COMPARATIVA - - - > Portátiles para teletrabajar

www.revistabyte.es
Mayo 2020
Nº 282 • 5,75 euros

byte TI

20 años

Síguenos en twitter: (@BYTE_TI)

ANÁLISIS

Samsung S20+ 5G

Cómo la nube salvó a las empresas del Covid-19

- Las principales ventajas
- La importancia de la seguridad
- Retos futuros

Herramientas de colaboración

Coronavirus: una oportunidad para la digitalización

8 424094 003815 00135

JAVIERLOPEZSAEZ

¡Gracias, Asesores!

Por ser siempre apoyo incondicional
para Pymes y Autónomos,
el 99,8% de las empresas del país

Nuestro aplauso es también para vosotros

#AplausoAsesores

Wolters Kluwer

Siempre pensando en mañana ;)

La tecnología decidirá quién acabará antes

En esta crisis es una obligación que todos arrimemos el hombro para ayudar a un montón de gente que se ha quedado sin nada. En nuestro sector, he visto acciones de calado por partes de las principales operadoras y de otras tecnológicas, pero me faltan contribuciones de los grandes de empresas como Google o Facebook...

El mes pasado, después de haber estado en un centro médico por un tratamiento periódico, tuve unos sospechosos síntomas de padecer el Coronavirus y me asusté bastante. Por lógica, con la congestión de las unidades médicas, en aquel momento, me tendrían que poner a la cola para tratarme, y yo no iba a ser una prioridad. Al final, todo quedó en una falsa alarma.

Esta disyuntiva, de salvar al que tiene más probabilidades, es un poco paradigmática de lo tenemos encima como sociedad.

Es una situación muy límite, pero me atrevo a abrir el debate de que tal vez en esta crisis haya que sacrificar vidas. Me explico: si no se normaliza la actividad económica, la situación puede ser más letal que el propio virus.

Y esto es lo que está aplicando en la actualidad el arrogante de Trump. ¿Alguien se cree que este demagogo puede estar tomando decisiones de calado? No nos engañemos, Estados Unidos, y quizás otros países como Alemania o UK, seguro que están utilizando las herramientas que proporciona Big Data o la IA para tomar las mejores decisiones, no tengo la menor duda. Disponen de mucha información sobre lo que ha pasado en China, Corea, Italia o España y otros muchos recursos para analizar: esos sistemas expertos, seguramente les están confirmando que la mejor solución es intentar volver a la normalidad, a costa de unos cuantos cientos de miles de vidas. No me atrevo a afirmar que esto esté bien o mal hecho.

Mientras tanto, en España tenemos un comité de expertos que te recomienda que lleves a los niños a los supermercados o a las farmacias para, a las pocas horas, cambiar de opinión. Tenemos que sufrir un Gobierno incapaz, en el que el jefe es un mentiroso compulsivo y su socio, vicepresidente, por no saber, no sabe ni cuál es la talla de su americana. Como dice mi amigo Héctor, en esta situación no se les exigía tener una vacuna, ni siquiera un tratamiento efectivo. Tan solo una cosa muy sencilla: que no fallaran en algo que está al alcance de unos buenos profesionales, la logística. Porque era un tema logístico tener los equipos adecuados para nuestros sanitarios y las demás protecciones para el conjunto de la ciudadanía. Han fallado en lo que tenían a su alcance y entre otros se lo han tenido que proporcionar empresas como Inditex, Telefónica, Santander, Iberdrola, ACS o BBVA que han puesto su dinero y su logística para traer el material mientras otros disfrutaban de su jardín..

Han fallado en todos los órdenes. Han demostrado que no sirven para gobernar. No han sabido responder al PP y a los nacionalistas, que también tienen su responsabilidad porque todas las competencias sanitarias están transferidas: los recortes los hicieron todos y ahora se ha notado.

Estamos a la intemperie. Lo único que nos puede salvar es una vacuna o un tratamiento efectivo. No va a dar tiempo ni a echarles.

SUMARIO

TEMA DE PORTADA

La nube como salvación

50

N.º 282 • ÉPOCA III

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

Managing Director
Ignacio Sáez (nachosaez@mkm-pi.com)

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

Redacción
Vanesa García (vgarcia@revistabyte.es)

Coordinador Técnico
Javier Palazon

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

Fotógrafos
E. Fidalgo, S. Cogolludo, Vilma Tonda

Ilustración de portada
Javier López Sáez

Diseño y maquetación
El Palíndromo Comunicación S.L.

WebMaster
NEXICA
www.nexica.es

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

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

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

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

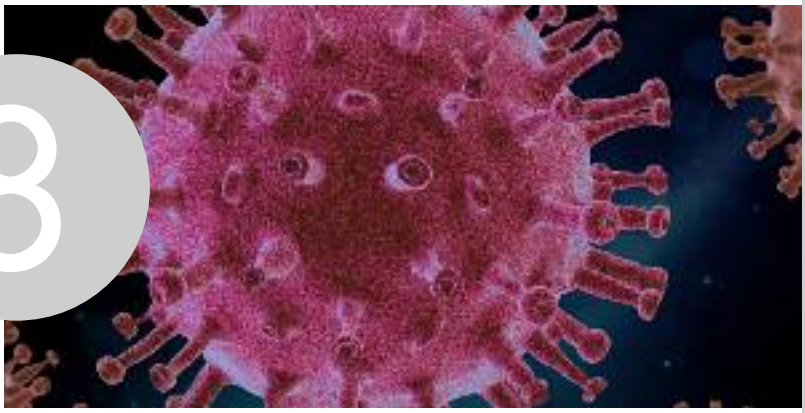
Depósito legal
B-6875/95

MAYO de 2020
Printed in Spain

EDITA
Publicaciones Informáticas MKM

ACTUALIDAD DEL MES

8



COMPARATIVA PORTÁTILES

38

TENDENCIAS

66

Dynabook Tecra A30-G

Dynabook ha ampliado su gama media Tecra con el lanzamiento del Tecra A30-G. El nuevo equipo, de sólo 1,2 kg de peso y pantalla de 13,3", tiene 15 horas de autonomía y un procesador Intel de 10ª generación.
Gracias a esta novedad, la compañía continua ampliando su gama media de portátiles profesionales para ajustarse a las necesidades de movilidad y de presupuesto de las pymes, así como de sectores como la educación o la administración pública. El dispositivo permite una alta legibilidad incluso con escasa iluminación gracias a su pantalla antireflejos, y su opción Full HD de bajo consumo de energía para una mayor luminosidad. Además, cuenta con un chasis de magnesio ligero pero resistente, y panel táctil con tecnología Precision Touch Pad.
Como todas las gamas de Dynabook, el A30-G incorpora una de serie prestaciones de seguridad avanzadas. En concreto, incluye;

- BIOS propia de Dynabook
- Chip Trusted Platform Module, para configurar los puertos con el nivel de accesibilidad.
- Autenticación biométrica, para iniciar sesión
- Smartcard opcional
- Windows Hello, basada en infrarrojos y lector de huellas dactilares.

También ofrece una gran variedad de opciones para su conectividad y la opción de conectarse a través de su puerto USB tipo C y otro opcional, su puerto de vídeo HDMI y su adaptador USB-C para conectividad VGA.

Adobe Productions

Adobe Creative Cloud ha presentado "Productions", una nueva novedad en su software de edición de video, Premiere Pro. Esta herramienta desarrollada con la contribución de los principales cineastas y equipos editoriales de Hollywood ha sido diseñada para ayudar a los equipos de producción a trabajar de forma más colaborativa y eficiente.
Las aplicaciones creativas de Adobe están en continua evolución, satisfaciendo las necesidades del mundo real de los cineastas modernos. Por ello, Productions proporciona a los profesionales consolidados y a los aspirantes a guionistas, nuevas herramientas para organizarse, gestionar proyectos de forma eficiente y colaborar fácilmente.
Con la nueva herramienta Productions el control es tuyo, y es que los proyectos y recursos pueden almacenarse en su totalidad dentro de la red local, lo que permite que ningún contenido se encuentre en el cloud sin previo consentimiento y sin necesidad de una conexión a internet para su uso. Mientras que los archivos de vista previa renderizados por un editor están disponibles para todos los editores que utilizan ese proyecto, ya que todos comparten una misma configuración.

Denon Home 150

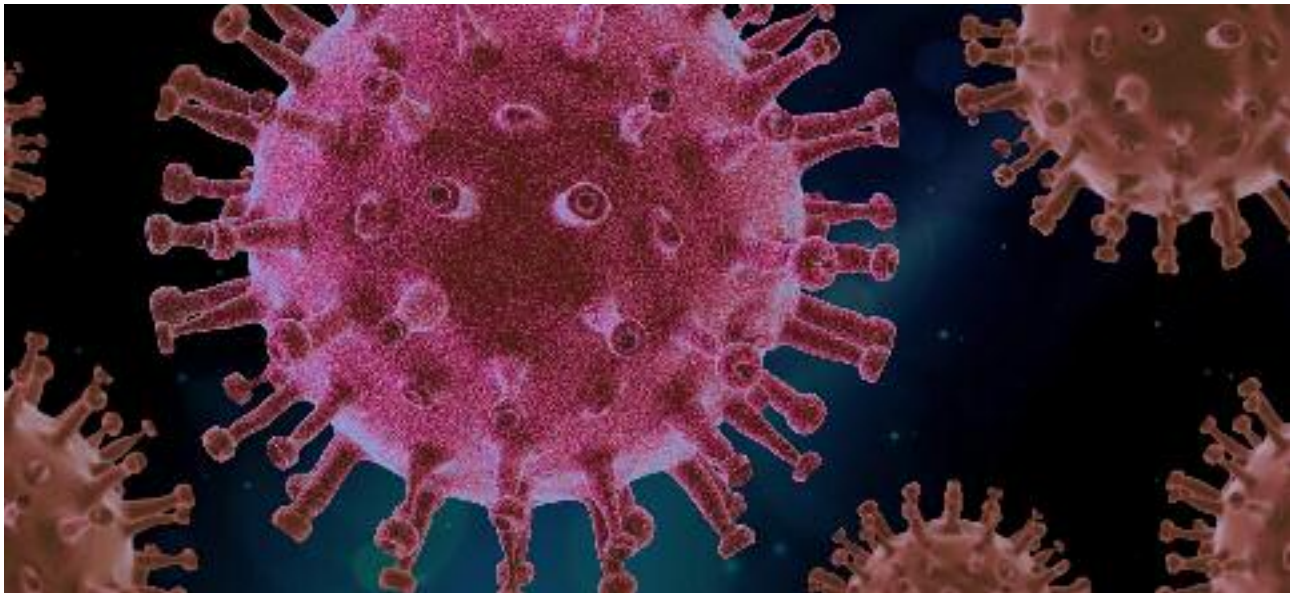
Denon cuenta con un nuevo sistema de audio compacto y portátil para disfutar del audio por toda la casa en total libertad: Denon Home 150. Un sistema de altavoces inalámbricos todo en uno con HEOS integrado, que combina un diseño moderno y limpio con la tecnología más puntera del momento

El equipo aporta la sencillez de configuración de un sistema de sonido multiroom y la experiencia de los 110 años que la compañía posee en el mercado del audio. Con unas reducidas medidas, es capaz de ofrecer un sonido impactante gracias a la combinación bidireccional de un woofer de 3,5 pulgadas y un tweeter de 1 pulgada. Bajo un elegante diseño desarrollado con materiales de elevada calidad, llama la atención su discrección, además de su resistencia al agua y a las manchas, que permite su uso en el baño o la cocina. Además, su nueva estética, que comparte con los otros altavoces de la línea Home, se centra en un panel sin botones que dispone de un sensor de proximidad, iluminándose los controles táctiles cuando se acerca la mano.

Es compatible con archivos ALAC, FLAC y WAV de hasta 192 kHz/24 bits y con pistas DSD 2,8 MHz y 5,6 MHz, consiguiendo una claridad cristalina. La versatilidad de la tecnología HEOS que lleva incorporada se traduce en una gran flexibilidad. Gracias a ella, es posible dotar de sonido propio a cada habitación, o bien, agrupar varios altavoces Denon Home o con barras de sonido compatibles, con el fin de reproducir la misma canción en toda la casa a través de la red doméstica.

Del mismo modo, dos altavoces Denon Home emparejados en estéreo pueden conectarse de manera inalámbrica a un subwoofer DSW-1H de Denon y, de esta forma, crear un sistema 2.1 capaz de ofrecer sorprendentes graves. Se pueden conectar un par de altavoces a modo de canales traseros envolventes a una barra de sonido Denon DHT-S716H y un subwoofer DSW-1H, creando así un sistema de sonido 5.1 completo.

Cómo los CIO también han hecho frente a Covid-19



Las empresas han tenido que adaptarse a la nueva realidad impuesta por Covid-19. Muchas de ellas han tenido que rescatar los planes de contingencia que tenían escondidos en el cajón y que nunca pensaron que llegaría un día en que se tendrían que utilizar.

Por Manuel Navarro

Pequeñas, medianas y grandes empresas. Ninguna de ellas estaba preparadas para mandar a la totalidad de sus empleados a trabajar desde su casa. Tal vez alguna de ellas ya tenía medidas para determinados trabajadores. Tal vez otras, por aquello de la conciliación de la vida laboral y familiar. Así que, todas han tenido que aprender de golpe. "La letra, con sangre entra" que decían antaño.

El departamento tecnológico es el que más ha sufrido. Muchas directivos han descubierto, por fin, el valor que tiene ese departamento y, gracias a la Covid-19, la figura del CIO, a quien muchos auguraban su desaparición, ha cobrado el protagonismo que se merece.

Ese protagonismo viene por haber hecho un trabajo intenso de todos los departamentos de tecnología de las empresas, en algunos casos de 24 horas diarias, todo con el objetivo de que las organizaciones pudieran mantener la productividad habitual. En algunos casos no sólo se trataba de mantener la actividad de los empleados sino también de otros usuarios. En el caso de las organizaciones educativas, por ejemplo, mantener conectados a los alumnos, mantener las clases y reforzar la comunicación profesor-alumno ha sido un hándi-

cap añadido que la mayoría de las instituciones han sabido superar con éxito. Un ejemplo es el de la Universidad Pontificia de Comillas donde "se han reforzado los canales de atención online, hemos actualizado los contenidos web que daban ayuda a estos canales de comunicación, y hemos reforzado la formación en herramientas y servicios TIC que ayudan al teletrabajo y la docencia online. Están siendo necesarias ingentes horas de videoconferencias para coordinar, alinear y sincronizar esfuerzos. Lo más importante ha sido informar y comunicar de la manera eficiente todo lo que ya existía en relación a procedimientos y usos de las TIC, y adaptarlo ligeramente a la nueva situación", asegura Luis Francisco Blanco, CIO de la Universidad.

Cada sector tiene su idiosincrasia y sus necesidades pero, en general, un porcentaje muy amplio de las necesidades TIC de las empresas son similares: conectividad, garantizar la comunicación,... En el caso de un despacho de abogados como Cuatrecasas fueron previsores y se adelantaron en casi una semana a la proclamación del estado de alarma. Tal y como afirma Francesc Muñoz, su CIO, "en la primera semana aceleramos un proyecto que empezábamos en piloto y por ejemplo el miércoles 11 instalábamos Zoom a toda la compañía y les asignamos también un auricular inalámbrico. Desde el viernes 13 toda la compañía, 1800 personas 98% con portátiles, estamos trabajando desde casa a pleno rendimiento y con todos los procesos y sistemas funcionando. Esa semana doblamos nuestro caudal de acceso a Internet en previsión de una posible saturación. El viernes 13 estresamos nuestro sistema de conexión remota (Firewall VPN). Al superar el millar de conexiones se saturó. Tuvimos que organizar inmediatamente una alternativa para dotar de los servicios más críticos y en paralelo a través del fabricante y distribuidor localizamos uno de mayor capacidad que instalamos esa madrugada. Todo al 100% desde entonces. Adicionalmente hemos lanzando multitud de sesiones de capacitación online tanto de uso de Zoom, como de trabajo remoto, etc., y también estamos aprovechando la oportunidad para desarrollar procesos más digitales como es la firma de contratos digitales, la realización de reuniones online y webinars con clientes, etc".

TRATO CON EL CLIENTE

Pero no siempre la tecnología puede valer, sobre todo si tus clientes tienen que ver con uno de los sectores más castigados por la pandemia de Covid-19 como es el turismo. En este caso una de esas empresas que prefiere mantenerse en el anonimatos afirma que "en el departamento de TI no hemos tenido problemas pues ya estábamos acostumbrados al teletrabajo y al uso de la VPN, crear cuentas nuevas no ha sido complicado y se ha afrontado bien. En los equipos de desarrollo, con equipos bastante más potentes de escritorio, en algún caso especial, se les ha autorizado a llevar el ordenador a casa firmando un papel de autorización. La mayoría de información y servidores ya estaban en la nube y por tanto no ha habido problemas con el teletrabajo. En algún caso para videoconferencias se ha tenido que ampliar contratando la aplicación Zoom que permiten más conexiones simultáneas. En las reuniones de con otras áreas noTI se está utilizando Teams y Hangouts de google sin problemas".

Sobresaliente

IBERMÁTICA

Ibermática ha alcanzado el nivel 5 de CMMI (Capability Maturity Model Integration) en sus servicios de Desarrollo y Mantenimiento de Aplicaciones para Kutxabank y ONCE, así como en su factoría de software, que está ubicada en Mérida. Se trata del máximo nivel de madurez que una organización puede lograr.

AYUDAS CONTRA EL COVID

Desde que se decretó el Estado de Alarma son muchas las ayudas que el Gobierno y las Comunidades están aprobando para ayudar contra el Covid-19. Pero hay para saber con seguridad si son beneficiarios de estas prestaciones o cómo, cuándo y dónde deben solicitarlas. Con el objetivo de hacer accesible todo este proceso, nace la iniciativa www.subsidioscovid19.es

Suspenso

MEDIOAMBIENTE Y TICS

La huella medioambiental del sector TIC, aunque no es la principal, sí es importante. Desde Commvault creen que una solución para reducirla pasa por apostar por los grandes proveedores de nube pública que operan sus centros de datos de forma muy eficiente y algunas generan su propia energía renovable

CIBERATAQUES Y COVID-19

Check Point ha advertido de la última estrategia de los cibercriminales en tiempos de covid-19, y es que están intentando obtener beneficios económicos con la situación en la que se encuentran muchas empresas y autónomos.A través del correo electrónico los cibercriminales envían mensajes con el asunto "Ayudas económicas frente al Covid-19" o "Pagos por el Covid-19" y adjuntan un archivo malicioso para distribuir malware como AgentTesla o troyanos como Zeus Sphinx

LA OPINIÓN DE
Fernando Jofre

El mundo será digital por defecto

COVID-19 nos está enseñando muchas cosas. Tanto en el plano personal como en el profesional. Salud, libertad, economía, seguridad y el valor de la información son las primeras ideas que me vienen a la cabeza. Y casi sin previo aviso nos ha abierto los ojos ante nuestro estado de madurez digital, del que tanto hablan las consultoras ante la realidad de la necesaria transformación digital de los negocios. Darwin nos vuelve a recordar la importancia de la capacidad para adaptarnos para sobrevivir. Y ponernos a teorizar sobre cómo será nuestro futuro no tiene mucho sentido, porque es un escenario inexplorado para todos nosotros.

Recibo en estos días un interesante estudio de la consultora Opinno que analiza las 10 tendencias post-COVID-19 que transformarán la sociedad. Y de todas ellas, quisiera resaltar dos: la primera, que el mundo será digital por defecto, y en el que la ciberseguridad será la clave. El consumo digital se disparará, las empresas y sus modelos operativos tendrán que adaptarse con automatización masiva (robótica e IA) y eliminación de la fricción de la tecnología. Y la segunda es la del "patriotismo industrial", de tal manera que el desabastecimiento reforzará la importancia de la investigación, de la producción propia y de la redefinición de la cadena de suministro.

Otro detalle importante que deja caer es que las predicciones se harán cada vez a más corto plazo, y que a las empresas no les quedará más remedio que contemplar escenarios más o menos apocalípticos para los que deberá tener previstos planes de contingencia. Por todo ello las empresas tenderán a ser cada vez más colaborativas, con la idea indiscutible de que todos juntos somos más fuertes: lo público y lo privado, investigadores, start-ups, instituciones académicas y filantrópicas... Un ecosistema preparado para protegerse ante futuras crisis.

Reino Unido no cede a las presiones sobre Huawei y su 5G

No habrá caso Huawei. La decisión del Reino Unido de permitir la implantación de la tecnología 5G de Huawei en las Islas es definitiva. Aprovechando la crisis provocada por Covid-19, y la creciente ola de denuncias contra el secretismo inicial del Gobierno chino sobre el origen del brote de coronavirus, varias voces y medios han venido asegurando que el Gabinete presidido por Boris Johnson estaba planteándose prescindir de la tecnología de la multinacional china a pesar de que el pasado mes de enero le concedió que pudiera desplegar la infraestructura necesaria, aunque, eso sí, con algunas restricciones.

Aunque minoritarias algunas voces en las Islas Británicas también pusieron en duda que Huawei pudiera seguir desarrollando su infraestructura 5G. Una de ellas fue la del antiguo miembro del Gabinete de Theresa May, Damian Green quien en declaraciones a Bloomberg, afirmó que "tenemos que diseñar una estrategia de salida adecuada y realista para dejar de depender de Huawei. Nuestros proveedores de telecomunicaciones necesitan saber que el gobierno está decidido a reducir la participación de Huawei al cero por ciento en un plazo de tiempo realista". Pero Boris Johnson no ha dado su brazo a torcer. El premier británico está más que seguro de ir hasta el final con su decisión y no ve motivo alguno para desconfiar de Huawei por mucha presión a la que le sometan. La decisión tomada el pasado mes de Enero por el Ejecutivo es firme y tal y como ha confirmado el Ministerio de Asuntos Exteriores los británicos quieren que "Huawei tenga un papel en la construcción de la red 5G del país y, este es un tema que no se va a reabrir".

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

go.eset.es/byte

LA OPINIÓN DE
Manuel Navarro

Hay más héroes y también aprovechados

Estamos aprendiendo a marchas forzadas. El mundo que imaginábamos se ha ido por el desagüe y gracias al virus estamos viendo desgracias, una gran multitud de políticos incompetentes que aún en esta situación solo piensan en su propio beneficio (electoral y personal), también una minoría de ciudadanos insolidarios... pero también están los denominados "héroes" que cuando se les pregunta dicen que "sólo cumplen con su trabajo" . Personal sanitario, conductores de autobús, cajeras de supermercado, policías, reponedores, transportistas, mensajeros,... la lista es larga y todos la conocemos.

