimos hacer eso evitamos trabajar dos veces; evitamos que cada vez que se plantea un nuevo problema tengamos que analizar todo otra vez, revisar todas las soluciones del mercado y además seguir aumentando la complejidad de nuestro Frankestein”. Mencionó la propuesta de un ecosistema de ciberseguridad adaptativo con el que “conseguimos simplificar mucho la ecuación y tener además un nivel de seguridad superior”.

El phishing ha sido uno de los caballos de batalla durante dos meses de la pandemia. En opinión de Guillermo Fernández, este incremento vino derivado “de tener a los empleados trabajando desde casa” y ha puesto de manifiesto la necesidad de llevar la protección que antes estaba en el perímetro a ese puesto de trabajo. “El empleado es la primera barrera de seguridad y los cursos de concienciación son importantes”, aseguró el directivo pare reducir su impacto.

Si la primera barrera de seguridad es el usuario, la segunda es el dispositivo y la tercera el sistema operativo, y le siguen las aplicaciones y las comunicaciones, explicó Melchor Sanz. Dijo el Director de Tecnología y Preventa de HP Inc. que se tiene que garan-

“Los empleados tienen que poder trabajar desde casa como lo hacían desde la oficina y sin cargarles de responsabilidad”

IVÁN MATEOS PASCUAL, SALES ENGINEER, SOPHOS

tizar que cada una de esas capas sea segura por sí misma desde el diseño, pero que entre ellas se hablen para tener un sistema de control homogéneo.

Los más rápido y fácil para los clientes que ya estuvieran utilizando sistemas y VPN antes de la pandemia fue ampliarlos “sin pararse a pensar”, apuntó Iván Rodríguez añadiendo que las VPN suelen ser complicadas de gestionar y que existen otras opciones, como el acceso remoto al PC de Citrix, que permite “acceder a mi escritorio con las mismas aplicaciones, mismo interfaz, mismo look&feel y con el protocolo nativo de Citrix para poder acceder a sus aplicaciones de la manera más segura y trabajar como en la oficina”.

Este nuevo modelo de trabajo en el que nos hemos visto inmersos por una parte nos ha alejado de los compañeros a los que veíamos prácticamente todos los días, pero también nos ha acercado, gracias a esas múltiples videoconferencias, a gente con la que antes no teníamos apenas relación. ¿Cómo han impactado esas dos tendencias en el trabajador remoto? “Al principio fue un shock”, aseguró Mª José Fernández, añadiendo que ahora se ha instaurado un modelo híbrido en el que “vamos sumando las relaciones personales y las relaciones digitales que ahora ya son cercanas a mí”.

La tecnología se ha democratizado. Por un lado, la pyme tiene acceso a herramientas tecnológicas para igualarse en muchos aspectos a grandes empresas, y también las grandes empresas tienen acceso a herramientas más ligeras o menos costosas y más sencillas de utilizar. Para Agustín Sánchez Fonseca, “el principal inconveniente para no disfrutar de estas ventajas y de esta democratización de la tecnología es la cultura, el inmovilismo y cierta resistencia por parte de algunos fabricantes y operadores con modelos perversos que retienen, por lo menos en el ámbito de las comunicaciones, a las pymes y a las no tan pymes”.

Siguiendo con el concepto “descomplicar”, dijo Sergio Martínez que modelos como Zero Trust, que se han visto reforzados por la pandemia “lo que intentan es utilizar tecnologías que lo hagan más fácil, pero sin fiarse ni confiar en nadie, ni siquiera en los accesos pri-

“Esperar que sea el empleado quien de forma proactiva y continuamente esté actualizando todo el software no es realista”

GUILLERMO FERNÁNDEZ, IBERIA SALES ENGINEER MANAGER, WATCHGUARD

vilegiados con los que hay que tener mucho cuidado”. Aseguró además que el futuro de la seguridad de la red está en el cloud, que la nube pública crecerá esta año un 35% y que las VPN serán sustituidas por tecnologías Zero Trust en casi un 60%.

“El trabajador remoto ha sufrido muchas amenazas y ha sido punto de mira durante este último año por ese aislamiento, y eso ha supuesto no solo un aumento del phishing, sino llamadas de falsos servicios técnicos o casos de ransomware que se han propagado desde la VPN a toda la red en más de una empresa”, puntualizó Iván Mateos. La solución, para el experto de Sophos, es contar con un ecosistema de seguridad que incluso disponga de un servicio de gestión de amenazas para que, si todo falla, si consiguen entrar, se pueda actuar en minutos.

Por último, preguntamos a Guillermo Fernández cómo cree que deben gestionarse las vulnerabilidades de los sistemas operativos y aplicaciones de terceros ahora que ni los empleados ni sus equipos están en la oficina. Empezó recordando que en un 80% de los ataques se están explotando vulnerabilidades que ya han ido corregidas previamente y que su experiencia es que los clientes “no son conscientes de cómo está la situación de todo su parque, y más en este entorno tan distribuido como tenemos ahora”. Esperar que sea el empleado quien de forma proactiva y continuamente esté actualizando todo el software no es realista, concluyó este experto, proponiendo que haya una capa por encima que lo automatice, que sea muy sencillo, que los empleados no tengan que hacer nada y que para el administrador no suponga una sobrecarga. ■

La respuesta al coronavirus no tiene precedentes y este experimento del “trabajo desde casa” lleva a muchas empresas a un territorio decididamente desconocido. Con la mayor parte de los usuarios finales trabajando ahora de forma remota, los enfoques de seguridad de confianza cero pueden ayudar a mantener la continuidad y la seguridad.

itTRENDS

Mejorando la experiencia del trabajador remoto: propuestas tecnológicas

“Lo importante es poder dar la misma experiencia al usuario esté donde esté” (Citrix)

“La cultura de la empresa y del empleado son claves en el nuevo modelo de trabajo remoto” (Grenke)

“Para el trabajo híbrido no vale cualquier dispositivo” (HP Inc.)

“La oferta de centralita y contact center básico de NFON cubre las necesidades del teletrabajo” (NFON)

“Cinco ideas para una nueva ciberseguridad” (SonicWall)

“Hay que dejar de pensar en soluciones Frankestein para empezar a hablar de ecosistemas” (Sophos)

“El teletrabajo nos hace más frágiles a los ataques de phishing” (WatchGuard)

Cambio de la Seguridad TI en entornos de Teletrabajo

Sophos ACE, hacia un ecosistema de ciberseguridad adaptativo

Haga frente a las nuevas ciberamenazas con soluciones coordinadas.

SOPHOS

Más información

Del Big Data al Small & Wide Data

Según Gartner, para el año 2025 el 70% de las organizaciones habrán cambiado su enfoque de Big Data a Small & Wide Data, lo que les proporciona un nuevo contexto para el análisis de datos y la inteligencia artificial. Porque a raíz de la pandemia muchos modelos de IA y aprendizaje automático han quedado invalidados, lo que requiere nuevas formas de aplicar los datos en los procesos de toma de decisiones.

Los modelos de entrenamiento de inteligencia artificial y aprendizaje automático se alimentan de datos históricos, pero a raíz de la pandemia el comportamiento de consumidores, socios y clientes ha cambiado de forma drástica, alterando los patrones previos e invalidando el trabajo de entrenamiento de algoritmos. Por ello, según los expertos de Gartner, para el año 2025 el 70% de las organizaciones va a cambiar su enfoque de Big Data hacia un de Small & Wide Data.

Según Jim Hare, vicepresidente de investigación de Gartner, "las interrupciones como la pandemia de COVID-19 están provocando que los datos históricos que reflejan las condiciones pasadas se vuelvan obsoletos rápidamente, lo que está rompiendo muchos modelos de producción de IA y aprendizaje automático (ML). Además, la toma de decisiones por parte de los humanos y la inteligencia artificial se ha vuelto más compleja y exigente, y depende de-

masiado de los enfoques de aprendizaje profundo hambrientos de datos".

Para hacer frente a la nueva situación, los expertos recomiendan a los líderes de D&A que recurran a nuevas técnicas de análisis conocidas como Small Data y Wide Data. Hare explica que mediante estas técnicas serán "capaces de utilizar los datos disponibles de manera más eficaz, ya sea reduciendo el volumen requerido o extrayendo más valor de fuentes de datos diversas y no estructuradas".

Small Data requiere menos datos para proporcionar información con valor comercial, empleando ciertas técnicas de análisis de series de tiempo o datos sintéticos o aprendizaje auto-supervisado. Wide Data permite el análisis y la sinergia de muchas más fuentes de datos, tanto estructuradas como no estructuradas, de pequeño o gran tamaño. Esta metodología trata de encontrar enlaces entre las variadas fuentes de datos y es capaz de trabajar con gran cantidad de formatos, como texto, imágenes, video, audio, formularios y toda clase de datos provenientes de sensores de diversa naturaleza.

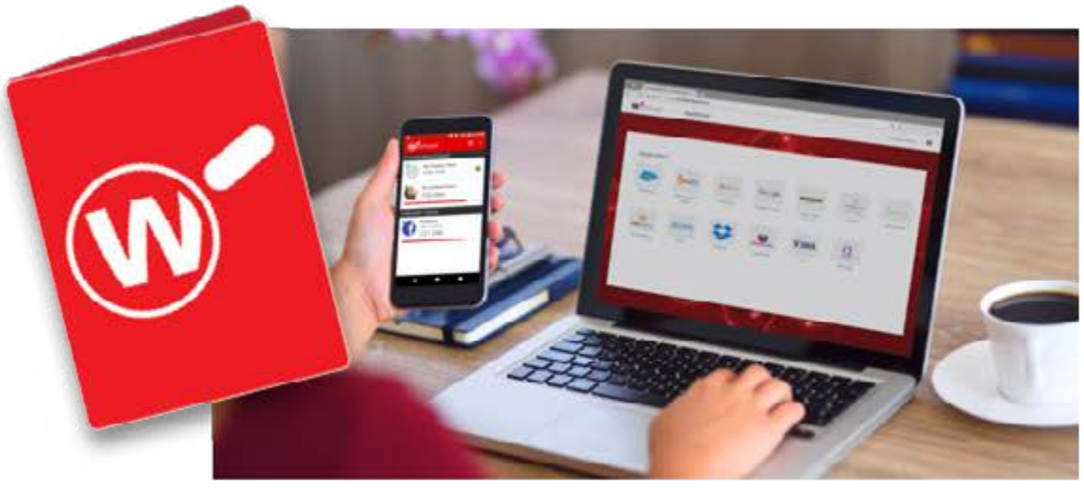
Hare explica que "ambos enfoques facilitan análisis e inteligencia artificial más robustos, reduciendo la dependencia de una organización del Big Data y permitiendo un conocimiento de la situación más rico y completo, o una vista de 360 grados". Y comenta que actualmente "los líderes de D&A aplican ambas técnicas para abordar desafíos como la baja disponibilidad de datos de capacitación o el desarrollo de modelos más sólidos, mediante el uso de una variedad más amplia de datos".

Los casos de uso más avanzados actualmente para el Small & Wide Data son la previsión de la demanda en el comercio minorista, y la inteligencia emocional y del comportamiento en tiempo real en la atención al cliente, lo que permite la hiperpersonalización y la mejora de la experiencia del cliente. Pero también está encontrando utilidad en la seguridad física, la detección de fraudes y los sistemas autónomos adaptativos, como los que rigen el funcionamiento de los robots con capacidades de aprendizaje a través de la experiencia y los datos que recogen del entorno. ■

5 USOS DE BIG DATA EN NUESTRA VIDA DIARIA

MÁS INFORMACIÓN

- Las empresas españolas destacan en la incorporación de la inteligencia artificial
- Las empresas buscan profesionales con una mente analítica



Passport. Trabaja sin inconvenientes.

WatchGuard Passport ofrece a tus empleados la seguridad en la nube que necesitan para trabajar sin inconvenientes desde la oficina, en casa o cualquier otro lugar. Cada servicio del paquete de Passport proporciona protección permanente y siempre activa que se mueve con el usuario.

Autenticación multifactor

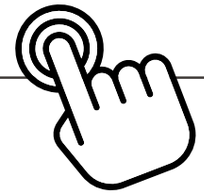
Autentique a las personas y aplique una solida autenticación multifactor en las VPN, las aplicaciones cloud, los endpoints y más.

Protección siempre activa

Proteja a los usuarios en Internet, bloquee los intentos de suplantación de identidad y aplique la política web en cualquier lugar y en cualquier momento sin necesidad de una VPN.

