byte TI

www.revistabyte.es

mkm PUBLICACIONES

Revista Byte TI
Febrero 2023

Nº312

LOS DESAFÍOS QUE PLANTEA LA NUBE

- TENDENCIAS EN LA INDUSTRIA 4.0
- ¿CÓMO GESTIONAN LOS DATOS LOS DEPARTAMENTOS IT?

COMPARATIVA Bases de datos

Protegiendo la infraestructura crítica

Los ciberataques interrumpen los sistemas de los que más depende la sociedad. Elija el socio con la experiencia, tecnología y enfoque en seguridad necesarios para una resiliencia superior.

Resultados de ciberseguridad probados **withsecure.com/es/**

WITH secure

Formerly
F-Secure Business

Depidos en el sector: una buena noticia para el resto

Manuel Navarro Ruiz
Director de BYTE TI

Google, Meta, Amazon, Spotify, Salesforce, son sólo algunas de las grandes empresas TIC que han anunciado despidos en el sector TIC. En total, en 2022, se produjeron 160.000 despidos en las tecnológicas.

La preocupación se ha extendido como el anticipo de una nueva crisis, pero si las cifras se trasladan a porcentajes en la mayoría de los casos no supone ni el 5% de la totalidad de empleados. Somos muy dados cuando hablamos de cifras económicas, a ser bastante catastróficos, pero lo cierto es que no nos hemos parado a pensar en la ingente cantidad de profesionales que han contratado estas empresas en los últimos años. En los últimos 10 años las grandes empresas tecnológicas han experimentado aumentos de plantillas superiores al 300% y en ese momento nadie hacía hincapié en ello. Empleos, por cierto, muy bien remunerados (no sólo económicamente), en la mayoría de los casos.

Lo que sucede, sobre todo es que las compañías tecnológicas se tienen que adaptar a un nuevo escenario. No son las únicas que están despidiendo personas, pero sí las que lo están haciendo en mayor grado, muy por encima de otros sectores. El problema actual para ellas es que se tienen que adaptar a una nueva coyuntura económica que no han vivido nunca en algunos casos. Ni tenían un entorno inflacionista elevado, ni los tipos de interés estaban tan elevados, ni se encontraron en un momento de tensión geopolítica.

Muchas de ellas, por otro lado, tuvieron que incrementar de forma notable sus plantillas en los años de pandemia, cuando se produjo una auténtica explosión de la demanda de soluciones y máquinas tecnológicas. A pesar de que la demanda (salvo en consumo) sigue alta, el crecimiento no es el mismo que el de los años 2020 y 2021. Es lógico pensar que tengan que realizar pequeños ajustes de plantilla.

No estamos ante una crisis como la de las puntocom de principios de siglo. Los analistas coincidem en que los despidos en el sector TIC son sólo una consecuencia de los crecimientos desorbitados de los últimos años. Estamos en un modo "pausa". No tengo duda de que el sector seguirá creciendo en los próximos meses como tampoco la tengo que ese 5% de personas que van a pasar a engrosar las listas del paro, no van a tardar en encontrar un nuevo empleo y con unas buenas condiciones. La crisis de talento es una de las realidades a las que se enfrentan los departamentos de TI tal y como nos comentan los encuentros constantes que mantenemos con los CIOs de las empresas españolas. A partir de ahora, las tecnológicas les van a aportar al resto de empresas esa mano de obra supercualificada a la que no tenían acceso.

SUMARIO

TEMA DE PORTADA

Los retos de la nube para el departamento IT

40

N.º 312 • ÉPOCA IV

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

BYTE TI
Director
Manuel Navarro (mnavarro@mkm-pi.com

Redacción
Vanesa García (vgarcia@revistabyte.es)

Coordinador Técnico
Javier Palazon

Colaboradores
M.Carpena, R.de Miguel, I. Pajuelo, O. González, M.López, F. Jofre, A. Moreno, MªJ. Recio, JJ. Flechoso, J. Hermoso, A López, C. Hernández.

Fotógrafos
P. Varela, E. Fidalgo

Ilustración de portada
Javier López Sáez

Diseño y maquetación
El Palíndromo Comunicación S.L.

WebMaster
NEXICA
www.nexica.es

REDACCIÓN
Avda. Adolfo Suárez, 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
Natalie Awe (nawe@mkm-pi.com)

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

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

Depósito legal
B-6875/95

FEBRERO 2023
Printed in Spain

EDITA
Publicaciones Informáticas MKM

ACTUALIDAD

COMPARATIVA

TENDENCIAS

FE DE ERRATAS

En el pasado número, en la sección Mujeres TIC se publicó que la protagonista, Fabiola Pérez, tenía una hija y estaba esperando un bebé cuando, en realidad no tiene hijos ni espera el nacimiento de ningún bebé

Los ataques a redes en la nube aumentaron un 48% en 2022

Los intentos de ataques a redes basadas en la nube, específicamente a Vulnerability Exploits, han ido en aumento en el pasado año. El mayor incremento se ha observado en Asia (+60%), seguida de Europa (+50%) y Norteamérica (+28%).

Por Vanesa García

Así lo ha informado Check Point Research, dando a conocer que ha habido un aumento interanual del 48% en los ciberataques basados en la cloud, como consecuencia del creciente traslado de las operaciones de las organizaciones a la cloud debido.

Además, los investigadores han descubierto que los cibercriminales están aprovechando los CVE más recientes registrados en los últimos dos años para atacar a través de la nube, a diferencia de lo que ocurre con los ataques locales.

ATAQUES CONTRA REDES CON BASE EN LA NUBE

En la actualidad, el 98% de las organizaciones globales utilizan servicios basados en la nube, y aproximadamente el 76% de ellas tienen entornos multicloud, con servicios de dos o más proveedores.

Al examinar los dos últimos años del panorama de las amenazas se observa que aunque el número actual de agresiones en redes alojadas en la nube sigue siendo un 17% inferior al de las redes que no lo están, al desglosar los tipos de ataques, y en concreto los exploits de

vulnerabilidades, se observa un mayor uso de los CVE más recientes.

En noviembre, el FBI y la CISA revelaron en un aviso conjunto que un grupo de amenazas no identificado respaldado por Irán pirateó una organización del Poder Ejecutivo Civil Federal (FCEB) para implementar el malware de criptominería XMRig. Los atacantes comprometieron la red federal después de piratear un servidor sin parches utilizando un exploit en remoto de la vulnerabilidad de ejecución de Log4Shell.

El salto a la nube viene de la mano de la adopción de nuevas herramientas de seguridad. Check Point Software recomienda las siguientes prácticas para mantener una seguridad más robusta:

• Controles de seguridad Zero trust en redes y microsegmentos aislados: hay que desplegar recursos y aplicaciones críticas para la empresa en secciones aisladas lógicamente de la red en la nube del proveedor, como las privadas virtuales (AWS y Google) o vNET (Azure). Para microsegmentar las cargas de trabajo entre sí, hay que utilizar subredes con políticas de seguridad granulares en las gateways de subred. Además, se deben utilizar configuraciones de enrutamiento estáticas definidas por el usuario para personalizar el acceso a los dispositivos virtuales, las redes virtuales y sus gateways, y las direcciones IP públicas.

• La seguridad como nueva prioridad: Se debe incorporar la protección y el cumplimiento de normativas en una fase temprana del ciclo de vida útil del software. Con las comprobaciones de seguridad integradas de forma continua en el proceso de despliegue, en lugar de al final, DevSecOps es capaz de encontrar y corregir vulnerabilidades de seguridad en una fase temprana, lo que acelera el tiempo de comercialización de una organización.

• Gestión de vulnerabilidades: el establecimiento de políticas de vigilancia garantiza que su despliegue cumple las políticas corporativas de integridad del código. Estas políticas alertarán sobre sus desviaciones y pueden bloquear el despliegue de los elementos no autorizados. Hay que crear procesos de corrección para alertar al equipo de desarrollo sobre los archivos no conformes y aplicarles las medidas correctoras adecuadas. Asimismo, se deben incorporar herramientas que permitan explorar las vulnerabilidades y la lista de materiales de software para identificar rápidamente los componentes con vulnerabilidades críticas.

• Evitar una configuración incorrecta a través del análisis continuo: los proveedores de seguridad cloud proporcionan una sólida gestión de su postura, aplicando sistemáticamente normas de control y cumplimiento a los servidores virtuales. Esto ayuda a garantizar que están configurados según las mejores prácticas y debidamente segregados con reglas de control de acceso.

• Proteger las aplicaciones con una prevención activa a través de IPS y firewall: hay que evitar que el tráfico malicioso llegue a los servidores de aplicaciones web. Un WAF puede actualizar automáticamente las reglas en respuesta a los cambios de comportamiento del tráfico.

Sobresaliente

CONEXIONES 5G IOT

Tal y como se pone de manifiesto en un informe elaborado por Juniper Research las conexiones 5G IoT van a alcanzar los 116 millones en todo el mundo en 2026, frente a los 17 millones de 2023. Según el estudio, el sector sanitario y los servicios de las ciudades inteligentes serán los responsables de que se produzca un crecimiento del 1.100 % en los próximos tres años.

DISCOS DUROS

En 2023 los discos duros (HDD) seguirán liderando el mercado del almacenamiento. En parte, debido al bajo coste de unidad de capacidad que ofrece esta tecnología, y es que, es cuatro veces menor que la de las SDD. Así lo avala Toshiba quien afirma que esto se debe a que la cantidad de SDD producida no podría satisfacer la demanda del mercado ante el crecimiento exponencial de los datos.

Suspenso

CLOUD

Las aplicaciones en la nube que distribuyen malware se triplicaron en 2022. Microsoft OneDrive generó el 30% de todas las descargas de programas maliciosos en la nube. Así lo ha asegurado Netskope en su Informe de Amenazas, donde se muestra los atacantes están abusando cada vez más de las aplicaciones en la nube críticas para el negocio para entregar malware

BRECHAS DE SEGURIDAD

En 2022, España fue el tercer país con más brechas de ciberseguridad en el mundo.La evolución del número de ataques ha aumentado con el paso del tiempo, siendo los atacantes más activos en 2021 que en 2020. Por ejemplo, Deloitte evidencia que el 94% de las empresas españolas sufrió al menos un incidente grave de ciberseguridad a lo largo de un año.

LA OPINIÓN DE
Fernando Jofre

El ataque de los chatbots

¿No os ha pasado de un tiempo a esta parte que estéis siendo machacados por un servicio de telemarketing que no hace más que llamar con una locución animada, cercana y agradable para venderos no sé qué cosa? ¿Y que ésta sea siempre la misma secuencia de frases, repetitiva y machacona, exenta de toda posible variación de tono? Pues yo ya he estado en ese bucle. Y lo más curioso es que a estas alturas ni me acuerdo de qué querían venderme. Internet con fibra, un cómodo contrato eléctrico sin sobresaltos, o un seguro de decesos. Terminé "mi relación" bloqueando el número del remitente.

He de reconocer que esa voz me engañó la primera vez, y por pura educación empecé a interactuar de manera inteligible, entablando lo que se podría entender como una conversación. Hasta que en la tercera llamada ya me di cuenta de que ni me escuchaba, en sentido literal. Iba totalmente a lo suyo. Era pues un chatbot mal programado y también mal entrenado. Olvidémonos pues de IA aplicada al análisis de tono, contenido y sentimiento, que generase una interacción individualizada, o de respuestas sintetizadas a preguntas formuladas por nosotros.

Sin duda alguna, en los entornos B2C y por qué no también en los B2B, estamos abocados a convivir con los chatbots. Y lamentablemente, preparar y poner en marcha algunas de estas soluciones resulta demasiado fácil para algunos.

La culpa no es tanto del fabricante que "democratiza" la tecnología, sino de quien la utiliza. Y también está nuestra indefensión. ¿No se supone que nos protege el RGPD para no caer en bases de datos descontroladas? Tengo alguna anécdota curiosa al respecto de falta total de protección de la AEPD frente a un operador insistente que incluso denuncié, para no servir para nada pasado un tiempo. Veamos si Chat GPT mejora la situación.

Cinco tendencias en el dato

Desde Bluetab han presentado las tendencias en este sector que impactarán en las empresas españolas durante 2023. Esta área es, sin duda, una de las tendencias tecnológicas más potentes del momento para todo tipo de empresas, y está revolucionando las compañías de todo el mundo.

Las cinco tendencias del sector de cara a este año son las siguientes:

• Los Data Warehouses seguirán creciendo en el Cloud. En el último año ha existido un fenómeno que ha llamado la atención de los expertos en data: el notable crecimiento de los Data Warehouses en Cloud. De hecho, en un informe de 2022, Gartner predecía que en 2024 el 75% de los data workloads estarán en Cloud.

• El Machine Learning se mantendrá como una de las grandes tendencias en datos. Se están produciendo avances muy notables en modelos de Machine Learning que tienen que ver con el lenguaje. Desde Bluetab anticipan que los casos de uso basados en los LLM van a tener un fuerte desarrollo.

• El dato será un eje transversal para impulsar las compañías data-driven. Cada vez existen más empresas que quieren ser data-driven, es decir, que quieren implementar estrategias y decisiones basadas en datos reproducibles que se puedan compartir dentro de la compañía a todos los niveles. Es por eso por lo que está aumentando la necesidad de producir aplicaciones de datos. .

• La formación en Data Science, una disciplina clave para las empresas. Conforme la inversión en datos no deja de crecer, aumenta la necesidad de contar con personas cualificadas capaces de gestionar y trabajar la ciencia de los datos. Actualmente son varias las compañías que están implementando programas para formar en Data Science a los universitarios y prepararlos para el mundo laboral.

• El Gobierno del Dato pasa de ser un "nice-to-have" a ser un "must have".

Wolters Kluwer

a3innuva

La generación online de software de gestión

a3innuva es la suite de soluciones online de Wolters Kluwer para despachos profesionales y empresas.

Un entorno de trabajo colaborativo entre el asesor y la pyme que mejora su eficiencia, con todas las ventajas y la seguridad de trabajar en la nube.

Más información
900 11 11 66
a3innuva.com
a3wolterskluwer.com

a3innuva
simplifica tu vida ;)

LA OPINIÓN DE
Manuel López

Creatividad Artificial

Desde que los robots y la IApasaron a primera plana del mercado tecnológico, siempre se ha defendido que la gran "amenaza" para el ser humano sería en relación con los trabajos repetitivos y "de poco valor añadido". Hemos mantenido que la creatividad humana nunca llegaría a ser imitada por la Inteligencia Artificial. Pero con ChatGPT, se han encendido muchas alarmas acerca de la Inteligencia Artificial. Los grandes avances que se están sucediendo en muy corto espacio de tiempo, desde que millones de personas han utilizado ChatGPT y han comprobado las increíbles capacidades para redactar textos con contenido realmente variado o responder a casi cualquier pregunta, muchos están (estamos) en estado de shock.

Las noticias están llegando de todas partes, por ejemplo en el mundo de la educación, donde se ha hablado mucho de que las Universidades se han visto en la obligación de cambiar la forma de examinar a los alumnos. Otro área que está bastante revuelta es el de el contenido fotográfico, donde varías webs han tenido que desarrollar soluciones para detectar fotografías creadas con IA. Quizás lo más relevante de todo esto es la inquietud que se está empezando a crear acerca del desarrollo de la IA. De ahí surge el concepto de Creatividad Artificial que es un campo de la inteligencia artificial que se centra en desarrollar sistemas y algoritmos que puedan generar contenido nuevo y original, como música, arte, escritura y diseño.

¿Está la creatividad artificial a la altura de la creatividad humana? Esta es la gran pregunta para el futuro próximo. Podemos discutir que la IA no tiene creatividad sino infinitos datos que relaciona para conseguir los resultados deseados; mientras que la imaginación humana no está basada en datos sino también en emociones, sensaciones, relaciones etc.

En cualquier caso, ha llegado el momento de que los humanos empecemos a perder el miedo a la IA y convivir con ella.

Movistar despliega IPv6 en su red móvil

Movistar ha comenzado a desplegar IPv6 (Internet Protocol version 6) o protocolo de Internet versión 6 en su red móvil de modo que cuando el terminal establece una conexión con la red móvil para acceder a Internet recibe tanto la tradicional dirección IPv4 como la nueva IPv6.

De este modo, la compañía de Pallete se convierte en el primer operador en España en direccionar con IPv6 el tráfico de Internet de sus usuarios móviles. Actualmente, la operadora cuenta con un total de 600.000 accesos sobre IPv6 y está previsto que el despliegue esté completado a lo largo del primer trimestre de 2023.

El principal beneficio de utilizar IPv6 es una mayor velocidad de acceso hacia los denominados hiperescalares que ofrecen los contenidos en IPv6. Además, este protocolo incluye mejoras en la seguridad y la movilidad, lo que permitirá el desarrollo de nuevos servicios de conectividad y soluciones avanzadas para el hogar basados en IPv6.

Esta nueva funcionalidad es trasparente para el usuario, ya que no tiene que contratarlo ni solicitar su activación al ser algo relativo a su terminal. En la actualidad, todos los terminales Android lo soportan y a lo largo de 2023 también estará disponible para iOS.

El usuario puede voluntariamente activarlo o desactivarlo de su terminal accediendo a los menús de configuración. Además, el cliente puede saber si está accediendo a los contenidos con IPv4 o IPv6 de diferentes formas.

La operadora comenzó en noviembre de 2022 el despliegue de la funcionalidad Dual Stack para poder proporcionar direcciones IPv6 a los usuarios de líneas móviles.

AUSAPE

XVIII FÓRUM AUSAPE 2023

PALMA DE MALLORCA

PERSUASIÓN TECNOLÓGICA

La próxima edición del Fórum se celebrará en Palma de Mallorca el 31 de mayo y 1 de junio de 2023

AUSAPE continua con su interés de llevar su evento más importante del año a todas las regiones de España siendo las Islas Baleares la primera vez que se celebrará el Fórum fuera de la península.

¡OS ESPERAMOS!

AUSAPE

ausape.com

LA OPINIÓN DE
Daniel Puente

¿Y si esta vez hay más riesgo?