Pero hay más: son otros responsables que le han echado horas de sueño para que las empresas puedan seguir trabajando y la mayoría tienen que ver con la tecnología: CIOs y CISOs han estado en la primera línea para que podamos teletrabajar; las empresas TIC y sus partners han donado soluciones a pymes que no habían avanzado en su digitalización de forma altruísta así como equipamiento a hospitales improvisados como el del Ifema. Y por supuesto, muchas de ellas también han hecho donaciones desinteresadas y la gran mayoría ha intentado no despedir a ningún empleado o practicar ningún ERTE. Y luego pagarán sus impuestos en España. Hablo de grandes empresas españolas y una gran parte de multinacionales extranjeras a la que los políticos ideologizados y poseedores de la verdad absoluta volverán a intentar defenestrar por estar dentro del IBEX 35 o porque sus directivos, con su trabajo, viven alejados de la realidad mientras ellos "tienen la suerte de tener jardín en su casa"

Office 365 pasa a llamarse Microsoft 365

Microsoft acaba con la marca Office 365. La multinacional de Redmond ha anunciado que a partir de hoy, Office 365 pasará a denominarse Microsoft 365. Según avanzan desde la compañía, el cambio en la nomenclatura es "una evolución que se construye sobre la base de Office, enriqueciéndola con Inteligencia Artificial, plantillas optimizadas y experiencias potenciadas por la nube. La mejora se proporciona de forma continua mediante actualizaciones del servicio y las más recientes llegarán a los más de 37 millones de suscriptores de Office 365 en los próximos meses."

La idea que se tiene es que Office 365 ya no es sólo un conjunto de herramientas ofimáticas y por eso había que dar un cambio a una marca que nació en el año 1989 y que desde ese momento se convirtió en una de las principales fuentes de ingresos de Microsoft. Según se desprende de la comunicación emitida por la multinacional, "este cambio de nombre refleja la nube de productividad de la compañía que reúne aplicaciones de Office, servicios en la nube y seguridad avanzada. En este sentido, permite a los usuarios y empresas conectar con las personas, la información y el contenido que necesitan para mejorar su productividad y transformar la colaboración de forma segura".

OPTIMIZACIÓN

Desde la compañía se incide en que la nueva Microsoft 365 "transforma la manera en que las empresas administran su negocio y simplifica la forma en que sus empleados hacen el trabajo con herramientas modernas que optimizan los procesos. Y, por otro, este servicio permite a los usuarios que su actividad personal sea más creativa, organizada y segura, pudiendo compartir y colaborar de forma fluida a tiempo real entre dispositivos".

econocom

Trabajamos para ti, pensando en tu futuro

Equipos, servicios y financiación para las empresas

www.econocom.es

CaixaBank, primer banco que trabaja con computación híbrida

La entidad bancaria presidida por Jordi Gual avanza en su estrategia de preparación para la llegada de la computación cuántica y le permitirá mejorar en la simulación de escenarios de riesgo y Machine Learning.

La CaixaBank ha presentado un esquema de computación híbrida, el cual combina en las distintas etapas del proceso el cálculo de computación cuántica y la computación convencional con fin de clasificar los perfiles de riesgos crediticios.

De esta forma la compañía presidida por Jordi Gual avanza en su estrategia de preparación para la llegada de la computación cuántica. Este esquema se llevó a cabo gracias a un conjunto de datos público, correspondiente a 1.000 supuestos usuarios, con un perfil muy similar a clientes reales, pero con información completamente figurada para la realización de la prueba.

Con este proyecto, la entidad mejora en la simulación de escenarios de riesgo y Machine Learning donde los algoritmos son cada vez más complejos y requieren de grandes cantidades de datos para aprender, a la vez que avanza en su análisis de las aplicaciones de la computación cuántica.

PRIMERA ENTIDAD DE ESPAÑA EN TRABAJAR CON COMPUTACIÓN CUÁNTICA

Previamente a este desarrollo, la compañía llevó a cabo un proyecto basado en simulaciones de evaluación del riesgo de activos financieros, a través de un algoritmo cuántico capaz de evaluar el riesgo financiero de dos carteras creadas específicamente por el proyecto a partir de datos reales, una de hipotecas y otra de bonos del Tesoro.

De esta forma, CaixaBank se convirtió en la primera entidad de España y una de las primeras del mundo en incorporar la computación cuántica a su actividad de innovación. Y es que, este ejercicio ha permitido a la entidad capacitarse en el despliegue de versiones cuánticas de algoritmos clásicos y validar la convergencia de la solución cuántica.

Con el objetivo principal de responder a los requerimientos de sus clientes y garantizar su crecimiento a la vez que se adapta a las necesidades de negocio y disponibilidad de información, CaixaBank realiza una gran inversión en tecnología.

Lo que implica una continua apuesta por tecnologías emergentes y pioneras, desde el blockchain a la robótica, pasando por la IA y la computación cuántica. Y es que, gracias a esta estrategia de transformación digital, la compañía se ha situado entre los bancos mejor valorados del mundo por la calidad de sus productos y servicios digitales.

Powering Digital Transformation

Software for bridging now and next

At Micro Focus we help you run your business and transform it. Our software provides the critical tools you need to build, operate, secure, and analyze your enterprise. By design, these tools bridge the gap between existing and emerging technologies—which means you can innovate faster, with less risk, in the race to digital transformation.

microfocus.com

MICRO FOCUS

Cisco Webex: seguridad por defecto y protección del teletrabajo

Cisco Webex tiene habitualmente más de 130 millones de usuarios mensuales en todo el mundo, y procesa más de 6.000 millones de minutos en reuniones cada mes. En marzo, superó los 300 millones de usuarios y los 14.000 millones de minutos.

Y es que dada la situación actual, millones de personas están empleando estas herramientas para teletrabajar y así mantenerse productivas y conectadas mientras dure la pandemia. Lo que implica importantes riesgos de ciberseguridad y la necesidad de disponer de las herramientas adecuadas para protegerse.

"La protección de usuarios, empresas e instituciones debe reforzarse con tres medidas clave: utilizar herramientas de colaboración con seguridad integrada, reforzar el blindaje con soluciones complementarias y actuar con conciencia y sentido común", afirma Eutimio Fernández, Director de Ciber-seguridad en Cisco España.

CIFRADO Y SEGURIDAD POR DEFECTO

La solución Cisco Webex ofrece cifrado de extremo a extremo para los datos en uso, en tránsito y en host con una clave que los clientes controlan. Y es que su configuración de seguridad predeterminada evita las intrusiones, con el fin de garantizar la identificación en cualquier sala de reunión.

Las transcripciones de Webex se efectúan internamente con la tecnología de IA de Voicea para que nunca salgan de su entorno Cloud. Y las posibles vulnerabilidades de seguridad son inmediatamente remediadas y reveladas de forma proactiva.

"Como el proveedor de seguridad corporativa más grande del mundo, nuestra máxima en Colaboración siempre ha sido facilidad de uso con seguridad por diseño. Por eso el 95% de las empresas de la lista Fortune 500 confían en Webex", concluye Fernández.

PROTECCIÓN ADICIONAL CON CISCO WEBEX

La red, los usuarios y los terminales constituyen el segundo pilar de protección, con cuatro soluciones clave:

- Conexión VPN
- Mecanismos de verificación multi-factor
- Seguridad Cloud y DNS
- Protección de cualquier dispositivo

Cisco Webex completa estas soluciones al integrar la plataforma Duo Security de y Advanced Malware Protection para proteger tanto a usuarios como a terminales corporativos y personales (ambas soluciones serán gratuitas hasta el próximo 1 de julio).

Además, la compañía extiende este soporte gratuito a otras dos herramientas de protección esenciales:

- Cisco AnnyConnect Secure Mobility Client (conexión de red privada virtual, VPN)
- Cisco Umbrella (seguridad Cloud y de dominios)

byte TI 20 años Fiesta 20 Aniversario

¡Nos hacemos mayores!

Byte TI y MKM Publicaciones cumplen 20 años y para celebrarlo haremos una **gran fiesta** a la que estás invitado y obligado a asistir.

Habrá **sorpresas, regalos, sorteos**... Contaremos con el **humor de Antonio Moar,** quien nos hará un repaso de lo acontecido en estos últimos 20 años y **un cóctel** que no te puedes perder y al que asistirán las estrellas más rutilantes del sector tecnológico español.

Y por supuesto, también aprovecharemos para, un año más, hacer entrega de los **Premios Byte TI con sus famosas estatuillas,** que este año tendrán un carácter más especial.

No lo dudes. Cumplimos veinte y vamos a por otros veinte. Así que **¡Vente, vente, vente!**

21 de Octubre | Círculo de Bellas Artes (Madrid) | 19:00

Confirma tu plaza a través del código QR o entra en:
https://paginas.revistabyte.es/20-Aniversario

Patrocinadores Gold

SOPHOS econocom VASS hp Hewlett Packard Enterprise

Patrocinadores Silver

SAMSUNG SAP DELL Technologies MICRO FOCUS

InterSystems Health | Business | Government D-Link Lexmark

La tecnología 5G lucha contra su propio Covid-19

La tecnología 5G lleva bastante tiempo copando titulares de todo tipo. Al principio se hablaba de sus ventajas. En los últimos tiempos, las tensiones China-EE.UU. tenían como telón de fondo al 5G.

Con lo que nadie contaba es con que 5G se convirtiera en otro elemento de la teoría de la conspiración. La nueva teoría conspiratoria tiene que ver con que el desarrollo de 5G y, concretamente sus antenas, han sido responsables de la expansión del Covid-19 a lo largo de todo el planeta. El desarrollo de esta teoría saltó a las redes sociales del Reino Unido donde se produjeron numerosos incendios en las antenas de telefonía 5G. La teoría conspiratoria ha llegado tan lejos que el director general del NHS, el equivalente al sistema sanitario español, Stephen Powis, ha tenido que salir a desmentir la relación entre el coronavirus y el 5G. Powis ha ido incluso más allá afirmando que "las teorías de conspiración que vinculan las señales de 5G con la pandemia de coronavirus siguen extendiéndose a pesar de que no hay pruebas de que las señales de los teléfonos móviles supongan un riesgo para la salud".

TODO TIPO DE TEORÍAS

Esta última relacionada con el coronavirus es sólo una más. Pero no sólo es el coronavirus. La típica relación entre cáncer y 5G también ha salido a escena, igual que lo hizo en su momento con el 4G o las redes WiFi. El pasado mes de Enero, Ecologistas en Acción pidió al Gobierno la paralización inmediata del despliegue de 5G. El argumento utilizado por la ONG se basa en un informe de la Agencia Internacional del Investigación del Cáncer, dependiente de la OMS, en el que advierte de los riesgos de la exposición a radiofrecuencias. Lo que no informa la ONG para hacer su propuesta es que se trata de un informe del año 2011 y en el que se analiza cómo puede afectar a la salud el uso masivo de teléfonos móviles. El estudio no se centra en las antenas de 3G, que eran las existentes en aquel momento, por lo que mucho menos se puede esgrimir como argumento para paralizar el despliegue de 5G. De hecho, el informe de la Agencia, aún consciente de que el uso masivo del móvil podría generar algún problema para la salud, afirma que "los estudios disponibles son de calidad insuficiente".

LO QUE SÍ DICE LA OMS EN 2020

Dejando a un lado el lejano 2011, la OMS sí se ha pronunciado sobre los efectos que sobre la salud puede tener la tecnología 5G. La organización dependiente de la ONU se ha pronunciado al respecto afirmando que "hasta la fecha, y después de muchas investigaciones realizadas, no se ha relacionado ningún efecto adverso para la salud con la exposición a las tecnologías inalámbricas. A medida que la frecuencia aumenta, hay menos penetración en los tejidos del cuerpo y la absorción de la energía se limita más a la superficie del cuerpo (piel y ojos). Siempre que la exposición general se mantenga por debajo de las directrices internacionales, no se prevén consecuencias para la salud pública".

Acer Chrome Enterprise: colaboración instantánea para un funcionamiento productivo desde cualquier lugar

Los dispositivos Chrome de Acer están diseñados para maximizar la productividad en entornos colaborativos de la nube

La hipermovilidad y el teletrabajo son dos factores muy presentes en la realidad de la mayoría de empresas. Por ello, si no disponen de la información corporativa necesaria de manera rápida y segura, puede suponer un gran problema de productividad para los trabajadores en remoto. La solución empresarial de Google Chrome Enterprise, presente en la nueva gama de productos de Acer, es la solución perfecta para compartir datos en la nube.

Gracias al sistema operativo Chrome, los usuarios dispondrán de un acceso rápido y seguro a la nube desde sus Acer Chrome Enterprise, un completo portfolio de dispositivos en el que encontrarnos equipos de sobremesa, portátiles tradicionales, convertibles, ultrafinos, AllinOnes y sistemas de videoconferencia.Todos han sido diseñados específicamente para dar respuesta tanto a las necesidades de las empresas (independientemente de su tamaño) y de diversos sectores empresariales, como al reto que supone la gestión eficaz de los empleados y su incorporación en la transformación tecnológica de empresas y personal del área de IT por igual.

Los administradores de IT ahora pueden gestionar de forma remota todos los dispositivos, ya que Chrome Enterprise les proporciona acceso sencillo a sus políticas y a las capacidades de supervisión de flotas desde la consola de administración de Google en la nube o desde alguna solución UEM (gestión unificada de terminales) de terceros, para simplificar la coordinación entre diferentes equipos. Además, también tienen la posibilidad de deshabilitar el hardware en caso de extravío o pérdida del dispositivo para garantizar la seguridad de los datos confidenciales de las empresas.

Por último, los equipos Chromebook Enterprise de Acer están diseñados para maximizar la productividad gracias a tiempos de arranque de unos 8 segundos, con interfaces que resultan familiares a los usuarios y a una enorme autonomía de más de 8 horas para el acceso instantáneo a las comunicaciones de la empresa y eficiencia durante toda la jornada laboral, ya sea desde casa, la oficina o desde cualquier otro lugar.

Toda la información sobre las soluciones Acer Chrome Enterprise en: acer.es/chrome-enterprise

El encuentro de Walldorf se celebró este año de modo virtual

El encuentro de coordinadores y delegados de SAP en Walldorf, se ha visto sustituido este año por una serie de webinars con preguntas y respuestas que tuvieron lugar el 26 de marzo.

En total, se celebraron 27 sesiones virtuales, conducidas por expertos de SAP y en las que participaron miembros de los grupos de usuarios. El formato fue sencillo: estos enviaban preguntas, que eran respondidas por los expertos en las sesiones. Todos los coordinadores y delegados de AUSAPE que participaron en los webinars Q&A destacaron que estos fueron interesantes y productivos.

En el webinar de Enterprise Asset Management, al que asistió el coordinador de nuestro Grupo de Industria Digital Pablo Juncosa, los expertos de SAP explicaron las novedades que están incorporando en las funciones para la Gestión Inteligente de Activos. Se hizo una introducción sobre las funciones adicionales disponibles y/o en construcción y los asistentes entraron en el sistema, donde les enseñaron una demo de los productos. Los asistentes también plantearon sus preocupaciones sobre la cobertura de S/4 HANA respecto a la existente en las versiones anteriores. Asimismo, se ofrecieron informaciones detalladas sobre la gestión inteligente de activos Intelligent Asset Management de manera integral, los roadmaps de productos y el programa S/4 Customer Connection.

La reunión de Solution Manager estuvo conducida por Time Steuer y contó con la colaboración de otros expertos de SAP en el área. Por parte de AUSAPE participó Ander Aristondo, responsable de la Delegación Norte. La base de la reunión fueron las preguntas enviadas con anterioridad, con cinco temas principales. El primero, las posibilidades de utilización de los tests automatizados a partir del Busines Process Content: SAP reconoció que cualquier test "automatizado" requiere una parte de trabajo manual previa de cara a preparar los juegos de datos necesarios para los tests. Sobre los casos de uso de Focussed Build y soporte DevOps, SAP confirmó que no aún está disponible ChaRM para Focussed Build y no lo estará en breve.

En cuanto a los planes para SAP Cloud ALM, anunció que hay novedades previstas para este mes que cubrirán aspectos como operations, integration monitoring, exceptions monitoring o Concur platform integration. La gestión en SOLMAN de las Best Practices durante la conversión a S/4 HANA fue otro de los temas y, respecto al roadmap de mejoras para SOLMAN 7.2, SAP explicó el plan de mejoras anuales basado en el feedback de clientes elegidos y de grupos de trabajo.

Al webinar de Enterprise Architecture asistieron ocho personas, entre ellas David Ruiz y Carles Viaplana, de los grupos de Movilidad & SCP e Industria Digital de AUSAPE, respectivamente. Se plantearon los roadmaps de SCPI y PO, que a día de hoy son paralelos y no está previsto que se crucen de momento. Se apuntó que SCPI debería estar cubriendo todos los escenarios que cubre PO, aunque este aspecto quedó abierto. En cuanto al SAP Gateway, su evolución es incluirlo en la misma instancia de S/4 HANA, aunque existe una limitación en la relación entre ambos, de modo que SAP está revisando la estrategia a seguir.

IA para garantizar la ciberseguridad de la red en tiempos de crisis sanitaria

Por Pedro Martínez Busto
responsable de desarrollo de negocio de Aruba, una compañía de Hewlett Packard Enterprise, para España

¿Quién no es consciente de que toda oportunidad conlleva un riesgo, pero que no podremos avanzar si no nos adentramos en un terreno desconocido? Este es el escenario al que se están enfrentando las empresas e instituciones de cualquier sector a medida que aumenta el uso de dispositivos IoT conectados; un escenario que se complica con situaciones de crisis sanitaria inesperadas que obligan a esas organizaciones a transformar drásticamente su forma de operar y, por tanto, apostar por lo desconocido.

IoT está facilitando procesos de operación más transparente, eficientes y resilientes, que es algo muy importante, pero cualquier incidente que ponga en riesgo la ciberseguridad del entorno puede suponer una amenaza directa para la salud de las personas en el caso de los entornos sanitarios.

La realidad es que los dispositivos IoT, pueden ser muy efectivos, pero al mismo tiempo muy vulnerables. Según un estudio de Aruba, el 84% de las organizaciones que adoptaban soluciones IoT habían experimentado una brecha de seguridad. Desde entonces, la adopción es cada vez más común, y los problemas de seguridad no han desaparecido. De hecho, es posible que se vuelvan más serios a medida que los dispositivos se vuelven más sofisticados y las soluciones de seguridad no son capaces de proteger frente a nuevas vulnerabilidades.

A medida que cada vez más dispositivos pueden conectarse a la red sin que intervenga el departamento de TI, el equipo de seguridad pierde rápidamente la visibilidad y el control. Por eso, las buenas prácticas – desde los protocolos de autenticación hasta los controles de acceso – son más importantes que nunca, ya que los atacantes pueden encontrar fácilmente nuevas puertas de entrada a la red, que no están protegidas.

Más problemático es incluso el hecho de que los dispositivos IoT, tales como sensores y controladores, a menudo no se pueden diferenciar entre sí, sino que simplemente se reconocen como equipos Windows o dispositivos Android. Esto compromete significativamente la capacidad de adaptar las políticas de acceso según la función del dispositivo. A medida que intentan mantener bajo control el entorno IoT, el desafío al que se enfrentan los administradores de seguridad y redes tiene que ver con la visibilidad y el volumen. ¿Cómo pueden controlar un conjunto extenso de dispositivos y asegurarse de que tienen la información necesaria para administrarlos correctamente? La respuesta es clara: con el potencial de la Inteligencia Artificial (IA), sobre todo asociada a soluciones de Analítica y Machine Learning, ya que van a ser clave para poder identificar patrones de comportamiento que permitan perfilar los dispositivos y discriminar, de forma automática, lo que es un comportamiento normal, de lo que no lo es.

Las empresas e instituciones tienen que hacer frente al reto de administrar redes con muchos dispositivos y cada vez más complejos, y aquí la IA y las herramientas de aprendizaje automático pueden ayudar a devolver el control de la red a los administradores, algo que es sin duda de la máxima importancia para ayudar a combatir cualquier crisis sanitaria.

Desde Aruba ponemos a disposición de las empresas una guía con los aspectos a tener en cuenta para seleccionar e implementar una solución de Teletrabajo que permita el acceso seguro de un trabajador desde una localización externa a los recursos y aplicaciones de la organización. Si desea que le facilitemos la guía póngase en contacto con **Pedro Martinez: pedro.martinez-busto@hpe.com**

Pulsa aquí para ver el encuentro

Ciberseguridad y elementos para posibilitar el teletrabajo

Uno de los aspectos positivos que tiene la crisis del coronavirus es la importancia que han adquirido la ciberseguridad y los entornos de teletrabajo. Byte TI junto con SonicWall organizó un encuentro para dar a conocer cual es la realidad de estas dos tendencias.

Por Manuel Navarro Ruiz

SonicWall es una empresa de ciberseguridad que cuenta con más de 27 años en el mercado. La firma y sus productos están presente en más de un millón de redes en todo el mundo con más de 200 patentes y una base instalada de más de millones de firewalls. Por ello, las propuestas de esta multinacional así como la valoración del mercado que haga son un punto de referencia para las organizaciones. Y es que, tal y como puso de manifiesto Sergio Martínez, Iberia Regional Manager de SonicWall, "somos muy conocidos en el mundo del firewall con un 32% de cuota en el mundo de la pyme y empresas distribuidas. Pero no solo hacemos firewalls sino que tenemos un amplio portfolio de soluciones de ciberseguridad, desde el endpoint hasta el Cloud, pasando por los puntos de acceso WIFI, el acceso remoto a redes (del que hablaremos hoy), los firewalls de nueva generación, etc.

El máximo responsable de la compañía en nuestro país aseguró que tras la crisis sanitaria provocada por el virus Covid-19 la vuelta a la normalidad va a ser bastante paulatina. "Lo cierto es que debido a la pandemia hemos pasado de un 20% de personas teletrabajando al 100%. Con ello, se ha visto que el perímetro ha desaparecido y los usuarios, en lo que se refiere a la ciberseguridad, están en un terreno hostil y aparecen nuevas preocupaciones para los CISOs".

SEGUIR OPERATIVOS DURANTE LA PANDEMIA

Eduardo Brenes, evangelista de ciberseguridad en SonicWall afirmó que "nos encontramos en una situación que nunca habíamos vivido. Por este motivo creemos que es importante centrarse en los peligros que se están produciendo y en cómo están apareciendo nuevas vulnerabilidades en las compañías, dado que se están dejando configuraciones de redes muy expuestas por el hecho de implementar tele trabajo en las organizaciones. En SonicWall disponemos de soluciones para reducir la superficie de exposición y complementar o completar la infraestructura de ciberseguridad existente".