Respuesta inmediata

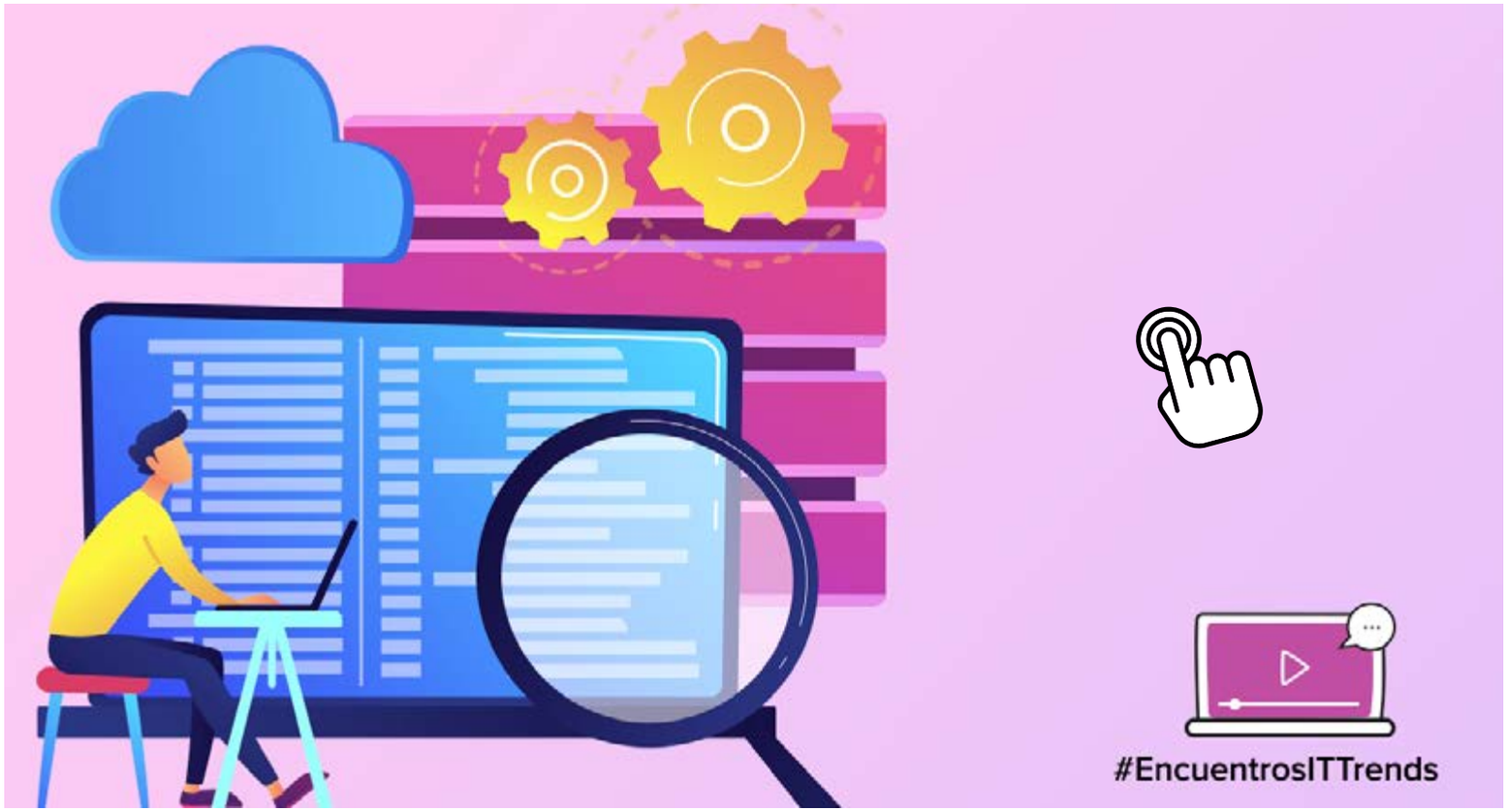
Responda mediante la detección y eliminación de malware y amenazas, y contenga el ransomware y los canales de mando y control (C&C) relacionados.



+34.917.932.531 spain@watchguard.com www.watchguard.com

#ENCUENTROSITTRENDS

Entendiendo la Era del dato: tecnologías y propuestas para gestionar la datificación



Actualmente se generan datos de todo lo que ocurre en el mundo digital y más allá. Las empresas, las personas, los sensores, las tecnologías... todo movimiento produce hoy en día datos que deben capturarse, almacenarse, analizarse, entenderse, hacer accesibles, garantizar su disponibilidad, protegerse... Y todo ello independientemente de su naturaleza, magnitud o uso.

Con los datos, las empresas están construyendo hoy sus estrategias empresariales, pero sin una correcta gestión en cada una de sus fases, se pierde el valor del llamado "petróleo del siglo XXI".

En este Encuentro IT Trends, celebrado bajo el título Entendiendo la Era del dato: tecnologías y propuestas para gestionar la datificación, hemos abordado los últimos enfoques tecnológicos para hacer que esta era del dato aporte valor a cada una de las estrategias empresariales, y, para ello, hemos reunido a un amplio grupo de expertos, tanto en el ámbito académico como en el empresarial. Así, hemos contado con las opiniones de Alfonso Castro, director del Máster en Data Science & Big Data en el Centro Universitario U-tad; Santiago Moral Rubio, director de DCNC Sciences; Quique Sánchez Candorcio, director comercial para EMEA de Ikusi; Ramsés Gallego, International Chief Technology Officer de CyberRes, a Micro Focus line of business; e Israel Serrano, director regional para Sur de Europa de Scality. ■

#ENCUENTROSITTRENDS

El dato como activo de valor para las organizaciones

La datificación es un proceso por el que se plasma un fenómeno en un formato cuantificado para su tabulación y análisis en un dato. Es una carrera imparable y con numerosas aplicaciones. Para entenderlas y conocer el futuro de estas ciencias que se pueden aplicar a los datos, Alfonso Castro, director del Máster en Data Science & Big Data en el Centro Universitario U-tad, y Santiago Moral Rubio, director de DCNC Sciences, ahondaron en el primer debate del Encuentor IT Trends Entendiendo la Era del dato: tecnologías y propuestas para gestionar la datificación, en la importancia de los datos para las estrategias corporativas y el comportamiento futuro de esos datos. Hoy, ya se suben cada minuto alrededor de 500 horas de vídeo en YouTube, mientras que la suma de las diferentes actividades digitales, como redes sociales, banca on-line... generan una cantidad de bits equivalente a un 1 seguido de 21 ceros, lo que nos deja sobrecargados de información.

(De arriba hacia abajo) Alfonso Castro (Centro Universitario U-tad) y Santiago Moral Rubio (DCNC Sciences), en un momento del debate. Clica en la imagen para ver el vídeo

“Ahora, esas arquitecturas que las empresas tenían que levantar on-premise para la gestión de datos, con un coste importante, pueden ser usadas en modo cloud, permitiendo una democratización del dato, siendo capaces de gestionar los datos para decidir y hacer predicciones sin grandes inversiones”

ALFONSO CASTRO, CENTRO UNIVERSITARIO U-TAD

La importancia del dato está generando un mayor interés por parte de los profesionales y un acercamiento estratégico de las empresas. En palabras de Alfonso Castro, “esta cantidad ingente de datos proporcionan un conocimiento más profundo de su organización, y lo que hacen es incrementar el beneficio de las mismas. Estas empresas son capaces de orientar toda su estrategia al dato, y, a partir de estos, tomar decisiones de negocio. Un ejemplo es el sector de la Banca. En nuestro móvil tenemos información anticipada de la estimación de nuestros gastos o, si pedimos un crédito, vamos a tener una respuesta basada en un análisis que se apoya en una información tan variada como, por ejemplo, cómo navegas por la propia aplicación. Las empresas financieras son un claro ejemplo de cómo se aprovecha el Big Data. Pero hay otros sectores, como la Fórmula 1, donde se analizan 400 canales de datos en tiempo real para saber cómo está el coche y ser capaces de ganar o no una carrera”.

Pero, ¿cómo ha evolucionado este interés por el dato en las empresas? Para Santiago Moral, “estamos viendo que, cuanto más jóvenes son las empresas, antes crean un modelo competitivo frente a las ya asentadas que es paradigmático, porque todas las nuevas empresas se basan en datos. Todas las compañías, tecnológicas o no, se están basando en datos. No hay ninguna que esté naciendo ahora que no piense en una estrategia comercial, de negocio o de posicionamiento que no pase por estar analizando los datos de su actividad comercial, de negocio y operativa. Sin embargo, las empresas muy establecidas tienen dificultades para asumir esta tendencia y esta velocidad. Lo que genera es un mercado importante de transformación digital poniendo siempre en el eje de todos los proyectos el dato. Es el elemento sobre el que se construye todo lo demás. Por tanto, tener buenos profesionales que puedan trabajar esa información y puedan proponer ideas de cambios operativos transformacionales, es el quid de la siguiente revolución

industrial que tenemos en marcha: la revolución industrial del dato".

EL IMPACTO DEL VOLUMEN

La generación exponencial e imparable de datos está impactando en el mundo tecnológico. Según Santiago Moral, "se está generando una situación curiosa e inesperada. Hace unos años pensábamos que iba a ser inmanejable por el volumen, pero están surgiendo tecnologías que, con menor coste y consumo, son capaces de manejar muchísimos más datos. El ejemplo más claro son los modelos de ciencia de datos. Ahora mismo, un modelo analítico bien basado en ciencia de datos es capaz de analizar volúmenes exponencialmente superiores a los de hace diez años, y de almacenarlos. Pensar en modelos basados en estructuras de datos no clásicas es complicado desde un punto de vista tradicional, pero existe tanto la tecnología base como los algoritmos para manejar volúmenes de datos que hace un lustro eran impensables".

En opinión de Alfonso Castro, "Big Data no es solo un gran volumen de datos, sino que es información procedente de muy diversas fuentes, de diferentes tipos, estructurados y no estructurados o semiestructurados, y que cambian con mucha rapidez. El tratamiento de esta información resulta muy complejo. Por eso, hace algunos años comenzaron a afianzarse nuevas arquitecturas y tecnologías de programación, procesamiento y almacenamiento de datos distribuidos, que nos permitió abordar la

"Tener buenos profesionales que puedan trabajar la información y proponer ideas de cambios operativos transformacionales, es el quid de la siguiente revolución industrial que tenemos en marcha: la revolución industrial del dato"

SANTIAGO MORAL RUBIO, DCNC SCIENCES

realidad de Big Data. Ser capaces de generar valor a partir de los datos y su análisis. Hemos contado con algoritmos que han podido ejecutar estos modelos basados en estas arquitecturas. Pero, incluso estas arquitecturas que las empresas tenían que levantar on-premise, con un coste importante, pueden ser usadas en modo cloud, permitiendo una democratización del dato, siendo capaces de gestionar los datos para decidir y hacer sus predicciones, sin grandes inversiones".

EL FUTURO DE LOS DATOS

Los datos han evolucionado, tanto por volumen como por tipología. Pero, ¿qué podemos esperar

a partir de ahora? En palabras de Alfonso Castro, "el análisis de datos es una técnica que se ha usado desde hace mucho tiempo. Todos recordamos conceptos como Business Intelligence, que lo que nos aporta es la primera parte de la analítica de datos. Pero, a partir de un conjunto de métricas se obtienen cuadros que permiten a las empresas tomar decisiones estratégicas. Pero esto ha evolucionado a una analítica de datos, que facilita, a partir de estas arquitecturas distribuidas de procesamiento y almacenamiento de datos, ser capaces de manejar algoritmos que no eran capaces de ser ejecutados en los plazos de tiempo necesarios. Ahora conseguimos ejecutarlos y generar modelos predictivos y prescriptivos que nos hacen anticipar qué es lo más probable que vaya a ocurrir, o nos capacitan para predecir las situaciones que podremos abordar en la empresa".

En opinión de Santiago Moral, "uno de los cambios que más está costando en las empresas, es pasar de modelos puramente exactos a modelos de comportamiento aleatorio. Cuando acabas el programa sólo has empezado a trabajar, y esto es complicado para las unidades de negocio y de tecnología. Ahora, el científico de datos tiene que estar pegado al algoritmo para ayudar a este algoritmo a seguir aprendiendo y evolucionando. Pasamos de una informática determinista, con una cadena de valor en la que cuando uno acaba empieza otro, a una informática no determinista, donde la efectividad siempre es relativa, las mediciones tienen que ser permanentes. Otro gran cambio que nos viene, y que estamos a ver cómo lo desarrollamos, es el de la ética de los algoritmos. Como cada vez ponemos más decisiones de forma automática en algoritmos, y estos aprenden de los datos, si los datos tienen sesgo, el algoritmo va a tener un comportamiento sesgado, aunque el propio algoritmo no lo tenga. La calidad del resultado tiene que ver con la calidad de la entrada. Pero son dos modelos que nos cambian mucho la forma de pensar".