Centenares de publicaciones se han llenado con posibles aplicaciones que tendría blockchain, la inteligencia artificial, computación cuántica y demás "moderneces" para la seguridad informática. Pero igual de cierto es que todavía no han fructificado, o al menos no en la medida que los catastrofistas auguraban. Ahora aparece un nuevo actor en escena, y no es otro que el tan hablado últimamente Chat GPT.

Si bien podríamos clasificarlo dentro de las soluciones de inteligencia artificial, algo lo hace destacar por encima del resto, y no es otra cosa que la facilitación que provee a gente no ducha en programación de realizar scripts tremendamente útiles.

Y como toda nueva tecnología, puede usarse tanto para el bien como para el mal. En fechas recientes hemos visto como una persona ha conseguido utilizarlo para buscar vulnerabilidades (y encontrarlas) en Facebook, y gracias a su política de compensaciones, conseguir una buena suma. Pero también existe la vertiente negativa, y es que se han encontrado diversas estafas realizadas mediante Chat GPT, y aprovechando su gran capacidad de simular conversaciones reales, llevando la estafa del CEO a otro nivel, y por favor, sentiros libres de cambiar la estafa del CEO por muchas otras que conocemos.

¿Puede Chat GPT llegar al nivel de amenaza que prometían las tecnologías antes comentadas? Modestamente considero que va a ser necesaria una revisión pormenorizada de muchos procesos en muchas empresas, y es que esta tecnología hace que debemos redefinir incluso la validez del mítico test de Turing.

Kyndryl ayuda a WOW con sus datos

La digitalización está obligando a las empresas de retail a mejorar continuamente su forma de operar y a buscar nuevas maneras de atraer y retener clientes. En este contexto, Kyndryl ha acudido a la exposición National Retail Federation 2023, de la mano de WOW Concept. La compañía esta ayudando a WOW Concept, un innovador formato de retail español, nacida en modalidad phygital, a recopilar, asegurar y aprovechar los datos como activo estratégico para conseguir la total conexión entre lo físico y lo digital.

"En WOW Concept recopilamos muchos datos y hablamos con cientos de marcas y miles de personas. Es clave tener una estrategia que nos permita optimizar ese flujo tanto de big como de small data", asegura Dimas Gimeno, Presidente de WOW Concept.

Además de esta solución de gestión avanzada de datos, Kyndryl presenta estas otras soluciones sectoriales en el evento:

- Señalización digital dinámica: permite ajustar los precios directamente desde los dispositivos, eliminando la necesidad de que se dedique tiempo y personal al cambio manual de las etiquetas de precios en la tienda
- Gestión predictiva de inventario: una herramienta para la gestión predictiva del inventario que permite a los minoristas una mayor visibilidad de sus stocks y, además, aporta eficiencia en momentos críticos en los que hay una mayor demanda.
- Almacenamiento inteligente: mediante la sensorización, los dispositivos inteligentes y la tecnología de realidad aumentada, los minoristas pueden supervisar y controlar la temperatura y humedad de los almacenes y prever con precisión las entradas y salidas de inventario, con lo que se minimiza la pérdida de artículos
- La retención del empleado: Kyndryl ayuda a muchos retailers en la adopción de tecnologías como los dispositivos móviles en tienda con aplicaciones personalizadas que permiten a los equipos ser más ágiles y eficaces.

Planear los costes de impresión: necesario y rentable

Lejos quedan los tiempos en que los productos y servicios tecnológicos raramente subían de precio y, cuando lo hacían, era para ofrecer una mejor calidad-precio. La pandemia y sus consecuencias, una inflación desatada y un presente turbulento tienen la culpa.

En este clima de incertidumbre, aún es posible detectar algunas certezas: por ejemplo, que la inversión en TI continuará creciendo un 4% este año en Europa, según la IDC.

En el caso de las pymes, toda inversión, incluida la tecnología, debe atenerse ahora más que nunca a criterios de eficiencia, ahorro de costes, productividad y automatización, revela el informe de IDC. Decantarse por soluciones de hardware- como las impresoras y escáneres- por encima de tecnologías cloud, por ejemplo, hace a un negocio más vulnerable ante los períodos de escasez.

Entonces, ¿qué tienen que hacer las empresas para que sus procesos de impresión, copia y escaneado sean más rentables?

ANALIZANDO LOS COSTES DE IMPRESIÓN

Si bien es cierto que la impresión sigue siendo fundamental en la mayoría de las empresas, también es un hecho que se imprime menos y de maneras diferentes. Por ejemplo, algunas empresas se encuentran con un parque sobredimensionado tras implantar el teletrabajo... y deciden que ha llegado el momento de evaluar sus costes de impresión. Con la reducción de los volumenes de impresión en las oficinas no será dificil encontrar opciones de impresión con un mejor equilibrio entre precio de hardware y coste por copia. Es importante saber de antemano cuánto nos está costando la cuota de renting y el coste de los consumibles que usamos (o el precio por página), para poder evaluar alternativas y tomar medidas.

Por otra parte, solo los dispositivos más modernos ofrecen sus propios indicadores de uso, autodiagnóstico y son capaces de ofrecer al usuario la información necesaria para planificar y gestionar con eficacia los recursos. Cuanta más información tengamos sobre los costes de impresión, más fácilmente podremos diseñar una estrategia rentable para ciertos servicios y evaluaremos la pertinencia de conservar, renovar o ampliar equipos.

DE LOS DATOS A LA ESTRATEGIA

Estrategias como reubicar los dispositivos, automatizar los pedidos de consumibles o el autodiagnóstico de funcionamiento pueden tener un impacto muy positivo. Sea cual sea el tamaño de una empresa, los servicios gestionados de impresión pueden revelarse como la solución óptima. Externalizar tareas como actualizaciones, reparaciones y pedidos de consumibles ahorra tiempo y aumenta la eficacia. Y además, dejar en manos de expertos temas tan sensibles como la seguridad documental supone una garantía adicional.

Los planes de renting a medida, transparentes y adaptables permiten por otro lado convertir el coste de estas operaciones en un gasto fijo y predecible.

Ya que resulta imposible predecir las transformaciones y retos a que nos enfrentaremos en un futuro próximo, lo más inteligente es desarrollar una estrategia que nos permita adaptarnos a cualquier cambio y afrontarlo con las máximas garantías.

Más información
https://bit.ly/3YdqqQp

DNS, un activo de TI convertido en una potente herramienta de ciberseguridad

La pandemia, con el auge del teletrabajo y las oficinas remotas, ha fomentado la aparición de redes complejas, híbridas y cada vez más distribuidas, que se han convertido en la piedra angular de estos nuevos modelos de trabajo.

Pero esta nueva realidad plantea retos de ciberseguridad adicionales para las organizaciones. Por ello, DNS, como servicio "core" de red, es un activo cada vez más crítico, por diversas razones: DNS ahora es la primera línea de defensa de toda infraestructura de red. Más del 90 % de las amenazas a la ciberseguridad utilizan DNS en una o más etapas de la cadena de ataque, lo que hace que la seguridad de DNS sea un punto crítico en la postura global de seguridad de una empresa.

En el contexto de redes híbridas, altamente distribuidas y basadas en cloud, con un perímetro de red cada vez más difuso, el DNS pasa de ser sólo un activo de TI que hay que proteger a convertirse en una valiosa y potente herramienta de ciberseguridad, que ayuda a agilizar la búsqueda de amenazas y anticiparse. Mediante el uso de inteligencia y análisis de amenazas en sistema de DNS interno, se puede detectar y bloquear dicha actividad antes de que el ransomware y otras amenazas se propaguen por toda la organización.

DISEÑAR UNA ARQUITECTURA "ZERO TRUST" RESILIENTE CON SEGURIDAD DNS

Una estrategia que permite reforzar significativamente la postura de seguridad de la red es integrar los valiosos metadatos residentes en los servicios "core" de red (DDI: DNS, DHCP e IPAM) dentro de la pila de seguridad. Esta información permite detectar rápidamente una amenaza o un comportamiento anómalo y compartir esa información con el resto del ecosistema de seguridad. Utilizando seguridad DNS y aprovechando la información relacionada con DNS dentro de una arquitectura Zero Trust pueden reducir el riesgo en todos los entornos, desde la nube al datacenter local.

Las capacidades de visibilidad y automatización son esenciales a la hora de desplegar una arquitectura "Zero Trust", y la seguridad basada en DNS las proporciona: identificación de todos los dispositivos y usuarios conectados a red, tanto en entornos virtualizados, "on-premise" o en nube/s híbridas, eliminación de compartimentos estancos, mediante el acceso compartido a las bases de datos de protocolos, direcciones IP, dispositivos de infraestructura de red, hosts finales, etc., reducción del riesgo de interrupción de los servicios gracias a la detección de dispositivos no autorizados, errores, dispositivos de red no gestionados, etc., que pasa desapercibidos para las herramientas estándar de IPAM.

Estrechamente relacionado con la visibilidad y la automatización está la idea de orquestación. Todo el sistema de ciberseguridad tiene que estar orquestado, de modo que cuando se detecta un ataque en un sistema, esa información sea conocida inmediatamente por el resto de sistemas y herramientas. Eso nos va a permitir reducir el tiempo del ataque, y por tanto del daño causado.

Por Joaquín Gómez
Cybersecurity Lead
para el Sur de Europa de Infoblox

La importancia de encontrar confianza en el mundo cloud

Si algo hemos aprendido en ICM durante estos más de 15 años de servicio, es que la mayor dificultad que existe en una empresa de tecnología es decidir qué tecnología desplegar y usar en los proyectos de sus clientes. Más aún si quieres ofrecer las últimas novedades. Y lo cierto es que dedicamos, cada año enormes cantidades de tiempo y dinero en laboratorios que nos permiten evaluar las opciones que van surgiendo, pero cuando firmas la compra de una nueva infraestructura, siempre tienes un pensamiento en tu cabeza «¡Anda que si la cagas!».

TECNOLOGÍAS GANADORAS

Hay que decir que, hasta hoy, hemos sido certeros en nuestros estudios y las tecnologías usadas han ganado la posición del estándar permitiéndonos salir al mercado con una solución reconocida y con solvencia. Algunos ejemplos de dilemas entre dos tendencias:

- iSCSI Vs Fiber Channel
- SAN Vs NAS
- Citrix Vs Vmware
- 40 Gbe Vs 40 Gb fibra

Tampoco es que estas fueran tecnologías opuestas o divergentes. Simplemente que, por exigencias de las partnerizaciones que los fabricantes exigen, una empresa de tamaño mediano o pequeño ha de hacer una apuesta y tirar adelante con ella.

Desde que apareció la virtualización, todo y que se basan en los mismos principios, lo que aprendes para un entorno, para el otro no te sirve nada. De hecho, tenemos la sensación de que los fabricantes, lo hacen adrede, pretendiendo diferenciarse con «cosas» que el otro no haga. Y es casi imposible, porque las miradas siempre están vigilantes y con ganas de copiar las novedades del rival.

Tanto es el grado de evolución y de divergencia que el temor a equivocarse va in crescendo e incluso llega a provocar que las empresas se vuelvan más conservadoras y mantengan un pie donde «siempre les ha funcionado».

El mejor ejemplo son las Clouds, existen 3 grandes formas de tener cargas de trabajo para tu negocio:

- Cloud Público (Azure, AWS, Google,....)
- Cloud Privado (Nutanix, HP Greenlake o su antiguo Simplivity...)
- On-Premise basados en fabricantes tipo Dell, HP, Lenovo....

INTEGRAR LA TECNOLOGÍA

Ahora la magia ya no está tanto en ver qué tecnología, si no en cómo integrarla de la mejor forma para los requerimientos de tu negocio. Un negocio no puede correr riesgos innecesarios y es primera necesidad aplicar un principio de prudencia. Y os preguntaréis, ¿Cómo aplicas la prudencia en un mundo con tantas opciones y tan evolutivo? Pues, desde el punto de vista de ICM, entendiendo qué necesitas y huyendo de las modas y los hypes.

El mundo de la tecnología se alimenta del hype, se dedican cantidades ingentes de dinero a promover tecnologías nuevas y como buen hypero, quien invierte, se convierte en legionario de su apuesta tecnológica.

Si me preguntasen cuál sería mi apuesta, usaría el método «Rajoy»: Depende. Creo que la mejor solución es recurrir a empresas consultoras/integradoras, como ICM, donde las inversiones están muy bien pensadas. Nuestra previsión para el 2023 es simple: No te la juegues. Pregunta a varias empresas qué recomiendan y qué usan. Cuando encuentres a alguno que te diga que usa tal tecnología pero que no te la recomienda, cásate con él. Lo más difícil es encontrar confianza. La pervertida frase «consejos vendo que para mí no tengo» debería estar alejada del comportamiento de un consultor como Dios (o Energía) manda.

La importancia de establecer una correcta estrategia de gestión del dato

El dato definirá el futuro de cualquier compañía. La rápida evolución tecnológica experimentada en los últimos años ha posibilitado que se pueda extraer su verdadero valor lo que permite a las organizaciones una toma de decisiones más ágil, rápida y efectiva ya sea para mejorar los procesos operativos, como para adaptar la producción o atender de forma inmediata las necesidades de los clientes, entre otros muchos apartados.

Por todo ello, es necesario establecer una cultura empresarial que gire en torno a los datos y para ello incorporar y definir una estrategia correcta es el primer paso. Se espera que, para 2025, el volumen de datos creados y consumidos en todo el mundo alcance los 180 zetabytes. Las empresas almacenan cada vez una mayor cantidad lo que supone que tengan que lidiar con diferentes problemáticas: aparición de silos, datos duplicados, incapacidad para conocer cuál es el dato valido y, por supuesto, proteger esos datos son sólo algunas de ellas.

CONTAR CON LA TECNOLOGÍA ADECUADA

El primer paso para establecer una correcta estrategia de gestión del dato es contar con un partner que oriente al departamento de TI. Contar con un experto como Lenovo, permitirá conocer cuáles son las necesidades de una empresa y de paso, establecer cuáles son las prioridades de la organización en materia de gestión de datos. Y es que las necesidades de una empresa, varían según el sector en el que opere, por lo que un mismo dato no tiene el mismo valor para una empresa dedicada a la fabricación que para una compañía que opere en el sector del retail. Lenovo cuenta con una amplia gama de soluciones que van desde el almacenamiento, soluciones en la nube, herramientas de backup y de recuperación de datos, soluciones de protección y también de analítica e IA.

En este sentido, la multinacional es uno de los grandes líderes del mercado de servidores. Todos ellos están capacitados para aplicar tecnologías de Big Data que se adaptan a las necesidades de las compañías de forma flexible y que permitirán aprovechar el valor de los datos, proporcionar conocimiento con mayor rapidez y acelerar la toma de decisiones. Todo ello se complementa con la inclusión de un conjunto de herramientas que ofrecen una escalabilidad excelente para que la organización pueda crecer al ritmo que lo hacen sus cargas de trabajo. Asimismo ofrecen una capacidad de alto rendimiento que permita responder de forma más rápida a las necesidades de la empresa gracias a sus sistemas optimizados y diseños validados para conseguir una rentabilidad más rápida.

La multinacional ofrece además una serie de añadidos como los Servicios de Infraestructura TruScale que permiten ampliar las capacidades de hardware, software y asistencia de TI a medida que evolucionan las necesidades de infraestructura, algo más que necesario en un entorno tan cambiante y variable como el actual. Asimismo ofrece un conjunto de Servicios de Implementación que permiten acelerar los procesos y gracias a ello incrementar la productividad de la empresa. Lenovo se encarga de simplificar la implementación de nuevas tecnologías para que la organización se centre en su verdadero negocio.

PROTECCIÓN DE LOS DATOS

Pero si algo es importante hoy en día es proteger todos los datos. Las empresas se encuentran con que los ciberataques están en aumento y no están exentas de que se pueda producir cualquier incidente que les impida recuperar determinados datos. Por ello, Lenovo está trabaja de forma conjunta con la firma experta en protección de datos Veeam Software que posibilita que se pueda combinar el hardware y software para lograr, que las soluciones de almacenamiento y gestión de datos sean fiables en cualquier lugar de la nube híbrida. Gracias a esta colaboración se garantiza la solidez del negocio, se elimina la pérdida de datos y se evitan los períodos de inactividad con soluciones diseñadas para crecer con la organización a medida que lo hacen los datos. Gracias a esta combinación se garantizan las copias de seguridad, la recuperación ante desastres y la protección de datos para infraestructuras virtuales, físicas y multicloud.

Modernización de SQL Server

Por Francisco Racionero
CEO de Aleson ITC, S.L.

Se habla mucho de que la nueva electricidad son los datos, que las analíticas son la base para la toma de decisiones de las empresas y tienen toda la razón, con el volumen de información de la que se dispone, es un suicidio no usar esta analítica para tomar mejores decisiones empresariales.Pero toda esa información parte de fuentes de datos transaccionales, como es Microsoft SQL Server.

La estimación de uso de SQL Server frente a sus competidores es del 37% del total de motores de bases de datos utilizados, pero ahora viene la cifra demoledora, más del 50% de estas bases de datos está en versiones SQL Server 2008 o anteriores.

Sin embargo, los negocios piden cada vez más rendimiento, más seguridad y más escalabilidad. Por ello, consideramos que es el momento de modernizar los sistemas en SQL Server. El proceso migración y modernización debe ir dirigido a versiones más actualizadas, que permitan a los negocios afrontar los retos con una visión clara de futuro, que ayude a las empresas mantener los niveles de rendimiento y seguridad adecuados a las necesidades del negocio y del entorno.

La experiencia nos dice que, aunque hayas hecho un mantenimiento de tus bases de datos, aunque te hayas preocupado por los sistemas, llega un momento en que la plataforma necesita modernizarse. No solo se trata de cambiar hardware, sino que esa modernización debe ser más profunda, debe partir de la resiliencia de los sistemas a los distintos cambios que se producen en las empresas, sin tener que estar pendiente si mi base de datos aguantará.

En Aleson ITC apostamos por la modernización de Microsoft SQL Server a la nube y de forma prioritaria a Microsoft Azure.

¿En qué nos basamos para hacer esta recomendación a nuestros clientes?

Empecemos por la parte que más beneficia al negocio, escalabilidad en los costes y adaptación al crecimiento empresarial sin tener que invertir en nuevo hardware y por supuesto OPEX vs CAPEX.