Desde SonicWall se han centrado en que sus clientes puedan continuar con su labor de forma eficiente y segura. Pero como afirmó Brenes, "el problema es que nadie había previsto nada como esto y hemos pasado de un entorno de un 20% de trabajadores que normalmente tele trabajaban, al 100% de un día para otro". Tal y como asegura este directivo, "las últimas cuatro semanas han sido muy intensas para

Pulse aquí para ver el encuentro

Sergio Martínez, Iberia Regional Manager de SonicWall

"En SonicWall tenemos un amplio portfolio de soluciones de ciberseguridad"

Eduardo Brenes, evangelista de ciberseguridad en SonicWall

"Es importante centrarse en los peligros que se están produciendo"

tratar de ayudar y dar respuesta a aquellas compañías más tradicionales, que no habían preparado sus sistemas para tele trabajar de forma segura. Si se produjera una segunda oleada de Coronavirus en Octubre de 2020, las empresas tendrán de Junio a Octubre para que esta situación no les vuelva a pillar de improviso".

Tal y como quedó patente durante el encuentro, éste ha sido el mayor experimento de teletrabajo a nivel mundial que se ha hecho nunca, por lo que los retos son también cada vez mayores. Esta situación supone que las TIC están cada vez más distribuidas, por lo que se multiplican también los puntos de exposición. "El perimetro desapareció y ya no funciona el modelo de mi castillo mis reglas".

Eduardo Brenes explicó que "el coronavirus también ha sido una oportunidad para los ciberatacantes, ya que desgraciadamente los cibercriminales, no hacen cuarentena de su labor, y saben cómo capitalizar con éxito este tipo de situaciones. Y el brote de coronavirus es una gran oportunidad para ellos, para lanzar campañas de phishing basadas en el miedo, malware móvil, ataques de ingeniería social, etc. Se han llegado a producir ataques a hospitales con variedades de "Ransomware-as-a-service" como NetWalker. Además, el Ministerio del Interior ha desactivado multitud de páginas web fraudulentas relacionadas con COVID-19.

Los ciberatacantes también saben que hay muchos usuarios que no han utilizado habitualmente herramientas de colaboración o de videoconferencia y también están aprovechando eso para realizar phishing relativo a esto…

SOLUCIONES PARA TELETRABAJAR DE FORMA SEGURA

SonicWall proporciona un amplio abanico de soluciones para hacer que el teletrabajo por parte de los usuarios se realice de forma segura. Alex Vázquez, Senior System Engineer de SonicWall afirmó que "una de las necesidades que estamos viendo que tiene mucha demanda últimamente por parte de las empresas son las soluciones de Acceso Remoto Seguro. Esto es así porque en estos momentos todo el mundo está teletrabajando y las compañías de Seguridad como SonicWall tenemos que proporcionar este tipo de soluciones porque muchas organizaciones no estaban preparadas para esta nueva situación". La gama de soluciones de seguridad de Acceso Remoto de SonicWall tienen un objetivo: intentar que la experiencia del usuario sea lo más parecida a estar físicamente en la oficina.

Para ello la multinacional propone su línea SMA (Secure Mobile Access). Gracias a este conjunto de soluciones de seguridad de acceso remoto las empresas pueden restringir los accesos de los usuarios a determinadas horas del día, o en función de la IP de origen tanto por reputación (AntiBotnet) como por ubicación geográfica (GeoIP). Otras características de estas gama de soluciones es que se puede enrutar todo el tráfico del usuario por el Túnel SSL (incluido Internet) para tener un mayor control de su actividad (Tunnel All mode) y también levantar la conexión VPN antes de que el usuario haga login en el equipo, y no permitir que desconecte la sesión (Always-On VPN).

Como comenta Vázquez, "desde SonicWall recomendamos encarecidamente la autenticación de doble factor para los usuarios. Además, nuestras soluciones se integran perfectamente con las soluciones de autenticación 2FA de Microsoft, Google o Duo Mobile". Entre otras ventajas de las soluciones SMA de SonicWall se encuentran los accesos clientless desde equipos no corporativos, sin necesidad de que los usuarios tengan que instalar

Pulse aquí para ver el encuentro

Alex Vázquez, Senior System Engineer de SonicWall

"Recomendamos encarecidamente la autenticación de doble factor"

ningún software para el acceso (portal SSL-VPN). Además de la autenticación de usuarios, también destaca la identificación y autorización de dispositivos (Device Management y EndPoint Control (EPC)) para tener un mayor control de los accesos. Por otro lado, la compañía propone un licenciamiento flexible para poder afrontar un incremento puntual de usuarios (Spike Licenses) mediante un sistema de licencias temporales que se pueden activar/desactivar a demanda en función de las necesidades de cada día.

SOLUCIONES VIRTUALES VS. FÍSICAS

Según estuvo explicando Alex Vázquez "se está produciendo una aceleración hacia el mundo virtual y hacia los servicios en nubes públicas por las ventajas que ofrecen. Nosotros tenemos soluciones para todos los retos que conlleva esta nueva realidad: soluciones virtuales, integración con nubes híbridas, con licenciamiento flexible para Azure y AWS y además equivalencia a nivel funcional con las soluciones físicas".

Otro apartado importante para la seguridad de las empresas es la protección del e-mail. Y es que como aseguró Vázquez, "este ha sido uno de los frentes de ataque más habituales. Los ciberdelincuentes saben que en estos momentos las organizaciones son muy vulnerables y que existe una mayor probabilidad de poder robar datos y credenciales estableciendo como gancho al coronavirus". En este caso, SonicWall propone sus soluciones Cloud App Security (CAS) que no sólo securizan el correo electrónico (O365 y GMail) sino también otras aplicaciones en la nube que ofrecen el almacenamiento de archivos (OneDrive, Google Drive, Dropbox, etc.) y aplicaciones para el uso compartido de archivos (SharePoint) proporcionando protección avanzada contra amenazas como los ataques de phishing dirigidos (Spear Phishing), las amenazas de día cero (0-day), las suplantaciones de identidad y la detección de cuentas comprometidas.

La solución de CAS de SonicWall se integra con todas estas aplicaciones en la nube mediante API's, y emplea herramientas que permiten monitorizar los logins de los usuarios (Account Takeover Protection) con el fin de detectar eventos anómalos o sospechosos, la inspección avanzada de phishing y antimalware con múltiples motores de sandboxing en la nube, y la prevención de fugas de información (DLP).

PROTECCIÓN DEL ENDPOINT

Ya venía sucediendo, aunque la crisis del coronavirus lo ha agravado y es que se está viendo como las amenazas desconocidas del tipo zero day están aumentando. El problema es mayor porque como afirmó Alex Vázquez, "los PCs personales no tienen el mismo nivel de seguridad que los de las empresas por lo que hay que tomar medidas para que sean más seguros, por lo tanto es necesario tener un cierto control de los dispositivos remotos para minimizar los riesgos. Algunos de estos controles ya se pueden aplicar desde el endpoint, como el filtrado web o la detección de aplicaciones vulnerables".

Para Vázquez las soluciones de SonicWall incorporan una serie de funcionalidades que son fundamentales: "Por ejemplo, el control de dispositivos USB o Bluetooth, el filtrado web y el análisis de aplicaciones vulnerables (Application Risk Management) son una parte importante de la protección del Endpoint. Por otro lado, en nuestra solución (Capture Client) tenemos un acuerdo con Sentinel One de forma que combinamos la potencia de este NGAV a nivel de análisis dinámico, con nuestra solución de sandboxing multimotor en la nube, que incluye tanto motores de sandboxing propietarios como motores de terceros para poder tener múltiples veredictos y tomar mejores decisiones. A pesar de esto la seguridad 100% no existe, por lo que nuestra solución también ofrece algunas alternativas de protección adicionales, como la posibilidad de hacer roll-back y restaurar a su estado anterior archivos que hayan podido ser cifrados (ransomware), como la posibilidad de aislar de forma virtual equipos que puedan estar infectados por algún gusano o troyano para que no se pueda propagar por la red. Por último, nuestra solución Capture Client incorpora funcionalidades de tipo EDR (Endpoint Detection and Response) para visualizar de forma gráfica la ejecución de amenazas y su comportamiento".

LA PLATAFORMA DE **MARKETING AUTOMATION**

 Pulse aquí para ver el encuentro

Colaboración: la salvación empresarial

A pesar de la crisis de Covid-19, muchas empresas han podido salir adelante gracias a las soluciones de colaboración. Byte TI organizó un webinar para charlar sobre ellas y que contó con la presencia de Albert Casadejust, CEO de Omega Peripherals; Genaro Escudero, EUC Sales Engineer de Dell Technologies; Melchor Sanz, Director de Tecnología y Preventa de HP Iberia; Ricardo Ciganda, Sales Expert Consultant de T-Systems y Guillem Giménez Badía, Director del área de aplicaciones de Sothis.

Por Manuel Navarro Ruiz

¿Se imaginan que esta crisis sanitaria hace 15 años? El resultado habría sido infinitamente peor. Muchas empresas se habrían ido directamente a la quiebra. Y es que tal y como afirmó Albert Casadejust, CEO de Omega Peripherals "la mayoría de las empresas han podido salir adelante gracias a este tipo de soluciones. Si no existieran, esto no habría sido posible".

Ante una crisis siempre hay soluciones que resultan ganadoras y ésta ha reforzado la importancia de las herramientas colaborativas y es que, como afirma Genaro Escudero, EUC Sales Engineer de Dell Technologies, "para los que llevamos tiempo dedicados a este mundo, ha representado una oportunidad para que las empresas pongan a prueba estas soluciones. La gente ha tenido que trabajar desde casa, sí o sí. La productividad se ha visto que se incrementa. Ahora es tiempo de replantearse las estrategias". La gran ventaja es que, como afirma Melchor Sanz, Director de Tecnología y Preventa de HP Iberia, "gracias a estas soluciones hemos desplazado los equipos y las personas pero no el trabajo. Lo que ha cambiado es que lo que pensábamos que era indispensable, como estar en la oficina de forma permanente, hemos visto que puede sobrar. Espacios como las salas de reuniones, hemos visto que no hacen falta en todo momento. Sin embargo, hay que buscar un punto intermedio entre la comodidad del teletrabajo y la proximidad de las personas porque en algunos casos es muy necesaria. En mi opinión, en el futuro no trabajaremos desde casa todo el tiempo, sino desde donde sea necesario".

Ricardo Ciganda, Sales Expert Consultant de T-Systems afirma que, "esta crisis está aportando un cambio de mentalidad con respecto al teletrabajo. Hay empresas que ya lo habían incorporado pero otras, más tradicionales, no. Las organizaciones, que han visto que esto mejora la productividad, van a ver que por ejemplo pueden reducir sus espacios de trabajo. Esta crisis también ha facilitado que muchas empresas se lancen al e-commerce. Esto ha proporcionado que haya afectado positivamente a la telemedicina, a la educación, etc.". También Guillem Giménez Badía, Director del área de aplicaciones de Sothis, cree que "esta nueva situación ha aportado continuidad de negocio y ha reducido tiempos en desplazamiento y tiempos de espera. Ahora todos trabajamos sobre un mismo documento de texto, por ejemplo. Y por último, nos ha permitido mejorar la conciliación".

DEMANDA

La demanda de este tipo de soluciones ha sido brutal. Algunas organizaciones ya habían empezado a confinar a sus empleados mucho antes del estado de alarma pero otras lo em-

pezaron a hacer nada más promulgarse y a partir de ahí las peticiones y la demanda se ha disparado. El sector ha podido con esa alta demanda. Como afirmó el portavoz de Sothis, "las herramientas han estado a la altura y los fabricantes han volcado todo su esfuerzo en que todos podamos seguir trabajando y sí se ha satisfecho la demanda".

Por su parte, el representante de T-Systems sí considera que se han satisfecho las necesidades de las empresas pero a costa de algo: "Se ha puesto en riesgo la seguridad porque muchas empresas han tenido que confiar en los PCs personales de los trabajadores llegando incluso a haber equipos de usuarios que se conectan a la red y ya estaban infectados previamente. Solucionar esto con VDI es algo que tampoco se puede hacer de la noche a la mañana. No obstante, en general la respuesta ha sido buena, sobre todo en soluciones en la nube que nos ha permitido compartir soluciones y documentos de forma colaborativa". El CEO de Omega Peripherals cree que "lo principal de esta situación es ver que las comunicaciones han funcionado muy bien, Otro apartado que ha ayudado es que, en lo que se refiere a las pymes, un 76% de los usuarios ya tenían equipos en su casa.r".

Una de las empresas afectadas ha sido HP que ha tenido que satisfacer una alta demanda de equipos. Según afirmó Melchor Sanz, "muchos clientes nos han pedido muchos equipos de golpe y hemos podido satisfacer la demanda. Lo que es cierto es que a muchos de ellos les hemos tenido que proporcionar equipos de la gama alta de consumo en vez de los equipos que tenemos para el sector empresarial. Otro apartado en el que hemos visto un auge importante es el de la impresión doméstica que se ha disparado".

Similar fue la situación de Dell Technologies. Como aseguró Genaro Escudero, "durante las primeras 3-4 semanas nos tuvimos que volcar al 100% porque el crecimiento de la demanda fue brutal. Tuvimos la suerte de que, aparte de tener muchos equipos en stock, y gracias a la ayuda de los partners pudimos satisfacer esa demanda. De hecho, hemos tenido algún cliente que nos pidió alguna solución para desplegar desde cero una herramienta de colaboración y se lo hemos podido dar"

ADAPTACIÓN DEL CLIENTES

Nos hemos encontrado ante una situación novedosa en un país en el que el teletrabajo era una *"rara avis"*. Incluso aquellas organizaciones que sí apostaban por este modelo, se han tenido que enfrentar a tener a toda la compañía trabajando desde su casa. Según Albert Casadejust, "la gente ha reaccionado rápido, ha hecho inversiones que no tenías previstas y lo ha hecho en tiempo record cuando es algo que es bastante complicado. Además está la cultura de la empresa: no todas las personas de la compañía están acostumbradas a trabajar de esta forma y tampoco ha habido tiempo para aprender. Creo que en general no se ha hecho mal". En la misma línea se situó Ricardo Ciganda que cree que "la adopción ha sido muy buena y la gente lo ha asimilado de forma rápida. Además se ha demostrado que el teletrabajo es perfectamente viable. Por ejemplo, en nuestro caso hemos tenido que correr para implementar Contact Centers en las Administraciones. Los funcionarios están confinados y hemos tenido la deman-

Albert Casadejust, CEO de Omega Peripherals

"Se han hecho inversiones no previstas y en un tiempo récord""

Genaro Escudero, EUC Sales Engineer de Dell Technologies

"Hay una brecha digital y esa sólo se soluciona con formación a los empleados"

Melchor Sanz, Director de Tecnología y Preventa de HP Iberia

"Es necesario buscar el equilibrio entre seguridad, inversión y productividad"

Pulse aquí para ver el encuentro

Ricardo Ciganda, Sales Expert Consultant de T-Systems

"Esta crisis va a afectar positivamente a la telemedicina o a la educación"

Guillem Giménez Badía, Director del área de aplicaciones de Sothis

"Las empresas han podido salir adelante gracias a este tipo de soluciones"

da de montar infinidad de contact centers para mucho personal y lo hemos hecho en pocos días, gracias entre otras cosas al cloud". Genaro Escudero cree que "somos muy afortunados. Los que nos dedicamos a esto damos por hecho que el resto de los usuarios van a saber usar estas herramientas porque nosotros estamos con ello todos los días. Hay que hablar de la gestión de la adopción: una empresa invierte en este tipo de cosas pero hay una brecha digital y esa sólo se soluciona con formación a los empleados. Ahora todos han hecho un curso acelerado de estas herramientas".

"La frase de "hacer necesidad, virtud" nunca ha sido más exacta que ahora. Toda la sociedad la ha tenido que aceptar porque no ha tenido más remedio. Esto sin embargo no va a ser sostenible al 100%, pero las empresas se han dado cuenta de la cantidad de opciones que ofrecen las soluciones colaborativas. Incluso la propia Administración se ha dado cuenta de esas ventajas. Los decisores, que antes tenían miedo a tomar estos cambios, ahora han visto que esta opción es válida", afirmó el portavoz de T-Systems. Para Guillem Giménez Badía, la dificultad de adoptar estas soluciones "ha dependido del grado de madurez en el que se encontraba el cliente. Nosotros tenemos clientes que tenían las plataformas pero que no estaba haciendo uso de esas herramientas, otros que no tenían la plataforma, otros que no la usaban correctamente y otros que sí lo usaban. Lo que importa es que una empresa puede tener la herramienta colaborativa pero si los usuarios no la saben utilizar y no tienen unas guías prácticas puede hacer que la implantación de estas herramientas sea un fracaso".

SEGURIDAD

Uno de los problemas de los que más se ha hablado es de la seguridad de este tipo de aplicaciones y como al haberlas implementado de forma muy rápida, muchas empresas no han tenido en cuenta la seguridad a pesar de que la totalidad de ellas son seguras. Es necesario hacer una configuración por parte de la empresa pero como afirma Albert Casadejust, "el problema es que en estos momentos hay empresas expuestas. Las organizaciones han salido de esta como han podido y no tengo claro que el tema de la seguridad esté perfectamente cubierto". Para Ricardo Ciganda el problema es que "la situación no ha dejado otra alternativa que la de asumir riesgos. Es imposible garantizar la seguridad cuando hemos tenido que improvisar. Ahora todos estamos en el Shadow IT con PCs que no podemos controlar y con herramientas que no están controladas. La seguridad tiene que venir sustentada por unos planes de seguridad corporativos". Para el portavoz de Dell Technologies hay que valorar la parte positiva. En su opinión, "los mensajes positivos son que existen herramientas. Incluso si es un equipo personal se pueden aplicar ciertas políticas de seguridad. Creo que la mejor seguridad es la formación de los usuarios". La clave, en opinión de Melchor Sanz es que "es necesario buscar el equilibrio entre seguridad, inversión y productividad. Si no hubiésemos asumido ningún riesgo, no habríamos podido trabajar desde nuestras casas. Si conocemos qué riesgos hemos tomado en la parte de seguridad hay que saber qué hacer para mitigar esos riesgos y sobre todo hay que formar a los empleados una vez que está asegurada la continuidad del negocio. Este es un punto que me parece clave". Finalmente y en la misma línea se situó el portavoz de Sothis que concluyó que "hay que intentar ir a plataformas que cumplan con los estándares de seguridad pero hay que tener en cuenta que el primer firewall es el usuario.

DELL TECHNOLOGIES

Para Dell Technologies el concepto de teletrabajo no es nuevo y ofrece en su portfolio soluciones completas que se adaptan a todos los presupuestos, necesidades y escenarios para facilitar el trabajo remoto, el trabajo desde casa o el puesto de trabajo flexible en general. Desde kits completos con dispositivos profesionales preparados para la movilidad como la serie Latitude o XPS, complementados con la gestión moderna integrada desde fábrica con Workspace One, hasta soluciones de acceso remoto y escritorios virtuales con VMWare. Sin descuidar además, la importancia de mantener la máxima seguridad con productos que garantizan la protección tanto en los dispositivos de acceso como en las conexiones de red y hacia Internet. En Dell Technologies entendemos que es imprescindible mantener una planificación y visión integral alrededor de las personas, las aplicaciones críticas, las políticas y necesidades reales de la empresa. Nuestra soluciones van de extremo a extremo, pero sabemos que son necesarias una evaluación y comprensión adecuadas para decidir cuál es la solución correcta.

SOTHIS

En Sothis dedicamos tiempo y esfuerzo a entender de forma detallada cómo definen nuestros clientes el éxito. Con ello, les ayudamos a beneficiarse de los avances tecnológicos, simplificar la complejidad de su TI y a definir la arquitectura de transformación que mejor encaje con su estrategia de negocio. Todo ello, con la finalidad de que estén mejor protegidos y sean más eficientes y más productivos mediante la integración de los tres principales activos de las organizaciones: personas, procesos e información.

HP

HP ofrece la más amplia gama de portátiles y accesorios profesionales para el teletrabajo, que permite viajar o trabajar desde casa con gran eficiencia y comodidad para el trabajador, con equipos tan exclusivos como HP Elite Dragonfly, bases de expansión USB-C, monitores desde 22" a 34 curvos, hasta impresoras tanto de tinta como láser. Y siempre con la más alta seguridad para el puesto de trabajo: esté donde esté, protegiendo al usuario contra la piratería visual, contra ataques de malware en la BIOS y reduciendo el tiempo de inactividad con recuperación automática, o con capacidades para dar seguridad al endpoint basado en Inteligencia Artificial, entre otras muchas opciones.

T-SYSTEMS

T-Systems ofrece soluciones avanzadas de conectividad VPN, de VDI o de Colaboración y además proporciona soluciones más enfocadas a resolver casuísticas específicas. Mediante Digital Connect replicamos el puesto de trabajo de oficina en el hogar del empleado separando de forma segura el entorno profesional del personal y pudiendo utilizar el teléfono, pc e impresoras corporativas desde el domicilio residencial. Por otro lado, podemos desplegar Contact Centers (tan sólo en días) con tecnología 100% Cloud para trabajar con agentes distribuidos en sus domicilios personales dando continuidad al negocio. Todas estas soluciones se ofrecen en modo pago por uso, completamente gestionadas y sin barrera de entrada.

OMEGA PERIPHERALS

Omega Peripherals es una compañía especializada en consultoría, implementación y mantenimiento de soluciones de almacenamiento y sistemas de seguridad de la información. Cuenta con más de 120 profesionales altamente cualificados y en constante formación capaces de entender y adaptarse a las necesidades particulares de cada organización. La empresa inició su andadura en el año 1993. En la actualidad tiene oficinas en Barcelona, Madrid, Bilbao, Vigo, Sevilla, Pamplona y Valladolid.

Pulse aquí para ver el encuentro

Ciberseguridad: más necesaria que nunca

Debatimos en un encuentro que contó con la presencia de Pedro García-Villacañas, Head of Presales de Kaspersky; Pedro Martínez, Director Desarrollo de Negocio en Aruba, a Hewlett Packard Enterprise; Ángel Domínguez, Presale Business Technology de V-Valley; Miguel López, country manager de Barracuda; Juan Grau, Regional Sales Manager de Bitdefender; Joaquín Gómez, NSX Enterprise Account Executive de VMware y Carlos Vieira, Country manager para Iberia de Watchguard

Por Manuel Navarro Ruiz

Después de haber puesto a teletrabajar a los empleados de todas las empresas que pueden hacerlo los ojos se pusieron en la ciberseguridad. Este hecho provocó que se cambiaran las prioridades y se tuvieran que cambiar sobre la marcha los planes de contingencia. Covid-19 ha afectado pero como aseguró Pedro García-Villacañas, Head of Presales de Kaspersky, "los retos, la base son los mismos que antes de la aparición de Covid-19 y son los de proteger los dispositivos que usamos habitualmente así como las aplicaciones y poder manejar los riesgos a los que nos enfrentamos casi a diario. Lo que ha cambiado es la preparación y la sofisticación de los ciberataques". En la misma línea se situó Pedro Martínez, Director Desarrollo de Negocio en Aruba, a Hewlett Packard Enterprise que afirmó que "efectivamente los riesgos siguen siendo los mismos pero el hecho de que una parte de la población esté teletrabajando amplía la superficie de ataque para intentar violar la seguridad de las compañías. Además hay organizaciones que ya tenían estrategia de teletrabajo y en este sentido, no ha habido un incremento importante de riesgo. También hay empresas que no tenían esto y han tenido que mandar a casa a los empleados de la noche a la mañana y estoy convencido de que en estas empresas han soportado un nivel importante de riesgo y han comprometido activos".