POTENCIANDO LAS CAPACIDADES PARA ANALIZAR LOS DATOS

A nivel de tecnologías, según Santiago Moral, "vamos a arquitecturas basadas en que jamás se borra. Esto hace que podamos tener sistemas de procesamiento casi infinitos. Estamos mezclando tecnologías, on-premise o en la nube, con posibilidades casi infinitas de almacenamiento, capacidades enormes de procesamiento, y con modelos donde la aplicación de la ciencia de datos exige menos conocimientos de la propia ciencia de datos. Son tecnologías que se van mucho de los modelos clásicos de bases de datos, muy basadas en tecnologías No-SQL, integrando datos no estructurados con estructurados, modelos en los que nunca se borra... tecnologías como Elastic en Amazon o BigQuery en Google. Y todo esto con programación en diferentes lenguajes". Para Alfonso Castro, "debemos hacer una división clara entre la gestión de datos y el análisis de datos. Dentro del análisis de datos, las tecnologías son las relacionadas con algoritmos de IA que permiten esos modelos para predecir y abordar el análisis de datos. Dentro de estos modelos, hay dos, fundamentalmente: los asociados a Machine Learning y los asociados al Deep Learning. En el primer caso, entrenamos el modelo con algunos datos y usamos otros para realizar las predicciones. En el segundo, se basan en algoritmos de redes neuronales que toman como referencia el funcionamiento del sistema nervioso. A nivel de gestión del dato, tenemos que ser capaces de manejar todos estos elementos para que el entorno funcione correctamente. Y abordar diferentes elementos, como la calidad del dato, la seguridad del dato, la integración de datos de diferentes fuentes, cómo se almacenan, cómo se operan... En este punto, estamos trabajando en la creación de frameworks que generen procesos claramente definidos para que cada uno de los participantes sepan lo que tienen que hacer en cada momento. No son solo avances tecnológicos, sino también en los procesos". ■

#ENCUENTROSITTRENDS

Maximizando el valor del dato

Tenemos una huella digital enorme. De hecho, el recuento de los datos del año pasado alcanza los 59 Zetabytes. Pero este número, de por sí muy grande, está creciendo con una tasa anual compuesta del 61%. Si esto lo trasladamos a las empresas, supone un gran volumen de información.

Así las cosas, los retos que planean los datos a las empresas son muchos, y para saber cómo responde la tecnología a ellos se abordaron las posibilidades tecnológicas junto a Quique Sánchez Candorcio, director comercial para EMEA de Ikusi; Ramsés Gallego, International Chief Technology Officer de CyberRes, a Micro Focus line of business; e Israel Serrano, director regional para Sur de Europa de Scality, en la segunda mesa de debate de este Encuentro IT Trends, Entendiendo la Era del dato: tecnologías y propuestas para gestionar la datificación.

RETOS CON LOS QUE ENFRENTARSE

¿Cuáles son las dificultades para almacenar, proteger, analizar o aprovechar toda la información que circula por las empresas? En opinión de Quique Sánchez, "son muchas, pero cuestiones como quién es el dueño del dato, la gestión distribuida, múltiples accesos, diferentes fuen-

(De arriba hacia abajo) Quique Sánchez Candorcio (Ikusi), Ramsés Gallego(CyberRes, a Micro Focus line of business) e Israel Serrano (Scality). Clica en la imagen para ver el vídeo.

“Almacenar datos que no tienen utilidad tiene un coste, y hay que saber cuándo y cómo eliminarlos”

QUIQUE SÁNCHEZ CANDORCIO, IKUSI

tes, un contexto hiperconectado, un volumen ingente… convierten en cruciales temas como el almacenamiento, la seguridad, la migración de los datos… y la capacidad de establecer cuál es el dato útil, porque no todos los datos son útiles. Almacenar datos que no tienen utilidad tiene un coste, y hay que saber cuándo y cómo eliminarlos. Estos puntos se convierten en cruciales, sobre todo para la seguridad”.

En palabras de Ramsés Gallego, “estas dificultades pasan por entender el contexto global en el que ya no solo la pandemia, sino el mundo en general nos ha llevado. Pero, sin duda, la pandemia acelera la necesidad de un trabajo remoto. La dificultad está en entender que, si todos los datos no son creados de la misma manera o con la misma finalidad, por qué debemos protegerlos, gestionarlos, maximizarlos… de la misma manera. Si los datos no tienen el mismo valor, deberíamos acercarnos a ellos de forma desacoplada, de manera distribuida. Cierto es que con políticas centralizadas y simplificadas, pero con una voluntad de maximización no solo de un dato, sino de los datos en su conjunto, para que se convierta en información. Lo contrario del gobierno no es el desgobierno del dato, que de por sí es malo, sino la complacencia, asumir que no tiene el valor suficiente el dato que estamos creando y protegiendo”.

Desde el punto de vista de Israel Serrano, “hay que analizar si los datos que se están almacenando tienen valor o no, y la dificultad para las empresas es poder hacer ese análisis a priori. Muchas veces no sabes si tiene valor hasta que no lanzas el proceso de análisis. Lo más importante para las empresas es que sean capaces de hacer económicamente factibles este tipo de iniciativas. Este componente económico es muy importante, así como la decisión de dónde quieren guardar estos datos, con elementos económicos, técnicos y de legislación”.

ENTENDIENDO LA ERA DEL DATO

En un entorno empresarial cada vez más complejo, con realidades híbridas, una computación que se reparte tanto en la nube como en el extremo, con millones de dispositivos conectados, y con un acceso por parte de los usuarios desde cualquier lugar y en cualquier momento, la gestión de los datos es un elemento fundamental. A partir de una adecuada y correcta gestión de los datos, es posible tomar las mejores decisiones para el negocio, apoyándose en las tecnologías más adecuadas en cada caso y modelo, pero analizando las operaciones de cada cliente como punto de partida para transformar el negocio de la mejor manera posible.

INCREMENTO DE VOLUMEN Y DE COMPLEJIDAD DE LOS ENTORNOS

¿Qué herramientas serían básicas para poner cierto orden en la situación que enfrentan las empresas? Según Ramsés Gallego, “hay que aplicar principios básicos de efectividad y eficiencia. No se trata solo de hacer las cosas bien, sino de hacerlas

“La dificultad está en entender que si todos los datos no son creados de la misma manera o con la misma finalidad, por qué debemos protegerlos o gestionarlos de la misma manera”

RAMSÉS GALLEGO, CYBERRES, A MICRO FOCUS LINE OF BUSINESS

correctamente. Otro axioma es que el trabajo es lo que se hace, no donde se está, de ahí que sean fundamentales herramientas de archivado, de resiliencia, de gestión y gobierno del contenido, de protección, de analítica avanzada…”.

Para Israel Serrano, “tenemos que hacer que los proyectos sean viables. Da igual que el dato tenga valor o no, si el proyecto no es viable, no lo vamos a saber nunca. Hay que ser capaces de establecer entornos de analítica de pruebas de concepto. Hay que facilitar que las empresas tengan resultados rápidos para poder evaluar si el proyecto tiene sentido. Además, tenemos que ser capaces de facilitar nuevos modelos de consumo de nuestros productos, movernos hacia modelos de pago por uso o de suscripción. Asimismo, como no todos los datos son iguales, no podemos tratarlos igual. Hay que analizar el coste por terabyte. No puedes pedir el mismo coste a todos los datos, porque para obtener el mismo valor necesitas más datos, y el coste debe estar ajustado al valor que van a proporcionar. Por último, si vamos a trabajar con datos no estructurados, no podemos estar trabajando con las mismas herramientas de las últimas décadas. Y aquí es importante el cambio de paradigma y mirar al almacenamiento de objetos”.

Desde la perspectiva de Quique Sánchez, “las herramientas son múltiples y variadas, pero es esencial la correcta organización de los datos, dónde tiene que estar para tener un acceso en tiempo real, y luego la correcta identificación y almacenamiento. Quizá es más sencillo con los datos estructurados, pero también hay que hacerlos con otros datos, que tienen que confluir con los datos estructurados. Si bien esto es básico, también lo es la trazabilidad que hemos de tener de estos datos. Hablamos también de correlación y coherencia de los mismos, para empezar a hablar de información y no solo de datos”.

CONVERTIR LOS DATOS EN ACCIONES

La información es el elemento que mueve las empresas en la Economía Digital. Son los datos la materia prima para poder tomar las mejores decisiones y aplicarlas al negocio como parte de la ejecución de la estrategia. No contar con una adecuada política o las correctas herramientas para la gestión y gobierno de los datos puede provocar desde decisiones erróneas para el negocio a brechas de seguridad con consecuencias catastróficas para la empresa.

“Hay que analizar si los datos que se están almacenando tienen valor o no, y la dificultad para las empresas es poder hacer ese análisis a priori”

ISRAEL SERRANO, SCALITY

INNOVACIÓN EN TORNO AL DATO

En palabras de Israel Serrano, “hay mucha innovación en muchas áreas. En nuestro caso, en la infraestructura que soporta estos datos. La innovación es el uso de protocolos y estructuras de datos que se adaptan mejor al tipo de datos que se están generando. Para 2024, según IDC, hablamos de 138 ZB de datos generados, de los que el 80% van a ser no estructurados. Tenemos que ser capaces de dotar a las empresas de las herramientas necesarias para analizar toda esta ingente información para extraer el verdadero valor. En términos de innovación, la pieza fundamental es el metadato, que me permite dotar de valor, de contexto de información adicional a un dato según va pasando por los diferentes procesos de negocio. Y esto permite a las organizaciones identificar si tiene valor. Por otra parte, cuando piensas dónde colocar el dato, no es algo que sea inamovible. Necesitamos que sea ubicuo y no tengamos la necesidad, a priori, de definir dónde está, salvo por criterios económicos, de negocio o legales, y tenemos que proporcionarles las herramientas para que puedan tomar la decisión adecuada”.

En opinión de Quique Sánchez, “el mayor impacto dentro de la gestión del dato lo está teniendo la Inteligencia Artificial, y es curioso, porque la IA tiene como punto de partida el dato, pero la mejora de la limpieza de datos para la propia calidad del dato se apoya en la propia Inteligencia Artificial. Por otra parte, podemos analizar dónde estamos obteniendo mayor beneficio del dato en base a la analítica. Y, pensando en la protección, encontramos la detección de amenazas analizando riesgos en tiempo real”.

En palabras de Ramsés Gallego, “en una era compleja y cambiante, todos hablamos de transformación y disrupción, pero hay que apostar por la innovación radical, haciendo las cosas de forma diferente. Hay que enriquecer el dato empleando IA y Machine Learning, y aprovechar los beneficios que aportan los algoritmos enriqueciendo los datos a cada paso. Cuando tienes inteligencia de datos para poder correlacionar los datos, es algo tremendamente innovador, un salto cualitativo y cuantitativo en la gestión del dato”. ■

Si te ha gustado este artículo, compártelo

Entendiendo la Era del dato:
tecnologías y propuestas para gestionar la datificación

“El dato es un valor que hay que convertir en información para tomar decisiones”, Ikusi

“Es fundamental proteger a las personas y la información”, CyberRes, a Micro Focus line of business

“La tecnología debe ser capaz de manejar la ubicuidad del dato”, Scality

cisco Partner

IKUSI velatia

Aryse 360°

UNA SOLUCIÓN INTEGRAL AVANZADA PARA TODAS TUS NECESIDADES

Te presentamos Aryse 360, la única solución integral de la industria que unifica **Conectividad**, **Seguridad y Colaboración** para que solo tengas que preocuparte de tu negocio.

CUOTA MENSUAL,
TODO INCLUIDO. HW, SW,
MANTENIMIENTO
Y SERVICIOS
PROFESIONALES.

www.aryse360.com

itTRENDS

OPINIÓN

Asegurando la calidad del dato con Data Quality

Paula Gómez,
Head of Data & Adtech
de Making Science

En el entorno de la analítica digital manejamos multitud de plataformas que nos ofrecen infinidad de métricas que debemos monitorizar para cada uno de nuestros activos digitales. Y es nuestro deber conocer perfectamente las peculiaridades de medición de cada una de estas herramientas para poder tomar las mejores decisiones.

En algún momento todos hemos sufrido el desasosiego de ver cómo, a pesar de disponer del mejor equipo técnico y llevar a cabo una implementación impecable en las plataformas de medición, obtenemos datos o métricas que suelen presentar ciertas discrepancias.

Los motivos de estas desviaciones de datos pueden ser diversas; desde que el tracking code no está presente en todas las páginas del site: puede ocurrir en sitios muy grandes o con una arquitectura compleja, la aplicación incorrecta de filtros de datos, inadecuada identificación de referrals, inclusión de auto-referrals o spambots, entre otros, distintos criterios para la asignación de la conversión o el rechazo de 3rd party cookies por parte del usuario.