En segundo lugar, SEGURIDAD, utilizando servicios avanzados disponibles solo en la plataforma SaaS de Azure, como el Vulnerability Assesment o al Advanced Threat Protection. Capacidad de licencia Enterprise como, por ejemplo, alta disponibilidad por defecto o capacidad de encriptación de la base datos de forma transparente a los aplicativos.

En tercer lugar, en los niveles operativos, funcionalidades como Automatic Tuning que ayuda en la mejora y mantenimiento del rendimiento de las bases de datos o Auditing que permite conocer el acceso a los datos por parte de terceros y está muy orientado al cumplimiento del RGPD.

Todos estos condicionantes, nos hace considerar la ventaja que nos da la nube a la hora de alojar las cargas de trabajo de SQL Server en Azure.

¿Cómo abordamos una migración a la nube de un sistema de bases de datos SQL Server?

Una migración a la nube de todo o parte de un sistema, viene dada por un estudio de los beneficios empresariales que obtendrá nuestro cliente, de una planificación exhaustiva y de un planteamiento técnico, robusto y funcional. Por supuesto, toda migración tiene que estar bajo el paraguas de la seguridad, el control del coste y el gobierno de los sistemas.

El equipo de Aleson ITC está al lado de sus clientes, tratando de ser parte de su equipo y coordinándose en todo momento para alcanzar las metas que se han propuesto.

Para concienciar a las empresas sobre la modernización de SQL Server y la importancia de la migración de las cargas de trabajo a la nube estamos preparando el Evento de SQL Data Tour que tendrá lugar el próximo 9 de Marzo a las 9.30H en las oficinas de Microsoft Ibérica, abierto al público y como segmento clave para CIOs y CTOs

Virtual Cable flexibiliza la estrategia cloud de las organizaciones

El crecimiento de la nube es imparable tal y como afirman los estudios de las principales consultoras. La virtualización de los puestos de trabajo es una de las áreas susceptibles de sumarse a esta tendencia, pero a día de hoy, son muchos los retos que plantea. Costes ocultos, complejidad de gestión,… Estos hándicaps ensombrecen los resultados de la estrategia cloud, incluso hay empresas que deciden abandonar la nube debido a una experiencia desfavorable que, entre otras cosas, les impide justificar una inversión que cada vez es más elevada debido al incremento de los costes y a un dimensionamiento poco acertado de las máquinas virtuales. En muchas ocasiones, la ausencia de un análisis previo pormenorizado es la causa del fallido viaje a la nube de los puestos de trabajo. Para poder realizarlo de forma eficiente y confiable, es necesario contar con las herramientas adecuadas, capaces de realizar pruebas reales y transparentes, que aporten seguridad y devuelvan el control del gasto a las organizaciones.

SOLUCIÓN VDI PARA ENTORNOS HÍBRIDOS Y MULTICLOUD

Virtual Cable, empresa especializada en el desarrollo de software para la transformación digital del puesto de trabajo, ha diseñado una solución VDI que ayuda a trazar una estrategia de digitalización de los puestos de trabajo totalmente adaptada a las necesidades y recursos de cada cliente. "La flexibilidad de nuestra propuesta invita a la reflexión, a valorar las múltiples tipologías y proveedores cloud antes de tomar una decisión", explica Fernando Feliu, Executive Managing Director de Virtual Cable. Esta afirmación hace referencia al rango ilimitado de posibilidades que ofrece la solución de la tecnológica madrileña.

UDS Enterprise incorpora funcionalidades específicas para configurar entornos heterogéneos, que permiten construir infraestructuras integradas por nubes híbridas, privadas, públicas y plataformas multicloud sin coste extra. "Nuestro propósito es ayudar a los clientes a rentabilizar al máximo sus recursos actuales, aprovechando las mejores ventajas del amplio abanico de tecnologías existentes", señala Feliu. Esta solución ofrece la posibilidad de gestionar las cargas de trabajo de manera inteligente, para desplegar cada puesto de trabajo en la plataforma que mejor rendimiento vaya a proporcionar a cada perfil de usuario, ajustando los costes al máximo. UDS Enterprise unifica y centraliza la gestión de los diferentes entornos, atajando la complejidad y añadiendo opciones de configuración avanzadas para automatizar desbordamientos entre distintas plataformas. Así, los administradores tienen capacidad de decidir en qué circunstancias se emplean recursos on-premise y cuándo los de uno o varios proveedores cloud determinados, como AWS o Azure. "Se puede dar la orden al sistema para que realice un desbordamiento automático a la nube una vez se agoten los recursos locales o, por poner otro ejemplo, que los escritorios de los trabajadores que utilizan gráficos 3D se entreguen desde la nube de Amazon, dimensionándolos de forma eficiente para que únicamente consuman los recursos exactos que necesitan", explica el directivo de Virtual Cable.

A estos beneficios hay que sumar la capacidad de programar el encendido y apagado automático de las máquinas, que se realiza a través de un sistema avanzado de calendarios que ayuda a reducir los costes del modelo de pago por uso de la nube al mínimo. Además, UDS Enterprise añade una sólida capa de seguridad que cumple con los estándares del Esquema Nacional de Seguridad (ENS) y blinda el acceso a los sistemas y datos corporativos desde cualquier dispositivo, sin importar el entorno en el que estén alojados.

La posibilidad de combinar virtualización de escritorios, aplicaciones y acceso remoto a equipos, además de su compatibilidad con cualquier tecnología de terceros, convierten a UDS Enterprise en una potente herramienta para digitalizar los puestos de trabajo de forma personalizada, aportando flexibilidad, simplicidad, seguridad y eliminando por completo las preocupaciones por los costes impredecibles de la nube.

Samsung Knox Suite: la solución para los negocios en movilidad

Por Isabel López,
responsable de soluciones y servicios B2B de Samsung España

Muchas organizaciones están apostando por estrategias móviles en su digitalización; con el fin de conseguir una mayor productividad y una mejor experiencia de sus clientes. El éxito de dicha estrategia es posible con una plataforma que ofrezca el mayor nivel de seguridad y fiabilidad, mediante una interfaz sencilla que permita implementar, administrar y obtener información útil sobre una gran flota de dispositivos de forma eficiente.

En Samsung resolvemos este desafío con Samsung Knox Suite, una solución todo en uno para resolver los requisitos de movilidad más complejos. Con soluciones como Knox Mobile Enrollment (KME), Knox Manage, Knox Enterprise Firmware-Over-the-Air (E-FOTA) y, más recientemente, Knox Asset Intelligence, ofrecemos a los clientes todas las facilidades que se necesitan para implementar, administrar y analizar su flota de dispositivos.

DESPLIEGUE MASIVO

Knox Mobile Enrollment que permite el despliegue masivo y en remoto de la flota de terminales de una empresa, con un registro automático y obligatorio en el MDM. Cuando un administrador de TI configura un dispositivo por medio del servicio, el usuario del dispositivo solo debe encenderlo y conectarlo. El terminal será registrado en su MDM durante el proceso de configuración inicial. Por otro lado, Knox Manage ofrece una gestión multiplataforma de terminales Samsung, Android, iOS y Windows 10 para aplicar las políticas de seguridad y gestión a los terminales de los empleados, y así, controlar de manera remota los equipos de la organización. De la misma forma, Knox E-FOTA, permite al administrador instalar la versión del Sistema operativo deseada, asegurar la compatibilidad con las aplicaciones internas y configurar cuándo y en qué condiciones se instalará la versión homologada del Sistema operativo.

MAYORES CAPACIDADES

La realidad es que seguimos desarrollando estas capacidades, y todas nuestras innovaciones se añaden a Knox Suite.

Un ejemplo de ello es Knox Asset Intelligence, un servicio que aporta visibilidad sobre el estado de los dispositivos móviles, con informes en tiempo real sobre el estado del dispositivo y la duración de la batería; hasta la estabilidad de la aplicación, la conectividad y el seguimiento de la ubicación. Este conocimiento ayuda a las empresas a tomar decisiones para mejorar la productividad, la utilización y el mantenimiento de los dispositivos.

Con Knox Suite, nuestros clientes aprovechan los beneficios de ser parte de nuestro ecosistema, porque estas herramientas les permitirán gestionar la inversión que realicen en un futuro en otros productos y servicios. Knox Suite proporciona una solución de extremo a extremo para facilitar la gestión a los administradores, sin tener que distinguir entre las características de una solución frente a otra, desde un único portal y con una única licencia.

Las necesidades de tecnología y el resto del negocio nunca deben disociarse. La colaboración entre ambas necesita de una plataforma que empodere a todos en la empresa. Knox Suite responde a esa necesidad, respaldando todo el viaje hacia la movilidad empresarial y consolidando todo lo que necesita una empresa en su proceso de digitalización.

¿Cómo gestionan los datos los departamentos IT?

La gestión y el posterior análisis de los datos parece ser una de las grandes prioridades de las empresas en los próximos meses. Con la intención de ver cómo están abordando esta materia, Byte TI organizó un encuentro que contó con el patrocinio de Lenovo y Zscaler

En el encuentro participaron José Manuel Casillas, CIO de LLYC; Concepción García, Sistemas de la Información de Madrid Digital; Mario Moreno Martínez, Responsable de Seguridad de Metrovacesa; Fernando Martín, Data & Integration Architect de Food Delivery Brands; Francisco Gonzalo Landwerlin, CIO de Sacyr; Alberto López, CIO/CISO de Solaria; Pablo de la Puente, CIO de Gestamp; Luis García, IT Lead de Data Management de ING; José Arbués Bedia, CDO de la Universicad Complutense de Madrid; David Rebollo, Storage Sales Specialist Iberia de Lenovo y Raquel Hernández, Directora Regional para España y Portugal de Zscaler.

Lo que habitualmente se está viendo entre las empresas es una obsesión por el dato. Lo que se intentó descubrir al inicio del encuentro es si esa obsesión era real. En este sentido, Mario Moreno Martínez, Responsable de Seguridad de Metrovacesa, aseguró que "el dato es fundamental. Tanto el interno como el externo ya que nos permite conocer a qué clientes elegimos para focalizar las ventas y a nivel interno para la toma de decisiones. Es fundamental en toda empresas". En su misma línea se situó Pablo de la Puente, CIO de Gestamp quien afirmó que el dato, efectivamente, "es algo disruptivo porque todas las iniciativas que salen adelante, en un 95%, están basadas en los datos. Consideramos al dato como algo esencial, por lo que en Gestamp hemos creado la "Oficina del dato", que nos ha ayudado a romper muchos silos. Gracias a ello hemos podido tomar decisiones de forma muy ágil y que está teniendo un impacto en las operaciones de la compañía. Hoy en día, por ejemplo, en todo aquello que respecta al IoT son proyectos, donde los datos en tiempo real nos permiten mejorar la eficiencia de nuestros activos". Sin embargo, no todos los asistentes son tan adeptos. Al final, también hay ciertos grises y como afirmó Luis García, IT Lead de Data Management de ING, "el dato es disruptivo aunque depende del sector en el que opere una empresa. Para un banco como nostors, en lo que tiene que ver con digitalización nos permite hacer una hiperpersonalización de los clientes, automatizar y agilizar procesos, por ejemplo en la tramitación de una hipoteca. Cada vez tomamos más decisiones basadas en el dato, pero claro, lo que vale para nosotros a lo mejor no sirve para otro tipo de empresa".

En este sentido, José Arbués Bedia, CDO de la Universicad Complutense de Madrid, mostró cómo el dato puede utilizarse para diferentes actuaciones: "El dato es una palanca de cambio. Nos puede servir para cambiar el la gobernanza, que en el

caso de la Universidad Complutense es como una ciudad. Entre otras actuaciones, queremos pasar a que la tecnología esté en todos los planteamientos que se realicen en la UCM. Tenemos que dar ejemplo de transparencia en los datos. Tenemos que poner al estudiante en el centro y lo más complicado es promover esa cultura interna. Considero que el dato es crucial como palanca de cambio".

El punto discrepante a todos ellos lo puso José Manuel Casillas, CIO de LLYC, que aseguró que "el dato no creo que sea la parte fundamental de la estrategia actualmente. Hay que tener claros los objetivos de las empresas y las necesidades del cliente y de los RR.HH. Al final cada uno vemos el dato de un punto de vista diferente, unos lo valoran desde el apartado de la seguridad y otros desde la analítica. En mi caso, observo que llevamos mucho tiempo hablando de datos pero no veo que haya algo disruptivo en torno a ellos". Finalmente, David Rebollo, Storage Sales Specialist Iberia de Lenovo, afirmó que "no hay dos empresas iguales. Desde nuestro punto de vista hay que analizar el estado en el que se encuentra una empresa y analizar qué pasos hay que dar. Ahora estamos en la filosofía del dato. La gestión del dato tradicional ha cambiado porque empieza a haber muchos dispositivos en la parte del edge lo que conlleva una gestión de datos que no se puede hacer de forma tradicional. Lo que hay que hacer es conectar el dato del perímetro hacia el entorno del Data Center. Nosotros creemos que una estrategia en torno al dato debe sustentarse en cuatro pilares. Federación: acceder a los datos de forma más rápida. Simplicidad: aprovechar a nube como rampa de acceso para poder gestionar los datos en frío. Protección: para potenciar la seguridad de los datos. Optimización: hay diferentes datos y hay que dar facilidad de acceso a esos datos".

PRINCIPALES DIFICULTADES

A la hora de analizar las dificultades para establecer una cultura del dato, Francisco Gonzalo Landwerlin, CIO de Sacyr, cree que "toda la digitalización ha puesto al dato como el activo más importante. Esa digitalización ha provocado cambios como la implementación de distintas medidas de seguridad, que se generen cada vez más datos, y que éstos se hayan convertido en activos cada vez más importantes. En mi opinión hay una dificultad clara que es la falta de talento y otro son los silos de información que se están creando y que son difíciles de organizar. Asimismo, a la hora de hacer proyectos alrededor del dato no todos entiende el proyecto de la misma forma. Al final se trata de definir y eso conlleva asegurar la calidad del datos para organizar una estrategia alrededor del dato". Alberto López, CIO/CISO de Solaria, afirmó que en su compañía "vivimos del dato, porque es fundamental para buscar y encontrar emplazamientos para realizar los despliegues y necesitamos información. Asimismo, el crecimiento orgánico hace que cada vez se incorpore gente nueva. Es decir, tenemos muchas fuentes heterogéneas de obtención del dato, por lo que debemos establecer una política en torno a él para establecer una mejor gestión". Fernando Martín, Data & Integration Architect de Food Delivery Brands (Telepizza), aseguró que "el dato es la clave de las decisiones de la compañía. Incluso antes, cuando no era digital, ya sea para abrir una nueva tienda o prevenir picos de demanda. El problema que vemos se encuentra en la heterogeneidad del dato. Al final se trata de obtener la información que viene de diferentes fuentes por eso nos estamos centrando en el gobierno del dato para al menos tener una fuente del dato confiable y que el resto de aplicacio-

LOS PARTICIPANTES

José Manuel Casillas, CIO de LLYC

Concepción García, Sistemas de la Información de Madrid Digital

Mario Moreno Martínez, Responsable de Seguridad de Metrovacesa

Fernando Martín, Data & Integration Architect de Food Delivery Brands

LOS PARTICIPANTES

Francisco Gonzalo Landwerlin, CIO de Sacyr

Alberto López, CIO/CISO de Solaria

Pablo de la Puente, CIO de Gestamp

Luis García, IT Lead de Data Management de ING

José Arbués Bedia, CDO de la UCM

nes esté sincronizada en tiempo y forma. Para la toma de decisiones además el dato tiene que estar bien limpio. Por su parte, Raquel Hernández, Directora Regional para España y Portugal de Zscaler consideró que en realidad, no hay nada nuevo: "toda la vida se han tomado decisiones en torno al dato. Lo que hay que hacer es facilitar que el acceso a los datos sea adecuado y que se haga de forma segura. Una parte muy importante del dato es saber cuál es el ciclo de vida de ese dato. A todos nos cuesta la gestión del cambio que es necesaria realizar en la actualidad y creo que ese es el reto principal porque hay que operar de forma diferente y tener una gestión del dato integral". Las políticas, estrategias y dificultades son, efectivamente, diferentes según el sector en el que opere la empresa. Por ejemplo, Concepción García, responsable de Sistemas de la Información de Madrid Digital aseguró que "en nuestro caso, tenemos aproximadamente 1.000 servicios al ciudadano, organizados por consejerías que en muchos casos se acercan para decirnos qué hace con la cantidad de datos que tienen. Es decir, tenemos un volumen de datos muy importante repartidos por diferentes lugares. Así que, lo que veo imprescindible es que el dato tenga calidad, saber qué indicadores de negocio tienes o qué iniciativas se quieren llevar a cabo con esos datos".

PROTECCIÓN DEL DATO

En lo que sí que hay unanimidad es el la necesidad de proteger los datos. En este sentido, la portavoz de Zscaler aseguró que "debe haber un punto de partida que es que se está intentando la protección del dato como si se estuviera en una arquitectura legacy, cuando el perímetro ahora está diluido: hay datos en la nube, en el centro de datos, en las aplicaciones... Con esa falta de perímetro intentamos protegerlo como si los datos estuvieran todavía en el data center. Y esto no funciona. Si seguimos trabajando así, se asumen más riesgos y no se es eficiente. Esto es una filosofía y una cultura que hay que cambiar para llevar a cabo una efectiva protección del dato". A esta problemática, Pablo de la Puente, CIO de Gestamp añadió un aspecto importante el la filosofía de protección del dato: "Hay que trabajar en dos ámbitos. El primero es la protección externa, pero el segundo es pensar que el problema de la protección se puede encontrar dentro de tu propia organización. Para ello, o se realiza una buena gobernanza del acceso a la información o la seguridad perimetral carece de sentido por mucho que se tengan las mejores soluciones o herramientas de protección del mercado". Para el CIO de LLYC, lo que ha cambiado es que "la superficie de ataque se ha diluido claramente".