Por su parte, Joaquín Gómez, NSX Enterprise Account Executive de VMware cree que dentro de los principales retos, "el fundamental es conectar al usuario con la aplicación a la que tiene que acceder pero fuera de la red. Para ello, hay que aplicar un control de seguridad en igual. Además el control de la productividad y el concepto de ir a la oficina es otro. Ese control es ahora otro reto que creo que no cambia pero sí se transforma". Miguel López, Country Manager de Barracuda cree que "tampoco es que los riesgos sean distintos a los que estábamos afrontando. Lo que sucede es que antes el teletrabajdor era la excepción y ahora es la regla. Esto tiene implicaciones importantes en materia de ciberseguridad. Es cierto que se pone el acento en esto y genera nuevos problemas porque antes nos exponíamos a dispositivos remotos que estaban controlados y ahora hay dispositivos que no están correctamente securizados. Realmente uno de los problemas es que no había un plan de contingencia para hacer frente a estos escenarios. Ahora las empresas

Pulse aquí para ver el encuentro

están estableciendo planes para hacer frente al nuevo escenario al que nos enfrentamos". En opinión de Ángel Domínguez, Presales Business Technology de V-Valley, "los retos a los que se enfrentan las organizaciones no son nuevos pero la situación ha cambiado porque ha sido un cambio brusco. Hay empresas que tienen bien desarrollado un plan de contingencia pero era impensable un cambio así. Todo cambio como este genera incertidumbre y genera riesgo. Creo este cambio va a suponer que las empresas cambien algo de cara a futuro. Tenemos mucha tecnología que nos va a permitir afrontar estos riesgos". Por su parte Juan Grau, Regional Sales Manager de Bitdefender cree que "el confinamiento se ha convertido en una gran prueba de concepto sobre el teletrabajo. Como todo lo que se hace deprisa se dejan cosas en el camino y yo creo que un tema es el de la seguridad. Ahora el perímetro es muy difuso: todos los empleados están en sus casas y supone un reto de seguridad de controlar la parte del endpoint y además el comportamiento de los usuarios es diferente en sus casas que en la oficina". Para Carlos Vieira, Country Manager para Iberia de Watchguard, "esto ha venido de forma rápida y empresas y partners han tenido que hacer un trabajo excepcional transformando empresas que estaban prácticamente en la prehistoria para transformarlas totalmente en dos semanas. Ahora nos encontramos con un perímetro muy difuso. Hemos visto empresas de sectores estratégicos que se han convertido en empresas transformadas. Phishing, ingeniería social, ransomware, son algunos de los retos por eso hay que enseñar a los trabajadores para que tengan cuidado con los correos, whatsapp y enlaces en las redes sociales. El trabajador tiene que estar sensibilizado".

INCREMENTO DE RIESGOS

Con la crisis sanitaria y el traslado de millones de trabajadores a sus casas los riesgos se han incrementado y, como afirma Vieira, " lo han hecho exponencialmente. Se ha incrementado el malware avanzado, phishing, ransomware, malware social,... ¡Ha aumentado todo!. Los medios están haciendo una labor muy importante para evitar que estos ataques se produzcan. Hay empresas que toman muchos riesgos innecesarios y esto ha ayudado a los CISOs para que las empresas inviertan en ciberseguridad. Y este es un dato importante, porque un problema de ciberseguridad puede provocar un cierre de empresa". Para Juan Grau, "antes las empresas combatían en el entorno que conocían. Ahora ha primado la eficiencia laboral y se ha hecho el cambio en la medida que han podido y se han tomado ciertos riesgos. En general en nuestro entorno ha habido clientes que nos han pedido ayuda, otros que trabajaban sobre equipos fijos, otros que trabajan sobre escritorio virtual y a los que ha habido que añadir las pautas de seguridad... Hay que entender que el empleado está en un entorno distinto y manejar las herramientas de seguridad no es sencillo y no

Pedro García-Villacañas, Head of Presales. Kaspersky iberia

"Ninguna empresa de forma consciente toma riesgos que les afecten"

Pedro Martínez, Director Desarrollo de Negocio en Aruba, HPE

"Creo que hay empresas que han soportado un nivel importante de riesgo"

Ángel Domínguez, Presale Business Technology de V-Valley

"Tenemos mucha tecnología que nos va a permitir afrontar los riesgos"

Pulse aquí para ver el encuentro

Miguel López, country manager de Barracuda

"La diferencia es que antes el trabajador era la excepción y ahora es la regla"

todos los responsables de seguridad pueden comprobar si la seguridad está funcionando de forma eficiente porque no lo pueden monitorizar en los entornos nuevos".

Lo cierto es que, ha aumentado el control de los riesgos y, como dice Joaquín Gómez, "esto es un error en sí. El control masivo de todos los trabajadores que están en remoto es un riesgo en sí y no se puede comprobar de manera eficiente la seguridad de cada usuarios. En el momento actual el mayor riesgo está en la suplantación de la identidad y también el control de acceso de los usuarios. Todo esto en la oficina es fácil pero en este entorno, no". La clave para Miguel López es que "no hay muchos nuevos riesgos, pero sí riesgos incrementados. Nosotros insistimos en dos vectores de ataque que son el e-mail y los recursos web de la empresa. Tenemos que tener en cuenta que son dos servicios activos 24x7 y en los que participan todos los usuarios de la empresa con los riesgos que conllevan ya que no están formados todos los usuarios en materia de seguridad. Esto ya era un vector de ataque anterior y ahora lo es más. Estamos viendo que los usuarios acceden desde un dispositivo que no está securizado, que es personal y al que acceden varios miembros de la familia. Esto afecta a la parte de navegación web y también al correo electrónico". Para Ángel Domínguez, "el principal riesgo es que esta transformación se ha hecho en periodo de tiempo muy corto y esto, en muchas ocasiones, hace que los riesgos se eleven de manera exponencial al no estar los dispositivos en un entrono seguro dentro de la organización. Esto debe servir para que las empresas cambien su forma de pensar. El nivel de acceso de un usuario ya no se debe hacer con una clave. Con esto no vale, porque el dispositivo también tiene que estar asegurado. Tenemos que evolucionar en todas las políticas de acceso". Por su parte Pedro Martínez cree que "la necesidad de muchas compañías de hacer visibles los servicios en una web pública es un riesgo. En determinados servicios, por ejemplo, a los que se accedía desde un proxy de la empresa siempre se podía impedir esa conexión, Al irnos todos a nuestras casas eso ya no puede ser porque nos van a llegar peticiones de acceso desde cualquier dirección IP. Otro punto es que ahora mismo, la mayor parte de nosotros estamos conectados a la red wifi doméstica que tiene unas características de seguridad muy por debajo de las que tiene una empresa. Sabemos que el tipo de cifrado que tienen las claves domésticas es un cifrado básico por lo que un atacante puede acceder a un dispositivo que no es muy seguro para intentar abrir una puerta de entrada a los activos de información de la compañía". Finalmente, Pedro García-Villacañas cree que "ninguna empresa toma riesgos de forma consciente. Los riesgos se han incrementado claramente y esto es lo que marca la diferencia en la actual situación que es el cambio de perímetro. Trabajar con los dispositivos empresariales hacía que el perímetro fuera seguro. Pero hemos hecho un cambio de acceso a nuestros recursos por ejemplo, tenemos el router de casa que en la gran mayoría, los usuarios usan credenciales que vienen por defecto, no actualizan el firmware del router, etc. Esto hace que ciertas campañas de ransomware o de phishing pueda encontrarse con ciertas ventanas por las que un ciberdelicunte puede acceder".

PAPEL DEL CISO

Con esta situación el papel del CISO se ha visto reforzado. En este sentido el portavoz de Kaspersky cree que "un CISO tiene que evaluar los riesgos de forma continua y buscar soluciones a las nuevas amenazas en la medida de los recursos de los que dispone, en base a la madurez, presupuesto y equipo de los que disponga. Esto va por oleadas. El CISO tiene que monitorizar de forma continua". Por su parte, el Director Desarrollo de Negocio en Aruba de HPE considera que "el papel del CISO no es distinto del que tenían hace

KASPERSKY

Kaspersky es la mayor compañía privada de ciberseguridad. Operamos en 200 países y territorios y disponemos de 35 oficinas en 30 países. Nuestra independencia nos permite ser más ágiles, pensar de forma diferente y actuar con mayor rapidez. Estamos continuamente innovando, ofreciendo protección eficaz, útil y accesible. Nos sentimos orgullosos de desarrollar tecnologías de seguridad líderes del mercado

BITDEFENDER

Bitdefender es una compañía líder mundial en ciberseguridad que protege más de 500 millones de sistemas en más de 150 países. Desde 2001, la innovación de Bitdefender ha brindado sistemáticamente productos de seguridad galardonados e inteligencia sobre amenazas para hogares conectados e inteligentes, usuarios de dispositivos móviles o empresas modernas y sus redes, dispositivos, centros de datos e infraestructuras cloud

VMWARE

El software de VMware potencia las infraestructuras digitales más complejas del mundo. La oferta en soluciones de cloud, modernización de aplicaciones, networking, seguridad y espacio de trabajo digital de la compañía ayuda a los clientes a ofrecer cualquier aplicación en cualquier nube en cualquier dispositivo. VMware ofrecer seguridad intrínseca a través de una cartera integral que abarca los puntos críticos de control de seguridad.

BARRACUDA

La realidad actual con millones de usuarios teletrabajando desde dispositivos externos a la empresa y, probablemente, no plataformados ni asegurados correctamente frente a ataques no hace más que subrayar la importancia de contar con una protección avanzada y de nueva generación del correo corporativo como la que proporciona Barracuda con su solución TEP (Total Email Protection)

WATCHGUARD

WatchGuard cuenta con productos y servicios de seguridad que ayudan a las compañías a recuperar la visibilidad de las actividades de sus teletrabajadores, ofreciendo y asegurando una protección sólida y permanente que acompaña al usuario en movimiento, ofreciendo el mismo nivel de seguridad, dentro o fuera del perímetro de la red corporativa.

V-VALLEY

La adopción empresarial de la seguridad Zero Trust está creciendo como parte de iniciativas clave para mitigar el riesgo cibernético. Con su principio de verificación de usuario, dispositivo y de la infraestructura antes de otorgar el acceso condicional basado en el mínimo privilegio, Zero Trust posee el promesa de usabilidad, protección de datos y gestión enormemente mejoradas. V-Valley puede convertise en su socio preferencial para ayudar a implementar esta solución

ARUBA, A HEWLETT PACKARD ENTERPRISE

La conexión a través de redes domésticas puede plantear riesgos en términos de Ciberseguridad. El incremento en el número de personas que teletrabajan, supone un aumento exponencial en la superficie que debemos proteger frente a ataques; este hecho no ha pasado desapercibido para los ciberatacantes, que pueden explotar nuevos vectores de ataque. Con Aruba, a Hewlett Packard Enterprise puede extender al hogar la misma experiencia de uso de la oficina.

Carlos Vieira, Country manager para Iberia de Watchguard

"Cuando esto acabe la profesión de CISO va a ser muy demandada"

Joaquín Gómez, NSX Enterprise Account Executive de VMware

"Ha aumentado el control de los riesgos y esto es un error en sí"

Juan Grau, Regional Sales Manager de Bitdefender

"Ha primado la eficiencia laboral por encima de la seguridad"

Pulse aquí para ver el encuentro

meses. Lo que está poniendo de manifiesto esta situación es que su labor tiene que ser totalmente transversal. Las empresas que no han hecho los deberes tendrán que hacer un plan de contingencia serio. Vamos hacia un nuevo modelo de IT y si un empresario relega sus impuestos o cuentas a un asesor lo mismo debe ser en lo que se refiere a la tecnología, porque la seguridad es crítica para su subsistencia". Para el portavoz de V-Valley, "el papel del CISO es fundamental y en una crisis como esta se ha visto la importancia de tener una estrategia clara en materia de ciberseguridad. Esperamos que esto haya provocado una concienciación por parte de las empresas y se den cuenta de la importancia que tiene. Hay organizaciones que no se pueden permitir tener esa figura pero esto nos tiene que servir para ver la importancia de, al menos, tener unos planes de contingencia". Miguel López de Barracuda, lo tiene muy claro: "El papel del CISO no ha variado. Su papel sigue siendo el mismo, que no es otro que de hacer de "Pepito Grillo", es decir, ser la conciencia de la empresa de hacer de freno a la estrategia habitual de la parte de producción que piensa en la seguridad en segundo plano. Con Covi-19 esto es más complicado: antes ya era difícil frenar determinados proyectos IT poniendo a la seguridad como freno y ahora lo es más porque ha habido que hacer muchas cosas con mucha urgencia y ha sido prioritario poner en marcha procesos productivos en modo online, con lo que la seguridad ha quedado relegada".

Desde VMware creen que "el CISO debe definir una estrategia de estado en ese nuevo perímetro. Nosotros creemos que el CISO debe definir una transformación completa. Manejar esto como un entorno de excepción para poder adaptar la estrategia de cara al futuro. El CISO debe aplicar una estrategia para saber si se quiere llevar a los usuarios a sus casas o la aplica para su empresa". Según el portavoz de Bitdefender, "los responsables de IT de las compañías se han convertido en los héroes del confinamiento. Dentro de ello, la seguridad es una tarea muy importante y su rol es fundamental. Tiene que ser el protector del buen nombre de la empresa. Es responsable de que la marca no se vea afectada por ataques o globos de información. De todas formas, en España, no todas tienen CISO, sólo las grandes. En la mayoría es el CIO el que toma las decisiones, muchas veces sin tener experiencia en ello. Si una empresa no puede tener a un CISO si deben buscar un CIO que conozca las técnicas de seguridad. No se puede llegar a ser un CIO si no se tienen conocimientos de seguridad".

Finalmente el portavoz de Watchguard, tiene claro que una vez que remita la crisis, "la de CISO va a ser una de las profesiones más demandadas en los próximos años. Además es importante el papel del CEO. Los CEOs de empresas de España deben tener ciertos conocimientos de TI de la misma forma que saben de finanzas, de gestión o de legislación. Ya se han visto despidos de CEOs por no haber dedicado presupuesto a TI".

EL DISEÑO QUE DEVUELVE LA VIDA A LA NATURALEZA

VEA

MADERA ALMA DISEÑO

Damos una segunda vida a la madera del arbol a través de un diseño sostenible
Ofrecemos mesas únicas, confeccionadas en base a las necesidades y gustos de cada cliente, por ello cada una de las mesas va sellada y numerdas.

Descubra los diferentes modelos, maderas y posibilidades en:

www.vea.com.es

Samsung Galaxy S20+ 5G

Samsung

Teléfono:
911 750 018
Web:
www.samsung.es
Precio:
Desde 1.000 euros

Valoración Global

Samsung se anticipó a todos. Su apuesta por realizar su lanzamiento antes del la celebración de MWC, luego cancelado, le salió redonda. Y todo, para presentar un terminal que mejora sensiblemente las propiedades de su antecesor sobre todo en lo que se refiera al apartado de la cámara. La idea de la compañía surcoreana pasa por dotar a la cámara de una nueva arquitectura y para ello se he centrado en incorporar la inteligencia artificial junto con un sensor que permite mejorar de forma espectacular la calidad de la imagen.

El dispositivo viene equipado con tecnología 5G y aunque todavía es incipiente el empleo de ésta, en aquellos puntos donde sí está disponible el teléfono responde a una gran velocidad si se compara con el 4G.

Pero vayamos por partes, y empecemos por la principal de las mejoras que, en este caso, se encuentra en la cámara. Samsung ha incrementado la resolución de la misma en este Galaxy S20+. El terminal incorpora una cámara de 64MP a la que Samsung a dotado de unos sensores mayores que captan más luz, por lo que se mejora la calidad de imagen incluso en situaciones de poca iluminación. La multinacional emplea en la cámara una combinación de zoom óptico y zoom digital de alta resolución con IA, que permite que se acerque al objeto que se quiere fotografiar incluso cuando estamos lejos. Este zoom es de hasta 30X. En cuanto a la grabación de vídeos, estos se pueden captar en 8K y además permite extraer una imagen de un video de 8K y convertirlo en una foto con alta resolución. Además, los videos más movidos simulan haber sido grabados con una cámara de acción, gracias a Super Steady y su tecnología de estabilización y análisis de movimiento con IA.

TELETRABAJO

En tiempos de confinamiento como las actuales el Samsung Galaxy S20+ destaca por facilitar las tareas de teletrabajo. Y es que fruto de un acuerdo con Google este smartphone mejora la experiencia de las video-llamadas con Google Duo, por lo que los usuarios pueden disfrutar de video-llamadas en Full HD.

Pero si algo es tradicional en cualquier dispositivo de Samsung ese no es otro que la seguridad que incorporan sus terminales. Los coreanos llevan años trabajando e invirtiendo mucho dinero en este aspecto, que es uno de los apartados que más preocupan a los usuarios de empresa. Nuevamente el teléfono está protegido por Knox que asegura el dispositivo desde el chip, hasta cada capa del software. Como novedad, el Galaxy S20+ también incorpora un nuevo procesador seguro que protege el equipo de cualquier ataque basado en hardware.

Encuentros tecnológicos

byte TI

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

TE ORGANIZAMOS UN ENCUENTRO AD HOC

INFÓRMATE

Encuentros tecnológicos byte TI

Portátiles para teletrabajar

La crisis sanitaria ocasionada por el coronavirus ha hecho que, en las últimas semanas, el teletrabajo cobre fuerza entre determinados sectores profesionales. En este sentido, todas las firmas que incorporan en sus catálogos portátiles cuentan con un amplio abanico de modelos que favorecen el trabajo a distancia; pero que también permiten que el usuario los pueda trasladar, cuando sea necesario, de un lugar a otro de forma cómoda gracias a su ligereza.

Un ejemplo de esta oferta es la siguiente selección. En ella, existen dos propuestas enfocadas a un target profesional muy concreto: son los casos de Gigabyte AERO 15 OLED para perfiles creativos y el Panasonic TOUCHBOOK 55, para quienes realizan labores o tareas de campo que luego deben continuar en el trabajo o su casa.

Otra opción para el teletrabajo son los convertibles Dell Latitude 7400 2-en-1 y HP Elite Dragonfly, este último fabricado con plásticos recuperados del fondo marino. Quienes tengan en mente la opción de un dispositivo que apueste al cien por cien por la nube informática, el portátil Acer Chromebook Enterprise 714 es una alternativa a considerar.

También participa en este artículo Asus de la mano de su ExpertBook B9 (B9450), presentado en el mercado hace escasas semanas, y Dynabook Portégé X30L-G que a pesar de sus 870 gramos es un ordenador que cubre perfectamente nuestras necesidades en el hogar. Lo mismo sucede con el Fujitsu Notebook LIFEBOOK U939, el Lenovo ThinkPad X1 Carbon o el LG Gram 15Z90N. Cualquiera de ellos es perfectamente válido no sólo para trabajar, sino también para disfrutar de momentos de ocio viendo una película, escuchando música o navegando por Internet. Sus configuraciones resultan completas y el rendimiento está a la altura de lo que uno puede esperar hoy en día de uno de estos dispositivos: configuraciones avanzadas, una alta autonomía de la batería, conectividad adecuada, pantallas de calidad… A esta lista, hay que añadir el equipo Microsoft Surface Laptop 3 disponible en dos tamaños de pantalla: 13,5 y 15 pulgadas.

Acer Chromebook Enterprise 714

Enfocado a proporcionar a los profesionales que utilizan la nube una forma más segura y eficaz de trabajar. La autonomía es de hasta 12 horas.

El modelo seleccionado por parte de la firma taiwanesa para este artículo pertenece a su hornada de portátiles Chrome Enterprise presentada en el mes de noviembre del año pasado. Este en concreto, con un chasis entero de metal, cuenta con una pantalla LED multitáctil de 14 pulgadas y 1.920 x 1.080 píxeles de resolución de bordes estrechos. Sobre ella, se sitúa una webcam HDR con un objetivo de 75º.

Con unas dimensiones de 323 x 238,6 x 17,70 mm, pesa 1,60 kilogramos, lo que favorece su transporte y muestra, además, una alta resistencia; de hecho, está reconocido con la norma MIL-STD 810G1: esto significa que puede sobrevivir, por ejemplo, a caídas desde 1,2 metros de altura y presiones elevadas. Otros datos a destacar es que dispone de Citrix-Ready Certification y un de huellas dactilares como medida de protección que siempre es bienvenido.

Entrando en detalle, está orientado a proporcionar a los profesionales que usan la nube informática una forma segura y eficiente de trabajar. En este caso, Chrome Enterprise ayuda a que los responsables de IT accedan a las políticas de dispositivos y a las capacidades de control del parque de equipos desde la consola de administración de Google, fácil de usar y basada en la cloud, o mediante una solución UEM (Unified Endpoint Management) de terceros. El tiempo de inicio del portátil es de solo ocho segundos, y la interfaz se ha simplificado para que al trabajador le resulte más fácil aprender a utilizarla y desplazarse a través de las opciones disponibles. Por otra parte, incorpora el asistente de Google que reconoce peticiones verbales incluso en condiciones ruidosas gracias a que integra un procesamiento de voz de dos micrófonos.

Desde el punto de vista tecnológico, está provisto de un procesador Intel Core i3 de octava generación que, entre otros beneficios, favorece la multitarea y facilita que las aplicaciones se carguen en menos tiempo. Su memoria RAM DDR4 tiene un tamaño de 8 GB y la capacidad de memoria flash 64 GB. Posee, asimismo, una ranura para tarjetas de memoria microSD y microSDXC, así como tres puertos USB: 2 USB 3.1 de clase C y 1 interfaz USB 3.1 DE clase A.

Incluye también estas otras características: Wi-Fi ac, bluetooth 4.2 y dos altavoces que reproducen sonido estéreo. Existe la opción de que el teclado sea retroiluminado y la batería de cuatro celdas promete una autonomía de hasta 12 horas de uso.

Acer

Tel: 934 92 24 00
Web: www.acer.es
Precio: 826,43 euros

Asus ExpertBook B9

Durabilidad militar, Wi-Fi 6 y chasis de aleación de magnesio y de litio. Estas son algunas de las características destacables de este equipo.