Y estas solo son algunos de los posibles problemas que pueden surgir, entre muchos otros.

Si este es tu caso (spoiler: no existe receta mágica), seguramente este artículo puede resultar útil o, al menos, trataremos de que esa situación te resulte más llevadera.

Con la finalidad de identificar rápidamente y resolver discrepancias de datos entre plataformas de medición y publicidad, detectar posibles cambios de tendencia, o incluso analizar la influencia de cambios en los sites, en Making Science contamos con nuestra solución Data Quality para asegurar la calidad de los datos controlando desviaciones y anomalías. Su funcionamiento es el siguiente:

1. **Seleccionamos las plataformas de medición y publicidad** que deseamos incluir en la comparativa así como los indicadores clave

“Dado que nuestro objetivo siempre es optimizar la inversión y tomar rápidamente decisiones eficaces tratando de minimizar estas discrepancias, la mejor forma de conseguirlo es monitorizando la evolución de todas las métricas importantes para el negocio”

a monitorizar. El sistema permite contrastar la información procedente de cualquier plataforma que disponga de exportación de datos a Bigquery.

2. **Sólo se requiere implementar en la web y en el Tag Manager el pixel Data Quality de Making Science**, y a partir de ahí podremos monitorizar el rastreo y la medición de cualquier evento, interacción o conversión que nos interese.

3. **Toda la información será analizada en Bigquery.** Cuando haya una discrepancia relevante entre los parámetros, el sistema generaría una alerta por correo electrónico, con el fin de poder anticiparnos y tomar medidas correctoras. Dispondremos un dashboard automatizado en Data Studio para tener una visibilidad completa de todos los KPI claves de nuestro negocio.

Definiendo los procedimientos de supervisión adecuados, implementando mecanismos para alcanzar una visibilidad completa de los principales parámetros de negocio en las diferentes plataformas de medición, dispondremos de un seguimiento del rendimiento de nuestros activos en todos los niveles para prevenir posibles contratiempos.

Dado que nuestro objetivo siempre es optimizar la inversión y tomar rápidamente decisiones eficaces tratando de minimizar estas discrepancias, la mejor forma de conseguirlo es monitorizando la evolución de todas las métricas importantes para el negocio.

Disponer de este tipo de soluciones que generan alertas automáticas cuando detectan ciertos cambios de tendencia, resultan vitales para el día a día de cualquier analista y/o responsable de negocio, y hacen que la organización que dispone de este tipo de soluciones se anticipen a la pérdida de datos y posean, gracias a ello, una visión real y completa de la actividad de su negocio. ■

MÁS INFORMACIÓN

CRM y Marketing Automation en el centro de la estrategia de tu compañía

Cloud Migration: Apuesta por el futuro de tu organización en la nube

“Eliminar las cookies no significará que las empresas pierdan fuentes de información” (Making Science)

itTRENDS

OPINIÓN

Siete razones
por las que las plataformas de edge cloud complementan el enfoque multi-cloud

Gonzalo de la Vega,
VP Strategic Projects, Fastly

El 84% de las empresas adoptan ya estrategias multi-cloud para sacar el máximo partido a las diferentes soluciones y mejorar su resiliencia. Esta aproximación presenta algunos retos al aumentar la complejidad de las arquitecturas, los marcos de trabajo o la variedad de API. El borde de la red es cada vez más un potente ecosistema para el desarrollo de aplicaciones modernas que aporta mayor agilidad, control y seguridad a los equipos.

Las plataformas edge cloud se están convirtiendo en un complemento eficaz para los entornos multi-nube, que aporta una capa uniforme a la infraestructura, así como herramientas para optimizar y aumentar su rendimiento y una mayor visibilidad.

EL CRECIENTE ATRACTIVO DE LA MULTI-CLOUD

El enfoque multi-cloud gana adeptos por algunas de sus ventajas clave. En primer lugar, la gestión de costes, ya que permite aprovechar los puntos fuertes de cada nube, asignando un proveedor de bajo coste para el almacenamiento en frío, y un presupuesto mayor para servicios avanzados como machine learning, por ejemplo. Es importante también la agilidad a la hora de desplegar nuevas aplicaciones y servicios allí donde mejor se adapten, usando contenedores y microservicios de diferentes proveedores. La resiliencia y la seguridad se ven favorecidas por la distribución de cargas de trabajo y servicios en varias plataformas. Finalmente, el enfoque multi-cloud mejora el rendimiento para los usuarios finales al permitir apoyarse en el proveedor con mejor presencia regional.

VENTAJAS DE USAR UNA PLATAFORMA EDGE CLOUD CON UNA INFRAESTRUCTURA MULTI-CLOUD

Añadir una capa adicional en el edge resuelve algunos de los retos de trabajar con varios proveedores cloud. Estas son algunas de sus ventajas:

“Incorporar una plataforma edge cloud a un entorno multi-cloud proporciona una capa uniforme sobre tu infraestructura en la nube que puede reducir enormemente la complejidad y aportar mejoras significativas en cuanto a visibilidad, rendimiento y seguridad”

1 Enrutamiento de solicitudes independientemente de la infraestructura: Las decisiones sobre balanceo de carga se toman en la capa 7 en lugar de en la capa DNS, lo que permite crear reglas personalizadas para enrutar el tráfico de manera inteligente o incluso realizar pruebas de forma segura encaminando una fracción del tráfico de producción al nuevo sitio o servicio.

2 Sistema de recuperación de fallos y redundancia: Las plataformas de edge cloud pueden redireccionar instantáneamente el tráfico o sistema de recuperación de fallos a una nube o región secundaria si falla el origen.

3 Reducción de las solicitudes enviadas a los proveedores: Es posible asegurar que solo pase una petición al origen, independientemente de cuantas solicitudes simultáneas se reciban en el edge para un único objeto, reduciendo costes de tráfico de origen y procesamiento y mejorando la resiliencia y el índice de aciertos de caché.

4 Supervisión en tiempo real y solución de problemas: Proporciona la visibilidad necesaria para entender cómo los clientes utilizan las aplicaciones y servicios, y diagnosticar problemas en cualquier lugar de la red, ya que permite transmitir logs desde el edge en tiempo real.

5 Desarrollo de aplicaciones modernas y microservicios en el edge: Trasladar la lógica de los microservicios al edge evita la complejidad que supone replicarlo en cada plataforma cuando se busca estar más cerca de los usuarios.

6 Una capa adicional de seguridad en el edge: Una plataforma edge cloud proporciona un “paraguas” de seguridad uniforme, independientemente de cuántos orígenes o nubes se utilicen, y con un impacto mínimo en el rendimiento. El uso de un WAF o DDoS en el borde, permite capturar la mayor parte del ruido antes de que llegue a la infraestructura en la nube.

7 Migración de datos sin tiempos de inactividad entre orígenes: Puede configurarse para buscar contenidos en diferentes ubicaciones facilitando las migraciones cuando se cambia o se incorpora una infraestructura.

En definitiva, incorporar una plataforma edge cloud a un entorno multi-cloud proporciona una capa uniforme sobre tu infraestructura en la nube que puede reducir enormemente la complejidad y, al mismo tiempo, aportar mejoras significativas en cuanto a visibilidad, rendimiento y seguridad. ■

MÁS INFORMACIÓN

- Identificación de ataques web
- “Decepcionar a los clientes cuando se acercan a nuestra plataforma puede resultar muy caro” (Fastly)
- Guía para implementar una CDN moderna
- La hoja de ruta de DevOps en materia de seguridad

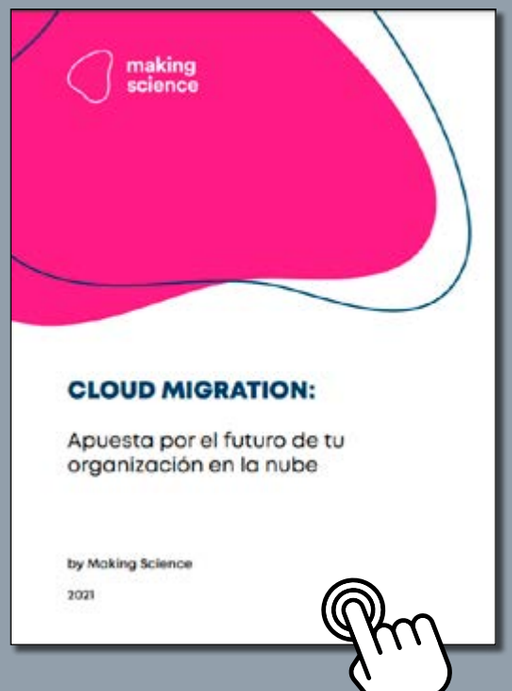
Si te ha gustado este artículo, compártelo

CÓMO ELEGIR UNA BASE DE DATOS PARA TUS APLICACIONES MÓVILES

¿Cuáles son los criterios que nos deben ayudar a decidir cuál es la mejor opción para encontrar una base de datos para aplicaciones móviles? Este documento repasa alguno de los más importantes, como el soporte multiplataforma, la capacidad de almacenamiento local de datos, la capacidad de sincronización con resolución de conflictos, la facilidad de desarrollo, la seguridad, el modelado ágil de datos, el despliegue flexible o las opciones de topología.

IT TRENDS 2021. ASIMILANDO LA ACELERACIÓN DIGITAL

¿Qué tendencias tecnológicas dominarán en el año post-pandemia? En este informe de IT Research desvelamos las principales claves de las estrategias TI para este 2021.



CLOUD MIGRATION: APUESTA POR EL FUTURO DE TU ORGANIZACIÓN EN LA NUBE

En tiempos de incertidumbre, la migración a Cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y en cualquier lugar. Este documento recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

IDENTIFICACIÓN DE ATAQUES WEB

Los equipos de seguridad de las empresas se enfrentan a diferentes tipos de ataques de alto riesgo contra sus organizaciones. La pregunta es, ¿cómo pueden reconocer los cuatro tipos de ataques más peligrosos? Este documento ayuda a identificar los ataques tales como relleno de credenciales, uso indebido de una API, inyección de SQL y vulnerabilidades de la lógica de negocio.

it whitepapers

itTRENDS

Encuentros IT TRENDS

La introducción de tecnologías como **RPA, ML o Inteligencia Artificial** en las empresas está generando un nuevo tipo de organizaciones más ágiles e inteligentes, capaces de automatizar muchos de sus procesos y de dar respuesta a situaciones de manera ágil. La toma de decisiones, la gestión de los datos, los recursos humanos o la ciberseguridad de la organización son algunos de los campos que se están viendo beneficiados por la aplicación de estas tecnologías. El resultado son organizaciones que ganan productividad y agilidad.

16 de septiembre – 11:00

REGISTRO

En plena era **cloud**, descentralizada, de trabajo remoto, la conectividad se da por hecho. No así una buena experiencia. **SD-WAN** se afianza mientras **5G** se abre camino, la computación se marcha al **Edge** y el **IoT** sigue avanzando sin freno y a lo grande. ¿Qué opciones tienes para gestionar una empresa cuyo perímetro está cada vez más diluido y potenciado por las nuevas tecnologías de conexión?

30 de septiembre – 11:00

REGISTRO

Las estrellas del ransomware

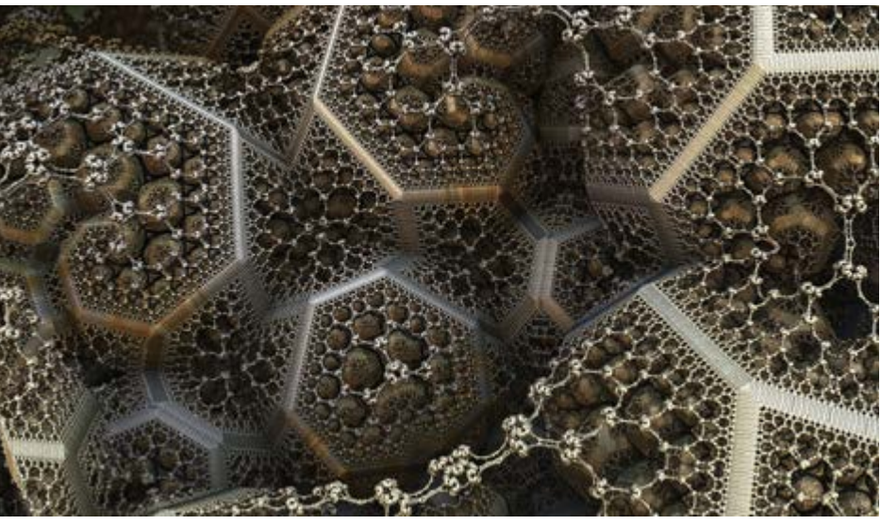
El ransomware se ha convertido en una terrible pandemia digital que avanza sin freno, evoluciona a peor y tiene en vilo a los responsables de ciberseguridad. Si bien su crecimiento explosivo en los últimos años puede hacer que parezca lo contrario, el ransomware no surgió de la nada ni es tan nuevo como puede parecer, y acumula entre sus víctimas algunos nombres relevantes. Estos son algunos de los ejemplos más destacados de los últimos meses.