David Rebollo, Storage Sales Specialist Iberia de Lenovo

Raquel Hernández, Directora Regional España y Portugal de Zscaler

Zero Trust ayuda a aprovechar todo el potencial de la transformación digital

Por Nathan Howe,
Vicepresidente de Tecnologías Emergentes y 5G, Zscaler

En el actual escenario de rápida transformación digital, el concepto de zero trust hace su aparición como modelo ideal para proteger a usuarios, cargas de trabajo y dispositivos de las empresas en un mundo distribuido en la nube y totalmente orientado a la movilidad.

Más del 90% de los responsables de TI que han iniciado su migración a la nube, ya han implementado una estrategia de seguridad de Zero Trust o están en proceso de hacerlo en el próximo año, según los resultados del estudio global "State of Zero Trust Transformation", realizado por Zscaler entre más de 1.900 directivos de empresas que han comenzado a migrar aplicaciones y servicios a la nube.

Este importante avance, y las causas que hay detrás, permite ser optimistas en cuanto a la implantación de una arquitectura de confianza en un futuro próximo. A pesar de ello, la presión sobre las empresas para que, en la medida de lo posible, aceleren este proceso, no deja de aumentar. A medida que nuestro entorno sigue experimentando vaivenes y creando condiciones económicas poco seguras, con una cadena de suministro inestable, con clientes y empleados con exigencias en constante evolución y con presiones en los presupuestos corporativos, a las organizaciones les resulta cada vez más complicado mejorar su negocio sin la velocidad, la agilidad, la flexibilidad y la eficacia de la nube.

La transformación digital no puede ser nunca una calle unidireccional. Al igual que la evolución de la red desemboca inevitablemente en cambios en la estrategia de ciberseguridad, estas nuevas soluciones de seguridad pueden ser catalizadoras del cambio en otras áreas de una organización. Un enfoque zero trust en la nube, con la visibilidad y el control que proporciona sobre los usuarios y el tráfico de la red, juega un papel impagable a la hora de facilitar la transformación digital segura y sin fisuras de una empresa.

VENTAJAS DE ZERO TRUST

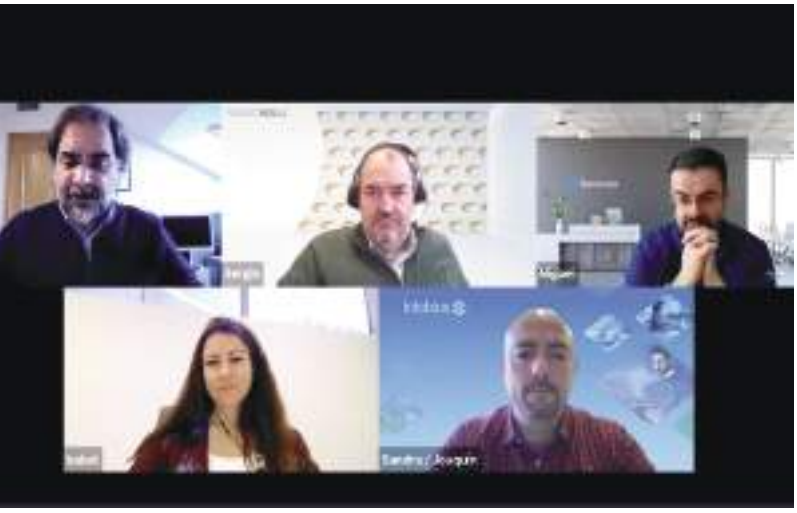
Gracias al modelo zero trust, las organizaciones pueden dejar atrás su antigua arquitectura de seguridad. Más de dos tercios (68%) de los responsables de TI creen que la transformación segura de la nube es imposible con una infraestructura de seguridad de red heredada y que el acceso zero trust a la red tiene claras ventajas sobre los firewalls y VPN tradicionales en relación con la seguridad del acceso remoto a las aplicaciones.

Solo el 22% de los encuestados confía plenamente en que su empresa sabe aprovechar todo el potencial de su infraestructura cloud. Es evidente la necesidad de ir más allá de la seguridad. Enfocada desde una perspectiva de TI integral, zero trust puede ofrecer numerosas oportunidades en un proceso profundo de digitalización. Puede evitar ciberataques a gran escala, de eso no hay duda, pero también puede hacer mucho más, desde impulsar la innovación en el negocio hasta apoyar un mayor grado de compromiso de los empleados o proporcionar eficiencias de costes tangibles.

Los resultados de la encuesta también evidencian una desconexión entre la empresa y el equipo TI, así como una incomprensión crítica de los fundamentos de la transformación digital. El estudio muestra que las empresas siguen considerando la transformación como una cuestión tecnológica -una forma de trasladar el gasto de la infraestructura a la nube- en lugar de una parte integral de la estrategia empresarial. Los líderes de TI preocupados por el negocio, entienden que la transformación no consiste solo en migrar las aplicaciones a la nube. Saben que, para que la empresa aproveche todo el potencial de la digitalización, la red y su seguridad también deben transformarse.

Existe una oportunidad única para que los líderes de TI eduquen a los directivos sobre zero trust y lo pongan sobre la mesa como un motor empresarial de gran valor. Es el elemento que faltaba para ayudar a las empresas a prepararse para las tecnologías del futuro.

Cómo establecer una estrategia de Ciberseguridad



Uno de los pilares fundamental sobre los que debe asentarse cualquier proceso de transformación digital es el de la ciberseguridad. Son numerosos los informes que acreditan que la protección de datos, sistemas, aplicaciones y usuarios se ha convertido en una de las mayores preocupaciones de los departamentos de TI de las organizaciones.

Por Vanesa García

Uno de los pilares fundamental sobre los que debe asentarse cualquier proceso de transformación digital es el de la ciberseguridad. Son numerosos los informes que acreditan que la protección de datos, sistemas, aplicaciones y usuarios se ha convertido en una de las mayores preocupaciones de los departamentos de TI de las organizaciones.

Para profundizar en el tema, y dar respuesta a cómo se debe implementar esa estrategia de ciberseguridad, desde BYTE TI hemos organizado un encuentro con la colaboración de Miguel López, Country Manager de Barracuda; Joaquín Gómez, Cybersecurity Lead para el Sur de Europa de Infoblox; Isabel López, B2B Tech Solutions Manager de Samsung y Sergio Martínez, Iberia Regional Manager de Sonicwall.

"Los ataques van más dirigidos a monetizar. Se están atacando a las aseguradoras para saber que empresa puede pagar el rescate. Ha crecido el malware en un 11%, así como los elementos de intrusión. Lo que más preocupa son las amenazas encintadas, que crecen a triple dígito desde hace años. Es una autopista de entrada del malware en las compañías", asegura Sergio Martínez, Iberia Regional Manager de Sonicwall.

ERRORES EN LA ESTRATEGIA

Los departamentos de TI tienen ante sí varios retos y, para superarlos, todos pasan por establecer una correcta estrategia, antes de incorporar una amalgama de soluciones que posiblemente no cubran sus necesidades. Esa estrategia pasa tanto por la prevención como por la defensa, teniendo en cuenta que el perímetro ya no existe y los ataques pueden provenir desde diferentes fuentes y lugares.

Para Isabel López, B2B Tech Solutions Manager de Samsung, el primer error radica en no implementar una estrategia, "en pensar que no necesitamos esa estrategia de seguridad, o que el malware a no nosotros no nos va a tocar. Tenemos que saber lo que ocurre en el mercado. Partiendo de saber lo que es necesario, debemos establecer unos mecanismos preventivos para protegernos contra el ataque. Es necesario prevenir, ejecutar y tener un plan de contingencia para cubrir cualquier problema y recuperarse con el mejor impacto".

Por su parte, Sergio Martínez, Iberia Regional Manager de

Sonicwall añade que el negocio del ciber crimen se estima que esta ya superando al propio del narcotráfico a nivel mundial, "hay miles de marketplaces en la deepkweb. Se calcula que solo el 5% de los cibercriminales son detenidos. Los mayores errores que se comenten se pueden centrar en que ha habido un alto cambio de paradigma, por lo tanto, las estrategias ya no son las mismas que las del pasado. Lo más importante es que estas estrategias estaban destinadas a prevenir y detectar, hay que dar un salto a poder responder. En la respuesta es donde fallan las empresas. Hay que prestar mucha atención en este nuevo paradigma a las amenazas encriptadas".

Siguiendo con el tema, Miguel López, Country Manager de Barracuda destaca que hay algo evidente, y es la falta de estrategia, "en muchas ocasiones incluso cuando hay estrategia, no se incluyen todos los elementos legacy, pues es una estrategia global, y no securiza los elementos nuevos, como podrían ser los de la nube. Otro de los fallos que vemos es el no incluir elemento humano, hay que formarles adecuadamente, para ue exista un nivel mínimo de conocimiento. Hay un error común que es considerar la ciberseguridad como un coste".

Mientras que Joaquín Gómez, Cybersecurity Lead para el Sur de Europa de Infoblox, explica que no tener una estrategia propia es uno de los errores más comunes, "estamos muy influenciados en las tendencias, y en las estrategias que vienen de los fabricantes. Hay que crear cada propia estrategia. Se ha abandonado un poco la prevención, y nos hemos ido mas hacia un modo reactivo, hay que invertir en ser predictivo. Otro fallo es pensamos estrategias de ciberseguridad, pero hay que invertir en visibilidad. Es un primer paso muy importante. Así como la operación, que debe ir hacia un modelo de automatización".

PRINCIPALES RETOS DE SEGURIDAD

Para el Cybersecurity Lead para el Sur de Europa de Infoblox los mayores riesgos a los que se enfrentan las compañías es en la parte de la operación de seguridad, "vemos que las compañías han invertido mucho, pero no han sabido como operarlas. Cuando quiero abordar la implementación de lo que he comprado, es muy difícil operarlo para que sea eficiente. Hay que invertir en la mejora de la respuesta del equipo de operaciones de seguridad como concepto. Hay que intentar adelantarte a la amenaza. Entendemos que lo mas importante es no abandonar y monitorizar los primeros pasos de los ciberdelincuentes. Y es que hay 180mil nuevos dominios al día, y el 85% según estadísticas son maliciosos. Si consigo cortar la infección desde su presencia, puedo estar mas relajado en su respuesta. Hoy en día, es imposible creer que con un proveedor voy a tener la protección completa. Hay que invertir en inteligencia de distintos sectores, y en tener una visión unificada".

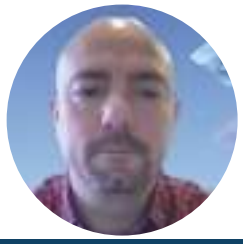
En palabras del Country Manager de Barracuda, lo que preocupa a las empresas es el temido ramsonware, "es el término de moda, a pesar de no ser algo super sofisticado. Preocupa por que es un tipo de ataque que se da con mucha frecuencia. En cualquier tipo de ataque hablamos de malware. Un reto importante son los diferentes objetivos que tienen cada departamento, cada uno los persigue, y muchas veces no existe la capacidad de poder hacer una implementación completa de todos los departamentos. La prevención es muy importante y debe incluirse en un ciclo continuo, tenemos que ser capaces de saber que por muchas medidas que tomemos puede haber un incidente, hay que tener los protocolos y políticas necesarios para poder reaccionar. Debemos de saber responder a cualquier tipo de amenaza".

El Iberia Regional Manager de Sonicwall destaca que los primeros meses del 2022 el ransomware descendió un 23%, "los ataques van más dirigidos a monetizar. Se están atacando a las aseguradoras para saber que empresa puede pagar el rescate. Ha crecido el malware en un 11%, así como los elementos de intrusión. Lo que más preocupa son las amenazas encintadas, que crecen a triple dígito desde hace años. Es una autopista de entrada del malware en las compañías".

Por su parte, la B2B Tech Solutions Manager de Samsung recalca que uno de los retos es recuperarse del ataque dirigido, "desde Samsung seguimos apostando por la innovación en términos de seguridad, en los últimos lanzamientos nuestros terminales ya traen un elemento seguro embebido en el terminal, que nada tiene que ver con el chip principal. Es un smartcard, donde se almacena la información mas sensible. Es necesario trabar desde el punto de vista de reto como em-

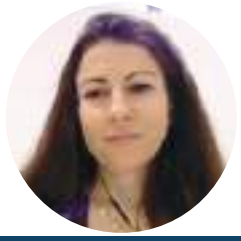
LOS PARTICIPANTES

Miguel López, Country Manager de Barracuda

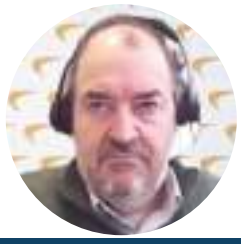


Joaquín Gómez, Cybersecurity Lead para el Sur de Europa de Infoblox

LOS PARTICIPANTES



Isabel López, B2B Tech Solutions Manager de Samsung



Sergio Martínez, Iberia Regional Manager de Sonicwall

presas, y utilizar el aislamiento de la información para protegernos".

QUÉ SOLUCIÓN ESCOGER

El departamento de TI tiene una gran cantidad de soluciones a su disposición. El problema llega cuando no se sabe por cuál optar. Para resolver esta cuestión, Isabel López explica que lo primero a tener en cuenta es conocer los activos de la empresa, "es decir, que podemos proteger, y valor lo que nos ofrece cada solución. Tener control de los endpoints, y por supuesto, que la solución esté respaldada por un partner serio, profesional con conocimiento, que nos garantice que nuestra organización va a estar protegida con lo que estamos adquiriendo". En esta misma línea, Sergio Martínez comenta que hay varios objetivos a tener en cuenta para seleccionar una estrategia, "hay que construir una defensa por capas, donde vayamos construyendo desde el perímetro hasta el endpoint. La siguiente es la visibilidad central para detectar y poder responder, si nuestra defensa de capas no está coordinada, no sirve para nada. Además, hay que tener la capacidad de detectar lo desconocido, pues el 80% del tráfico está encriptado. El 4 paso, sería el acceso remoto seguro, para dar seguridad a la hibridez, con dobles o triples factores. Por último, un dato a tener en cuenta es el TCO".

Miguel López, coincidiendo con sus compañeros, destaca la simplicidad, "al final, tenemos diferentes estrategias y hay que considerar múltiples vectores y tecnologías. Muchos responsables de IT la capacidad que tienen de digerir las nuevas tecnologías que se van creando, hace que sea muy difícil una respuesta rápida. Es muy importante el transmitir la sensación de poder acometer todo esto pero con simplicidad. Lo ideal sería implementar una solución sencilla, que se sepa manejar, y que sea eficiente".

Para finalizar con esta cuestión, Joaquín Gómez dice que lo primero que hay que hacer a la hora de elegir una solución, es ver que hace el cliente, "muchas empresas tienen mas capacidades de las que realmente están explotando. Además, la defensa debe estar por capas, pero estas capas debe prevalecer. Cuando elijo una solución u otra no tienen que ser las capas del mismo fabricante, porque si la plataforma falla, fallan todas las capas. Por su parte, la Inteligencia de Amenazas es esencial, esto va a ayudar a proteger la empresa".

FALTA DE PERFILES ESPECIALIZADOS

La única solución para acabar con la falta del talento especializado, en palabras de Joaquín Gómez, es intentar optimizar las operaciones y los procesos de las amenazas, "estamos viendo que los partners pueden ayudar, pero da igual que las operaciones estén en el cliente, porque todas tienen el mismo problema. Hay que reducir el coste y el tiempo de reacción. Necesitamos una herramienta de investigación para investigación, con el objetivo de saber a donde va la información de la amenaza y cómo actúa". Mientras que por parte de Miguel López, lo básico es implementar políticas de prevención y recuperación, "esto simplifica mucho la gestión, y evita movilizar una cantidad de recursos. Para hacer frente a esto debemos darle una gran importancia al Canal, que juega un papel esencial en esto. Tenemos que ser capaces de transferir nuestros conocimientos al canal, de forma que cada partner pueda coger las soluciones de cada empresa y adaptarlas al cliente. Las empresas deben buscar su canal de empresas especializadas".

Para Sergio Martínez el canal también es básico para las pymes, "para ser eficientes, las empresas deben ir transformándose en algún tipo de MSP, al final, para poder ser eficaces hay que desarrollar habilidades de este tipo, ya que el talento es ilimitado, y las pymes necesitan cada ves más su trabajo".

"La solución es contar con un partner que cubra las necesidades que tiene la empresa y ofrecer la solución que mejor se adapte, así como dar un soporte continuo. Sobretodo la formación, tanto de fabricante a canal, como de canal a la pyme o al cliente final, con el fin de que vaya cogiendo los conceptos y se van familiarizando con los servicios que se están explotando", finaliza Isabel López.

EMPRESAS PARTICIPANTES

BARRACUDA

El panorama actual de la ciberseguridad parece complicarse cada día. Surgen innovadoras amenazas y nuevos paradigmas se consolidan como el Zero Trust o el SASE. Ante esta circunstancia parece claro que las aproximaciones que consoliden la seguridad y la simplifiquen se hacen cada vez más necesarias. Cualquier estrategia de ciberseguridad actual debería considerar la necesidad de contar con soluciones que permitan la prevención, detección y respuesta frente a ataques, así como avanzadas capacidades de recuperación frente a los mismos. La gestión unificada y simplificada de entornos heterogéneos tanto on-premise como cloud junto con la incorporación de tecnologías Zero Trust y SASE nativas en el Cloud permiten disponer a los clientes de Barracuda de una herramienta integrada desde la que gestionar y proteger los principales vectores de ataque (web, mail, correo, dispositivos remotos, cloud,…) permitiendo el despliegue de una estrategia de ciberseguridad completa, sólida y coherente de manera sencilla y accesible.

INFOBLOX

Infoblox BloxOne Threat Defense es una solución de Ciber defensa basada en DNS e Inteligencia de Amenazas con datos curados y dominios emergentes, que además incluye una plataforma de "threat research" para investigación, contexto y atribución de estas. Es la perfecta combinación para ser vuestra Primera Línea de Defensa de cara a reducir el tiempo de detección y respuesta ante todo tipo de amenazas (Malware, Ransomware, Fuga de datos, comando y control…) desde cualquier dispositivo o infraestructura. Permite reducir muchísimas horas de innecesario tiempo en investigación por vuestros equipos SOC, obteniendo un retorno de la inversión claro, reducción de riesgos y ahorros en la operación.