Disponible desde hace solo unas semanas, tiene un peso a partir de los 870 gramos y un perfil de 14,9 mm. Asus ha apostado por una pantalla NanoEdge sin marcos que hace que la proporción entre la pantalla y el cuerpo sea del 94%, lo que ha permitido instalar un panel de 14 pulgadas en un chasis con unas dimensiones propias de un portátil de 13 pulgadas.

Este ExpertBook B9 ofrece un alto rendimiento, encontrándose disponible con procesadores Intel Core de décima generación, un diseño de almacenamiento doble con dos unidades SSD PCIe 3.0 x4 de hasta 2 Terabytes, un máximo de 16 GB de RAM y conectividad Wi-Fi 6 (802.11ax). Asimismo, está certificado por el Proyecto Athena de Intel, un programa que dictamina la capacidad de respuesta de los portátiles teniendo en cuenta elementos como la duración de la batería, las opciones de conectividad y la calidad de su diseño. Brinda, por otra parte, conectividad HDMI, dos puertos Thunderbolt 3 y una bisagra (recibe el nombre de ErgoLift) que optimiza la posición al escribir.

Cabe también destacar otros detalles como su matriz de cuatro micrófonos con soporte de campo lejano y cancelación de ruido, y la presencia de una barra de luz delantera que se activa al interactuar con los asistentes Microsoft Cortana y Amazon Alexa. Mientras, Harman Kardon ha optimizado el sistema de sonido del portátil con unos altavoces que realizan ajustes dinámicos para aumentar la claridad y filtrar el ruido. Este B9 llama la atención, en otro orden de cosas, por emplear la tecnología Asus NumberPad 2.0, un teclado numérico LED integrado en el touchpad que permite introducir números de forma sencilla y eficiente.

Ha superado el estándar militar MIL-STD-810G, una batería de pruebas de laboratorio que incluye ensayos de caída, impacto, vibraciones, altas y bajas temperaturas, días funcionando al 95% de humedad y horas de exposición a arena y polvo. Combinando un chip de seguridad del Módulo de Plataforma de Confianza 2.0 (TPM), una cubierta de cámara web y una cámara de infrarrojos para iniciar sesión de forma segura, el B9450 es un equipo provisto de funciones que salvaguardan los datos de la empresa y la privacidad personal.

La variante equipada con batería de dos celdas y 33 Wh permite ser productivo durante un máximo de 12 horas, mientras que la configuración con batería de 66 Wh llega a durar hasta 24 horas bajo la misma carga de trabajo.

Asus

Tel: 902 889 688
Web: www.asus.es
Precio: 1.799 euros

Dell Latitude 7400 2-en-1

Con protección Gorilla Glass 5, su rendimiento térmico adaptable le permite detectar su entorno y ajustar el rendimiento para que controle su propia temperatura.

Con unas dimensiones de 319,77 x 199,9 x 8,57-14,89 mm y un peso de 1,26 Kg, este dispositivo dos en uno ha sido provisto de una pantalla táctil de marcos reducidos Full HD de 14 pulgadas antirreflectante y antimanchas, y una prestación que le hace especial: puede detectar su entorno y ajustar así el rendimiento para poder controlar la temperatura en consecuencia. Del mismo modo, dispone de un sistema de aislamiento térmico ultracompacto GORE, que le lleva a proporcionar unos niveles de conductividad térmica inferiores al aire. Está preparado para utilizarse con lápices digitales.

Sus desarrolladores, por otro lado, han incorporado un sensor de proximidad (Dell ExpressSign) que incluye Intel Context Sensing. Esto hace que el sensor detecte la presencia del usuario con la ayuda de la cámara de infrarrojos encendiendo de manera automática el sistema gracias a Windows Hello.

En lo que a diseño se refiere, luce un acabado en aluminio mecanizado y protección Gorilla Glass 5 que aporta una mayor durabilidad y resistencia. ¿Y la batería? Integra un modelo de cuatro celdas de 52 Wh para que funcione durante varios días y, además, es compatible con Dell ExpressCharge, una tecnología que según indica el fabricante puede cargar hasta un 80% de la capacidad del portátil en una hora.

Este Dell Latitude 7400 2-en-1 se encuentra disponible en diferentes configuraciones para que el público elija la que más de adecue a sus necesidades. En el apartado del procesador, descubrimos que la firma norteamericana ha empleado la octava generación de procesadores Intel Core hasta i7 con tecnología vPro de cuatro núcleos para, de este modo, incrementar la capacidad de gestión y la productividad de los trabajadores. El tamaño de la memoria RAM oscila entre los 8 GB y los 16 GB, y a nivel de almacenamiento SSD las opciones que incluye son dos: 256 GB o 512 GB. Las cuatro versiones que existen de esta máquina integran el mismo sistema operativo, Windows 10 Pro de 64 bits.

El apartado de conectividad resulta muy completo: dos USB 3.1 de primera generación (con PowerShare, USB tipo-A), dos Thunderbolt 3 con suministro de alimentación y DisplayPort (USB tipo-C), un puerto HDMI 1.4, una bandeja para tarjeta uSIM externa opcional (solo WWAN), un lector de tarjetas de memoria uSD 4.0, un lector de tarjetas inteligentes por contacto opcional y un lector de huellas dactilares táctil opcional en el botón de encendido.

Dell

Teléfono: 91 722 92 00
Web: www.dell.es
Precio: 1.595,99 euros

Dynabook Portégé X30L-G

Bañado por un chasis fabricado en magnesio, su peso ligero (a partir de los 870 gr) no le impide proporcionar una alta resistencia.

Dynabook (anteriormente conocida como Toshiba) lanzó a primeros de este año, en el marco internacional de la feria CES de Las Vegas, su nuevo portátil profesional, el modelo Portégé X30L-G. Se trata de un dispositivo de 870 gramos de peso y una autonomía que escala hasta las 14,5 horas de uso en un cuerpo que tiene unas dimensiones de 308,8 x 211,6 x 179 mm. Comparte, con otros dispositivos que participan en este artículo, la función de carga rápida que proporciona cuatro horas de batería con una carga de solo 30 minutos.

A pesar de su ligereza, tiene un chasis de magnesio, lo que lo convierte en un equipo robusto, y ha sido sometido a pruebas de calidad militar MIL-STD-810G que ha superado; estas pruebas incluían, por ejemplo, resistencia a caídas, tests de humedad y polvo, temperaturas extremas... Su pantalla, con un tamaño de 13,3 pulgadas, integra un panel LCD FHD antirreflejos e IGZO (del inglés Indium gallium zinc oxide), un tipo de tecnología que, entre otros beneficios, arroja un menor consumo energético. El nivel de brillo se sitúa en los 470NIT.

El Dynabook Portégé X30L-G incorpora una amplia selección de opciones de almacenamiento SSD, incluyendo SATA, PCIe rápido e Intel Optane, para permitir flujos de trabajo ágiles y una mayor productividad. Además, cuenta con un lector de tarjetas microSD y memoria RAM DDR4 para soportar las demandas de las aplicaciones empresariales de hoy en día. Es posible elegir entre diferentes clases de procesadores que pertenecen a la décima generación de Intel.

A pesar de su diseño ultraplano, está equipado con un puerto USB tipo C, un puerto HDMI de tamaño completo y 2 puertos USB 3.0. También puede conectarse con un solo clic a una base USB-C opcional. En cuanto a conectividad de red, incorpora el último módulo Intel 802.11ax (WiFi 6) para soportar velocidades más rápidas y un mayor ancho de banda, y puerto Gigabit-LAN, entre otros. También viene con Bluetooth 5.0. Los altavoces son estéreo.

Por lo que se refiere a la seguridad, el Portégé X30L-G cuenta con autenticación biométrica facial y de huellas dactilares a través de Windows Hello e Intel Authenticate que evita accesos no autorizados. Otros componentes de seguridad, como el chip Trusted Platform Module 2.0 (TPM) y la BIOS de fabricación propia, proporcionan una capa adicional de protección. El sistema operativo que utiliza es Windows 10 Pro de 64 bits.

Dynabook

Teléfono: 91 660 67 00
Web: es.dynabook.com
Precio: 1.376,88 euros

Fujitsu Notebook LIFEBOOK U939

Este modelo de 13,3 pulgadas cuida de manera especial la seguridad. Ofrece la opción de incorporar identificación biométrica a través de las venas de la mano.

La familia de portátiles Notebook LIFEBOOK de la multinacional japonesa está dividida en tres grandes grupos y cada uno de ellos incluye una serie de equipos. Estos grupos son tres: 'Superior', 'Advanced' y 'All-Round'. El modelo que aparece en estas líneas se encuadra dentro del primero.

Es posible elegir entre dos colores (negro o rojo), tiene un peso de 920 gramos y una batería capaz de soportar algo más de 14 horas de uso según datos proporcionados por el fabricante. Con unas dimensiones que invitan a su cómodo transporte al igual que otros modelos de su clase (mide 309,3 x 213 x 15,5 mm) y Windows 10 Pro como sistema operativo, brinda características de seguridad empresarial avanzadas como la tecnología integrada PalmSecure que emplea las venas de la mano como sistema de identificación biométrica; la otra opción es un sistema de huella dactilar. Tampoco falta un lector smartcard, soporte de bloqueo Kensington y TPM 2.0.

La carcasa ha sido fabricada en magnesio, mientras que la pantalla (es antideslumbrante) tiene un tamaño de 13,3 pulgadas y 1.920 x 1.080 píxeles de resolución. El usuario tiene, además, la opción de elegir, en función de sus necesidades, si quiere o no un panel táctil.

Encima de ella, se encuentra una cámara de infrarrojos Full HD que permite el reconocimiento facial con Windows Hello. ¿Y la conectividad? Este apartado se ha resuelto muy bien: HDMI y LAN de tamaño completo, dos puertos Intel Thunderbolt 3 de clase C con función de suministro de energía, dos USB de clase A, uno de ellos con función de carga USB que permite alimentar la batería de otros dispositivos compatibles, ranura para tarjetas de memoria (SD/microSD card hasta 2 GB, SDHC/microSDHC card hasta 32 GB y SDXC/microSDXC hasta de 2 Terabytes) ...

Procesador. Las dos versiones de este modelo se encuentran disponibles con las siguientes opciones: Intel Core i7 8665U, Intel Core i5- -8365U e Intel Core i5 8265U; todos ellos con cuatro núcleos. En cuanto al disco duro, las posibilidades son dos. De un lado unidades SSD SATA III con capacidades que oscilan entre 256 GB y un Terabyte, o discos PCIe-SSD de 256 GB, 512 GB o 1024 GB. La memoria RAM tiene un tamaño de 8 GB pero si en el futuro el usuario necesita ampliarla puede hacerlo porque el portátil está preparado para soportar hasta 16 GB.

Fujitsu

Teléfono: 91 784 90 00
Web:
www.fujitsu.com/es
Precio: 1.317,69 euros

Gigabyte Notebook Aero 15

El perfil de usuario al que se dirige es el de los profesionales creativos y la pantalla es su principal reclamo: un panel AMOLED 4K de 15,4 pulgadas.

La serie AERO incluye los primeros ordenadores portátiles diseñados especialmente para creativos profesionales, integrando unos paneles OLED que se caracterizan por una elevada precisión del color. En este sentido, y aunque la certificación de calibración X-Rite Pantone garantiza al usuario la precisión del estándar Adobe RBG, la gama incluye también una tarjeta Nvidia RTX Studio completamente calibrada para un rendimiento superior.

Gigabyte continúa apostando por su tecnología de refrigeración Supra Cool que ha obtenido una actualización en este AERO 15. Recibe el nombre de Supra Cool 2 e integra los siguientes componentes: cinco tubos de calor, dos ventiladores de 71 cuchillas y once rendijas de ventilación que ayudan a que la disipación del calor se incremente en un 30%.

El centro neurálgico de esta máquina lo preside un procesador que forma parte de la novena generación Intel Core (i7-9750H). Para la memoria, sus desarrolladores han optado por un modelo de Samsung que promete un alto rendimiento, transferencias ultrarrápidas y un consumo de energía reducido. Admite hasta dos ranuras de memoria DDR4 y un máximo de 64 GB. En cuanto a su capacidad de almacenamiento, es posible almacenar hasta 512 GB de información.

No obstante, y tal y como se hacía intuir al principio de este texto, su principal reclamo lo encontramos en su pantalla AMOLED 4K de 15,6 pulgadas; especificaciones que la hacen muy interesante para el público al que se dirige. Esta pantalla cuenta, por otro lado, con un marco-parachoques que sirve para amortiguar posibles impactos. La webcam fijada en la parte superior integra una pestaña para proteger la privacidad.

Una pantalla de estas características necesita un sonido que esté a la altura y para garantizar la experiencia en este apartado se brinda un sonido envolvente virtual 7.1 de la mano de NAHIMIC 3. Éste se puede ajustar través del software que se proporciona para adaptarse a cualquier entorno y, de este modo, disfrutar de la mejor experiencia ya sea en una conferencia telefónica o visualizando contenidos multimedia.

La elección de los materiales se ha cuidado de manera especial. Esto permite que no sólo luzca una atractiva apariencia, sino que además proporcione un diseño idóneo para el día a día. Así, todo el chasis ha sido fabricado en aluminio comprimido que aporta una estructura resistente. A pesar de ser junto al equipo de Panasonic, los dos portátiles de mayor peso, sus 2 kg no impiden un transporte relativamente comodidad si las circunstancias lo requieren.

Gigabyte

Web:
www.gigabyte.com/Contact
Precio: 1.492 euros

HP Elite Dragonfly

Diseño dos en uno para este equipo convertible y ultraligero que ha fabricado HP con plásticos que se han recuperado del océano.

Representa a la nueva joya tecnológica de la firma en su gama premium y, además, hace un guiño al medio ambiente al convertirse en el primer portátil fabricado con plásticos que han sido recuperados del océano. Además, este modelo ultraligero convertible de menos de un kilogramo de peso promete una autonomía de hasta 24,5 horas según apunta el fabricante. Luce, por otra parte, un teclado ultrafino y retroiluminado, y una nueva almohadilla táctil más ligera para una mejor una experiencia de trabajo.

Con un panel de 13,3 pulgadas y resolución Full HD, es posible disfrutar de la última conectividad Wi-Fi 6: ésta se caracteriza por arrojar velocidades de transferencia de archivos hasta tres veces más rápidas que Wi-Fi 5 para, así, escalar hacia un rendimiento superior. Desde el punto de vista de la seguridad, incluye HP Sure Sense que protege al equipo de los ataques de malware aplicando capacidades de inteligencia artificial y también HP Sure Recover con restablecimiento de imagen integrado para una recuperación rápida, segura en cualquier momento y desde cualquier lugar. Gracias a la presencia de HP Sure View y HP Privacy Camera es posible controlar lo que el usuario comparte con otras personas. El 4G LTE Gigabit es opcional, permitiendo a los usuarios conectarse y colaborar desde casi cualquier lugar.

Otro detalle que llama la atención es que ayuda a mejorar los hábitos de trabajo y prácticas que son buenas para la salud gracias al software HP WorkWell. Se trata de una herramienta a través de la cual el equipo envía recomendaciones de cuando tomar descansos y proporciona consejos de productividad personalizados y adaptados para cada usuario.

Es posible elegir entre cuatro configuraciones, todas ellas con un denominador común: la presencia de un procesador que forma parte de la octava generación Intel Core vPro. El modelo seleccionado funciona a las órdenes del chip Intel Core i5-8265U, una memoria LPDDR3 de 8 GB y un disco duro de 256 GB PCIe NVMe SSD más PCIe NVMe Intel Optane de 16 GB. El sistema operativo es Windows 10 Pro de 64 bits y los gráficos permanecen integrados (Intel UHD 620).

Por otro lado, las opciones de conectividad incluyen una interfaz HDMI, un combo de auriculares/micrófono, un USB 3.1 (de carga) y dos puertos Thunderbolt (conector USB de clase C con soporte de suministro de energía 3.0). El sonido lleva el sello de la firma Bang & Olufsen, con cuatro altavoces estéreo y micrófono de matriz múltiple frontal.

HP

Teléfono: 902 027 020
Web:
www.hp.es
Precio: 1.820,38 euros

Lenovo ThinkPad X1 Carbon

Ofrece visibilidad, datos en tiempo real y protección. Además, accede a servicios en la nube y aplicaciones privadas desde cualquier lugar y en cualquier dispositivo.

La serie ThinkPad de Lenovo se caracteriza por integrar equipos portátiles con un diseño compacto, baterías con una gran autonomía y una estructura todoterreno: en este caso, son probados con 12 especificaciones de nivel militar y sometidos a una gran batería de pruebas que permiten autentificar su durabilidad y resistencia en condiciones extremas. En esta gama, el usuario puede elegir entre diferentes dispositivos en función de sus necesidades y uno de ellos es este ThinkPad X1 Carbon de séptima generación.

Es un 6% más fino que su predecesor, posee unas dimensiones de 323 x 217 x 14,95 mm, pesa 1,09 kilogramos y su batería brinda una autonomía de hasta 18 horas según apunta el fabricante. Además, integra tecnología de carga rápida (Rapid Charge) que en solo una hora es capaz de recargar un 80% de su capacidad.

El usuario tiene a su disposición diferentes configuraciones entre las que elegir con procesadores que forman parte de la octava generación Intel (hasta Core i7 vPro), una memoria LPDDR3 de hasta 16 GB y almacenamiento SSD PCI de hasta 2 TB de tamaño que garantizan altos niveles de rendimiento y productividad. En cuanto a su pantalla de 14 pulgadas, la multinacional de tecnología china propone paneles de diferentes resoluciones: desde la 'clásica' Full HD al 4K (3.840 x 2.160 píxeles) con Dolby Vision y 500 nits; por cierto, que los portátiles con pantalla 4K incorporan una cubierta superior de fibra de carbono. Sobre esta pantalla se ha colocado una cámara HD (720p) con tapa de privacidad ThinkShutter: se trata de una tapa física que bloquea la lente para, así, garantizar, que solo nos ven cuando queremos. El sonido corre a cargo de un sistema de altavoces Dolby Atmos y cuatro micrófonos de 360º de largo alcance. Por su parte, el teclado se retroilumina con una iluminación LED de color blanco y es resistente a las salpicaduras.

El paquete de funciones de seguridad ThinkShield garantiza la privacidad de la información del usuario, protegiendo los datos que almacena. También se ha incorporado un chip dTPM 2.0, lector de huellas dactilares Match-on-Chip y funcionalidad de autenticación FIDO (Fast Identity Online). Si nos fijamos en sus opciones de conectividad, soporta WLAN y Bluetooth 5.0. La tecnología NFC es opcional, al igual que la banda ancha móvil global integrada 4G LTE-A. Con esta última, la tecnología WWAN permite que el portátil funcione como un teléfono inteligente cuyo servicio de telefonía móvil siempre puede conectarse en línea.

Lenovo

Teléfono: 917 896 872
Web:
www.lenovo.es
Precio: 1.736,17 euros

LG Gram 15Z90N

Posee un chasis fabricado en magnesio y nanocarbono, y su disco SSD se acompaña de una ranura adicional que permitiría llegar a los 4 Terabytes.

Con unas dimensiones de 357,6 x 225,3 x 16,8 mm y un peso que apenas rebasa en unos gramos el kilo, este miembro de la ya conocida gama de portátiles LG Gram se 'empapa' de toda la filosofía que la caracteriza. Esto implica, por ejemplo, que a pesar de ser un dispositivo ultraligero brinda una importante resistencia. Lo pone de manifiesto su chasis fabricado en nanocarbono y magnesio. También que haya superado con éxito hasta siete pruebas del estándar militar MIL-810G. De igual forma, comparte con otros dispositivos de esta serie una alta autonomía: su fabricante asegura una batería de 80 Wh y 18,5 horas de uso.

Si ahondamos en sus prestaciones a nivel técnico, a la cabeza de este modelo de la firma surcoreana se sitúa un procesador que forma parte de la serie Intel Core de décima generación. Se combina con gráficos Intel Iris Plus 655 para una mayor fluidez de la imagen; una memoria RAM de 8 GB con ranura de ampliación para llegar a los 24 GB si el usuario lo necesita; y un disco SSD de 256 Gb de serie que se acompaña de una ranura adicional para ampliar hasta los 4 Terabytes.

La pantalla del LG Gram 15Z90N deja buenas sensaciones y experiencia de uso.

Contamos con un panel ISP Full HD de 15,6 pulgadas de tamaño (el ratio es de 16:9) que cubre hasta un 96% del espacio de color sRGB. Mientras, desde el punto de vista del audio, se garantiza un sonido inmersivo gracias a que soporta el formato DTS:X. Comparte con otros dispositivos portátiles que el teclado se retroilumina en entornos oscuros, pero con una diferencia: es posible elegir el tipo brillo y escoger así entre dos niveles de iluminación. El lector de huellas dactilares se ha colocado en el botón de encendido.

En lo que se refiere al apartado de la conectividad, junto al puerto de alimentación y la toma de auriculares de 3, 5 mm, descubrimos tres puertos USB 3.1 de clase A y otro más de tipo C con Thunderbolt incorporado para una carga ultrarrápida. Además, y como explica LG, se podría llegar a visualizar contenido 5K y transferir datos con una velocidad de hasta 40 Gb/s de ancho de banda y cargar un dispositivo conectado sin necesidad de utilizar ningún cable adicional. Todo ello al mismo tiempo. Estas opciones de conectividad se completan con una ranura para tarjetas microSD 3.0 y una entrada HDMI.

LG

Teléfono: 91 211 22 00
Web:
www.lg.com
Precio: 1.499 euros

Microsoft Surface Laptop 3

Este nuevo miembro de la familia Surface con una cubierta de aluminio está disponible en dos versiones: una de 13,5 pulgadas y otra de 15 pulgadas.

Manteniendo el diseño delgado y elegante de su predecesor, el portátil Surface Laptop 3 equilibra una estética elegante (por ejemplo, la cubierta exterior es de aluminio) y una alta productividad. En este caso, ofrece hasta un 50% más de rendimiento que la generación anterior y es posible disfrutar de un panel táctil un 20% más grande que favorece el confort.

Sugiere, de igual forma, una nueva serie de colores y acabados, con materiales como el aluminio y el tejido Alcantara, y el usuario tiene la posibilidad de elegir entre dos tamaños de pantalla 'PixelSense'; ambas multitáctiles y compatibles con el lápiz para Surface. Por un lado, existe una versión de 13,5 pulgadas que cuenta con un panel de 2.256 x 1.504 píxeles de resolución. Por otro, descubrimos un segundo tamaño de 15 pulgadas que escala hasta los 2.496 x 1.664 píxeles.