El troyano AIDS, también conocido como PC Cyborg por ser el nombre de la empresa ficticia que exigía el pago, es la primera muestra de ransomware documentada. Se lanzó a finales de los 80 a través de un disquete y pedía el envío de 189 dólares a un apartado de correos de Panamá para restaurar el acceso a los sistemas. Los discos infectados tenían un programa para analizar el riesgo de una persona de contraer el SIDA y el malware que se activaba después de que una computadora infectada se encendía un número determinado de veces tras lo cual ocultaba directorios, cifraba los nombres de todos los archivos en la unidad C y mostraba un mensaje exigiendo el pago. En los años siguientes aparecieron ataques similares, pero lo cierto es que el ransomware siguió siendo una amenaza relativamente menor hasta el cambio de siglo, cuando el uso de Internet en los países desarrollados superó el 50%.

Hacia 2005 la banda ancha se expandió y esa capacidad de acceso a un Internet más rápido se convirtió en terreno fértil para una nueva generación de ransomware que utilizaba un cifrado RSA asimétrico más efectivo. Sus principales valedores fueron Archiveus, que cifraba todo el directorio Mis Documentos y pedía a los usuarios que realizaran compras en una farmacia online para conseguir una clave de 30 dígitos que desbloquería sus archivos; y GPcode, que se extendía a través de adjuntos de email que parecían ser solicitudes de empleo y que, como Archiveus, utilizó una clave pública RSA de 660 bits para cifrar archivos en el directorio MyDocuments de una computadora, y las víctimas

El coste de recuperación de un ataque de ransomware se ha duplicado en un año, pasando de los 761.106 dólares de 2020 a los 1,85 millones de 2021

El objetivo del rasomware Nephilim son las 'One Billion companies' y ejecuta tácticas de doble extorsión para asegurar el pago de sus víctimas



tuvieron que pagar una tarifa para obtener esa clave. A partir de entonces, el ransomware ganó un impulso constante.

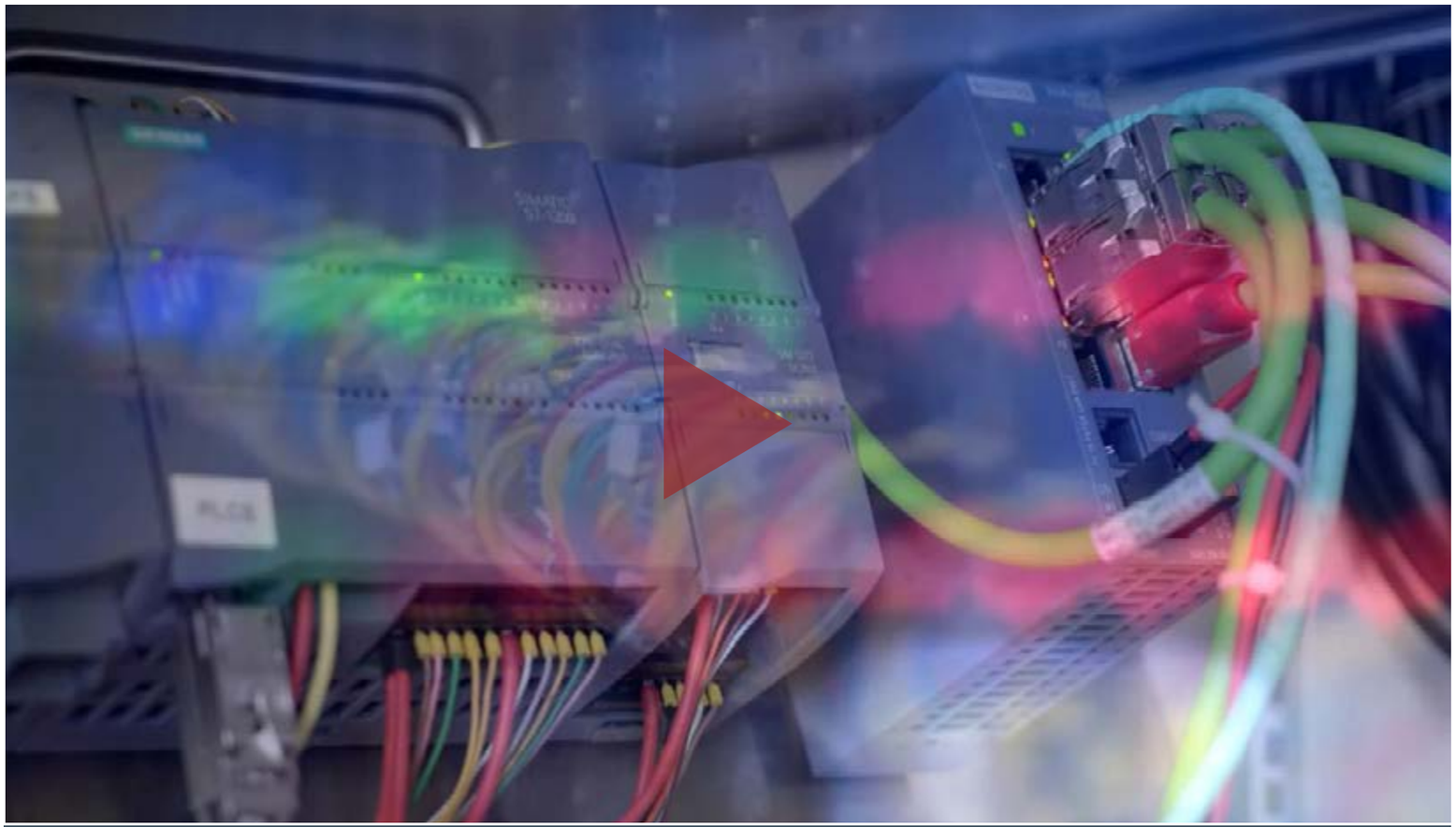
Inventado en 2008, los Bitcoin, una moneda digital descentralizada que permite transacciones entre pares, sirvió para impulsar el ransomware por su naturaleza descentralizada, que permite su uso en la web oscura y para actividades ilegales. Una vez que los ciberdelincuentes pudieron exigir el pago en una forma que no se podía rastrear hasta ellos, se animaron.

El ransomware se expandió sin freno y explotó en 2011, cuando se detectaron cerca de 60.000 nuevas muestras de ransomware sólo en el primer trimestre de ese año, cifra que se incrementó hasta los 200.000 en el tercer trimestre de 2012 y siguió aumentando creando una fiebre del oro alrededor del ransomware.

La ubicuidad de internet, la digitalización, algoritmos de cifrado más potentes y las monedas digitales prepararon el terreno para la llegada de CryptoLocker en 2013. Esta nueva generación revolucionaria de ransomware no solo aprovechó el poder de las transacciones de Bitcoin, sino que lo combinó con formas más avanzadas de cifrado. Usó pares de claves RSA de 2048 bits generados a partir de un servidor de comando y control y entregados a la víctima para cifrar sus archivos, asegurándose de que las víctimas no tuvieran salida a menos que pagaran una suma de unos 300 dólares por la clave.

La rentabilidad de la amenaza quedó patente cuando llegaron al mercado las primeras ofertas de Ransomware como servicio (RaaS), que permitió la entrada de ciberdelincuentes sin amplios conocimientos técnicos y disparó los ataques.

Mucho revuelo causaría el uso del troyano bancario Gameover Zeus como mecanismo para expandir el ransomware CryptoLocker. La botnet creada, y que permitiría a sus creadores darse cuenta del valor



RANSOMWARE: LA GRAN AMENAZA PARA LAS EMPRESAS

CLICAR PARA VER EL VÍDEO

El grupo responsable del ransomware Maze fue uno de los primeros en robar datos antes de cifrarlos. Si la víctima se negaba a pagar el rescate, los ciberdelincuentes amenazaban con publicar los archivos robados.

potencial del ransomware, estuvo activa durante algo más de un año y fue cerrada en una operación encabezada por el FBI. En pocos meses se detectarían una gran cantidad de clones de CryptoLocker y cómo los grupos de ciberdelincuentes competían entre ellos por crear la amenaza más letal.

Nos adentramos entonces en un periodo de ataques a gran escala. Fueron los años de CryptoWall, de Locky o Wannacry, que impactó en más de 200.000 ordenadores de unos 150 países con daños de miles de millones de dólares. Poco después llegaría la familia Petya, una de cuyas variantes, NotPetya desató el caos con un ciberataque global que afectó a Rusia, Ucrania, Francia, Alemania, Italia, Polonia, Reino Unidos y Estados Unidos. Ucrania fue uno de los países más afectados, con 1.500 entidades, incluidas instituciones financieras, informando del ataque.

Es en este proceso cuando se dejan los kits y servicios de ransomware para ciberdelincuentes menos avanzados y empiezan a desarrollarse propuestas más avanzadas de ransomware dirigido. Es la era moderna del cibercrimen, ya organizado; con departamentos de desarrollo e innovación, o calls center que gestionan los pagos del rescate.

Se da una maléfica vuelta de tuerca y aparece el malware de doble extorsión, porque no sólo cifra y se apropia los datos, sino que amenaza con publicarlos, muchas veces peor que la propia pérdida porque puede generar multas por incumplimiento de reglamentos de protección de datos, además de la pérdida de confianza.

Más recientemente ha aparecido el de triple extorsión que integra una amenaza adicional, el chantaje

Conti es uno de los ransomware más rápidos. Utiliza 32 hilos simultáneos de CPU, lo que permite que cifre muy rápido todo el disco duro o cualquier fichero que se le ponga delante

a los clientes. El primer caso notable de triple extorsión fue el golpe sufrido por la clínica Vastaamo, en octubre de 2020. Esta clínica de psicoterapia finlandesa, que contaba con 40.000 pacientes, sufrió una brecha de seguridad a lo largo de todo un año que culminó con un amplio robo de datos de todos sus pacientes mediante un ransomware. Tras la ofensiva, se exigió un cuantioso rescate al proveedor de servicios sanitarios, pero, en este caso también se solicitaban sumas menores a los pacientes, que recibieron las peticiones de rescate individualmente por correo electrónico. En esos emails, los ciberdelincuentes amenazaban con publicar el contenido de las sesiones con sus terapeutas.

La pandemia sanitaria, que obligó a descentralizar aún más las empresas llevó a un incremento de los ciberataques, también los de ransomware. Durante el último año se han estado lanzando ciberataques consecutivos para violar los datos de pequeñas y grandes empresas y varias familias de ransomware son capaces de robar datos confidenciales a través de técnicas altamente sofisticadas. Las verticales de la industria como BFSI (banca, servicios financieros y seguros), TI, gobierno, manufactura, etc., se han convertido en minas de oro en este momento para que estos ciberdelincuentes roben datos confidenciales.

Las estrellas de ransomware más impactantes de los últimos meses

1. REvil, también conocido como Sodinokibi

En febrero de 2021 el grupo de ransomware REvil anunció que había añadido dos etapas a su doble esquema de extorsión: ataques DDoS y llamadas telefónicas a los socios comerciales de la víctima y a los medios de comunicación. Este conjunto,

El ransomware y las criptomonedas

La explosión del ransomware como una empresa criminal lucrativa ha estado estrechamente relacionada con el auge de Bitcoin y otras criptomonedas, que utilizan libros de contabilidad distribuidos, como blockchain, para rastrear transacciones. El uso de criptomonedas se suma al desafío de identificar a los delincuentes de ransomware, ya que los pagos con estas monedas son difíciles de atribuir a cualquier individuo.

Los delincuentes de ransomware suelen exigir que las víctimas envíen sus pagos de rescate a través de Bitcoin, pero después de recibir el pago en una "billetera" digital designada (software que almacena claves públicas y privadas), los delincuentes suelen ocultar estos fondos lo más rápido posible para evitar la detección y el seguimiento. Sus métodos incluyen el chainhopping, o "salto en cadena", que implica el intercambio de fondos en una criptomoneda por otra utilizando, por lo que esos fondos pueden ser extremadamente difíciles de rastrear. Por otra parte, para protegerse aún más, los actores de ransomware pueden usar proveedores de servicios de dinero para configurar cuentas o usar cuentas con credenciales falsas o robadas.

El ransomware REvil también es conocido por afectar a grandes celebridades de y filtrar sus datos en la darkweb

responsable de la distribución del ransomware Sodinokibi, opera con un modelo de negocio as-a-service.