SONICWALL

Nunca hemos estado tan expuestos, ni con una superficie de exposición tan elevada. Así, la construcción de una nueva ciberdefensa es necesaria, por capas, preparada para detectar todo tipo de ataques de corte conocido y desconocido, con visibilidad central para poder responder en tiempo real, y todo a un TCO asequible para una PYME. Y en todo este nuevo entorno, la puesta en marcha firewalls de nueva generación, puntos de acceso WIFI con capacidades de ciberseguridad, switches para segmentar la red, protección del correo electrónico y de las aplicaciones en la nube, y los antivirus de nueva generación, con capacidad de roll-back, como última línea de defensa. Todo ello, construyendo una defensa por capas inteligente, es fundamental para sobrevivir en este nuevo entorno tan hostil

SAMSUNG

Ayudar a los empleados a que su teléfono funcione de manera correcta, a navegar de manera segura, a acceder a datos corporativos sin temor a sufrir una pérdida de información confidencial, a tener su terminal configurado con las aplicaciones y opciones requeridas es posible. Para ello, Samsung pone a disposición de las empresas el conjunto de soluciones Knox Suite que permite aplicar seguridad, mantener los teléfonos actualizaciones con la versión del SO elegida, aplicar políticas de gestión y además, muestra al administrador un análisis sobre el comportamiento de los teléfonos de la compañía, a nivel tanto hardware como software. El equipo de Samsung puede ayudar a las empresas a elegir y configurar, con las políticas correctas, la solución que mejor se adapta a su negocio

Bases de datos

Las bases de datos se han convertido en una herramienta esencial para las empresas. A continuación, recogemos cinco propuestas de programas para crearlas explicando sus características y beneficios más importantes. Como suele ser habitual, se ha respetado en orden alfabético y por este motivo la comparativa abre con Claris FileMaker 19. Se trata de una plataforma enfocada en la creación de aplicaciones personalizadas disponible en dos versiones: una se despliega en un entorno cloud y la otra es para las compañías que prefieren la modalidad on premise; dentro de esta última hay varios productos, uno dirigido específicamente para dispositivos móviles con sistema operativo iOS para que los trabajadores no vean interrumpida su actividad.

Por su parte, IBM Netezza Performance Server es una base de datos analítica que puede desplegarse tanto en entornos cloud como en la plataforma Cloud Pak for Data on-premise en modo appliance. En este caso, la plataforma permite conectarse a los datos, controlarlos, gobernarlos y utilizarlos para el análisis, poniéndolos al servicio de los usuarios adecuados en cada momento. Además, estos pueden colaborar desde una interfaz común que da soporte a múltiples servicios. IBM Cloud Pak for Data puede desplegarse on-premise, en entornos cloud y como servicio gestionado. Le sigue InterSystems IRIS Data Platform, una plataforma de datos orientada a cloud que proporciona gestión de bases de datos multimodelo y multicarga de trabajo de alto rendimiento, smart data services, interoperabilidad y capacidades analíticas; todo ello, integrado desde cero en un único producto. Por su parte, Microsoft ha seleccionado su base de datos Azure Cosmos DB que incluye características como escrituras multi-región e integración con otros servicios de Azure como Kubernetes Services o Synapse Analytics, y compatibilidad con varios niveles de coherencia como eventual, prefijo coherente, sesión y obsolescencia entrelazada para una flexibilidad completa

Por último, la base de datos autónoma Oracle Autonomous Database proporciona un servicio de datos gestionado en la nube.

Claris FileMaker 19

Se encuentra disponible en dos modalidades, una basada en una implementación on-premise y otra en la nube para adecuarse a las necesidades de cada compañía.

Las empresas interesadas en la plataforma FileMaker tienen a su disposición dos opciones de implementación entre las que elegir, aunque la tecnología que hay detrás de ellas es la misma: una se basa en la nube y la otra se dirige a las organizaciones que desean tener sus bases de datos alojadas en sus instalaciones, es decir, que se trata de un modelo on-premise que incluye los productos Pro, Server, WebDirect y Go.

La primera de estas opciones, Claris FileMaker Cloud, reúne un conjunto de herramientas para que las compañías creen y compartan apps en la nube con sus equipos, pudiéndo integrarse con otras apps y servicios web. Enfocada a perfiles como usuarios empresariales, administradores de equipos, desarrolladores y personal de TI, la solución garantiza una implementación casi instantánea e incorpora además una consola unificada que ayuda a administrar usuarios y grupos de manera fácil. Con cifrado de extremo a extremo, certificados SSL integrados, cifrado automático de archivos, autenticación multifactorial opcional y copias de seguridad, la asistencia dedicada 24x7 garantiza que el rendimiento de la empresa no se vea afectado en ningún momento.

La solución provee asimismo notificaciones de actualización de software automáticas y ha sido diseñada para admitir inteligencia artificial, Machine Learning, Internet de las Cosas, realidad aumentada y virtual... Claris FileMaker Cloud facilita, incluso, utilizar servicios Web a través de una API REST para realizar tareas administrativas. También emplear las mismas credenciales para acceder a varias apps con un nuevo sistema de inicio de sesión único, entre otras características.

CLARIS FILEMAKER PRO 19

Claris FileMaker Pro 19, por su parte, permite a las empresas crear apps personalizadas para gestionar contactos, organizar proyectos, realizar un seguimiento del inventario o elaborar informes sobre la marcha. Una de las novedades que introduce esta versión es que ofrece una opción que se llama 'Apertura rápida' que establece una preferencia para abrir un archivo específico a la hora de inicio. Destaca, por otro lado, la característica JavaScript en un visor web para usar bibliotecas de JavaScript disponibles o con el propio código personalizado de la compañía para crear aplicaciones pudiendo insertar directamente elementos como mapas, gráficos animados, visualización de datos...

Claris FileMaker Pro 19 incorpora, asimismo, la opción de solicitar datos en formato JSON desde una aplicación FileMaker alojada localmente en FileMaker Cloud o FileMaker Server, y la posibilidad de ejecutar modelos de aprendizaje automático para, por ejemplo, clasificación de imágenes, detección de objetos y análisis de opiniones. Destacan también estas

otras características: instalador de MacOS Arrastrar y Soltar, y compatibilidad con macOS Dark Mode para que la herramienta se muestre con la apariencia elegida desde preferencias del sistema. Se ha previsto próximamente agregar más funciones a las aplicaciones como tableros kanban, galerías de fotos o generadores de códigos de barras, entre otros.

CLARIS FILEMAKER SERVER 19

Claris FileMaker Server es un software de servidor rápido donde alojar de manera local y segura las apps personalizadas de FileMaker para compartir desde cualquier dispositivo en tiempo real. Como característica complementaria, las organizaciones pueden integrar sus apps con los sistemas que utilice y tecnologías con las que cuente para garantizar la mejor disponibilidad.

Ahora, la plataforma permite ahora las apps en Linux (antes solo permitía en Windows y macOS) y crear ventanas con un tamaño automático y una ubicación adecuada en la pantalla principal. Esta característica recibe el nombre de Tarjetas en FileMaker WebDirect y permite, en otro orden de cosas, abrir ventanas u otros archivos sin tener que cerrar primero la tarjeta.

Claris FileMaker Go 19

En el caso de Claris FileMaker Go, disponible a través de la App Store para su descarga en dispositivos iPad e iPhone, las empresas tienen a su disposición una solución recomendada para los trabajadores que están fuera de la oficina. Además, si utilizamos Claris FileMaker Pro para crear

apps luego es posible acceder a ellas desde FileMaker Go. Precisamente, el producto FileMaker Go 19 comparte con FileMaker Pro 19 la ejecución de modelos de aprendizaje automático para clasificación de imágenes y detección de objetos, entre otros ejemplos. Se puede, por otro lado, utilizar la voz para ejecutar automatizaciones como buscar registros, iniciar un proceso o actualizar el inventario gracias a su compatibilidad con Siri. De igual forma, gracias a la lectura de etiquetas NFC se puede obtener información sobre productos etiquetados o dirigirse hacia un producto específico dentro de una base de datos.

CLARIS FILEMAKER WEBDIRECT 19

WebDirect se presenta como un cliente de Claris FileMaker utilizado tanto con Claris FileMaker Server como Claris FileMaker Cloud que permite a los usuarios interactuar con sus aplicaciones personalizadas en la web. En concreto, admite implementar una app personalizada para cualquier usuario con un navegador web compatible sin necesidad de utilizar herramientas de creación de páginas web u otras tecnologías. O implementar una aplicación web ocultando y bloqueando la barra de menús y la barra de herramientas de estado.

Claris

Teléfono: 93 272 62 00
Web: www.claris.com/es
Precio: 16€ usuario/mes

InterSystems IRIS Data Platform

Proporciona gestión de bases de datos multi-modelo y multi-carga de trabajo de alto rendimiento, smart data services, interoperabilidad y capacidades analíticas.

Desarrollada en torno a una base de datos de alto rendimiento, es idónea para crear soluciones que necesitan gestionar grandes volúmenes de datos complejos; análisis en tiempo real de datos históricos y transaccionales; procesamiento de transacciones de alto rendimiento; y consultas a alta velocidad en diferentes tipologías de datos.

Entrando en detalle, InterSystems IRIS DATA Platform -que se integra en las infraestructuras existentes y soporta una amplia gama de entornos y requisitos- ha sido dotada de una base de datos multi-modelo; escalable horizontalmente; y que almacena y tiene acceso a datos modelados como objetos, datos sin esquema, datos relacionales y arrays multidimensionales en una representación única. Además, procesa de manera simultánea cargas de trabajo transaccionales y analíticas a gran escala.

CARACTERÍSTICAS PRINCIPALES

Con varias opciones de despliegue entre las que elegir (en las instalaciones del cliente, en la nube a través de SaaS o por hosting, o en arquitecturas híbridas), la plataforma proporciona capacidades de análisis que permiten combinar las herramientas y tecnologías favoritas de cada organización para explorar datos, business intelligence, realización de predicciones y análisis eficaz de flujos de datos.

Por otra parte, y gracias a su conectividad abierta basada en estándares, IRIS DATA Platform puede conectar y aprovechar herramientas avanzadas y estándares analíticos incluyendo Apache Spark, PMML (Predictive Model Markup Language) y UIMA, (Unstructured Information Management Architecture).

Sus características incluyen también soluciones con un análisis embebido en tiempo real para datos estructurados y no estructurados, mientras que a nivel de seguridad autentica y autoriza a los usuarios a través de contraseñas. De igual forma, admite la autenticación de dos factores, soporta el estándar OAuth, y asegura datos en reposo y datos en movimiento a la vez que minimiza la carga en el rendimiento de la aplicación. Al reducir la complejidad de la gestión del sistema, rebaja los tiempos de inactividad, tanto los previstos como los imprevistos.

VENTAJAS MÁS IMPORTANTES

Como herramienta que provee de todas las capacidades críticas para el desarrollo rápido de aplicaciones de uso intensivo de datos y de misión crítica (incluyendo gestión avanzada de los datos, la interoperabilidad, el procesamiento de las transacciones y el análisis), la plataforma brinda al ámbito empresarial varios beneficios como, por ejemplo, un motor de base de datos de alto rendimiento que permite aplicaciones transaccionales y analíticas en tiempo real que eliminan latencias y proporcionan información y acciones inmediatas a partir de los datos transaccionales y contextuales.

En otro orden de cosas, como las

aplicaciones de InterSystems IRIS necesitan menos código, recursos del sistema y mantenimiento, esto evita que se deban utilizar múltiples tecnologías de integración. La transparencia también es importante, al integrarse en las infraestructuras existentes y contar con tecnología capaz de soportar una amplia gama de entornos de clientes y requisitos de aplicación. Como plataforma escalable vertical y horizontalmente, esto le ayuda a ajustarse tanto al crecimiento de las cargas de trabajo como al volumen de datos y número de usuarios simultáneos.

AUMENTO DE LAS CAPACIDADES ANALÍTICAS

Los lanzamientos recientes de InterSystems IRIS DATA Platform incluyen nuevas capacidades y mejoras que aceleran y simplifican la creación de arquitecturas Smart Data Fabric, incluidos Embedded Python e IntegratedML, facilitando así la colaboración entre analistas y científicos de datos: esto significa que mientras que los analistas de datos que operan con inteligencia de negocio (BI) pueden desarrollar mediciones, dimensiones y etiquetas ajustadas a las necesidades del negocio, los científicos de datos que operan con inteligencia artificial (IA) pueden utilizarlas de inmediato. Por otra parte, los modelos de Machine Learning , creados por los científicos de datos, están disponibles directamente para los analistas para su utilización en paneles, informes y aplicaciones; esta funcionalidad conecta la IA y el BI sin necesidad de mover los datos, agilizando las operaciones y ofreciendo información en tiempo real a la empresa.

Además, se han realizado mejoras en Adaptive Analytics, que ofrece capacidades de autoservicio, permitiendo que los usuarios de negocio exploren libremente los datos, hagan consultas ad hoc y profundicen en los hallazgos iniciales con consultas adicionales. Asimismo, se han mejorado el rendimiento y la escalabilidad para gestionar casos de uso de análisis transaccional de alto rendimiento.

Cuando se integran en data fabric, estas capacidades de análisis sitúan lo 'inteligente' en el enfoque arquitectónico de 'Smart Data Fabric' de próxima generación que defiende InterSystems. Al hacerlo, tanto los usuarios comerciales como los científicos de datos se benefician de una amplia gama de capacidades analíticas integradas que incluyen exploración de datos, inteligencia comercial, procesamiento de lenguaje natural y aprendizaje automático.

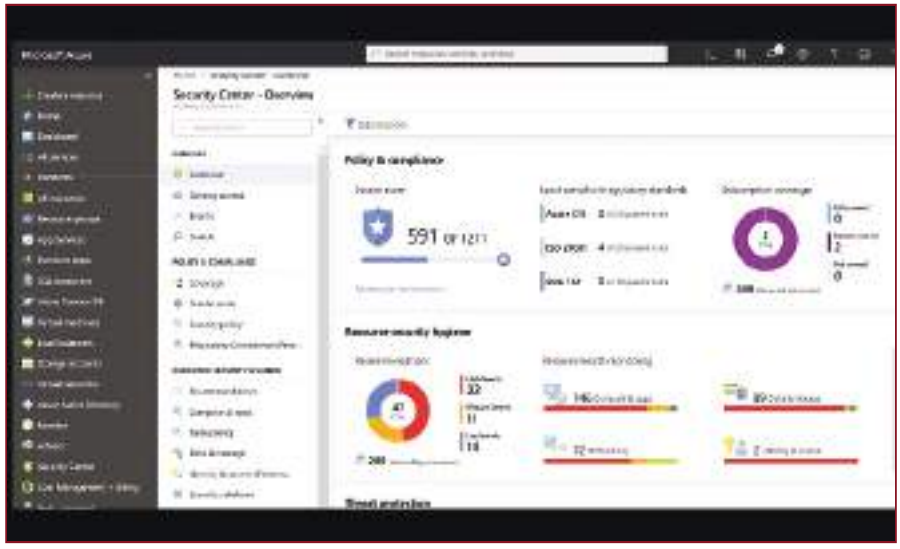
Para finalizar, añadir que InterSystems ha anunciado una asociación con Collibra, una plataforma de inteligencia de datos creada para el gobierno, la calidad y la privacidad. La integración entre las dos plataformas ayuda a que las compañías aprovechen estas capacidades ampliadas en datos que residen en cualquier lugar de la organización.

InterSystems

Teléfono: 91 484 18 80
Web: www.intersystems.es
Precio: 544 € por usuario

Microsoft Azure Cosmos DB

Garantiza lecturas rápidas y escrituras en cualquier lugar, así como numerosas APIs de consulta que proporcionan la flexibilidad necesaria en función del caso de uso.



Azure Cosmos DB es una base de datos relacional y NoSQL totalmente administrada para el desarrollo de aplicaciones modernas de alto rendimiento de cualquier tamaño o escala. Con tiempos de respuesta de milisegundos de un solo dígito -según indica su desarrollador- y escalabilidad automática e instantánea, las novedades introducidas recientemente son dos. De un lado, destaca la expansión de su disponibilidad geográfica, escalabilidad y distribución. De otro, el nuevo soporte de base de datos distribuido para PostgreSQL, el popular motor de base de datos de código abierto. Esto significa que ahora los desarrolladores de PostgreSQL pueden aprovechar la velocidad, la escala y el rendimiento de Azure Cosmos DB para acceder a datos estructurados y no estructurados en un servicio de base de datos familiar.

Entre las soluciones que se benefician de la herramienta desarrollada por el Gigante de Redmond destacan las aplicaciones del Internet de las Cosas y telemática, para dispositivos móviles, juegos, y comercio minorista y de marketing, entre otros.

BENEFICIOS A DESTACAR

Dentro del contexto de estas aplicaciones, su desarrollo más rápido y productivo se debe a tres elementos clave: la distribución de datos entre varias regiones 'llave en mano' en cualquier parte del mundo, las API de código abierto y los SDK de código abierto para lenguajes populares. Esto se traduce en una serie de ventajas principales como, por ejemplo, un acceso en tiempo real con latencias globales de lectura y escritura rápidas, rendimiento y coherencia, todo ello respaldado por distintos acuerdos de nivel de servicio. También escrituras en varias regiones y distribución de datos en cualquier región de Azure con tan solo un botón.