Profundizando en sus prestaciones técnicas, este portátil ha sido equipado con procesadores de cuatro núcleos que forman parte de la décima generación Intel Core: las opciones son los modelos i5-1035G7 e i7-1065G7. El tamaño de la memoria RAM LPDDR4x también es seleccionable. Así, por ejemplo, en el caso del equipo de 13,5 pulgadas el consumidor puede optar a dos tamaños (8 GB o 16 GB). El de 15 pulgadas, en cambio, permite escoger entre tres capacidades: 8 GB, 16 GB o 32 GB. ¿Y la capacidad de almacenamiento? Las capacidades entre las que elegir son las siguientes: 128 GB, 256 GB, 512 GB o 1 Terabyte.

El modelo de batería que ambas versiones incorporan, alcanza una autonomía de hasta 11,5 horas en condiciones de uso normal. Como característica complementaria, se ha introducido un sistema de carga rápida que en aproximadamente una hora puede alimentar hasta un 80% de su capacidad. Se ha mejorado, por otra parte, el modo de espera para prolongar la duración de esta batería cuando el usuario no está en casa.

Se han mejorado igualmente las cámaras frontales y, desde el punto de vista del sonido, hay que destacar la presencia de altavoces OmniSonic con sonido Dolby Audio y micrófonos duales que gracias a su alta sensibilidad prometen un audio nítido; ya sea para comunicarse, por ejemplo, a través de videoconferencia como para escuchar música o ver una película.

Para concluir este repaso, comentar que integra Wi-Fi 6 y tecnología Bluetooth 5.0. A nivel de conectividad, sus opciones incluyen un puerto USB-C, otro USB-A y puerto Surface Connect.

Microsoft

Teléfono: 913 91 90 00
Web:
www.microsoft.es
Precio: 1.749 euros

La nube: la salvación empresarial

La gran mayoría de las empresas y de los usuarios ya estaban acostumbrados al uso de cloud. Sin embargo, gracias a la pandemia originada por Covid-19 son muchas las compañías que se han dado cuenta de sus ventajas.

Por Manuel Navarro

El coronavirus lo ha cambiado prácticamente todo. También en el mundo de las tecnologías. Y, en este caso, se puede afirmar que a mejor. La crisis provocada por Covid-19 ha nutrido del impulso necesario para esas organizaciones y responsables de empresa que no confiaban en determinados apartados tecnológicos. Una de esas tendencias es Cloud. Aunque se ha generalizado mucho la utilización de la nube, todavía había ciertos aspectos en los que, a pesar de los consejos de los CIOs y de los responsables de tecnología de las empresas, los CEOs y máximos responsables no confiaban del todo.

Pero el mundo ha cambiado y la tecnología va a ser un pilar fundamental en la evolución de las sociedades que nos encontremos cunado en unos meses o años, la Humanidad supere la pandemia. Y la nube va a ser uno de los actores protagonistas. Y es que, como dice Ignacio Arrieta, Director de Ingeniería de Sistemas de Dell Technologies, "el coronavirus está consiguiendo lo que muchos CIOs y responsables de tecnología no habían conseguido: transformar digitalmente las organizaciones. Hay un concepto muy interesante que es el de la "Deuda Técnica". Este incluye todas aquellas acciones e iniciativas estratégicas que las organizaciones de TI han ido dejando de lado porque el día

a día les ha comido. Debido a la pandemia, y de la noche a la mañana, mucha de esta deuda ha golpeado a las organizaciones de TI como un boomerang: el proyecto de re-arquitectura de la aplicación de ventas, el piloto para habilitar el tele-trabajo, etc.".

A falta de datos más concretos parece que el uso de la nube se ha incrementado de forma sensible. Los grandes proveedores cloud como AWS, Microsoft o Google se han realizado una fuerte inversión para mejorar la resiliencia de su infraestructura y poder gestionar la mayor demanda que se está produciendo. Oracle por su parte ha anunciado que la crisis del coronavirus no sólo no ha impactado en su negocio, sino que ha incrementado un 4% sus ingresos trimestrales. Así que como afirma Robert Assink, director general en España de Interxion, "todos estos datos demuestran que las empresas se han volcado al cloud para impulsar su negocio y mantener la actividad. Es el caso de muchos proyectos de teletrabajo en los que se ha optado por soluciones cloud para facilitar su implantación y despliegue, así como el acceso a aplicaciones colaborativas para trabajar a distancia."

Las empresas están viendo que la nube les ofrece muchas posibilidades y, hay que reconocerlo, la prisa por implementar de forma muy rápida ha hecho que las medidas de seguridad se relajen y hayan pasado a un segundo plano hasta que la continuad de los negocios se haya consolidado. Entre otros motivos, los modelos as a service que permiten pagar por lo que realmente se consume y se pueden cancelar en cualquier momento son uno de los factores que han hecho posible este incremento exponencial de todo tipo de soluciones cloud. También la escalabilidad porque como afirma Javier Corella, director de marketing de IECISA, "la escalabilidad ha resultado fundamental en muchos sectores. Tal es el caso del retail, supermercados cuyo core de negocio ha pasado de la tienda física a la página web y el comercio on-line con unas infraestructuras que, en algunos casos, no estaban preparadas para dar respuesta al aluvión que están sufriendo. Gracias al cloud y a la escalabilidad que proporciona han sido capaces de responder a los picos de demanda y, cuando este incremento de peticiones disminuya, la aplicación volverá al uso de infraestructuras necesarias en cada caso".

Una de las ventajas es que la nube ha permitido a muchas empresas que apenas estaban digitalizadas adaptarse a una nueva realidad y hacer esa transformación digital a pasos agigantados. Así lo afirma Galo Montes, director de preventa de HPE España que afirma que "a una parte de empresas les ha pillado con los deberes por hacer para adaptarse a esta nueva realidad por falta de transformación digital, teniendo que acometer ahora de forma precipitada soluciones técnicas que les permitan poder mantener parte de su actividad. En este contexto, la nube ha sido uno de los recursos más demandados por la capacidad de dar soluciones casi inmediatas. Esto ha provocado que los hiperescalares hayan llegado a cerca del máximo de su capacidad y que las soluciones implantadas no hayan sido, en muchos casos, las más óptimas. Así que se puede ver de forma clara que efectivamente la nube ha sido una solución, pero entendemos que ahora se redefinirán

dichas soluciones urgentes, adoptando unas más permanentes y efectivas económicamente".

LO MÁS DEMANDADO

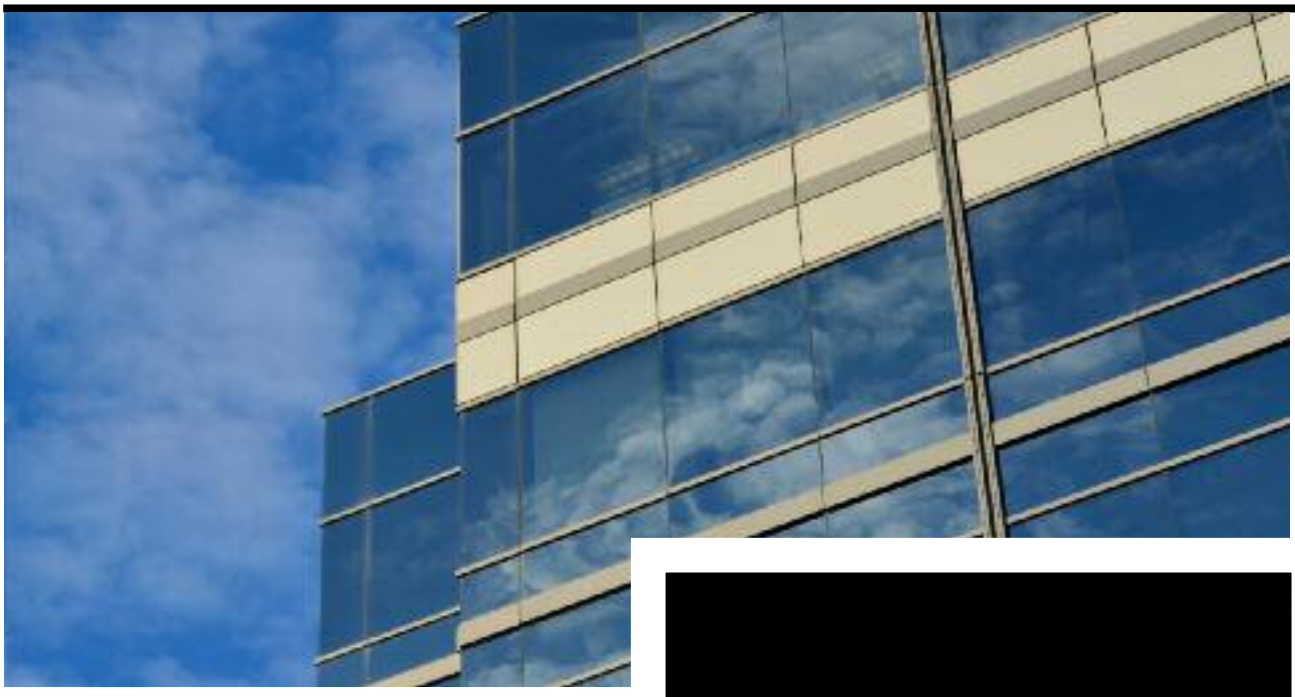
De la noche a la mañana la práctica totalidad de las empresas han tenido que cambiar sus procesos de negocio. Para ello han tenido que incorporar nuevas soluciones, formar a los empleados en tiempo récord, adaptarse a la nueva realidad y descubrir un mundo nuevo de herramientas que les ha permitido seguir adelante. Aunque la demanda de soluciones va por sectores y como afirma Marc Granados, director comercial y de marketing de Econocom Nexica, "podemos dividirlo en dos grandes bloques: el de empresas afectadas en su productividad motivado por Covid-19, que se inclinan más por reducción de costes o una rearquitectura de la plataforma, y por otro lado, empresas que han disparado su actividad, que de forma usual ya adecúan su plataforma para absorber los picos".

En estos momentos, lo que se busca es asegurar la continuidad del negocio a través de modelos de teletrabajo así que esa es la prioridad de todas las empresas pero "cuando esta crisis se supere, las organizaciones volverán a recuperar los proyectos en los que estaban inmersas y que tenían como objetivo el ahorro de costes o las migraciones de on-premise a la nube, pero ahora lo que necesitan es mantener lo que ya tienen y facilitar la actividad de empleados y clientes a través de herramientas de colaboración y de virtualización de escritorios. No se están planteando mover nada ni iniciar nuevos proyectos", afirma José Manuel Marina, director general de Crayon.

En los inicios del cloud, la prioridad eran los costes de TI, beneficiarse de las economías de escala, ahorros en infraestructuras, comunicaciones, personal técnico, etc., algo que se sigue teniendo en cuenta con la crisis de Covid-19 pero como señala Marc Canela, product marketing manager en Ekon, "en estos momentos a todos estos ahorros se añade la posibilidad de mejorar la eficiencia en los procesos de negocio. Una pyme de cualquier tamaño puede tener acceso al mismo servicio de cloud que una gran empresa. Las soluciones empresariales de cloud se presentan al mercado cada vez más preconfiguradas, más sectorizadas, más ajustadas, lo que conlleva menos tiempo de implantación, menos tiempo en la incorporación de nuevos procesos, sean comerciales, de producción, etc. lo que reduce considerablemente el time to market de los nuevos productos, frente a soluciones tradicionales".

En general, los proyectos que tienen más demanda por parte de las organizaciones son los que buscan dar conectividad y dotar de continuidad al negocio. Según Galo Montes de HPE "los tres principales son el aumento de la capacidad y el despliegue de líneas de comunicaciones en las casas y en las empresas, junto con acceso seguros VPN. En este último aspecto, HPE está aportando a muchas compañías soluciones de conectividad de Aruba mediante las cuales, con un simple dispositivo enviado al domicilio del usuario, se puede tener acceso inmediato y sencillo, evitando complejidades en la configuración y en el soporte al usuario"

Como segundo gran requerimiento, está dotar



de movilidad a los puestos de usuario. La movilidad es fundamental y los usuarios tienen que acceder a su escritorio independientemente de su ubicación. Montes apunta que "en este sentido hay dos tendencias, proveer de portátiles, opción que no es ágil y aumentaría mucho la complejidad de la gestión para un despliegue rápido; y por otro lado, proveer de puestos de usuarios virtuales (VDI), lo cual vemos mucho más factible. En este aspecto, los proveedores de IT estamos haciendo un gran esfuerzo para suministrar, de forma muy ágil y rápida, VDI a las empresas a través de soluciones fáciles de instalar y en un formato de pago por uso. Finalmente,el tercer proyecto más demandado es permitir la colaboración entre personas. Aquí es fundamental disponer de herramientas que permitan tener reuniones virtuales internas y externas de forma segura y sencilla, hacer eventos de marketing (webinars) y todo tipo de acciones que permitan tener relación con los canales digitales, los cuales se están volviendo más críticos que nunca. En este sentido, es importante contratar o desplegar una o varias plataformas corporativas que aporten toda la comunicación con la seguridad adecuada".

CAMBIO DE PRIORIDADES

Lo que ha sucedido con esta crisis es que las empresas han cambiado sus prioridades. Y lo han hecho de un día para otro, aunque es verdad que muchas de ellas, sobre todo grandes compañías ya se adelantaron y empezaron a implementar medidas hasta dos semanas antes de que el Gobierno declarara el estado de alarma. Esta situación ha provocado que las empresas TIC hayan tenido que ser muy ágiles para ofrecer las soluciones adecuadas ante el parón

de la actividad de sus clientes, algo que han logrado. Como afirma Ricardo Casanovas, CTO de Linke "las empresas han tenido que cambiar de golpe las prioridades y lo han podido hacer aprovechando el potencial de cloud computing, en lo que respecta a su flexibilidad y el modelo de pago por uso. Así, se han priorizado las iniciativas de reducción de costes para adaptar la infraestructura a las nuevas necesidades, con menos cargas de trabajo y algunos procesos prescindibles. Además, cloud ha sido un buen aliado para crear y configurar de forma muy rápida escritorios remotos y redes privadas virtuales (VPNs) que permiten teletrabajar de forma segura, así como sistemas de videoconferencia y call centers virtuales, para atención al cliente. El estado de alarma también está siendo aprovechado para realizar tareas que, en situaciones normales, son más complejas de gestionar o no se acometen por la sobrecarga habitual de trabajo de los equipos de TI, como implementar controles de calidad y cumplimiento, localizar oportunidades de reducir costes, revisar las arquitecturas, agilizar las migraciones o mejorar sistemas esenciales, como los de backup".

En lo que sin duda ha supuesto un cambio total es en la forma de trabajar. Se ha producido la explosión del teletrabajo, admirada fórmula ahora incluso por aquellos partidarios de la permanencia constante en la silla de la oficina. Y ese teletrabajo ha sido posible gracias a soluciones cloud. Como afirma Juan Rodríguez, director general de F5 Networks, "la tecnología de teletrabajo, segura y confiable, ha estado disponible durante años, y la nube ha llevado la escalabilidad, la disponibilidad y la seguridad de estas soluciones a nuevas alturas. Gracias a las tecnologías en la nube, un mundo de aplicaciones basadas en la web, escritorios virtuales, cifrado de punto final, software de conferencia, redes privadas virtuales (VPN) y otras herramientas mejoradas en la nube han hecho posible el trabajo remoto desde casi cualquier dispositivo, en cualquier parte del mundo". Todo sea por que la empresa continúe funcionando y se pueda desarrollar la prioridad única: "La prioridad actualmente es, más allá de hacer frente a aquellos proyectos o inversiones ineludibles por fechas de vencimiento de acuerdos (licenciamientos, renovaciones de mantenimiento, actualización tecnológica, etc.), conseguir el mejor y más eficiente funcionamiento de la empresa en el presente incierto y en el futuro próximo, durante la reactivación paulatina de la economía", afirma Julio Saíz, BDM Infrastructure and Cloud Services de Alhambra IT.

Pero ¿cuándo se producirá esa reactivación? ¿qué sucederá cuando termine esta situación? ¿volveremos a la empresa tradicional y abandonaremos la digitalización? Galo Montes lo tiene muy claro: "Una vez superada la situación inicial de urgencia, cuando podamos volver a la nueva normalidad, las empresas se replantearán seriamente digitalizar todos sus procesos y reformular cualquiera que no pueda acometerse en un entorno digital y remoto. Se producirá una redefinición muy seria de cómo se relacionan las personas, las empresas y las instituciones, produciéndose un boom en la transformación digital. En este proceso veremos como la implantación de la firma electrónica se generalizará, el dinero efectivo disminuirá espectacularmente, desaparecerá en gran medida el papel como elemento de almacenamiento y transmisión de información y se integrarán aplicaciones para lograr la mayor automatización posible. Como consecuencia de todo ello, se prevé que al final de 2020 y durante el año

2021 tengamos una expansión importante del mercado de TI. La demanda de especialistas que ayude a esa transformación digital será importante, así como los sistemas de computación, almacenamiento y seguridad".
El portavoz de Dell Technologies también lo tiene claro y pone un ejemplo de un sector que también se encuentra al alza en estos momentos: el de los supermercados. En su opinión, "muchos de ellos contaban con plataformas de comercio electrónico que aunque desfasadas les permitía ir tirando. Acumulaban mucha deuda técnica, porque el mundo del retail es un mundo complejo: compras, logística, inventario, operaciones, productos perecederos… En un breve plazo de tiempo estas aplicaciones han multiplicado muchas veces el tráfico medio que recibían, lo que ha hecho que muchos potenciales compradores desesperados por la espera se vayan a comprar a otro sitio. ¿Qué pensará el CEO de esto? No me gustaría estar en los zapatos de ese CIO. La deuda técnica cuesta dinero, siempre, pero ahora es mucho más patente. Todos los proyectos que tengan que ver con cómo se relacionan las organizaciones con sus clientes o usuarios, pasan a ser prioritarios. Igualmente pasa con proyectos relacionados con el tele-trabajo, con la salud, etc.".

QUÉ ENTORNO CLOUD

Está claro que ahora mismo el entorno que tiene más éxito entre las empresas es el híbrido, pero también Covid-19 va a hacer que esto cambie y las organizaciones empiecen a apostar por modelos de cloud abiertos, sobre todo en lo que se refiere a las pequeñas y medianas empresas. Una vez que, debido a la situación de confinamiento actual, han empezado a probar soluciones y servicios de nube abierta, va a ser difícil que cuando la crisis acabe lo dejen. En este sentido, José Manuel Marina, director general de Crayon "en estos momentos lo normal es que las empresas se estén moviendo en la cloud híbrida, ya que aún necesitan mantener la inversión que realizaron en su momento en tecnologías on-premises. La cloud híbrida les da la posibilidad de poder seguir manteniendo conocimiento y recursos en entornos tradicionales al tiempo que pueden ir abriendo nuevos proyectos en la nube. Además, esto les permite también ir adaptándose al entorno cloud de una forma no disruptiva pero lo público irá ganando más peso de forma progresiva. Lo privado tiene sentido mientras dura el proceso de amortización de la inversión tecnológica realizada, pero cuando esta inversión ya está amortizada y la empresa tiene que volver a plantearse una nueva adquisición para poder seguir proporcionando unos servicios, lo lógico es que se imponga la opción de la cloud pública, ya que proporciona modelos de pago por uso que evitan el desembolso de grandes inversiones en proyectos concretos y que permite un control de costes mucho más eficiente".
Las ventajas que proporcionan las soluciones en la nube son beneficios para los usuarios finales, clientes o empresas, independientemente del tamaño de la empresa o filial. Como ya no es una tendencia sino un hecho real y Covid-19 lo ha aumentado muchas empresas empezarán a apostar por la nube pública, aunque como asegura vicepresidente de producto y nuevos negocios de NFON
"la apuesta por lo público dependerá del tipo de servicio y el tamaño de las empresas. Los servicios específicos, como los de comunicación por voz, video, pantalla compartida y chat, se pueden proporcionar con la mejor experiencia de usuario fuera de la nube, generalmente en una plataforma pública multitenant. Las nubes híbridas tienen sus propios beneficios, como el nivel de personalización y requisitos de seguridad más específicos a cambio de un coste más elevado. En cuanto a las pequeñas y medianas empresas, creemos que las plataformas públicas multitenant serán predominantes y el modelo de elección en el futuro".
Y, ¿qué ocurre con multicloud? Según Jaime Balañá, director técnico de NetApp, "el escenario multicloud es fruto de las mismas necesidades de gestión de los datos de algunas compañías y sectores de actividad, sumado a la completa oferta de los proveedores de servicio local y a los diferentes hyperescalares, así como es una clara muestra que el mercado español está migrando a la nube y cada vez es más consciente con qué tipo de nube y con quién quiere hacerlo. Y es que la principal diferencia entre la nube híbrida y la nube múltiple es que la estrategia híbrida es una estrategia de implementación utilizada para realizar una única tarea. Los datos pueden entremezclarse entre su nube local y la nube pública, pero permanece con la misma carga de trabajo. Una estrategia de varias nubes, por otro lado, es una estrategia de gestión de la nube que utiliza varios proveedores o hyperescalares para realizar más de una tarea, tal vez dentro del mismo departamento o como una colaboración entre diferentes departamentos".
Lo cierto es que a medida que surgen más opciones de plataformas en la nube para diferentes usos, el 85% de las em-

presas comienzan a adoptar estrategias multicloud (RightScale 2019 State of the Cloud Report), como parte de su enfoque de transformación digital. Cualquiera de las grandes plataformas cloud tiene diferentes servicios para la gestión de los datos. En este sentido, el director general de Interxion afirma que "las empresas buscan las aplicaciones y recursos que mejor se adapten a su negocio. La adopción de una estrategia multicloud facilita elegir entre diferentes proveedores el servicio más adecuado y la mejor solución para cada caso. La gran variedad de recursos cloud públicos y privados disponibles en la actualidad es una oportunidad para encontrar servicios que se adapten a necesidades muy específicas". Javier Corella, director de marketing de IECISA cree que "el escenario multicloud llega como consecuencia de que se selecciona a los proveedores de cloud según la solución presentada en cada necesidad de negocio. No es necesario casarse con una sola nube, ya que, una vez que migramos, el cliente busca lo mejor de cada proveedor. De todas formas, multicloud tiene múltiples ventajas, pero también presenta retos a resolver como son los aspectos relacionados con el gobierno y gestión, la gestión de los costes, la seguridad y la monitorización. La gestión de costes es uno de los procesos más complejos en entornos multicloud.

> Las soluciones multicloud vienen para quedarse pero no como las conocemos ahora

La razón se debe a que cada proveedor cloud tiene una forma de facturar y gestionar costes. En el caso de grandes empresas, pueden encontrar dificultades a la hora de repercutir el coste de cada servicio cloud a los diferentes departamentos o empresas dentro de las grandes empresas".