En la actualidad, este grupo ofrece ofensivas DDoS y llamadas de VoIP codificadas a periodistas y socios como un servicio gratuito para sus afiliados, con el objetivo de presionar aún más a la empresa víctima para que cumpla con las demandas de rescate en el plazo designado.

El ransomware REvil también es conocido por afectar a grandes celebridades y filtrar sus datos en la darkweb. Según The Times, se filtraron una serie de capturas de pantalla que incluían un documento legal del contrato de gira de Madonna y docenas de archivos informáticos de famosos como Bruce Springsteen, Barbara Streisand, Robert De Niro, Rod Stewart o Elton John.

2. Netwalker, también conocido como el ransomware Mailto

Entre sus objetivos se encuentran gigantes de la logística, grupos industriales, corporaciones energéticas y otras grandes corporaciones. Según datos de

Desde que se identificó hace seis meses, Tycoon ha mostrado un enfoque agresivo

un informe de McAfee en solo unos cuantos meses de 2020, los ciberdelincuentes han recaudado con este ransomware más de 25 millones de dólares.

Sus creadores ofrecieron alquilar Netwalker a estafadores solitarios a cambio de una porción de la ganancia por el ataque. Como parte de su mayor desarrollo, Netwalker lanzó un sitio de filtración de datos automatizado que permite a los afiliados cargar datos robados y programarlos para su publicación en una fecha y hora específicas.

En enero del 2021, la policía acabó con los recursos de Netwalker en la dark web y acusó al ciudadano canadiense Sebastien Vachon-Desjardins de obtener más de 27,6 millones de dólares en actividades de extorsión. Vachon-Desjardins era el responsable de encontrar víctimas, violar su seguridad y desplegar Netwalker en sus sistemas. La operación policial acabó con Netwalker.

3. Conti, también conocido como el ransomware IOCP

Conti apareció a finales del 2019 y estuvo muy activo durante el 2020; fue responsable de más del 13 % de todas las víctimas de ransomware durante ese periodo y sus creadores siguen en activo.

Su principal característica es que es uno de los ransomware más rápidos. Conti utiliza 32 hilos simultáneos de CPU, lo que permite que cifre muy

El primer caso notable de ransomware de triple extorsión fue el golpe sufrido por la clínica Vastaamo, en octubre de 2020

rápido todo el disco duro o cualquier fichero que se le ponga delante. Como explican los expertos, cuanto más rápido es el ransomware, antes puede pasar desapercibido ante cualquier sistema de alerta, desde los reactivos hasta los preventivos.

Este ransomware no solo cifra, sino que también envía copias de los archivos desde los sistemas atacados a los operadores del ransomware. Después, los ciberdelincuentes amenazan con publicar la información online si la víctima no cumple con sus exigencias. Entre los ataques de Conti de más alto perfil se encuentra el ataque a una escuela de los Estados Unidos, seguido de una demanda de rescate de 40 millones de dólares. (La administración afirmó que habría afrontado hasta un pago de 500000 dólares, pero que no iba a negociar una suma tan desorbitad como la que proponían).

4. DoppelPaymer

A principios de diciembre de 2020, el FBI emitió una advertencia sobre DoppelPaymer, una familia de ransomware que apareció por primera vez en 2019 cuando lanzó ataques contra organizaciones en industrias críticas. Sus actividades han continuado a lo largo de 2020, incluidas una serie de incidentes en la segunda mitad del año que dejaron a sus víctimas luchando por llevar a cabo adecuadamente sus operaciones.

Se cree que DoppelPaymer se basa en el ransomware BitPaymer (que apareció por primera vez en 2017) debido a similitudes en su código, notas de rescate y portales de pago. En todo caso, el aspecto más exclusivo de este ransomware es el uso de una herramienta llamada Process Hacker, que utiliza para finalizar servicios y procesos relacionados con la seguridad, el servidor de correo electrónico, la copia de seguridad y el software de base de datos para afectar las defensas y evitar la violación de acceso durante el cifrado.

Como muchas familias modernas de ransomware, las demandas de rescate de DoppelPaymer por el descifrado de archivos son considerables, oscilando

No more Ransom!

No More Ransom (NMR) es una iniciativa del Centro Europeo de Ciberdelincuencia de Europol, la Unidad Nacional de Delitos de Alta Tecnología de la policía de los Países Bajos y McAfee para ayudar a las víctimas de ransomware a recuperar sus datos cifrados sin tener que pagar a los delincuentes, ofreciendo una tercera opción que antes no tenían. NMR muestra el valor de la cooperación público-privada para interrumpir las actividades delictivas con conexiones de ransomware.

Lanzado en julio de 2016, el portal en línea ha ayudado a más de 200 000 personas, y se ha convertido en más de 150 socios de apoyo de las fuerzas del orden, el sector privado y el mundo académico. Los recursos están disponibles en 36 idiomas diferentes y cuenta con más de 90 herramientas capaces de descifrar más de 100 tipos diferentes de ransomware.

entre 25.000 y 1,2 millones de dólares. Además, a partir de febrero de 2020, los actores maliciosos detrás de DoppelPaymer lanzaron un sitio de filtración de datos y amenazan a las víctimas con la publicación de sus archivos robados en este site como parte del plan de extorsión del ransomware.

5. Maze, también conocido como ChaCha

Desarrollado como una variante del ransomware ChaCha, Maze se descubrió inicialmente en mayo de 2019 por Jerome Segura y desde finales del mismo año ha estado muy activo para convertirse, el año pasado es una de una de las más notorias familias de ransomware que amenazan a grandes empresas y organizaciones. Docenas de ellas han sido víctimas de este vil malware, como LG, Southwire, y la ciudad de Pensacola.

El grupo responsable de Maze fue uno de los primeros en robar datos antes de cifrarlos. Si la víctima se negaba a pagar el rescate, los ciberdelincuentes amenazaban con publicar los archivos robados. La técnica demostró su eficacia y más tarde fue adoptada por muchas otras operaciones de ransomware.

Otra innovación es que los ciberdelincuentes comenzaron a informar sobre sus ataques a los medios.

6. Nephilim

Su objetivo son las 'One Billion companies' y ejecuta tácticas de doble extorsión para asegurar el pago de sus víctimas

Cuando apareció por primera vez, los investigadores de ciberseguridad descubrieron que los códigos de recursos de Nephilim son muy similares al ransomware Nempty. No solo los códigos eran similares, sino también el diseño, la actitud era la misma. Ambos amenazaron a su víctima con publicar datos sensibles en caso de que no pagaran el rescate exigido.

Las víctimas de Nephilim suelen ser grandes organizaciones y empresas. En diciembre, los atacantes planearon atacar organizaciones gubernamentales y empresas utilizando la debilidad que descubrieron en los dispositivos de Citrix Gateway. Además, lograron cifrar los datos de las víctimas utilizando la vulnerabilidad de una red de escritorio remota y una VPN.

El Ransomware como servicio (RaaS), que permitió la entrada de ciberdelincuentes sin amplios conocimientos técnicos y disparó los ataques, puso de manifiesto la rentabilidad de la amenaza

Como muchas familias modernas de ransomware, las demandas de rescate de DoppelPaymer por el descifrado de archivos son considerables: entre 25.000 y 1,2 millones de dólares

En la nota de rescate, se ha enfatizado que los datos han sido encriptados por un algoritmo de nivel militar y se han violado datos confidenciales. Para demostrar su autoridad, los atacantes Nephilim exigen dos archivos cifrados a las víctimas, los descifran y los envían de vuelta a las víctimas para que las víctimas se convenzan de que son las únicas que pueden descifrar los archivos.

7. Tycoon Ransomware

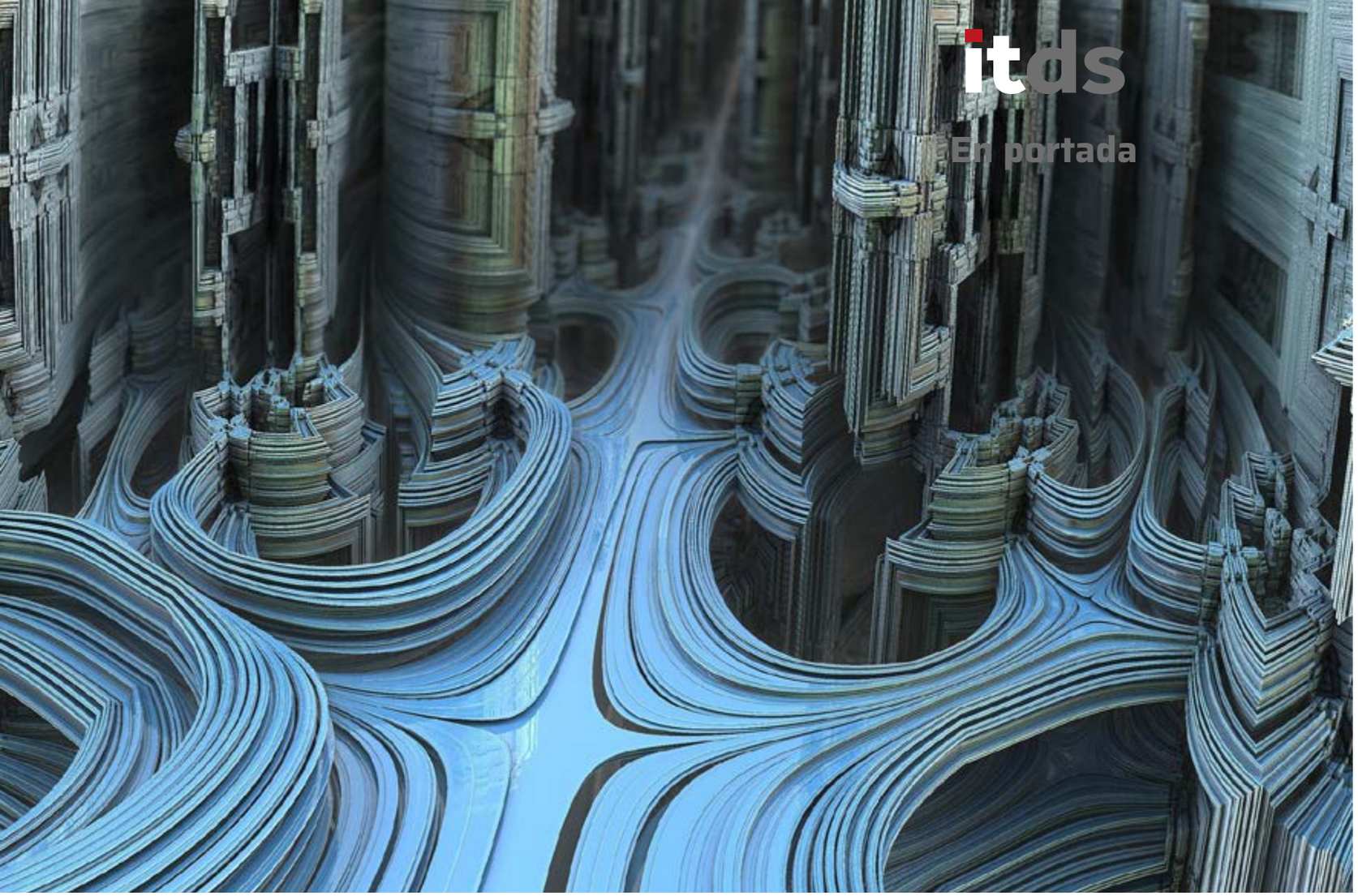
Tycoon es un tipo de ransomware descubierto recientemente y que se dirige contra el sector educativo, principalmente institutos, el mercado del software y las pymes.

Ha sido escrito en Java y según investigadores de Blackberry y KPMG las técnicas utilizadas por los atacantes son inusuales y dignas de mención porque se agregó a una versión troyana de Java Runtime Environment. También es la primera vez que una compilación JRE personalizada y maliciosa utiliza el formato JIMAGE en Java.

Desde que se identificó hace seis meses, Tycoon ha mostrado un enfoque agresivo. Sin embargo, el número de víctimas de este ataque es limitado. Se sabe que sus atacantes utilizan diversas técnicas para permanecer ocultos.

El Coste del Ransomware y otros datos

El coste de recuperación de un ataque de ransomware se ha duplicado en un año, pasando de los 761.106 dólares de 2020 a los 1,85 millones de 2021 lo que significa que el coste medio de recuperación de un ataque de ransomware es ahora 10 veces el tamaño del pago del rescate, en promedio, según datos del Informe El estado del ransomware 2021 publicado por Sophos, que recoge también



que el rescate medio pagado es de 170.404 dólares. Al respecto comentar que, si bien el rescate más alto pagado por los encuestados fue de 3,2 millones de dólares, el más habitual fue de 10.000 dólares. Además, diez organizaciones pagaron rescates de un millón de dólares o más.