Se garantiza, por otro lado, la continuidad empresarial con un 99,99% de disponibilidad, rendimiento, latencia baja y coherencia para todas las cuentas de una sola región, y la reducción del tiempo en tareas de gestión y de mantenimiento: en este caso, Cosmos DB gestiona todas las actualizaciones y operaciones de escalado de forma transparente. Otro de los beneficios a destacar es la implementación de la indexación automática de los datos sin esquema que ayuda a reducir los tiempos de consulta, así como la integración con otros servicios de Azure como Functions (provee de la infraestructura y recursos necesarios para la ejecución de aplicaciones), Synapse Analytics (enfocado en tareas de análisis, reúne el almacenamiento de los datos empresariales y el análisis de macrodatos) y Azure Kubernetes

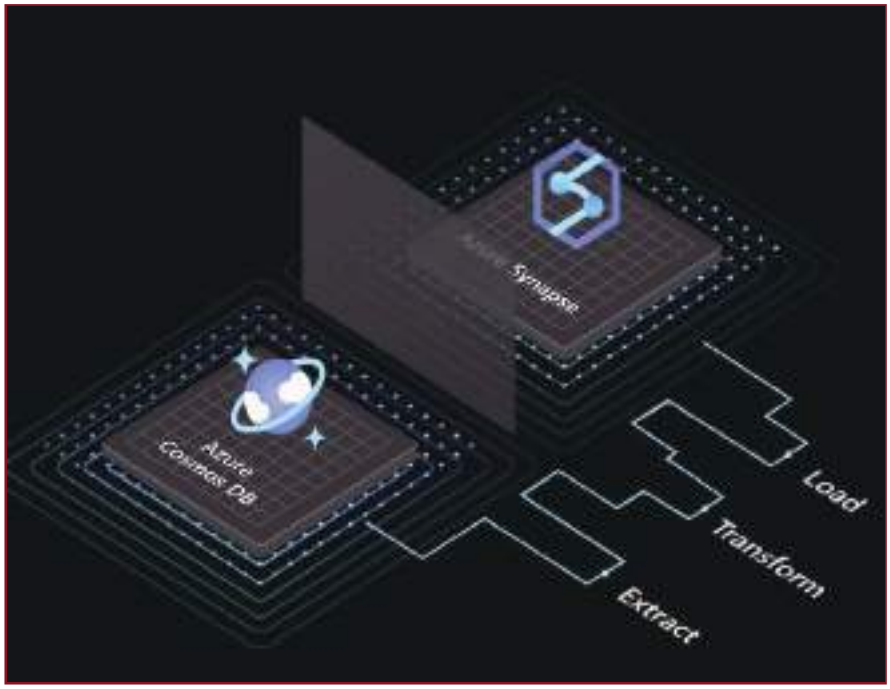
Service (para la administración automatizada y la escalabilidad de clústeres de Kubernetes).

LA SEGURIDAD

Desde el punto de vista de la seguridad, el cifrado en reposo se encuentra disponible tanto para los documentos como para las copias de seguridad almacenadas en Azure Cosmos DB en cualquiera de sus regiones. Así, este reposo se aplica de manera automática, sin necesidad de configurar nada, tanto a los nuevos clientes como a los ya existentes: se emplean para ello claves administradas y existe la alternativa de agregar una segunda capa de cifrado.

A nivel de seguridad, Microsoft Azure Cosmos DB ofrece también a los entornos empresariales otras medidas importantes como la autorización. Consiste en que cada solicitud se cifra mediante la clave de cuenta secreta, y el hash codificado base64 subsiguiente se envía con cada llamada a Azure Cosmos DB. De este modo, para validar la solicitud, el servicio Azure Cosmos DB emplea la clave secreta y las propiedades correctas para generar un valor hash para luego comparar el valor con el que muestra la solicitud. Si los dos valores coinciden, la operación se autoriza correctamente y se procesa la solicitud. Si los valores no coinciden, se produce un error de autorización y se rechaza la solicitud.

En otro orden de cosas, es posible crear recursos de usuario y de permiso por base de datos; aplicar replicaciones locales y globales; efectuar copias de seguridad en línea automatizadas; o usar los registros de auditoría y los registros de actividad para supervisar la actividad normal y la anómala de su cuenta, entre otras opciones.



TAMBIÉN DE INTERÉS

Para utilizar Cosmos DB hay que indicar una cuenta dentro de un grupo de recursos de Azure y, a continuación, crear la base de datos y los contenedores correspondientes dentro de esta misma cuenta; una cuenta que contiene un nombre DNS único que se puede administrar mediante Azure Portal, la CLI de Azure, Azure PowerShell o cualquiera de las API de REST o del SDK de administración de Azure.

En una sola suscripción de Azure es posible contar con un máximo de 50 cuentas de Azure Cosmos DB. A su vez, para administrar los datos y el rendimiento aprovisionado, se puede crear una o varias bases de datos dentro de la cuenta y luego uno o varios contenedores para almacenar los datos. Hay que tener presente que estos contenedores poseen un conjunto de propiedades definidas por el sistema.

Microsoft

Teléfono: 91 391 90 00
Web: www.microsoft.es
Precio: consultar

Oracle Autonomous Database

Entre sus últimas novedades destacan las innovaciones en las bases de datos para simplificar el desarrollo y mejorar la protección de las aplicaciones de misión crítica.

Se trata de una base de datos autónoma que automatiza el ciclo de vida completo de operación y gestión de los datos más críticos utilizando para ello mecanismos basados en Machine Learning (ML). Además, es capaz de reducir los costes de explotación hasta en un 90% -según indica Oracle- al automatizar múltiples tareas y puede operar de forma nativa con diversos tipos de datos, tanto relacionales como documentales, grafos o geoespaciales.

CARACTERÍSTICAS PRINCIPALES

Oracle Autonomous Database se ejecuta de forma nativa en Oracle Cloud Infrastructure y proporciona un servicio de datos gestionado en la nube que permite gestionar cargas de trabajo transaccionales y analíticas. Provista con características de autogestión (automatización del aprovisionamiento, ajuste y escalado de las bases de datos), a nivel de seguridad protege automáticamente los datos confidenciales y regulados, aplica parches a la base de datos para evitar vulnerabilidades de seguridad e impide accesos no autorizados.

Por otra parte, las capacidades de autorreparación que incorpora le sirven para detectar y proteger (también automáticamente) las bases de datos contra fallos del sistema y errores de los usuarios. También proporcionar conmutación automática a las bases de datos de reserva en caso de fallo sin pérdida de datos.

ÚLTIMAS NOVEDADES INTEGRADAS

Fue a mediados del mes de octubre del año pasado cuando Oracle anunció la última versión de su base de datos. Destaca por ofrecer nuevas y avanzadas capacidades que permiten un importante avance en la productividad de los desarrolladores para las aplicaciones escritas con JSON, Graph o microservicios, al tiempo que mejora SQL para que sea aún más fácil de usar, y añade JavaScript como lenguaje de procedimientos almacenados. Introduce, asimismo, un nuevo enfoque llamado JSON Relational Duality para abordar el desajuste entre cómo las aplicaciones representan los datos y cómo las bases de datos relacionales los almacenan. De igual modo, simplifica el desarrollo de las aplicaciones al 'soportar' que los datos se utilicen simultáneamente como documentos JSON de fácil uso para las aplicaciones.

En el caso de una de sus herramientas asociadas, Autonomous Data Warehouse (optimizada para el procesamiento analítico), sus creadores han introducido nuevas capacidades para que las organizaciones mejoren la colaboración entre equipos compartiendo datos con el protocolo de código abierto Delta Sharing y modelos de negocio mediante vistas analíticas en la base de datos. Junto con el soporte integrado existente para Oracle Analytics y herramientas como Tableau, hay disponible un

nuevo complemento para Microsoft Excel y una herramienta de integración de datos completa e integrada con Transforms. Además, los nuevos Oracle Application Accelerators para Oracle E-Business Suite proporcionan modelos de datos, KPI e integración de datos listos para usar.

Otra de las novedades es Transaction Manager for Microservices Free (ahora gratuito para su uso por parte de posibles clientes, desarrolladores y estudiantes) que permite el uso de transacciones distribuidas en aplicaciones basadas en microservicios desplegadas en Kubernetes. Los clientes pueden, de este modo, crear una transacción global que incluya múltiples microservicios desarrollados en varios lenguajes de programación y en diferentes plataformas de aplicación. A todas estas nuevas características se suman otras de interés como la disponibilidad de un nuevo componente de aprobación de flujos de trabajo para integrar la gestión de las tareas en las aplicaciones APEX, un tipo de herramienta enfocada al desarrollo rápido de aplicaciones. Además, los desarrolladores tienen ahora acceso a integraciones listas para usar con aplicaciones y datos de terceros, lo que proporciona una plataforma de desarrollo de aplicaciones más rica.

BENEFICIOS A DESTACAR

En cuanto a sus ventajas, Oracle Autonomous Database utiliza el aprovisionamiento y el ajuste automáticos para simplificar la creación y optimización de todos los almacenes de datos en la nube. Esto significa que se encuentra preparada para comenzar con el coste y el compromiso mínimos, escalando automáticamente a medida que crezca la organización. A nivel de seguridad, los datos confidenciales se protegen usando la encriptación por defecto, siempre activa, y facilitando el cumplimiento normativo con Oracle Data Safe, un servicio en la nube de seguridad de bases de datos que se incluye con Autonomous Database. La actualización de las sucesivas versiones no significa que el servicio se pierda, al contrario, se mantiene.

En otro orden de cosas, el acuerdo de nivel de servicio de disponibilidad del 99,95% de Autonomous Database incluye el ciclo de vida completo del servicio de base de datos. Se proporcionan, de igual modo, acuerdos de nivel de servicio de principio a fin con respaldo financiero que cubren el rendimiento, la disponibilidad y la capacidad de administración de los servicios.

En el caso de la solución Autonomous Data Warehouse (antes indicada) la creación y evaluación de modelos de aprendizaje autónomo incluye capacidades de Auto-Machine Learning. Esto, unido a los algoritmos analíticos y de Machine Learning embebidos en la propia base de datos, acelera el rendimiento y evita el trasiego de datos entre sistemas.

Oracle

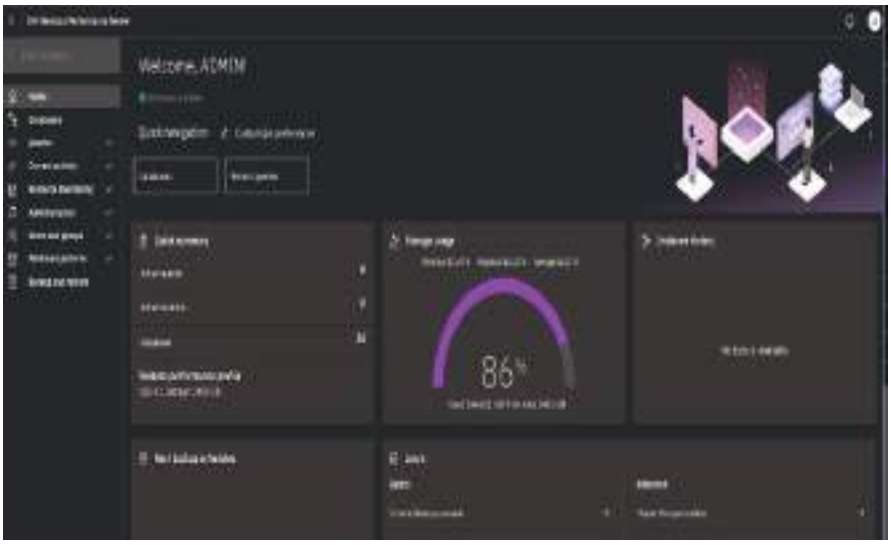
Teléfono: 902 302 302
Web: www.oracle.es
Precio: consultar

IBM Netezza Performance Server

Una base de datos analítica que puede desplegarse tanto en entornos cloud como en la plataforma Cloud Pak for Data on-premise en modo appliance.

El nuevo Netezza Performance Server se encuentra disponible como un servicio totalmente gestionado listo para utilizarse tanto en Microsoft Azure como en modo 'Tech Preview' dentro de Amazon Web Services (AWS). El servicio gestionado permite, a este respecto, desplegar un entorno analítico de forma sencilla y rápida, garantizando a su vez un escalado flexible y granular con funciones de pausa y reanudación para controlar costes y recursos según las necesidades de rendimiento de cada empresa.

Por otro lado, dado que el nuevo Netezza está disponible en IBM Cloud, AWS, Azure y Cloud Pak for Data System, esto facilita que las compañías pongan en marcha sus estrategias de multicloud híbrido de manera flexible y sin renunciar a su alto rendimiento; en este caso, IBM Netezza Performance Server para IBM Cloud Pak for Data se presenta como una plataforma de almacenamiento y analítica de datos avanzada disponible tanto en modo local como cloud. Así, dentro de este contexto y gracias a las mejoras realizadas en las funciones analíticas dentro de la base de datos, Netezza facilita que las organizaciones accedan a ciencia de datos y aprendizaje automático con volúmenes de datos que llegan a medirse en petabytes.



CARACTERÍSTICAS Y BENEFICIOS

Como herramienta de análisis, Netezza Performance Server posee la capacidad de asegurar una alta disponibilidad gracias a sus características de detección y recuperación rápida de anomalías. De igual modo, ofrece las funciones de realojamiento en el cloud y la virtualización de datos: con la primera, se brinda una actualización única de la línea de comandos de control a los sistemas actuales mientras que la segunda hace referencia a su capacidad para realizar búsquedas en varios sistemas al mismo tiempo.

En lo que respecta a sus beneficios, la plataforma de IBM brinda a las organizaciones una serie de ventajas que se pueden agrupar en tres puntos principales. El primero está relacionado con las actualizaciones: en este caso, es totalmente compatible con cargas de trabajo en Twinfin, Striper y Mako. El segundo aspecto está relacionado con un coste de la propiedad bajo (la administración y el ajuste continúo son mínimos) y el tercero con la eliminación de los silos de datos que enlaza con lo antes comentado, la virtualización de los datos para las búsquedas en varios sistemas.

IMPLEMENTACIONES

Dado que cada empresa tiene unas necesidades diferentes a

cubrir, es posible elegir entre varias implementaciones. Una de ellas es el sistema hiperconvergente para una implementación rápida en un sistema preconfigurado con almacenamiento, computación, redes y software. En un cloud privado, Netezza está integrado en IBM Cloud Pak for Data System, una plataforma de datos e inteligencia artificial nativa en cloud que combina los elementos citados en nodos plug and play para agilizar esta implementación. Ésta, que se presenta como una solución completa e integral de entramado de datos local en cloud híbrido, ha sido provista de un único panel de control para simplificar las tareas de gestión y supervisión.

Es posible, en otro orden de cosas, agilizar la obtención de información mediante los paneles de control de IBM Cognos Analytics junto con las prestaciones de virtualización de datos y bases de datos. También acceder de manera rápida a los datos y mitigar los problemas de calidad; conectar e integrar datos fácilmente en todos los clouds; y fusionar los datos y los servicios de inteligencia artificial con IBM Watson Studio para crear y preparar estos datos para luego desplegar modelos y gestionarlos a escala. El sistema, que está basado en Red Hat OpenShift Container Platform, combina almacenamiento, cálculo, red y software en nodos de tipo conectar y listo para poder escalar fácilmente según las necesidades de su negocio. Por otro lado, y para acelerar el despliegue de modelos y llevarlos a producción más rápidamente, es posible incrementar el rendimiento con las bibliotecas de deep learning y machine learning existentes; ambas, bibliotecas ajustadas al sistema.

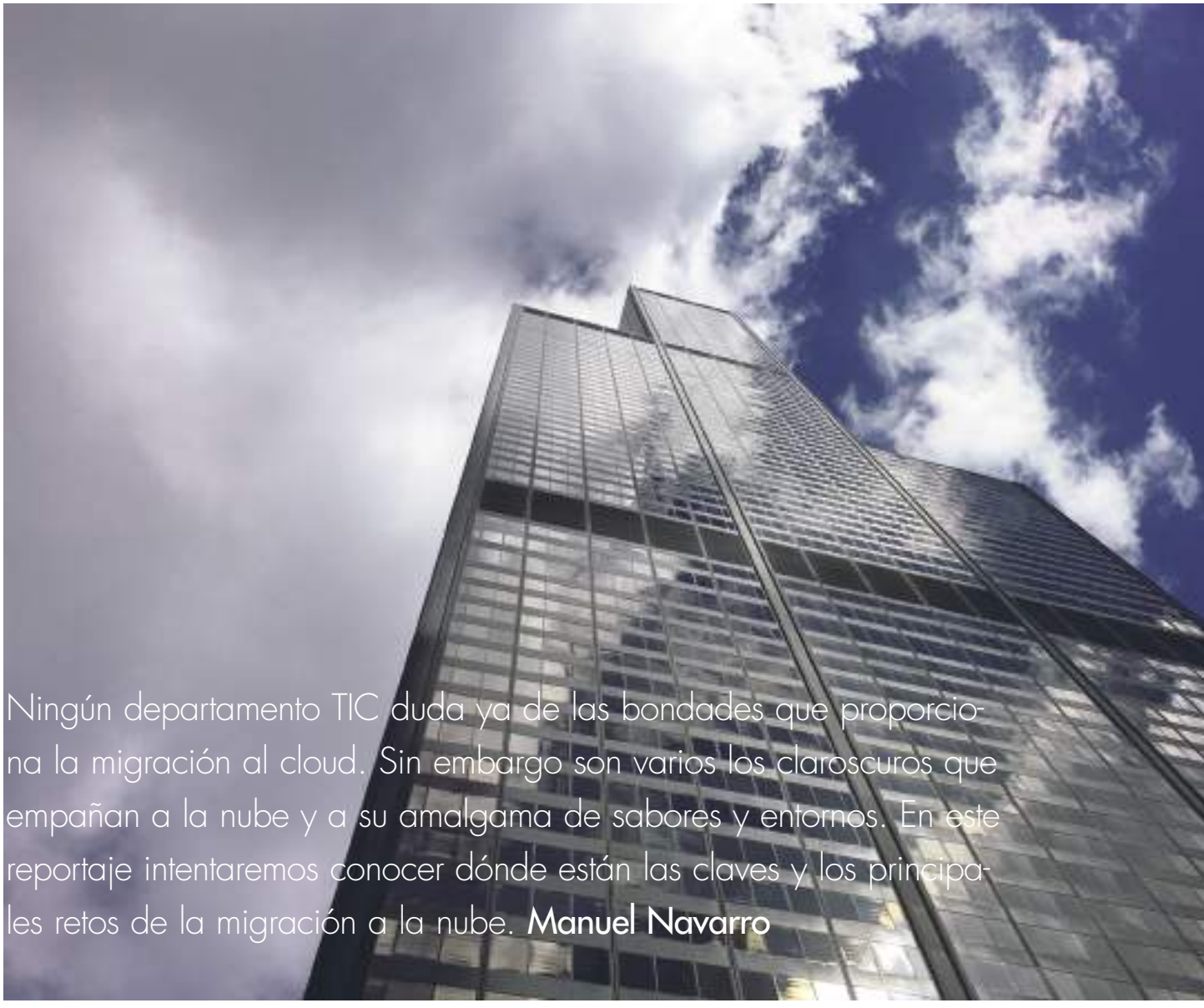
La segunda implementación hace referencia a la opción de servicio gestionado para optimizar el rendimiento con un despliegue flexible y autoservicio incluido que incluye un perfil de costes predecible tanto en Microsoft Azure como en Tech Preview en AWS.