Las soluciones multicloud vienen para quedarse, pero no tal cual las conocemos actualmente. Tener todo en un solo Cloud no es efectivo ni recomendable, pero por otro lado disponer de varios entornos cloud tan distintos en su gestión y administración hace que se complique mucho el IT en general. Para Galo Montes de HPE, "la solución definitiva es el Cloudless computing. Este concepto significa que nuestras cargas de trabajo deben de poder correr, ser gestionadas y operadas de forma similar independientemente de donde estén localizadas. Un usuario o desarrollador necesita transparencia para ver si las cargas están on-premise o en la nube; el responsable de IT elegirá el mejor entorno para cada una de ellas. Para que esto pueda ser una realidad, se exigirá una automatización importante del ciclo de vida de las aplicaciones y también disponer de herramientas que provean de un entorno único de ges-

tión. En este aspecto vemos que empiezan a surgir una gran cantidad de iniciativas. Desde los fabricantes de hardware tradicionales que están haciendo un gran esfuerzo cloudificando los entornos de data center on-premise con soluciones de pago por uso, componibilidad, hiperconvergencia e inteligencia artificial, hasta que las Cloud tendrán que estandarizar en gran medida sus APIs" .

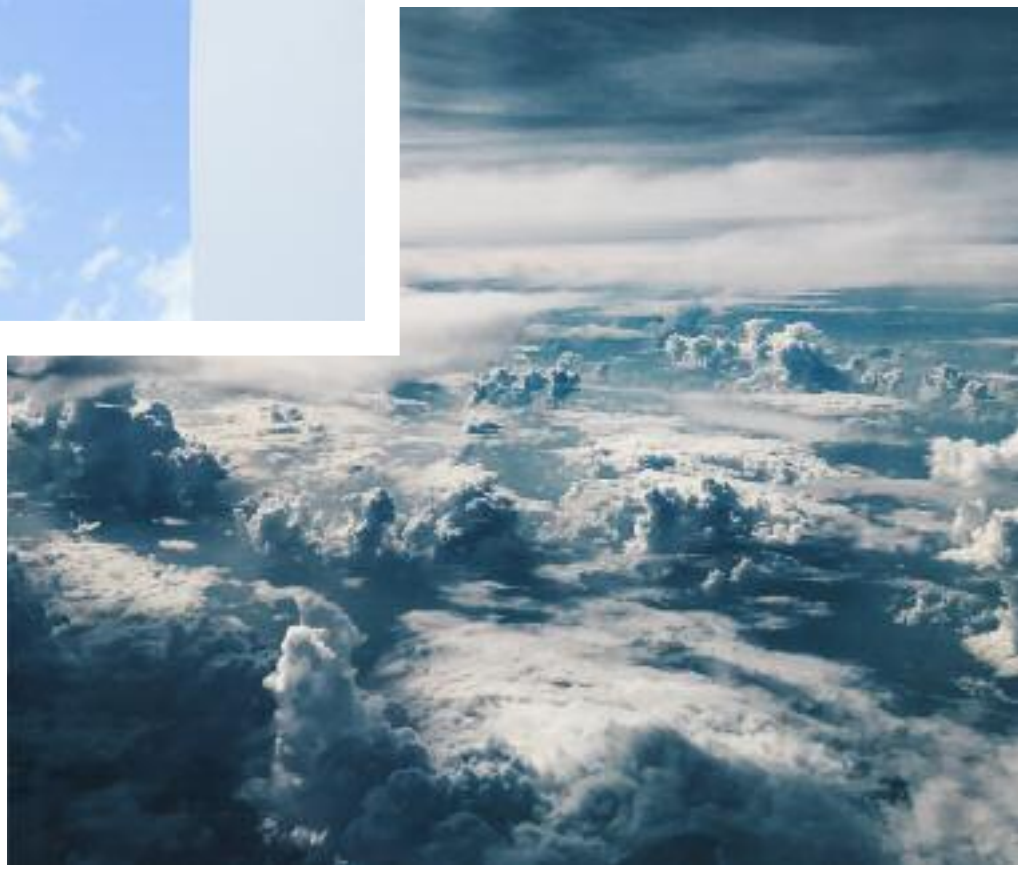
TRABAJAR EN MULTICLOUD

El único problema es que en estos momentos muchas organizaciones no saben trabajar en un entorno multicloud. Cuando una empresa considera que necesita ir a un entorno multicloud, lo lógico es que estudie los requerimientos y recursos necesarios, y que se preocupe de hacer un diseño de arquitectura que cubra sus necesidades en términos de rendimiento, flexibilidad, seguridad, cumplimiento normativo, etc. Esto se tiene que contemplar en cualquier despliegue de infraestructura cloud, pero la cuestión que puede ser más compleja es la gestión, el gobierno TI y la orquestación, y a ello tiene que dedicar tiempo para luego no tener problemas. En este aspecto, el CTO de Linke afirma que "lo más co-

> La seguridad en los entornos cloud debe ser compartida entre proveedor y cliente

mún hoy en día en las estrategias multicloud de las empresas es el reparto de las cargas de trabajo entre diferentes proveedores. A modo de ejemplo, podemos encontrar empresas que deciden trabajar con las herramientas de productividad cloud de Microsoft, utilizan Google Cloud para sus aplicaciones basadas en contenedores y hospedan cargas de trabajo como SAP en AWS. Estas estrategias intentan usar lo mejor de cada proveedor y aislar cada carga de trabajo en uno solo de ellos. En contraposición, este modelo implica un mayor esfuerzo de gestión de múltiples proveedores, que para grandes empresas puede ser beneficioso a la hora de negociar condiciones ventajosas".

Lo cierto es que ahora mismo multicloud no tiene porqué ser lo necesario para todas las empresas. Cada compañía tienes sus necesidades y casuísticas que hace que requieran de una solución de medida. Pero como afirma el portavoz de Econocom Nexica "en un futuro no muy lejano, las infraestructuras multicloud se van a estandarizar porque recogen lo mejor de cada uno de los clouds públicos y privados, tanto a nivel económico, de disponibilidad, seguridad y en definitiva para alojar las aplicaciones del cliente al entorno que más convenga según los criterios establecidos. Estamos en una etapa temprana de adopción del verdadero multicloud, por lo que en este escenario nos encontramos



que hay algo de desconocimiento en no solo qué es realmente multicloud, sino cómo operarlo eficientemente. Inexorablemente esta pared irá cayendo a medida que los clientes vean madurez en el servicio y partners especializados que ayuden a diseñar una arquitectura acorde a las necesidades presupuestarias, de negocio y seguridad que requieren".

Y además está la elección del proveedor. Muchas empresas se quejan de que al contratar cualquier tipo de servicio o herramienta a través de cloud, no se cumplen con las expectativasgeneradas. Por eso multicloud ofrece la ventaja de la flexibilidad que es clave a la hora de ver qué nube en el entorno multicloud es la que mejor se adapta a la carga de trabajo. Es importante asegurarse de que el marco esté alineado con los objetivos técnicos en términos de alojamiento de aplicaciones, ya sea alojando máquinas virtuales, ejecutando plataformas de contenedores escalables o explotando las ofertas de PaaS de la nube pública, etc. En este sentido desde Pure Storage creen que "es importante considerar detenidamente cómo se integra la nube local en la arquitectura multicloud. Si se intenta integrar un entorno de TI tradicional con la nube pública para crear una nube múltiple, se corre el riesgo de simplificar todo el entorno hasta el mínimo común denominador. Los beneficios de la nube se basan en la flexibilidad y la agilidad; la automatización completa es clave para lograr esto y esa automatización debe aplicarse a todos los componentes dentro del multicloud. Es importante asegurar que los entornos de nubes públicas y en las instalaciones estén completamente automatizados a través de las API subyacentes en todo el entorno. No poder equilibrar varias soluciones de varios proveedores, puede provocar problemas de compatibilidad de las soluciones y de superposición de tecnologías, lo que se traduce en costes innecesarios para las empresas. Es por ello que un conjunto de API comunes para ofrecer los servicios de datos con independencia del proveedor de nube pública es fundamental para evitar situaciones de ´vendor lock-in´que compromentan la libertad de elección".

SEGURIDAD

Como decíamos al comienzo de este reportaje, la seguridad es uno de los apartados que más importancia está cobrando desde que apareció el coronavirus en nuestras vidas. Las empresas han montado su entorno laboral en las casas de los empleados y lo han hecho sin adoptar todas las medidas de seguridad necesarias. Una vez que se han establecido en este nuevo entorno laboral, la situación está cambiando, hasta tal punto que se puede decir que ahora mismo la protección frente a ciberataques es una prioridad. Las dudas en cuanto a la seguridad de la nube ya venían disipándose. Sin embargo, al aumentar el consumo de aplicaciones y servicios en la nube, la mayoría de las empresas ya han asumido de forma definitiva que los entornos cloud son más que seguros. Como afirma el portavoz de Linke, "cloud es mucho más fiable y seguro que la mayoría de las infraestructuras existentes onpremise o gestionadas por un tercero en modelo de cloud privada. Tanto AWS Microsoft o Google ofrecen servicios y funcionalidades asociadas a la seguridad y fiabilidad de las aplicaciones que hasta hoy solo estaban al alcance de unos pocos y requerían grandes inversiones para implantarse. Ha sido un democratizador de las tecnológicas asociadas a la privacidad, seguridad y fiabilidad de las aplicaciones y los datos que procesan".

De todas formas, Marc Granados de Econocom Nexica cree que "hay que distinguir dos escenarios: si se busca un proveedor de cloud exclusivamente, es cierto que la seguridad corre a partes iguales entre el cloud provider y la empresa, securizando infraestructuras core y aplicaciones respectivamente. Por el contrario, si una empresa contrata el cloud y los servicios gestionados al mismo proveedor incluyendo aspectos relacionados con la seguridad, el cliente debería quedar cubierto en este aspecto. En cuanto a si es fiable la nube, solo digo que los cloud provider como Econocom Nexica invertimos constantemente en formación y herramientas de seguridad para la propia infraestructura de servicio, mientras que la mayoría de empresas no se puede permitir por su coste. Ese es precisamente nuestro valor y lo que aprecian nuestros clientes".

Como las empresas se han visto obligadas a migrar al cloud la nube ha experimentado un crecimiento pero también es cierto que las dudas, sobre todos entre los acérrimos del modo onpremise, acerca de la seguridad se mantienen. Para Javier Corella, "el problema está en un símil que en IECISA utilizamos normalmente con clientes. Los grandes proveedores de nube pública son cajas fuertes. Pero las aplicaciones son la puerta a esa caja fuerte, ya que la gente entra a tu organización a través de esas aplicaciones. El problema está en dejar abierta la puerta en la aplicación. Es importante, por tanto, concienciar a las organizaciones de que se trata de un modelo de "seguridad compartida" en el que el proveedor se hace responsable del entorno, los sistemas y la disponibilidad. Pero hay otra parte, la seguridad de las aplicaciones y los datos, que es responsabilidad del cliente, no del proveedor; es tarea del cliente securizar sus propias aplicaciones, y securizar las infraestructuras o servicios que utiliza".

Finalmente, el portavoz de Ekon cree que "existen diferentes calidades, y los proveedores de cloud son claros candidatos a recibir ataques por su efecto de difusión pública y la notoriedad que pueda incrementar la publicidad del grupo de hackers, pero la nube correctamente dimensionada no reviste dificultades y pueden asegurar la protección y privacidad de los datos".

Límites en el uso militar de la tecnología

El ser humano es capaz de lo mejor y de lo peor. Así, la tecnología, como creación humana, es susceptible de ser usada para infinidad de aplicaciones que mejoran la vida de las personas, pero también puede ser empleada para otros fines. Uno de los que genera más polémica es su aplicación para usos militares. A su favor se argumenta que el uso de la tecnología ha facilitado que las guerras sean más precisas y, por tanto, con menos daños colaterales, y que en el futuro, en lugar de enviar seres humanos a batallar, los ejércitos serán de robots, al modo de los clones de Star Wars.

Sin entrar en esta polémica, lo cierto es que gracias a la inversión en gastos militares (muy superior a la realizada en investigación científica), se han producido grandes inventos como Internet, el microondas o los drones, que más tarde han pasado a ser de uso generalizado por la sociedad civil. Pero, ante la imparable generalización de la inteligencia artificial (IA), ¿hasta qué punto podrá ser utilizada con fines militares? ¿Habrá un momento en el que será un algoritmo el que dedica cuál debe ser un objetivo y, en consecuencia, que deben perder la vida los seres humanos que allí se encuentren?

En el caso de los drones, su uso para fines bélicos hace tiempo que es una realidad. La primera ocasión de la que se tiene noticia que se usaran con objetivos militares, fue en una misión norteamericana en Pakistán el 23 de enero de 2009; y la más reciente ha sido el un ataque con drones en el aeropuerto de Bagdad (Irán) realizado por Estados Unidos el pasado 3 de enero de 2020, que tuvo como resultado la muerte del general iraní Qasem Soleimani.

Respecto a los robots, hace décadas que la empresa Boston Dynamics, asentada en Massachusetts (Estados

Unidos), que cuenta con financiación de DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa de Estados Unidos) desde 2003, fabrica robots que imitan la forma, movimientos y características de animales y del ser humano, como "Big Dog" o "Spot Mini", que tienen la apariencia de un perro; "LS3", una mula robótica con una autonomía de 24 horas y capaz de cargar 180 kilos; así como "Petman" o "Atlas", humanoides capaces de correr y acceder a lugares imposibles para una persona.

También existen los insectos robóticos, como "RoboFly", un mini dron dotado de un micro controlador y que no necesita batería, al contar con una célula fotovoltaica que convierte la energía lumínica en electricidad, alimentándose por un rayo láser invisible, que fue presentado en 2018 por la Universidad de Washington (Estados Unidos) en la Conferencia Internacional sobre Robótica y Automatización de Brisbane (Australia); o como el minirobot "RobobeeX-Wind", presentado en 2019 por la Universidad de Harvard, de 250 miligramos y 3,4 centímetros, dotado de foto receptores que canalizan la energía hacia sus alas como hacen las abejas.

Además, la resistencia de estos artefactos puede ser considerable, como la de "DEAnsect", un insecto robótico de un gramo de peso, inalámbrico y autónomo, diseñado por la Escuela Politécnica Federal de Lausana (Suiza) en 2019, que alcanza los tres centímetros por segundo gracias a músculos artificiales y que es capaz de sobrevivir al impacto de un matamoscas.

USO MILITAR Y ORDENAMIENTO JURÍDICO

El potencial militar de estas tecnologías es innegable, ya que en estos dispositivos sería relativamente sencillo instalar sistemas de video o escucha, geolocalizadores o micro armas. Pero ahí no acaba la cosa, también se están desarrollando prototipos de robots de tamaño microscópico (nanobots), que podrían ser inyectados dentro del cuerpo de un animal o, incluso, un ser humano, como en la película "Un viaje alucinante" de 1966: Lo que entonces parecía ciencia-ficción, hoy ya estaría más cerca de la realidad. Esto tendría utilidades fantásticas en la curación de enfermedades, pero también podría usarse con fines bélicos. Así las cosas, el pasado mes de diciembre de 2019, se dio a conocer que el Departamento de Defensa (DOD) de Estados Unidos pretende disponer en 2050 de un ejército de cyborgs de combate, equipados con visión y capacidad auditiva aumentadas, trajes capaces de mejorar el rendimiento físico y el estado muscular durante el combate y comunicación telepática en tiempo real de órdenes de los mandos, posición del enemigo, etc. Aunque por el momento solo se trata de una aspiración plasmada en un informe llamado «Soldado Cyborg 2050: La fusión entre Humano/Máquina. Fusión y las implicaciones del futuro del DOD", tarde o temprano estos "supersoldados" acabarán convirtiéndose en una realidad.

Pero, ¿cómo encajan todos estos avances en el ordenamiento jurídico español? La Exposición de motivos de la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, promulgada a partir de la habilitación normativa conferida por el artículo 8 de nuestra Constitución prevé expresamente que "debemos tener en cuenta la revolución tecnológica de las últimas décadas, algunas de cuyas innovaciones proceden del propio entorno de la Defensa o bien han encontrado aplicación en el mismo", y el artículo 2-2-n) del Real Decreto 1399/2018, de 23 de noviembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, que desarrolla dicha norma, dispone que la Dirección de Comunicación Institucional de la Defensa es la encargada de analizar la legislación vigente para la incorporación de nuevas tecnologías al Ministerio de Defensa.

En consecuencia, la incorporación a las Fuerzas Armadas de los desarrollos tecnológicos gozaría de cobertura legislativa, en la medida que contribuyan a cumplir el mandato marcado por el citado precepto constitucional para garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional; y se cumpla la finalidad de la Política de Defensa (artículo 2 de la Ley Orgánica 5/2005): protección del conjunto de la sociedad española, de su Constitución, de los valores superiores, principios e instituciones que en ésta se consagran, del Estado social y democrático de derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial de España, así como contribuir a la preservación de la paz y seguridad internacionales, en el marco de los compromisos contraídos por España.

Javier López. Écija Abogados

"La gente no está concienciada de la importancia de la seguridad"

¿A qué se dedica la parte principal del presupuesto de TI de la empresa?
A los servicios de mantenimiento de aplicaciones. Gracias a ellos las aplicaciones están actualizadas, algo imprescindible para la operativa diaria.

¿En qué área se está invirtiendo más este año?
En movilidad y digitalización. La información debe fluir rápido y centralizarse para la toma de decisiones lo antes posible. Suena bonito pero digitalizar el mundo que antes no lo era es complejo.

¿Qué proyecto es del que está más satisfecho?
Recuerdo un proyecto de migración a la nube, luchando contra barreras culturales, formas de entender el trabajo y demás. Fueron un par de meses convenciendo a escépticos, y transfiriendo años de históricos a la nube.

Si le pusieran todos los beneficios de la empresa a cargo del departamento de TI,

¿qué le gustaría implementar?
Me encantaría usar Bigdata para la toma de decisiones, creo que los resultados serían sorprendentes, aunque lo bueno sale caro, y ahora es muy difícil de vender y sobre todo de explicar.

¿La seguridad es un problema?
Sí sin lugar a dudas, y lo peor es que la gente no está en absoluto concienciada con ello. Yo como hacker ético conozco maneras muy sencillas de entrar en algunos sistemas de manera invisible y permanecer allí sin levantar sospechas, quizás meses o años si el administrador es perezoso. Hay personas que dicen que a ellos no les ha pasado nunca nada, yo les digo, ¿y como está tan seguro de que no tiene el intruso dentro ya?.Los insiders o personal malicioso dentro de la organización pueden también hacer muchísimo daño, los trabajadores a veces solicitan acceso a más información de la que realmente necesitan, hay que valorar esto con mucho cuidado. En una organización el personal tiene que saber que son la parte más vulnerable en temas de ciberseguridad, tienen que saberlo y concienciarse para mitigarlo.
No recuerdo salir de ningún congreso de Ciberseguridad menos preocupado que a la entrada. Normalmente es todo lo contrario.

¿Qué tendencias principales observa en el mundo TIC?
Para mí son cuatro muy importantes, Inteligencia Artificial, Big Data, Ciberseguridad e IoT que está despegando con la conectividad a alta velocidad. También diría que la primera acabará estando muy presente en las otras tres por ser multifacética.

Bajo ningún concepto en su móvil puede faltar…
Ahora mismo Whatsapp, TeamViewer, Google authenticator, Google drive y Gmail. Con esto estoy conectado al mundo.

¿Cuál es la herramienta que realmente le cambió la vida?
La herramienta de conexión remota cuando se perfeccionó, me ahorró infinidad de desplazamientos, incluso de avión, me permitió irme de vacaciones tranquilo y/o llegar a casa antes, trabajar desde otra provincia u otro país, estar sin estar, un cambio radical sin duda.

¿Harto de solucionar los problemas tecnológicos de la familia y amigos? ¿Qué le suelen pedir?
Hace tiempo que me niego, uno es bueno pero no tonto.

¿Qué es eso de la transformación digital? ¿Slogan o necesidad?
La tecnología es tan beneficiosa, que se implantará sin pedirnos permiso, no es una opción, o te subes al tren o te quedas fuera.

¿La movilidad urbana pasa por la electricidad?
Sí, creo que no se requiere la potencia de los combustibles fósiles para desplazamientos urbanos, esta es otra transformación que se mira con un poco de escepticismo o incluso con miedo por una parte de la industria.

Fernando García Domínguez

CTO y CISO en Grupo Manserco

Fecha de nacimiento: 16/09/1973
Estado civil: casado
Hijos: dos
Deportes que practica: Pilates
Hobbies: Fotografía
Estudios: Ingeniero Superior en Informática, Director de Seguridad privada, Offensive Security Certified Professional.
Personas a su cargo: 3
Antigüedad en la empresa: 14 años
Trabajos anteriores: Analista programador junior/senior, Administrador de sistemas

Aprovechar Covid-19 para implantar una cultura del cambio

Completamente inmersos en la crisis del coronavirus, las PYMEs han tenido que acelerar sus planes de transformación digital para poder seguir operando en remoto y en un escenario de cambios constantes. Veamos en qué les ha pillado el toro a las empresas y cómo pueden aprender de la situación para no cometer los mismos errores en el futuro.

Desconfiar del teletrabajo

La diferencia más visible durante esta crisis ha sido quién tenía los deberes hechos con las políticas de teletrabajo: mientras unas empresas llevaban días teletrabajando en remoto al 100%, otras seguían esperando a recibir los portátiles para poder mandar a la gente a casa. No obstante, una cosa es poder seguir trabajando en remoto y otra muy distinta es hacerlo de manera productiva, sin que afecte al rendimiento de los equipos y de manera sostenida en el tiempo.

Para esto es fundamental que el teletrabajo vaya acompañado de un cambio cultural que permita a la empresa mantener su identidad y sus valores en un escenario de trabajo en remoto. Desconfiar de los empleados e intentar mantener políticas y prácticas presencialistas (horarios cerrados o ausencia de flexibilidad por citar algunas) sólo dificultarán el éxito del cambio.

FALTA DE PROCESOS

Más allá del teletrabajo, uno de los puntos clave de la transformación digital en esta crisis es la falta de procesos claros y definidos. Adaptar un proceso ya existente a un escenario de trabajo en remoto y 100% digital sobre la marcha ya es complejo de por sí, pero si ni siquiera existe ese proceso de antemano, la tarea se vuelve titánica. En estos días hemos visto cómo algunos de nuestros clientes más avanzados en sus procesos de transformación digital modificaban toda su operativa en dos semanas para adaptarla a la crisis, para volver a tener que modificarla de nuevo al cabo de otros quince días. Sin una base sólida, abordar ese cambio es directamente imposible.