El informe, elaborado con las respuestas de 5.400 responsables de IT de empresas medianas en 30 países de Europa, América, Asia-Pacífico y Asia Central, Medio Oriente y África, también recoge que solo el 8% de las organizaciones lograron recuperar todos sus datos después de pagar un rescate, y que el 29% no recuperó más de la mitad de sus datos.

Explica también la compañía que, si bien la cantidad de organizaciones que experimentaron un ataque de ransomware se redujo del 51% de los encuestados en 2020 al 37% en 2021, y menos organizaciones sufrieron cifrado de datos como resultado de un ataque significativo (54% en 2021 en comparación con 73% en 2020), los resultados de la nueva encuesta revelan tendencias ascendentes preocupantes, particularmente en términos del impacto de un ataque de ransomware.

Más de la mitad (54%) de los encuestados cree que los ciberataques son ahora demasiado avanzados para que su equipo de TI los maneje por sí mismos.

El panorama de las ciberamenazas continúa volviéndose más complejo y sofisticado. Los intentos de ataques y violaciones de datos son inevitables, y ninguna organización quiere enfrentarse a la decisión de pagar un rescate o perder datos importantes. Con esto en mente, las organizaciones deben abordar la ciberseguridad y la protección contra amenazas con las últimas tecnologías y por capas para estar un paso por delante de los malos actores.

Enlaces de interés...

- Así ha evolucionado la cadena de ataque del ransomware
- El ransomware crece un 160% en el último año
- El 80% de las empresas que pagaron un rescate sufrieron un nuevo ataque de ransomware
- Diez imprescindibles para prevenir un ataque de ransomware

Compartir en RRSS

SECURE ACADEMY

TU CENTRO AVANZADO DE FORMACIÓN EN CIBERSEGURIDAD

www.secureacademy.es

Secure&IT by LKS

MAR LÓPEZ GIL

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN

Jefa de la Oficina de Ciberseguridad y lucha contra la desinformación del Departamento de Seguridad Nacional, Mar López Gil es Licenciada en Administración y Dirección de Empresas, posee diversos master, entre ellos: Dirección y Gestión de la Seguridad de la Información, Dirección y Planificación de Proyectos, y cursos de especialización en dirección de empresas, tecnologías aplicadas y gestión de proyectos.
El 1 de octubre de 2012 entro a formar parte de la Oficina de Asuntos Estratégicos del Departamento de Seguridad Nacional y, en abril de 2013 es nombrada Jefa de Seguridad, y posteriormente Jefa de la Oficina de Ciberseguridad.
También es miembro del Management Board de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y es Vicepresidenta del capítulo español del Women4Cyber.

¿Preparados para la transformación digital?

Llevamos muchos años en el camino de lo que hoy venimos a denominar transformación digital. Llevamos también años hablando sobre la necesidad de conocimientos y habilidades tecnológicas y, aunque se han hecho esfuerzos en este sentido, parece que en ningún momento nos hemos dado cuenta de que esto seguía avanzando. Ahora nos enfrentamos al reto de esta transformación digital y aunque hemos gestionado la incertidumbre de la mejor manera posible, no estábamos preparados, ni creo que lo estemos ahora.

No hemos sabido responder a la demanda del mercado laboral, nos encontramos con que no contamos con el número de profesionales que el mercado demanda.

Por otro lado, me gustaría reivindicar que no falta talento. Creo sinceramente que el talento es innato, que existen personas con habilidades y capacidades innatas en uno o varios ámbitos o actividades. En el caso de la ciberseguridad así lo es y así lo creo. Como apunto, el talento está, pero en muchas ocasiones hay que orientarlo, hay que formarlo, atraerlo y retenerlo, cuestiones sumamente complejas y difíciles de abordar en los tiempos actuales.

En cuanto a la retención, es esencial la motivación. Algunas encuestas plantean que el personal de ciberseguridad es el más difícil de retener - en

La Nueva Estrategia de Ciberseguridad de la UE, aprobada en diciembre de 2020, incluye como objetivos mejorar las capacidades de la población activa, desarrollar, atraer y retener un talento más diverso en materia de ciberseguridad e invertir en investigación e innovación

comparación con el 25% de todos los empleados, el 65% de los trabajadores de ciberseguridad están considerando activamente dejar su puesto-.

La permanencia promedio de un director de seguridad de la información es de menos de dos años y algunas de las razones podrían ser: la falta de concienciación de la importancia de la ciberseguridad por parte de la alta dirección; las expectativas laborales poco claras o la falta de oportunidades formales de desarrollo de habilidades o, muy importante y ligado al mundo de las certificaciones: la falta de oportunidades formales de desarrollo de habilidades o declaración clara de deberes y responsabilidades.

Siguiendo con la motivación, en España, el Foro Económico mundial en su Índice global de competitividad del talento, en base al análisis de 132 países, plantea que nuestro país se encuentra en el puesto 32 del Ranking, en la media, pero en el puesto 45 en atracción de talento y en el puesto 53 en lo que se refiere a la disponibilidad de trabajadores con habilidades técnicas y vocacionales, aunque no situamos en el nivel 23 en calidad de vida.

En resumen y siendo crítica sobre la situación, creo que no hemos sabido adaptar la formación y la cualificación a la demanda de profesionales digitales, y mucho menos en el marco de la ciberseguridad; no hemos sido capaces de preparar suficientemente a trabajadores con habilidades técnicas y profesionales y por supuesto quizás menos en las soft skills, y por último no hacemos los suficientes esfuerzos en lo que se refiere a la retención del talento desde una perspectiva ligada la motivación, el reconocimiento, las expectativas laborales y el crecimiento profesional.

La situación no es fácil, ni quizás hayamos alcanzado los objetivos que se persiguen para dotar al mundo de la ciberseguridad de profesionales suficientes, pero este problema global se viene trabajando desde organizaciones internacionales y europeas para hacer que esta brecha sea cada vez menor.

No hemos sabido adaptar la formación y la cualificación a la demanda de profesionales digitales, y mucho menos en el marco de la ciberseguridad

Por poner algunos ejemplos

La Unión Internacional de Telecomunicaciones de Naciones Unidas apunta que la brecha de la fuerza laboral en ciberseguridad y a la necesidad de profesionales en ciberseguridad sigue siendo alta.

Así y, basándose en datos del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información o (ISC) para 2021, el número de puestos de ciberseguridad sin cubrir será de 4,07 millones y para llenar este vacío, apuntando a que la sociedad debe tomar medidas para aumentar al menos un 145% de la fuerza laboral en esta área.

Algunas de las medidas que apoya son la atracción de mujeres que aportan, por una parte efectividad y crecimiento organizacional (las organizaciones con tres o más mujeres en funciones de alta dirección puntúan más alto en todas las dimensiones del desempeño organizacional); y por otro lado de atracción de jóvenes que, no solo pueden aportar enfoques frescos e innovadores al campo, sino que son esenciales si pretendemos cubrir la creciente brecha de mano de obra en este ámbito; más aún a medida que aumenta la dependencia de las tecnologías digitales.

Por otro lado, en 2016 la Organización para la Seguridad y la Cooperación en Europa (OSCE), formada por 57 Estados participantes repartidos entre tres continentes (América del Norte, Europa y Asia), fomenta el programa Mujeres en la Primera Dimensión que busca promocionar su participación como expertas y ponentes en reuniones y conferencias de la OSCE para dar visibilidad a las mujeres dedicadas al ámbito de la Seguridad

En cuanto a la Unión europea, la Nueva Estrategia de Ciberseguridad de la UE, aprobada en diciembre de 2020, incluye como objetivos mejorar las capacidades de la población activa, desarrollar, atraer y retener un talento más diverso en materia de ciberseguridad e invertir en investigación e innovación. También alude al Plan de Acción de Educación Digital dirigido a aumentar la concienciación sobre la ciberseguridad entre los ciudadanos, especialmente los niños y jóvenes, y las organizaciones, particularmente las pymes.

Asimismo, la estrategia recoge el fomento de la participación de las mujeres en el ámbito de las TIC y por supuesto a la educación —incluida la formación profesional (FP), la concienciación y los ejercicios— aumentando así las capacidades en

materia de ciberseguridad y ciberdefensa a nivel de la UE.

A su vez, la Agencia Europea de Ciberseguridad (ENISA) viene desarrollando diversos proyectos y publicaciones en este sentido como, por ejemplo: el Desarrollo de habilidades de ciberseguridad en la UE, donde reconoce la escasez de mano de obra en ciberseguridad y la brecha de habilidades, y que Europa está rezagada en el desarrollo de un enfoque integral para definir un conjunto de roles y habilidades relevantes para el campo de la ciberseguridad e indica que es una preocupación tanto para el desarrollo económico como para la seguridad nacional, especialmente por la rápida digitalización de la economía global.

A la par, apuesta por el desarrollo de un marco europeo de competencias en ciberseguridad como paso esencial hacia el futuro digital de Europa que tenga en cuenta las necesidades de la UE y de cada uno de sus Estados miembros, creando un entendimiento común de las funciones, competencias, habilidades y conocimientos utilizados por y para las personas, los empleadores y los proveedores de formación en los Estados miembros de la UE con el fin de abordar la escasez de competencias en ciberseguridad.

Resaltar que ENISA puso en marcha un grupo de trabajo ad hoc sobre el marco europeo de competencias en ciberseguridad para reunir a un grupo multidisciplinar de expertos con el objetivo de promover la armonización en el ecosistema de educación, formación y desarrollo de la fuerza laboral en

En 2021 el número de puestos de ciberseguridad sin cubrir será de 4,07 millones

ciberseguridad y desarrollar una lengua europea común en el contexto de las habilidades en ciberseguridad.

En el ámbito nacional, España cuenta con tres documentos oficiales, que avalan las acciones que se están llevando a cabo en materia de talento y habilidades en Ciberseguridad.

- **La Estrategia Nacional de Ciberseguridad en su Objetivo IV:** Cultura y compromiso con la ciberseguridad y el empoderamiento de las capacidades humanas y tecnológicas" y en su "Línea de acción 5: Fortalecer la industria española de la ciberseguridad y la generación y retención de talento, para el fortalecimiento de autonomía digital (medidas 5 a 8) "podemos encontrar todas las medidas relacionadas con la promoción del talento.
- Por otro lado, **la Agenda Digital "España Digital 2025" en su línea 4:** Ciberseguridad (medida 14.2 - (2), recoge la generación, identificación y desarrollo de talento en ciberseguridad, para

El Plan de Acción de Educación Digital está dirigido a aumentar la concienciación sobre la ciberseguridad entre los ciudadanos, especialmente los niños y jóvenes, y las organizaciones, particularmente las pymes

incrementar capacidades y dar respuesta al crecimiento del sector y de la industria de la ciberseguridad española).

- **El Plan Nacional de Habilidades Digitales** prevé reformas públicas e inversiones por importe de 3.750 millones de euros y sus objetivos son garantizar la inclusión digital, reducir la brecha digital entre hombres y mujeres, garantizar la digitalización de la educación, promover la adquisición de las competencias digitales de los desempleados y de trabajadores, aumentando el número de especialistas en TIC y promoviendo las competencias digitales necesarias de las empresas.

Con este marco en mente, se puso en marcha en julio de 2020 el Foro Nacional de Ciberseguridad (FNCS). Un espacio de colaboración público-privada impulsado por el Consejo de Seguridad Nacional, con la presidencia del Departamento de Seguridad Nacional y la colaboración de INCIBE (Instituto Nacional de Ciberseguridad de España) y el CCN (Centro Criptológico Nacional), que ostenta las dos vicepresidencias.

El Foro, alineado con los documentos antes mencionados, está trabajando en varias actuaciones enfocadas a generar cultura de ciberseguridad; apoyo a la Industria e I + D + i y formación y talento en ciberseguridad conforme a las demandas de la industria en cuanto a talento y habilidades.

Recientemente, se han finalizado los primeros trabajos que han tenido como resultado el Libro Blanco sobre cultura de ciberseguridad, el Libro Blanco sobre el sector de la ciberseguridad en España y el desarrollo de un Esquema nacional de certificación de responsables de ciberseguridad. El Esquema determinará los perfiles y competencias y los procedimientos para certificar a los responsables de ciberseguridad de los sectores público y privado. Constituye un marco de competencia en ciberseguridad para responder a las necesidades del mercado laboral, promueve la capacitación especializada y el desarrollo de los profesionales y estimula al mismo tiempo la detección y retención de talento.

Paralelamente y de manera coordinada, INCIBE está ejecutando acciones adicionales en el ámbito de las competencias en ciberseguridad que incluyen la puesta en marcha de un Servicio de Análisis y Diagnóstico del Talento en Ciberseguridad con el fin de determinar la necesidad real de perfiles a nivel nacional.