La tercera y última implementación está vinculada a la nube pública y significa que IBM Netezza Performance Server para IBM Cloud Pak for Data está disponible en IBM Cloud, AWS y Microsoft Azure. Aquí, Netezza Performance Server se presenta como un sistema de datos con inteligencia artificial incorporada basado en estándares que integran -además de las capacidades propias de las bases de datos- servidor, almacenamiento y análisis avanzado en una plataforma fácil de administrar. Se basa en IBM Red Hat OpenShift (una de las plataformas de Kubernetes para empresas que existen) y está optimizado para tareas análisis de alto rendimiento.

IBM

Teléfono: 91 397 66 11
Web: www.ibm.es
Precio: consultar

Los **desafíos** que plantea **la nube**



Ningún departamento TIC duda ya de las bondades que proporciona la migración al cloud. Sin embargo son varios los claroscuros que empañan a la nube y a su amalgama de sabores y entornos. En este reportaje intentaremos conocer dónde están las claves y los principales retos de la migración a la nube. **Manuel Navarro**

Las empresas y los organismos públicos empezaron a abrazar la nube mucho antes de que apareciera la pandemia. La seguridad, que era uno de los principales frenos para migrar al cloud dejó de serlo atraídas las empresas como estaban por un modelo de costes hiperreducido si se comparaba con los costes que traía consigo cualquier solución on-premise. La pandemia, lo que hizo fue acelerar los procesos. Se puede decir que tras la aparición del coronavirus, las organizaciones comenzaron a descubrir nuevas ventajas además del precio. Entre otras, la escalabilidad o la flexibilidad. Las bondades de la nube empiezan a estar tan asimiladas que tal y como apunta la consultora IDC, cualquier acción que se lleve a cabo en un departamento de TI se realiza bajo un enfoque cloud. Y no parece que ese enfoque vaya a detenerse, toda vez que la propia consultora establece que de aquí al año 2025 se producirá una tasa de crecimiento anual compuesto de 21,9% en este ámbito, y que para ese año, el 55% de las organizaciones habrán migrado sus sistemas de protección de datos a un modelo centrado en cloud para gestionar todos los datos de forma centralizada desde la nube.

Si nos centramos en el ámbito privado, cada vez son más las empre-

sas que están dando el salto a la nube. Pero, a pesar de lo que pudiera parecer, todavía hay organizaciones que mantienen sus viejos sistemas on-prem, por mucho de que los cantos de sirena para realizar una migración sean constantes. Y es que, tal y como indica Pablo Boixeda, Solutions Engineer, Sr. Manager Iberia e Italia de Cloudera "casi la totalidad de las compañías es consciente del potencial de la migración por temas de agilidad o ahorro de costes, pero todavía tenemos empresas rezagadas a causa de barreras como la capacidad o la complejidad de la implementación. No obstante, la balanza se inclina hacia lo positivo, y quien no está ya inmerso en el proceso, está a punto de hacerlo o con el planteamiento estratégico encima de la mesa".

Entre esa serie de empresas que aún se muestran reticentes se encuentran las medianas y, por supuesto, las más pequeñas. En este caso, como apuntan desde Seidor, "la evolución en la migración a los entornos cloud en la pequeña y mediana empresa se encuentra en una fase muy incipiente. Sin embargo, entre las de mayor tamaño, la migración a la nube se sitúa en una etapa más avanzada". No obstante y, tal y como aseguran desde este integrador, también depende en gran medida de los servicios de los que se hable. "Por ejemplo hay una serie de servicios que ya están en entornos de cloud en un porcentaje muy elevado, como, por ejemplo, el correo electrónico. Pero, en términos generales, aún sigue habiendo una gran cantidad de compañías que tienen todo o parte de sus sistemas core en un modo on-premise. Éste es el motivo por el cual la adopción de la nube, por parte de las empresas españolas, continuará creciendo en los próximos años", aseguran desde la firma.

Noel Bravo, director de servicios cloud y alianzas de Kyndryl considera que "la adopción de la nube por parte de las empresas es buena y ha ido evolucionando a buen ritmo. En los últimos años, las empresas han desplegado la mayoría de sus nuevos proyectos en cloud, eso sí, es ahora cuando las grandes compañías y los organismos públicos han empezado a plantearse de verdad migrar el core de su negocio y sus entornos de misión crítica al cloud de manera masiva, una tarea que se debe realizar con máximas garantías de eficiencia y de seguridad, para lo que necesitan el apoyo de proveedores con una gran experiencia en estos entornos".

Y es que, lo de contar con un partner que apoye y esté pendiente de que la migración se realice de forma correcta y exitosa es uno de los grandes problemas que han tenido las empresas. Sobre todo aquellas que empezaron a mover cargas a la nube hace varios años. En muchos casos vieron como ese movimiento

no les proporcionaba las ventajas que prometía. Básicamente esto se producía porque no se contaba con ese partner que apoyara la migración y que diseñara la estrategia de forma correcta, por lo que en muchos casos, se añoraba cuando se trabajaba bajo el modelo onpremise. En muchos casos, además toda la migración se realizó de forma muy apresurada, por lo que los errores que se cometían eran constantes. Pero, poco a poco, la situación está cambiando y es que, tal y como afirma Carolina Mulero, Release Train Engineer en Wolters Kluwer, "en estos momentos, nos encontramos en un proceso de cambio; la digitalización acelerada que provocó la pandemia está cristalizando en una transformación de los modelos de negocio en un sentido muy amplio. La migración a la nube se enmarca en este contexto de transformación: el mercado avanza hacia el cloud y todos los actores se están adaptando –con diferentes ritmos– a esta nueva realidad que ahora ya se percibe como un imperativo para ser competitivo en el mercado. Y en este sentido, es importante contar con un partner estratégico como Wolters Kluwer que les acompañe en este proceso de cambio".

La realidad es que las organizaciones han tenido que agilizar muchas de sus gestiones para poder mantener la interacción con sus empleados y el servicio a los clientes sin perder el negocio y el día a día. Incluso las pymes, más reticentes hasta no hace mucho tiempo a implementar procesos de digitalización se han dado cuenta de que es un proceso irreversible que les va a ayudar a crecer y a escalar de forma más eficiente.

¿Qué es lo que motiva ese cambio de mentalidad para apostar por los modelos cloud. Juanjo García, director de la unidad de negocio Cloud de Microsoft cree que "en la actualidad, las organizaciones se han dado cuenta de que su futura viabilidad pasa por el análisis y la explotación de los datos a gran escala. La implementación del Big Data y la Inteligencia Artificial a través de la nube permiten extraer conclusiones, cruzar datos, enriquecer modelos analíticos para dar respuesta a necesidades más concretas e, incluso, realizar predicciones. Por ello nos encontramos diferentes estadios de la migración al cloud, que van desde la utilización de las herramientas de colaboración y productividad hasta el desarrollo de soluciones a medida con plataformas como PowerApps o el uso de Inteligencia Artificial para acelerar y optimizar procesos de negocio. Hay compañías que necesitan implementar el trabajo híbrido, otras que necesitan beneficiarse de una gestión de cliente más eficaz u otras que requieren replantear sus costes de infraestructura".

CLOUD Y EL VIL METAL

Como decíamos al comienzo de este artículo, la migración a la nube en las empresas, empezó por un motivo fundamental: el ahorro de costes. Justo coincidió con la crisis del año 2008 con lo que una tecnología que permitía importantes ahorros en momentos en los que la caja de las empresas no fluía a todo ritmo, siempre era de agradecer. Poco a poco, aspectos básicos y que

> Cualquier estrategia de migración a la nube debe llevar asociado un plan de transformación Cloud que identifique objetivos

no representaban un valor importante para el negocio, se fueron migrando a la nube. Hoy la percepción empieza a ser la contraria: son numerosos los CIOs y responsables de TI que se quejan de los costes que tiene la nube. Muchos de ellos, afirman que en muchos casos se tratan de costes ocultos de los que nadie informó cuando se estaba contratando el servicio. Y el problema con el que se encuentran es que ahora no se puede cambiar de proveedor de forma sencilla. Muchos aseguran que la nube es el nuevo on-premise y que no sólo les cuesta mucho tener que justificar al Comité de Dirección por qué se producen determinados cosas y lo que es peor, por qué es una tarea casi imposible cambiarse de proveedor.

Félix Casado, CEO de Virtual Cable cree que "este cambio de opinión se produce al pasar de la teoría a la práctica, al recibir las facturas mensuales y descubrir los costes ocultos derivados de la complejidad de los modelos de facturación de la cloud. Un despliegue dimensionado de forma errónea puede incrementar el coste esperado en miles de euros si, por ejemplo, el cálculo de capacidad de cómputo y almacenamiento necesaria es erróneo, o si se dejan encendidas las máquinas cuando no se están utilizando con la idea errónea de que al ser un servicio virtual no conlleva costes. Por otra parte, no hay que olvidar que los costes se han incrementado, y que la mejor manera de obtener rentabilidad es aprovechar las inversiones ya realizadas. ¿Por qué subir todas nuestras cargas de trabajo a la nube cuando tenemos una infraestructura on-premise infrautilizada? ¿No sería más lógico sacar el máximo partido a lo que ya tenemos y utilizar la nube para gestionar picos de demanda o para garantizar la continuidad del negocio? En definitiva, la opinión acerca de la rentabilidad de la nube es fruto de un análisis previo erróneo de la estrategia cloud de la compañía, muchas veces provocado por unos modelos de costes complejos proporcionados por los ISPs2".

Igual que AWS y Google, Microsoft es una de las compañías que dominan el mercado de la nube. Al trío le suelen achacar buena parte de sus males, además de acusarles de monopolizar el mercado. Juanjo García, de Microsoft, considera que el problema de los CIO es que "han de entender la digitalización como un proceso continuo, en el que la nube sea un aliado para ser más eficiente, mejorar la capacitación digital de los empleados, conectar los equipos, y ganar en agilidad y seguridad. Desde su posición debe tener una visión global, no solo centrada en los sistemas e infraestructuras de su empresa, sino con una mentalidad abierta a la innovación capaz de analizar las tendencias de mercado para implementar soluciones integrales y transversales a toda la organización. Un motivo importante que puede ocasionar que los CIO consideren que la nube no es tan rentable como esperaban puede venir derivado de la complejidad en algunos entornos para gestionar y garantizar la

seguridad de la plataforma con los estándares oportunos. En este sentido, desde Microsoft contamos con propuestas enfocadas precisamente a unificar y simplificar la gestión. Es el caso de Azure ARC, nuestro servicio para proteger recursos de infraestructura en todos los entornos cloud, incluidos despliegues multicloud o escenarios híbridos que conservan servidores on-premises. Con su ayuda, las organizaciones pueden aplicar políticas de cumplimiento y seguridad, automatizar tareas de gestión y operaciones, y obtener una visibilidad centralizada de sus recursos en todos los entornos, todo ello, reduciendo sus costes operativos".

Alejandro Solana, director técnico de Nutanix cree que "como en cualquier otra decisión trascendental de negocio, el movimiento a cloud ha de ser la respuesta a las necesidades y expectativas reales de las aplicaciones y los datos relevantes que tenga sentido cubrir en cada empresa. Por ejemplo, ciertos tipos de aplicaciones no están pensadas para ser ejecutadas en la nube pública y, debido a su consumo de recursos, tiene más sentido llevarlas a entornos tradicionales. Plantear una migración de estas aplicaciones a la nube pública supone un coste significativo y, a la larga, ha generado proyectos de repatriación para devolver estas cargas a entornos "on-premise". Para garantizar la rentabilidad de cualquier proyecto de migración a la nube, es fundamental la fase de análisis, un momento crítico en el que es necesario optar por la aproximación más adecuada según la arquitectura de las aplicaciones. Además, debería-

mos intentar simplificar y plantear una aproximación operacional única y estándar para nuestro entorno multi-cloud, de otra forma estaríamos convirtiendo a las distintas nubes públicas en nuevos silos, añadiendo complejidad en la gestión de cada entorno, y por tanto, incidiendo en el coste. En definitiva, toda empresa debe tener en cuenta tres aspectos fundamentales para garantizar un proyecto de migración a la nube pública de manera efectiva, segura y rentable: las personas, que habitualmente están acostumbradas a hacer las cosas de una manera y que necesitarán aprender nuevas formas de trabajar, los procesos y la tecnología. Empezar por este último aspecto sin tener en cuenta los demás, ha sido probablemente el problema más significativo al que se han enfrentado muchas organizaciones".

Los motivos de las quejas, el sector tecnológico lo achaca a diferentes causas. Por ejemplo, David Mañas, VP Cloud Infrastructure & Cibersecurity Services de T-Systems cree que uno de los motivos de esas quejas puede venir motivado porque "si simplemente movemos workloads del Cloud privado al Cloud público y no realizamos ajustes en la arquitectura o el modelo de servicio. Es muy posible que el movimiento no sea rentable. La rentabilidad hay que buscarla aplicando las ventajas que el Cloud público nos ofrece, como el sizing dinámico, ajustes horarios, migración de componentes a Cloud native, etc…".

Quizá uno de los problemas de esta situación es haber trasladado las cargas a la nube sin establecer una estrategia previa. También que, de repente, los departamentos de TI han empezado a trabajar con diferentes proveedores y en diferentes entornos de nube. Gestionar todo ello, también se ha vuelto más complicado, por lo que aquella empresa que tenga presencia en todos los proveedores y ofrezca la posibilidad de manejarse con una plataforma entre nubes de forma sencilla, tiene todos los visos de llevarse una buena parte del negocio del futuro. Eso es algo que ya observó VMware hace unos años y que lleva tiempo trabajando por hacer que la nube sea mucho más sencilla. Por eso, Ignacio Arrieta, Solutions Engineering Director de VMware, pone claro que " la nube pública tiene una característica propia, y es su relación directa entre lo que consumes y lo que pagas. Si consumes poco pagas poco, si consumes

mucho pagarás mucho. Cuando consumes mucho, la economía de escala hace que sea rentable repensar tu modelo de nube, yendo hacia arquitecturas donde puedas tener lo mejor de las nubes públicas (elasticidad, servicios avanzados de datos) y lo mejor de las nubes privadas (control de coste, soberanía). En VMware tenemos todas las piezas para la construcción de este tipo de plataformas". Este directivo señala que muchos de los problemas con los que se encuentran las organizaciones parten de un diseño de estrategia erróneo. "Muchas empresas, incluso a nivel departamental, han ido adoptando modelos cloud sin una estrategia clara y una visión de futuro. Eso genera descontrol. Los stacks tecnológicos de cada uno de los hiperescalares no son compatibles entre sí, lo que potencia la creación de silos y genera problemas de control, de costes, de seguridad, pero también los derivados de tener los datos repartidos en diferentes contextos. Uno de los retos está relacionado con las plataformas de gestión de la nube. Se trata de contar con un plano de control que permita abstraerse de la infraestructura subyacente y que, los equipos de tecnología puedan, independientemente de la infraestructura, observar desde un único lugar, todas sus aplicaciones y proporcionar recursos en función de reglas de negocio. Otro error habitual es no pensar en la reversibilidad o plan de salida cuando se plantean arquitecturas en la nube. La clave es tener la posibilidad de elegir lo bueno de cada nube de una manera sencilla, segura, controlando los costes, y con una visibilidad de conjunto de toda de toda la tecnología de la empresa".

ESTABLECIENDO LA ESTRATEGIA CLOUD

No parece una labor sencilla adoptar esa estrategia cloud, sobre todo con todo el legacy que poseen muchas empresas. No hay una fórmula mágica, pero sí hay que tener en cuenta determinados puntos. Para Santiago Sánchez, Advisory Solution Architect de Dell Technologies "a la hora de establecer una estrategia en torno al cloud, lo primero es recabar información de empresas que se encuentren en una situación similar (o con socios tecnológicos fiables) para anticiparse a posibles contingencias. A continuación, hacer un análisis por proyecto o por entorno, tanto técnico como económico (recordemos que lo primero suele estar incluido en lo segundo) y fijar unas expectativas realistas. Implantar siempre la solución contando con equipos humanos adecuados para este tipo de proyectos o bien contar con empresas que tengan una experiencia comprobable en este tipo de actuaciones, para facilitar su puesta en marcha y (en su caso) traspasar la gestión de esos entornos al personal de la organización de una manera adecuada".

En realidad, de lo que se trata es de que la estrategia Cloud debe llevar asociado un plan de transformación

Cloud y una identificación de los objetivos que esta migración persigue. Desde Seidor afirmas que "este plan de transformación debe analizar las diferentes aplicaciones y necesidades para poder realizar un salto a la nube, de forma ordenada y correcta, y adaptarse a los objetivos marcados. Dentro de la estrategia también es esencial la identificación de los riesgos y las posibilidades de actuación frente a los mismos. Es decir, para tener una estrategia efectiva es básico tener claro los objetivos, los riegos y una planificación e implementación cuidadosa, que permita abordar el proyecto de forma ordenada. En esta estrategia, otro punto importante es la elección de proveedor, desde el punto de vista del hiperescaler y también desde el punto de vista del integrador que pueda acompañar al cliente en la transición".

Si bien, elegir (mal) un proveedor es uno de los errores más habituales hay varios más. Así desde Virtual Cable, su director general asegura que "el mayor error se está cometiendo cuando se decide migrar a la nube sin estudiar a fondo las necesidades reales de cada grupo de usuarios dentro de una organización. El escritorio en la nube no deja de ser una extrapolación del VDI on-premise y se rige por el mismo dilema, la Cloud/VDI es para todas las organizaciones, pero no para todos sus usuarios. Si tenemos una infraestructura on-premise, conviene determinar si puede seguir dando soporte a parte de los usuarios, si ese es el caso, debemos considerar aprovecharla al máximo y configurar solo desbordamientos automáticos a la nube cuando se agoten los recursos on-premise. También podemos combinar despliegues on-premise con cloud, derivando a la cloud solo a aquellos perfiles que necesiten recursos de los que no disponemos on-premise. La clave es optimizar nuestros sistemas, de manera que podamos ajustar el gasto todo lo posible".