EQUIPOS Y SISTEMAS

Afirmar que para teletrabajar se necesita un equipo portátil parece evidente, pero de nuevo hay que evitar caer en lo inmediato. Para teletrabajar un día necesito un portátil, pero para teletrabajar un mes en condiciones necesitaré mis dos pantallas, mi tableta, mi elevador de escritorio... Por otro lado, los sistemas de muchas empresas que aún confían en las soluciones on premise (servidores físicos) pueden ser un terrible cuello de botella, ya que requieren estar físicamente en la oficina para conectarse al servidor o sistemas centralizados. Muchas empresas han tenido que poner en marcha VPNs a la carrera para poder teletrabajar, y esto no es un producto que se pueda adquirir en grandes superficies como un ordenador portátil.

MODELOS DE NEGOCIO PRESENCIALES

Probablemente una de las mayores limitaciones para muchas PYMEs a la hora de acelerar su transformación digital de urgencia ha estado en su mismo modelo de negocio. ¿Cómo se vuelve remoto un negocio de atención al público? Una conocida panadería madrileña ha comenzado estos días a vender por teléfono, repartir a domicilio y cobrar por Bizum. ¿Entraría esta opción en sus planes hace dos meses? Otros modelos, como los servicios asistenciales o el outsourcing, tienen difícil solución en este contexto. Los centros de enseñanza y forma-

ción -oficial y no oficial- han corrido a implantar soluciones de videoconferencia, y está por ver cómo afecta este cambio a su modelo de negocio en el futuro una vez pase la crisis. ¿Seguirá yendo la gente a aprender inglés a las academias? ¿Es relevante esa pregunta en un momento en que está en juego la propia supervivencia de la academia?

CULTURA DE LO PRESENCIAL

De nuevo, una de las mayores barreras a la transformación digital en muchas empresas es un problema cultural y de costumbre. Digitalizar un proceso manual o que se lleva haciendo en papel muchos años es un esfuerzo que puede haberse ido despriorizando o no haber entrado nunca en los planes, porque "lo hemos hecho así toda la vida" o "ya habrá tiempo para cambiarlo". El trabajo remoto, flexible o por objetivos está radicalmente reñido con la cultura de estar en la oficina de 9 a 19, y más todavía con la desconfianza hacia los empleados y modelos muy paternalistas de dirección.

En definitiva, la transformación digital es un proceso que requiere un cambio tanto de cultura y actitud corporativas como de operativas, procesos y compras. Las empresas que han tenido que arrancar a la carrera sus ciclos de transformación digital por la crisis del coronavirus se encuentran en una posición inmejorable para dar continuidad al proceso: se han tenido que subir al tren en marcha, pero está en su mano aprovechar el viaje y hacerlo suyo. En un escenario de incertidumbre respecto a qué nos espera a la vuelta de la crisis, sólo podemos recomendar a las PYMEs que no abandonen este cambio; en su lugar, es mejor convertirlo en cultura.

Jaime Serrano,
COO y Cofundador de Cloud District,

Seguridad continua de aplicaciones para DevOps

Aquellas organizaciones que buscan alcanzar un mayor ritmo de innovación han de ir más allá de los recursos tradicionales, que limitan la colaboración interdepartamental y la automatización; coordinar sus procesos de seguridad y DevOps brinda una ocasión excepcional para potenciarla.

Los procesos que detectan y resuelven las vulnerabilidades de seguridad deben ir de la mano de los ágiles procesos DevOps que crean y producen el software. Contar con un proceso de seguridad de aplicaciones que funcione correctamente en un entorno DevOps resulta complicado si ambos procesos y recursos no están coordinados.

Las funciones DevOps se han centrado sobre todo en la automatización para generar flujos de trabajo continuos que mejoren la unidad de innovación de las empresas o la dinámica de las productoras de software. Como consecuencia de ello, son muchas las start-ups y proveedores consolidados que han sacado nuevos productos para dar respuesta a esta necesidad. El problema es que estas nuevas herramientas se centran en segmentos concretos del flujo de trabajo, como el registro de incidencias, el seguimiento o la integración continua. Por su parte, esta fragmentación requiere a su vez una gran cantidad de API e interfaces que conecten los diversos segmentos en una cadena de herramientas DevOps que sirva al ciclo vital de desarrollo de software (SDLC) de extremo a extremo.

La integración de estas nuevas herramientas de seguridad en una cadena de herramientas DevOps, ya compleja en sí misma, conlleva una maraña de interfaces de usuario y núcleos de flujo de trabajo, además de la desconexión de los datos. Por otro lado, el planteamiento comercial de las empresas de seguridad ha exagerado la cuestión de la complejidad y muchas han creado su cartera mediante adquisiciones y siguen vendiendo estas nuevas tecnologías de manera individual o como productos de panel. El resultado es una cantidad ingente de productos de seguridad distintos que todavía no ha alcanzado su potencial para mejorar la eficacia de los programas de seguridad DevOps. Los clientes que están sometidos a una gran presión para ofrecer innovación a mayor velocidad precisan una alternativa práctica a la gestión de una web de seguridad y herramientas DevOps. Sin embargo, ¿está la disciplina de seguridad en condiciones de adoptar de manera realista un enfoque iterativo similar al proceso de desarrollo?

PRUEBAS

Esta alineación exige la realización de pruebas de seguridad de aplicaciones, bautizadas como DevSecOps, que se pueden incorporar al proceso de trabajo de los desarrolladores y en la integración continua. Con este planteamiento, los análisis de seguridad se automatizan con cada remisión de código, lo que permite evaluar todos y cada uno de los cambios en el código para comprobar que no presenten vulnerabilidades. Se evalúa cada cambio individualmente y se ofrecen los resultados al desarrollador dentro de los flujos de trabajo existentes, en lugar de esperar a una prueba de seguridad conjunta al final. Esto permite a los desarrolladores ver los efectos de sus modificaciones sin verse obstaculizados por las vulnerabilidades introducidas por otros colegas.

Este análisis de seguridad, claro e iterativo, propicia además un mejor uso de los recursos de equipo. El desarrollador puede resolver rápidamente muchas vulnerabilidades, mientras que el equipo de seguridad puede centrarse en las excepciones que no tienen una solución sencilla. Es posible que los profesionales de seguridad para aplicaciones no vean nunca muchas vulnerabilidades, o que tengan que dar prioridad a unas sobre otras porque es el desarrollador el encargado de detectarlas y resolverlas.

Al descomponer los «núcleos» de recursos, se da lugar a una colaboración interdepartamental entre las divisiones de desarrollo y seguridad en la que cada una de ellas estudia los datos en el contexto adecuado. Las correcciones de seguridad y de errores alcan-

zan la paridad, puesto que ya no se ven dificultadas por la fragmentación de los sistemas.

Las ventajas de este planteamiento son trascendentales:

- El análisis de seguridad de aplicaciones se vuelve iterativo, paralelo al desarrollo
- Las vulnerabilidades quedan claras en el momento de su introducción.
- La responsabilidad también es clara: quién creó la vulnerabilidad y dónde, así como la causa y el efecto
- Los desarrolladores pueden resolver las vulnerabilidades con menos reelaboración y sin cambiar de contexto
- La automatización puede resolver los errores sustituyendo las bibliotecas de código con parches más seguros mientras el desarrollador todavía tiene el código en su poder.
- Reducción del seguimiento y selección, con una mejora de la productividad para los desarrolladores y para la seguridad.

Mejorar la eficiencia es una forma eficaz de que un programa de seguridad de aplicaciones crezca y evalúe más aplicaciones en la cartera DevOps. Para lograr estos cambios es necesario que el equipo de desarrolladores cuente con personas y procesos adecuados, mientras que una herramienta que permite nuevos procesos de seguridad constituye un punto de partida muy práctico.

Una aplicación única para todo el ciclo vital DevOps es una manera de ofrecer pruebas de seguridad para aplicaciones incorporadas al proceso de integración continua. Con este nuevo enfoque, los programas de pruebas de seguridad de aplicaciones solucionan las vulnerabilidades durante el desarrollo, en vez de detectar todas las vulnerabilidades antes de la producción. Los procesos de análisis que son capaces de detectar cualquier problema pueden descubrir miles de vulnerabilidades, lo que puede dar lugar a cuestiones como que el equipo de seguridad tenga que decidir qué resolver primero, o la desmotivación del equipo de desarrollo al constatar todo el trabajo que tendrá que volver a realizar.

Cindy Blake,
CISSP, evangelista de seguridad en GitLab

Dev(QA)Ops: decálogo para la eficiencia en entregas de software

DevOps es una visión avanzada de los principios de desarrollo y entrega de software con eficiencia. Una visión que implica a profesionales capaces de cocrear software con mentalidad ágil y un alto grado de organización técnica para disponer de un entorno de trabajo eficiente. Todo ello, al mismo tiempo, tiene como objetivo que el software entregado asegure los niveles óptimos de calidad desde una perspectiva global, donde calidad significa todo aquello que debe prevenir los defectos y potenciar la excelencia en el momento de la entrega, desde las diferentes perspectivas de un usuario.

En DevOps, la calidad de software es, por tanto, un principio fundamental, que debe ser transversal y continuo durante todo el proceso de entrega del software, de principo a fin. Por ello, las actividades de aseguramiento de calidad (QA) como el testing adoptan una destacable diversidad de formas (funcional, de rendimiento, de seguridad, de carga, de usabilidad…) y se abordan en distintos niveles (tests unitarios, tests de integración, tests end-to-end…). Este es también el motivo por el que debe hacerse hincapié en una metodología Dev(QA)Ops, con un cometido principal: lograr entregas rápidas con un alto nivel de calidad. Para entender mejor Dev(QA)Ops y sacar el máximo partido de esta práctica, debemos tener en cuenta el decálogo de principios que lo imbuyen de sentido y utilidad.

1. En DevOps se requiere liderazgo (con foco en los procesos, personas y tecnología) y gobernanza. Las nuevas contribuciones de software necesitan ser gestionadas con sentido a través de flujos orquestados con la mayor automatización posible y que comprueben de forma sistemática que los umbrales de calidad son capaces de detectar los posibles defectos en cada potencial foco de generación de estos, para así impulsar el progreso de las versiones candidatas de software hacia su puesta en producción.

2. El sentido de equipo y los valores asociados son críticos. Por eso, en DevOps es necesario cultivar y adoptar una mentalidad ágil, con una visión única y compartida dirigida a cogenerar valor.

3. Las contribuciones de software deben fluir desde el código hasta su puesta en producción mediante una pipeline que coordine, para cada nueva entrega, una secuencia de acciones y validaciones contínuas de calidad a través de quality gates con dosis de automatización. Cuando a través de este flujo se valida que existe un nivel de calidad suficiente, se asegura un despliegue en cada entorno de acuerdo con el riesgo asumible y definido en los quality gates. Como proceso tecnológico, el pipeline debe sustentarse en herramientas que impulsen la optimización de procesos para una entrega continua más fluida.

4. El desarrollo de software es un proceso de creación, por lo que entre sus valores se encuentran la creatividad, la mentalidad abierta y la creación colaborativa. Los artefactos en DevOps se apalancan en procesos de cocreación en los que, desde el comienzo del proyecto, intervengan diferentes roles de especialización y multitarea que lo enriquezcan. Además, el modelo de integración continua debe ser aplicado a través de un enfoque sistemático de ramas de código, contribuciones y fusiones con políticas claras.

5. Disponer de datos y analizarlos de manera avanzada es la base de la eficiencia. Es crucial, pues, utilizar los datos generados en los proyectos para incorporarlos como asistencia a las decisiones (manuales o automatizadas) en los entornos DevOps, utilizando la analítica avanzada y la inteligencia artificial como técnicas clave. Así se pueden mejoran las decisiones estratégicas, aplicar umbrales de indicadores de calidad autoadaptables y progresar con mayor eficiencia y anticipación a lo largo de la pipeline.

6. Uno de los principios que se ha consolidado en los últimos años es la usabilidad: en DevOps siempre debe aspirarse a mejorar la experiencia de usuario. Por eso, más allá de ser ágiles, en cada proyecto hay que

velar por la calidad del software bajo todos los prismas que puedan afectar a la percepción de los usuarios.

7. La potencia de DevOps está impulsada principalmente por la automatización, que libera el tiempo de los empleados en tareas más rutinarias y permite ampliar su capacidad de trabajo en tareas especializadas y de creación de mayor valor. Por esto, en el entorno del desarrollo de software resulta crítico que los procesos de creación integren con más intensidad estrategias de automatización.

8. El despliegue a los diferentes entornos y los despliegues finales a producción pueden ser automatizados o, según el caso, semiautomatizados. Para ello, son clave los enfoques cloud y su arquitectura, así como la generación y gestión de datos estructurados que permitirá avanzar en estos caminos.

9. La fuerza del DevOps como metodología está en aprovechar los conocimientos de un equipo multidisciplinar, por lo que la existencia de un canal de comunicación centralizado es crítico en la coordinación. En DevOps, los profesionales necesitan comunicarse y disponer de herramientas que se integran en el pipeline, que notifican e interactúan con otras herramientas y profesionales. En este sentido, irá ganando más popularidad el enfoque de ChatOps.

10. De igual manera que los equipos DevOps cuentan con profesionales especializados en diversos campos, las habilidades de esto no deben centrarse solo en aptitudes técnicas, sino que incluirán conocimientos de diversas áreas. De esta manera, el perfil T-Shaped será esencial, fomentando conocimientos de visión transversal y especialización técnica en algunas disciplinas necesarias en DevOps.

En definitiva, la era Dev(QA)Ops está aquí para quedarse y, apoyada por unos principios que le ofrecen potencia, agilidad y efectividad, promete dar un nuevo impulso al desarrollo de software con y de calidad.

Albert Tort, CTO Sogeti España y Director del SogetiLabs España

ÁNGEL PINEDA, CEO DE ORIZON

"El rendimiento que las empresas extraen a sus inversiones TIC podría ser mucho mejor"

Orizon elimina sobrecostes por el mal rendimiento tecnológico de las empresas, algo que la crisis Covid-19 va a hacer más que necesario. Hablamos con su CEO

¿Por qué es necesaria una empresa como Orizon?
Básicamente, porque le ofrecemos a las empresas un servicio que ahora mismo no ofrece nadie: asegurar la calidad y el buen funcionamiento de su software y de sus aplicaciones de negocio. En otras palabras, garantizamos a nuestros clientes que su software cumpla con los requerimientos con los que ha sido desarrollado y con la calidad de servicio adecuada, tanto interna como externamente. Esto significa que sea capaz de soportar los procesos de negocio y las expectativas de sus usuarios o clientes, tanto en tiempo de respuesta, como en forma (completitud, acuerdos de nivel de servicio...). Además, una consecuencia de este objetivo es los ahorros de costes que les proporcionamos a las empresas que, aunque muchas veces pueden pasar desapercibidos, pueden llegar a ser muy altos.
Las áreas de desarrollo y sus costes asociados han crecido muchísimo en las empresas y hay una verdadera obsesión en las organizaciones para tratar de dar respuesta a las necesidades que impone el mercado en el que se mueven ahora mismo los negocios. Esta situación ha llevado aparejada una progresiva pérdida del control sobre las aplicaciones y el concepto de calidad ha ido perdiendo peso a favor de los costes o la rapidez. Aunque la externalización en sí misma no tiene porque ser negativa la evolución de la industria (enfocada al commodity) ha hecho todavía más daño que los factores anteriores. El problema de la calidad de software es achacable a los precios y a los proveedores y, como consecuencia, las organizaciones tienen una falta de control evidente sobre su infraestructura tecnológica y sobre qué rendimiento puede sacar de ella buscando, desesperadamente, eficiencia ante el caos, y es lo que ofrecemos nosotros, soluciones, sentido común y ahorro. A las organizaciones les faltan, sobre todo, mecanismos de medición. Si no sabes lo que te ocurre no vas a poder mejorarlo.

¿Tan mal funcionan las grandes empresas españolas en lo que a tecnología se refiere?
Desde el punto de vista del rendimiento que las empresas extraen a sus inversiones en tecnología, yo diría que podría ser mucho mejor y, en consecuencia, su eficiencia. Además, otro problema asociado a esta falta de rendimiento es el lastre que supone a muchas organizaciones para avanzar en la adopción de nuevas tecnologías o para desarrollar nuevos servicios. Y esta derivada es de especial gravedad si tenemos en cuenta el alto grado de protagonismo que la tecnología ha adquirido para definir la competitividad permanente en la que viven los negocios y con unos clientes cada día más digitalizados y exigentes con los servicios que reciben.

Todas las grandes empresas cuentan con un CIO y su correspondiente departamento TI, ¿qué consejos les daría?
Que sean exigentes con el buen rendimiento de su tecnología y también con sus proveedores terceros a fin de asegurar la calidad y evitar quebraderos de cabeza y sobrecostes. Según nuestra experiencia, los problemas de rendimiento se concentran en pocos procesos, pero si se ejecutan muchas veces y no se detectan y corrigen, se generan muchas ineficiencias.

Las grandes empresas tienen fallos, pero cada vez gastan más en TIC. ¿Qué solución les ofrece Orizon?
Orizon asegura el rendimiento en función de los objetivos de negocio que, en términos generales son bastante similares: ahorro de costes, tiempos de respuesta rápidos, reducir el número de paradas o acabar los procesos batch a tiempo. Nosotros, diariamente medimos los procesos de negocio e identificamos qué partes del código o de la infraestructura son responsables de fallos o de funcionamientos no adecuados. Para ello, analizamos diariamente terabytes de información técnica y sacamos conclusiones en función de aquellos procesos que, de verdad, son los que pueden afectar al negocio.
Pero además de identificar automáticamente qué es lo que está provocando que algo vaya mal, también proponemos la solución que, en muchos casos, se resuelve con un proceso automatizado o puede requerir la intervención manual por parte de analistas. Nuestro objetivo es que, cada vez más, la resolución sea también una tarea totalmente automática.

En una situación como la actual, ¿han visto que el número de fallos se incremente?
Los procesos en las grandes empresas son muy similares y lo que sí varía es la tecnología que subyace, pero en cada escenario hay una serie de fallos muy específicos que, además, se suelen replicar. La gran diferencia está en qué umbral de tolerancia, en cuanto a calidad y tiempo de respuesta, tiene cada organización.

Ciber delincuencia

Por Miquel Barceló

Escribo al principio de la quinta semana del confinamiento por culpa del coronavirus. Debo recordar que soy persona de riesgo por la edad, la diabetes, un cierto sobrepeso y alguna cosa más que ahora me parece secundaria. Por la cuenta que me trae, sigo a pies juntillas las normas del confinamiento y me sorprende ver la mala gestión que del mismo se está haciendo.

Se decía, antes y me temo que ahora también, que un error muy humano y sumamente frecuente es la capacidad de tropezar dos veces con la misma piedra.

Nuestros gobernantes parecen ser terriblemente humanos: estuvieron casi dos semanas sin poder proveer de EPI's (Equipos de Protección Individual) a los sanitarios que nos cuidaban y ahora, ya en la quinta semana del confinamiento, se nos dice que, pese a la nueva disposición de la OMS (Organización Mundial de la Salud) que recomienda desde hace seis o siete días el uso de mascarillas, nuestro gobierno nos repite que se trata de una medida "complementaria". Haciendo de la necesidad virtud, nos recuerda que no hay porqué usarlas, "de momento". Me temo que seguiremos así hasta que se disponga de mascarillas y se puedan obedecer al cien por cien las recomendaciones de la OMS.

Tal vez por eso, por esa incapacidad de gestión, en todo el mundo, España es el país que tiene más fallecidos por cada millón de habitantes (265) y también más infectados (2786 por millón de habitantes), según datos del domingo 12 de abril. Un triste record de difícil digestión...

En todo ese panorama, día tras día, tanto la Guardia Civil como la Policía Nacional nos recuerdan los problemas de las fake news y, lo que me parece mucho peor, el incremento de nuevos caminos para la ciberdelincuencia nacidos con el coronavirus. Parece que han aumentado y mucho los ataques de spear-phising que redirigen a los incautos a sitios web falsos y sólo movidos por la piratería. Me cuesta entenderlo.

Debo decir que he vivido muchos años sin Facebook (creado en 2003), Twitter (creado en 2006) o Instagram (aparecido en 2009). En realidad he vivido sesenta o más de mis años sin ninguna de esas herramientas que, simplemente, no me hacen falta. Básicamente aprendí a vivir sin nada de todo eso. (Sí uso WhatsApp, creada en 2009, en un grupo cerrado simplemente porque me permite ver con gran facilidad fotos de mis nietos...).

También soy un verdadero experto en eso tan necesario de tirar (sin ni siquiera mirarlos...) diversos mensajes que llegan por correo electrónico de fuentes que no conozco ni controlo. No me interesan ni voy a arriesgarme digan lo que digan. He vivido sesenta años sin ello y, simplemente, no me hacen falta.

Por eso la nueva ciberdelincuencia nacida con el Covid-19 parece no afectarme demasiado, aunque imagino que, en manos menos expertas o menos decididas, pueda ser molesta y generar problemas graves.

Lo que no logro entender es la mentalidad de quien, dados los tiempos que corren, pierde su tiempo creando esos ataques de ciberdelincuencia o, también, crea nuevas fake news. Sinceramente creía que mi sorpresa por la maldad humana y su terrible capacidad para usar todo tipo de herramientas había llegado al límite y no es así. La mente humana, además de los asesinos múltiples de las películas estadounidenses, da para muchas más crueldades y bajezas. Curioso.

En uno de los muchos globos sonda ideológicos que nuestro gobierno de turno hace circular (incapacidad para tomar decisiones se llama la figura... aunque este caso me guste citarlo como un ejemplo más de posible ciberdelincuencia...) ahora circula la idea de que, poco a poco, se trata de emular a países como Corea del Sur que según parece (los datos son siempre de parte...) usó aplicaciones de smartphone para advertir del peligro de contagio.

Simplemente, me parece una aberración. En la eterna lucha entre libertad y seguridad, pese a los peligros, siempre voy a optar por la libertad. La libertad ha costado a la Humanidad demasiadas vidas y siglos de historia para que ahora un miedo (fundado, eso sí) nos lleve a prescindir de lo que parte de nosotros (no todos, por desgracia) ha conseguido.

econocloud

WE YOU

Backup & Disaster Recovery para la continuidad de tu negocio

¿Estás preparado para afrontar una caída de servicio o un ciberataque?

Seguro que ya tienes tu Backup, pero ahora es posible recuperar en minutos lo que antes se tardaba días.

En **Econocloud**, la nube de confianza de Grupo Econocom, garantizamos la disponibilidad de su negocio. Tenemos **Disaster Recovery Services & Backup** para darte cobertura desde nuestros *data centers* en Madrid, Barcelona y Marsella, con la última tecnología y las máximas garantías.

Descubre qué podemos hacer para ti desde Econocloud, la nube de confianza de Grupo Econocom:

hola@econocloud.es | T. 900 800 297 | www.econocloud.es

econocom