Enlaces de interés...

- Trabajar desde los cimientos para construir un futuro diverso e inclusivo en la ciberseguridad
- La gestión de los datos está en el corazón de la seguridad en la nube
- Women4Cyber Spain en el Día Internacional de la mujer
- Te han 'hackeado', y ahora, ¿cómo se lo comunicas a tus clientes?

it User
TECH & BUSINESS

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

Quitar al cliente del centro de la organización...

...Y ponerlo al principio y al final de la cadena de creación de valor de la compañía debería ser objeto de reflexión para replantear la relación entre ambas partes. Hace más de medio siglo que el concepto *"customer centric"* fue avanzado por Lester Wunderman cuando desarrolló las bases de lo que sería el marketing directo, y más tarde el relacional, para poder personalizar la comunicación de la oferta de productos y servicios

JOSÉ MANUEL NAVARRO

CMO MOMO GROUP

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

Compartir en RRSS

de una empresa tomando como punto de referencia el perfil de los consumidores, construido a partir del seguimiento de su conducta de consumo. De esta forma nació el marketing centrado en el cliente que, luego, daría lugar a la idea de situar al cliente en el centro de la organización.

El tiempo, la tecnología y los nuevos modelos de negocio han ayudado a formalizar las relaciones con los clientes de una manera más estrecha, a generar un conocimiento más profundo de sus necesidades y expectativas y a alcanzar el objetivo de generar una adecuada experiencia de usuario con independencia de los puntos o canales de contacto que se establezcan en la estrategia comercial. Organizar la empresa en torno al cliente implica la creación de procesos de toma de datos relevantes para las métricas que deben ayudar a analizar cada una de las etapas del denominado "Customer journey", o fases por las que "viaja" un cliente desde que toma conciencia de una necesidad hasta que realiza la compra y, más allá de ese instante, actúa como prescriptor de la marca. En este modelo, todas las áreas de la organización ponen su foco en los procesos que aportan valor a la relación a largo plazo con el cliente, pero es ésta una relación básicamente unidireccional en lo que a diseño, producción y distribución de los productos y servicios se refiere. Aunque se construyan en base a la información obtenida de los consumidores que más rentabilidad aportan a la empresa, existe un "gap" entre lo que estos necesitan, lo que creen que necesitan, lo que la empresa entiende que son sus necesidades y lo traslada al diseño de los productos o servicios que pueden cubrirlas y la satisfacción de las expectativas de aquellos.

> Escuchar quizá sea la actividad más trascendente que pueda realizar una empresa, ya que, escuchando a sus clientes y a sus empleados, de manera activa, obtendrá información directa y veraz que le permitirá establecer vínculos más estables y fuertes al desarrollar empatía hacia ellos

Para salvar esta situación, se creó el concepto de "buyer persona" que conjuga las características de los mejores clientes, y de los potenciales a los que conquistar, para construir el perfil del cliente ideal o perfecto. El que ha de servir de referencia para orientar los esfuerzos de diseño y de desarrollo de producto/servicio, de creación de acciones de

Nuevos tiempos exigen la reorganización de la compañía para integrar al cliente (todos, no solo el mejor ni el ideal) en sus procesos, incluidos los de innovación y desarrollo

comunicación y argumentarios comerciales, de determinación de los canales más efectivos de venta y los más resolutivos de postventa y de atención al cliente. En definitiva, el "buyer persona" es el que orienta los objetivos de cada una de las áreas de la compañía para incrementar, no el porcentaje de ventas (que será la consecuencia), sino el número de clientes fieles y la consolidación de los atributos de marca que encajan con las expectativas y aspiraciones de estos.

Construir el perfil de "buyer persona" implica la recopilación y análisis de infinidad de datos cuantitativos y cualitativos de variables sociodemográficas, de conductas de uso de los canales de búsqueda y de compra, de tendencias y de asociación de atributos racionales y emocionales. Todo un ejercicio que conlleva la integración de información proveniente de acciones de investigación de fuentes internas (bases de datos históricas, red de empleados y stakeholders) y externas (informes, estadísticas y estudios públicos o particulares), de entrevistas o encuestas directas al público objetivo, de analíticas web y de redes sociales y, sobre todo, de investigaciones realizadas aplicando técnicas neurocientíficas para acceder a las respuestas inconscientes de los individuos.

Todo ello puede proporcionar una idea aproximada de quién es el cliente perfecto, quien toma la decisión de compra y, también, de quiénes pueden influir positiva o negativamente en ella. Todo ello aporta indudables ventajas a la compañía, ya que estará en disposición de conocer en profundidad a sus mejores clientes y, por consiguiente, cómo acercarse a ellos con mayor eficiencia (dónde están, cómo le prestarán atención, qué determinará el impulso de compra y cómo le recomendarán), sin perder de vista que este perfil ideal ha de ser dinámico, alineado con la evolución del mercado y el contexto social. Circunstancias como la pandemia de la Covid-19 han evidenciado cómo los usuarios han cambiado o modulado conductas y motivaciones que se creían estáticas y que, sin embargo, se han visto impedidas a adaptarse a unas circunstancias diferentes a las vividas hasta el momento.

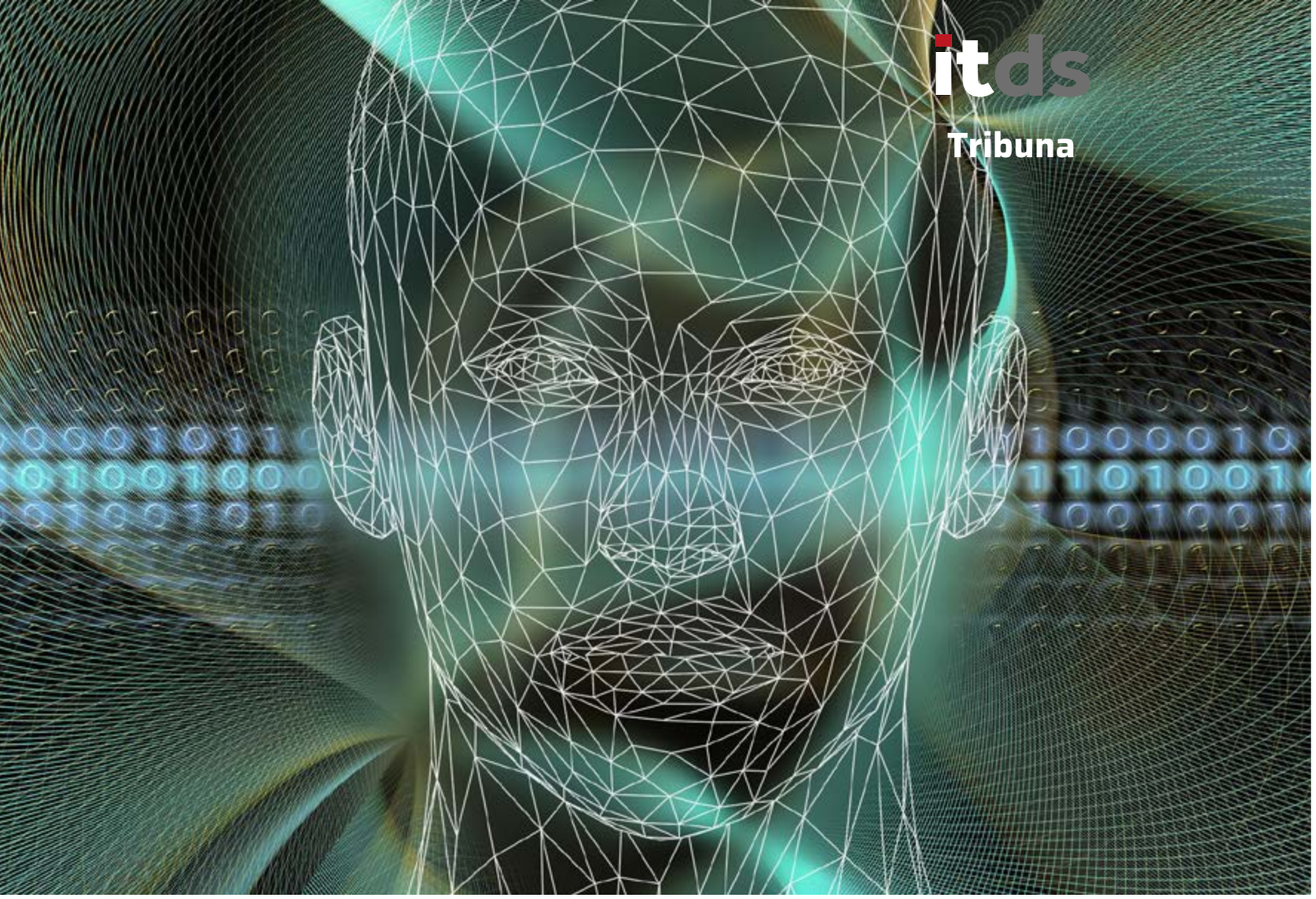
En ambos modelos, "Customer centric" y "Buyer persona", se priorizan a los mejores clientes, los más valiosos, o al perfil ideal para establecer la

estrategia de negocio en la que la inversión principal recaerá sobre ellos para obtener un adecuado retorno, aunque no se debe olvidar al resto de consumidores que aportan menos valor, pero que sí ayudan a hacer caja cada día a pesar de que lo hagan de manera ocasional. En conjunto todos deben ser importantes, unos porque ya son fieles a la marca y otros porque tienen un largo recorrido de mejora que puede generar más valor del esperado si pasan de adquirir un producto o servicio a establecer un vínculo más estrecho. Para establecer la mejor estrategia con cada uno de ellos para que obtengan una experiencia única y completa en todos los puntos de contacto, se han de seguir unos criterios y procesos específicos como son la asignación del valor que supone cada cliente (adquirirlo, mantenerlo y perderlo), la personalización de las acciones de comunicación y de la oferta, el uso de herramientas de análisis de datos (CRM) y la habilitación de canales para hablar con ellos, no solo como un servicio convencional de atención al cliente, sino para escucharlos.

Escuchar quizá sea la actividad más trascendente que pueda realizar una empresa, ya que, escuchando a sus clientes y a sus empleados, de manera activa, obtendrá información directa y veraz que le permitirá establecer vínculos más estables y fuertes al desarrollar empatía hacia ellos. Algo que debería estar priorizado en la cultura corporativa para entender las necesidades reales de los consumidores, quienes, en la mayoría de las ocasiones, no saben definir con exactitud qué puede satisfacer una necesidad subyacente porque ésta no ha pasado a su lado consciente y, por tanto, les es imposible verbalizarla.

Ser una empresa empática implica que toda la organización (todos los empleados sin excepción) deben participar en ese proceso, asumiendo que es fundamental conectar emocionalmente con sus clientes desde cualquier área de la compañía, no

El tiempo, la tecnología y los nuevos modelos de negocio han ayudado a formalizar las relaciones con los clientes de una manera más estrecha



Enlaces de interés...

W Cómo el Covid-19 está forzando a los CEOS a cambiar la estructura organizativa de los negocios

solo desde la comercial o de negocio. Para ello, es necesario que todos los empleados tengan acceso a la información relevante que permite comprender y conocer a cada cliente, y disponer de los canales necesarios para que ese contacto sea efectivo y para que de él resulte una experiencia útil para el cliente (CX) y para el empleado (BX). A pesar de que la tecnología permita la habilitación de canales automatizados (como los chatbots), los usuarios siguen prefiriendo el contacto personal para interactuar y ser atendidos. Predilección que no debe ser despreciada en aras a la omnidigitalización, ya que se dejan escapar muchas oportunidades en las que los clientes pueden aportar "pistas" sobre las soluciones que están buscando e, incluso, a "cocrear" o participar en los procesos de diseño de los productos y servicios (figura que, en su momento, se denominó "prosumer").

Nuevos tiempos exigen la reorganización de la compañía para integrar al cliente (todos, no solo el mejor ni el ideal) en sus procesos, incluidos los de innovación y desarrollo, facilitando compartir valores y perseguir el mismo propósito como colectivo que reclama formar parte de un objetivo común, aunando esfuerzos y creencias en torno a causas justas, comprometidas con el futuro particular de cada parte y con el general de la sociedad. Los modelos "Customer Centric" y "Buyer persona" se han fortalecido usando los sistemas CRM (Customer Relationships Management) en los que la tecnología ha jugado un papel crucial para capturar, analizar y gestionar miles de millones de datos; es el momento de dejar este papel a los sistemas DRM (Dasta Relationships Management) y que tome forma el sistema CMR (Customer Manages the Relationship). Priorizando, para lograrlo, cambios en la estructura y en la forma de trabajar que antepongan la relación de personas a personas como estrategia principal de la empresa.

it Reseller
TECH&CONSULTING

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