Para Carolina Mulero de Wolters Kluwer, la parte positiva es que los errores de antaño ya no se cometen. En su opinión, "Al inicio, los principales errores residían en que las empresas no estaban preparadas para el cambio desde un punto de vista cultural y tampoco contaban con un equipo técnico suficientemente formado para ello. Otro de los puntos negativos durante los primeros años fue la urgencia por migrar provocada por la necesidad del trabajo en remoto. Esto derivó en estrategias agresivas y aceleradas que, en la mayoría de casos, no fueron del todo satisfactorias. Sin embargo, estamos mejorando y cada vez las organizaciones están más maduras para gestionar su migración a la nube. Derivado de la criticidad del proceso, muchas compañías deciden contratar a expertos (interna o externamente) para llevar a cabo tanto la de-

finición de la estrategia como para posteriormente la implementación de la misma".

GESTIONANDO EL MULTICLOUD

Multicloud se ha ido imponiendo poco entre las empresas por diferentes motivos. Al final, precio, escalabilidad y flexibilidad harán que las empresas se decanten por un proveedor o otro. Pero eso trae consigo que al menos se trabaje con dos proveedores y por tanto, la gestión del entorno multinube se torna más compleja. La nube al final se convierte en todo lo que se odiaba del modelo onpremise: mala usabilidad, gestión compleja, creación de silos… Así que son varias las voces que empiezan a apostar por que se tengan todos los huevos en la misma cesta: es decir, "un único proveedor que se encargue de gestionar todo". Normalmente, todas esas opiniones vienen de un modo interesado, por lo que en general, los analistas y expertos señalan que contar con varios proveedores siempre ofrece mayores ventajas: sobre todo la de poder cambiar de proveedor si no se está satisfecho con el servicio que se ofrece. En este punto se sitúa el portavoz de Cloudera quien asegura que "tener distintas cartas sobre la mesa nunca es malo. Ahora bien, también hay que ser consciente de que no se puede – ni se debe – elegir algo porque sí, porque "esté de moda" o porque la competencia lo haya hecho antes. Hay que estudiar bien todo lo que ofrece este entorno y decantarse por aquello que realmente va a proporcionar beneficios".

Alejandro Solana, ha pasado por diferentes compañías y es todo un experto en la evolución cloud prácticamente desde que nació la terminología. Y sí cree que ahora mismo, los departamentos de TI están perdidos a la hora de gestionar los entornos cloud y de elegir entre la amalgama de proveedores y servicios que se les presentan. Pero conoce la solución al problema: "aquellas empresas que sigan considerando la nube como un destino tendrán que enfrentarse a los prejuicios: demasiada estandarización, complejidad, silos, etc. Sin embargo si la migración se plantea como la adopción de un nuevo modelo operacional (de multicloud híbrida), estaremos consiguiendo una mayor capacidad de elección, más flexibilidad y la personalización que muchas organizaciones de mayor tamaño requieren. El desafío al que deben hacer frente los negocios es el hacer convivir "pasado y futuro" de forma efectiva, aprovechando los beneficios de ambos modelos (la capacidad de personalización de los entornos on-premise tradicionales y la flexibilidad y escalabilidad de los modelos cloud), facilitando tanto la entrada como la salida a cada uno de ellos".

La cuestión es que como afirma el portavoz de Microsoft, "cada situación requiere de una solución específica para dar una respuesta óptima a las necesidades. Si hablamos de entornos híbridos, la mayoría de empresas pueden combinar el uso de IaaS, PaaS o SaaS. Por ejemplo, una empresa puede utilizar los servicios de Azure en modo IaaS para albergar bases de datos, pero también soluciones SaaS para las tareas administrativas o el uso de Microsoft Dynamics 365 Customer Service para la gestión de las relaciones con los clientes. En cuanto a diferentes proveedores o, incluso, la combinación de on-prem con cloud pública, como decía, es algo habitual y depende en gran medida de las necesidades específicas y estrategia de cada organización. En definitiva, no se trata de una elección binaria, por eso Microsoft Azure proporciona tantos "sabores" de nube como necesidades particulares tiene cada empresa, haciendo posible desplegar soluciones heterogéneas para permitir a cada organización contar con las mejores herramientas para centrarse en su misión y lograr sus metas. De hecho, la clave está en algo que ya comentaba antes: Microsoft Azure ARC, nuestra solución para permitir a empresas administrar, monitorizar y controlar recursos de infraestructura en una amplia variedad de entorno, incluyendo multicloud con datos y servicios sobre las nubes de Amazon con AWS o Google con GCP".

En cuanto al futuro, parece claro que la nube va a seguir jugando un apartado fundamental en las estrategias de TI de las empresas. Pero para su gestión va a ir de la mano de nuevas tendencias. Y es que, como afirma Ignacio Arrieta de VMware, "Los motores de inteligencia artificial (IA) van a ser claves dentro de la estrategia cloud de cualquier empresa. Permitirán hacer mejores predicciones, anticipar los cambios o entender mejor lo que ha pasado. En el futuro, la inteligencia artificial hará posible que, de forma automática, las aplicaciones se puedan mover de una nube a otro en función de reglas de negocio, de niveles de consumo de infraestructura o de su criticidad. Avanzamos hacia un mundo en el que la IA nos dirá que, atendiendo a una razón de negocio o de rendimiento, deberíamos mover una aplicación, y esta se moverá de forma automática con nuestra aprobación; o detectará un evento de seguridad y recomendará cambios en las reglas para evitar esa exposición… Eso no está tan lejos, no es ciencia ficción. En un horizonte de dos o tres años estaremos viendo muchas de estas cosas".

Michelle Linares,
Chief Operations Officer de TheCUBE

Fecha de nacimiento: 26/07/1995
Hijos: no
Hobbies: Wakeboard, Kitesurf y Pádel
Estudios: Ingeniería Industrial

¿Cómo llegó al sector TIC?
Tenía 16 años cuando elegí mi carrera profesional y en ese momento solo tenía claro dos cosas, me quería dedicar a crear cosas nuevas y a hacer negocios. Luego de descartar otras carreras, me decidí por una ingeniería. Me encantaba la idea de que fuera desafiante como carrera y era justo lo que buscaba, al final ingeniería viene de la palabra ingenio, la capacidad de inventar nuevas cosas y la ingeniería industrial además tenía ese componente de negocio que buscaba. Y a día hoy sigo convencida de que fue la mejor decisión que pude haber tomado, me creó un modelo mental sistemático y totalmente extrapolable a cualquier disciplina.
Al cuarto año de carrera, me fui a Italia, hice un año en el Politecnico di Milano y confirmé mi deseo de vivir en Europa. En el 2017, me mudé a España a hacer mi master en Diseño e Innovación enfocado en Productos y Servicios Sostenibles.
Al finalizar el máster, tuve la oportunidad de entrar en una gran corporación y darme cuenta, por suerte, que no era mi camino. Lo mío era la innovación, la tecnología y las startups. Busqué de quien aprender, era lo que quería, encontrar gente que estuviera en este mundo y aprender de ellos. Así es como a finales del 2018 encuentro a Alberto, Fabiola y Diego, emprendedores en serie, que habían creado Unlimiteck, donde lanzaban sus propias startups tecnológicas y tenían un departamento de Open Innovation, que apenas empezaba. Aún recuerdo mi primer día, no me equivoqué, estaban desarrollando cosas impresionantes. Aposté por lo que me apasionaba, desarrollamos TheCUBE y hoy en día llevo las operaciones de este ecosistema de innovación que ayuda a las grandes empresas a resolver sus retos mediante la innovación radical, y crear un planeta más accesible y sostenible.

¿Qué es lo que más valora de su trabajo?
Algo que me encanta, es que por lo general en otras empresas se motiva poco el proponer nuevas ideas y por lo tanto la gente que destaca, es esa que es valiente, insiste y lograr proponer cosas nuevas. En TheCUBE, ese es nuestro día a día, es nuestro trabajo, en el mundo de la innovación radical vivimos enfrentandonos a una constante hoja en blanco, que nos exije si o si, pensar de otra manera, proponer cosas nuevas y además hacer que pasen, y eso hace la diferencia.

En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?
Para empezar, hoy en día hay más mujeres que nunca estudiando carreras STEM. Un buen inicio sería dar a conocer las que ya hacen parte de este sector, las que tienen y están creando carreras profesionales brillantes. Al final, uno de los principales problemas es la falta de referentes, y no me refiero a que no hayan mujeres muy cracks, porque las hay, pero no las han dado a conocer lo suficiente.
Por otro lado, es importante saber que también se puede cambiar de profesión y entrar en este mundo sin haber estudiado una carrera STEM. Todas las experiencias hacen parte de un proceso de formación y te permiten adquirir habilidades que al final te ayudan en tu carrera. Si realmente quieres entrar en

el mundo tech, vas a ir aprendiendo y cada vez te va gustar más y te vas a formar más en el tema. Al final, es un sector apasionante, que combina innovación, creatividad y resolución de problemas.

¿Cree que existe el "techo de cristal" en las empresas TIC? ¿Cuál debería ser la solución?

He visto varias mujeres en las posiciones más altas de liderazgo en empresas TIC, sin embargo aún nos queda camino. Lo bueno es que ya se ven los resultados positivos, según la revista de Harvard, las empresas con más mujeres en puestos directivos son más rentables, más responsables socialmente y ofrecen experiencias de cliente mayor calidad, de hecho, pasar de no tener ninguna mujer en el liderazgo corporativo a una cuota femenina del 30% se asocia con un aumento de un punto porcentual en el margen neto, lo que se traduce en un aumento del 15% en la rentabilidad de una empresa típica. Además, en temas de atracción de talento, que varias empresas ya lo empiezan a sufrir, para las nuevas generaciones cada vez esto cobra más relevancia. La gente en posiciones de liderazgo, hombres y mujeres, tienen la responsabilidad de informarse sobre los beneficios tangibles de contar con una plantilla y un comité de dirección diverso.

¿Una política de cuotas puede resolver el problema?

No, una política de cuotas por sí sola no resuelve el problema de raiz. Creo que es una forma de aumentar en el corto plazo el número de mujeres que trabajan en una compañía, o que ocupan cierto cargo, sobre todo en sectores más tradicionales y menos diversos. Pero desde mi punto de vista, en algunos casos, puede llegar a ser contraproducente y en vez de ayudar, puede obstaculizar la inclusión. Se puede conseguir contratar a mas mujeres o gente perteneciente a una minoría, pero esto no garantiza necesariamente que vayan a recibir un trato justo una vez contratadas.

¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?

Desde que entré a TheCUBE, como becaria en el 2018, sabía que la empresa tenía mucho potencial y que me iba a llevar tan lejos como yo quisiera. Llegué cuando eramos dos personas y ahora somos un equipazo de más de 30, he tenido la fortuna de trabajar en proyectos con empresas de tanto nivel como Mercedes-Benz, Enel, Ikea, Pfizer y muchas más. Además en proyectos de innovación y tecnología, testeando y lanzando nuevas ideas al mercado e impactando en la vida de las personas. He trabajado con compañeros estupendos, que me han enseñado un montón y hemos crecido juntos. Hemos llevado a TheCUBE a lo que es hoy, y solo puedo decir que estoy ansiosa por ver lo que vamos a conseguir en los próximos años en Europa, Latam y quien sabe donde más. Así que dificultades, por ser mujer en un sector tech, ninguna.

¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?

Siempre lo digo, de las cosas que estoy más orgullosa es del equipazo que hemos creado en TheCUBE, la densidad de talento es muy alta y la mitad somos mujeres. No ha sido algo a propósito, nunca hemos buscado cubrir cuotas. Pero hemos tenido la fortuna de que así sea y que además se queden y crezcan con nosotros. Esto es consecuencia de muchas cosas, pero sobretodo del ambiente y la cultura de TheCUBE.

En TheCUBE no buscamos gente experta, no nos importan los años de experiencia o los muchos diplomas que puedan tener, lo que buscamos es gente con ganas, actitud y ambición. Gente que no es conformista, que quiere hacer las cosas diferentes, gente que disfruta surfear el caos y con una constante sed por aprender.

En conclusión, la integración de la mujer que hemos tenido en TheCUBE es exitosa porque todas las personas, hombres o mujeres, brillantes, con ganas y disciplinadas son bienvenidas a crecer junto con TheCUBE.

"El futuro se encuentra en la nube híbrida"

¿A qué se dedica la parte principal del presupuesto de TI de la empresa?
Actualmente la mayor partida es para personal, con un 45% del presupuesto, el resto del presupuesto, a su vez, se distribuye entre Comunicaciones y Seguridad, Licencias y Servicios en la nube, y Hardware, en porcentajes bastante equilibrados.

¿En qué área se está invirtiendo más este año?
La principal línea de inversión para este año es en proyectos relacionados con la seguridad y con la estrategia, como por ejemplo la preparación a la ISO 27001, o el proyecto del Gobierno del Dato.

¿Qué proyecto es del que está más satisfecho?
El año pasado estuvimos inmersos en un proyecto de Restructuración del Departamento, que cambió a nivel sustancial nuestra forma de trabajar y de relacionarnos con los demás departamentos (áreas de negocio) de la universidad. Implantamos nuevas figuras, tanto dentro de TI como en los demás departamentos y áreas de la UCV, que sirven de cohesión entre el negocio y sus necesidades, y el Departamento de programación de la UCV. El proyecto, no sin dificultad, ha generado un mejor entendimiento dentro de TI respecto a las necesidades de las demás áreas, y por parte de estos últimos una mayor profesionalidad a la hora de pedir necesidades de programación. Asimismo, establecimos herramientas de control del tiempo y productividad, lo que nos da información de donde estamos invirtiendo mas esfuerzos de programación, para poder así analizar si esta alineado con la estrategia general de la universidad, y si no es así, poder rectificar y canalizarlos en coherencia con la misma

Si le pusieran todos los beneficios de la empresa a cargo del departamento de TI, ¿qué le gustaría implementar?
Nuestro departamento es un departamento interno de apoyo a las misiones principales de la universidad, que no son otras que la formación y la investigación, por tanto, estratégicamente nos debemos de alinear a esos objetivos y no pensar en implementar proyectos tecnológicos que sólo gusten al Departamento. Si fomentaría la innovación educativa, pero el impulso no debe nacer desde mi departamento, sino de la parte académica de la universidad.

¿La seguridad es un problema?
La seguridad es un problema, y a la vez una oportunidad. El pensamiento anterior de que tengo que hacer para que no me Hackeen, a día de hoy se ha convertido en que puedo hacer para que mi empresa pueda subsistir el día que lo hagan. Por supuesto debemos establecer las normas de seguridad para ponerlo difícil, pero sobre todo debemos de establecer los planes de contingencia para que, una vez haya pasado, sepa-

mos como reestablecer nuestros sistemas lo antes posible, generando los mínimos inconvenientes y daños posibles a la empresa. Por eso mismo, la seguridad es un problema al que nos debemos anticipar, y a su vez es una oportunidad para mejorar los métodos de trabajo y tener mayor capacidad de previsión cuando nos veamos comprometidos.

¿Se puede trabajar desde casa?
No veo ningún problema tecnológico al teletrabajo, la pandemia puso de relieve, que, pese a que no nos habíamos preparado, fuimos capaces de pasar a la modalidad de teletrabajo en un tiempo record.
Cosa diferente es si existen los procedimientos necesarios para el control de la productividad en el mundo del teletrabajo. En España, en muchas ocasiones, seguimos con la equivocación de que calentar el sillón es sinónimo de trabajar mucho. El teletrabajo es importante para la conciliación y optimización del tiempo, si bien, en su justa medida.
En nuestro caso, las herramientas de supervisión que hemos implantado para el control del tiempo e imputación de los desarrollos a cada Departamento nos servirían para gestionar correctamente el personal en teletrabajo, y se podría utilizar para gestionar la productividad, e incluso para premiar a los mejores trabajadores. No obstante, depende también del tipo de trabajo a realizar, y de los parámetros y directrices que tenga cada empresa. Hay que valorar también la importancia que, a mi juicio, tiene la presencialidad, o los entornos mixtos, como herramienta fundamental a la hora de hacer equipo

¿Qué tendencias principales observa en el mundo TIC?
Bueno, realmente creo que todos nos las sabemos ya casi de memoria: Nube y Virtualización. Pago por uso. Data Driven, empresas con decisiones basadas en datos. Gobierno del Dato e Inteligencia artificial yRobótica...Pero lo que también veo es que la legislación sobre todas estas nuevas realidades que genera la tecnología está dando ahora pasos muy grandes hacia delante con el RGPD, que esta totalmente vivo y pretende proteger a las personas del mal uso de la tecnología. La proactividad y privacidad desde el diseño se están convirtiendo cada vez vas en algo a tener muy en cuenta para protege las constantes vulneraciones de derechos.

Bajo ningún concepto en su móvil puede faltar…
El móvil lo uso principalmente para comunicarme, así que Mail, Teams, Whatsapp

¿Cuál es la herramienta que realmente le cambió la vida?
La primera que me impactó, favorablemente, sin duda fue Excel. A día de hoy, entiendo que las herramientas que más nos han cambiado la vida son todas las de Videoconferencia, ya sea, Zoom, Teams, Meet, etc…

¿Harto de solucionar los problemas tecnológicos de la familia y amigos? ¿Qué le suelen pedir?
La verdad es que, como hace muchos años que ya no estoy en el día a día de los problemas cotidianos, y debe ser muy evidente, excepto los muy cercanos no suelen pedirme muchas cosas. Con mi familia más cercana cualquier cosa es posible: no me conecta la wifi, no me va el correo, no consigo hacer este trámite... Pero en general, la mayoría de las veces son cosas que ellos mismo podrían hacer, aunque es más cómodo tener apoyo.

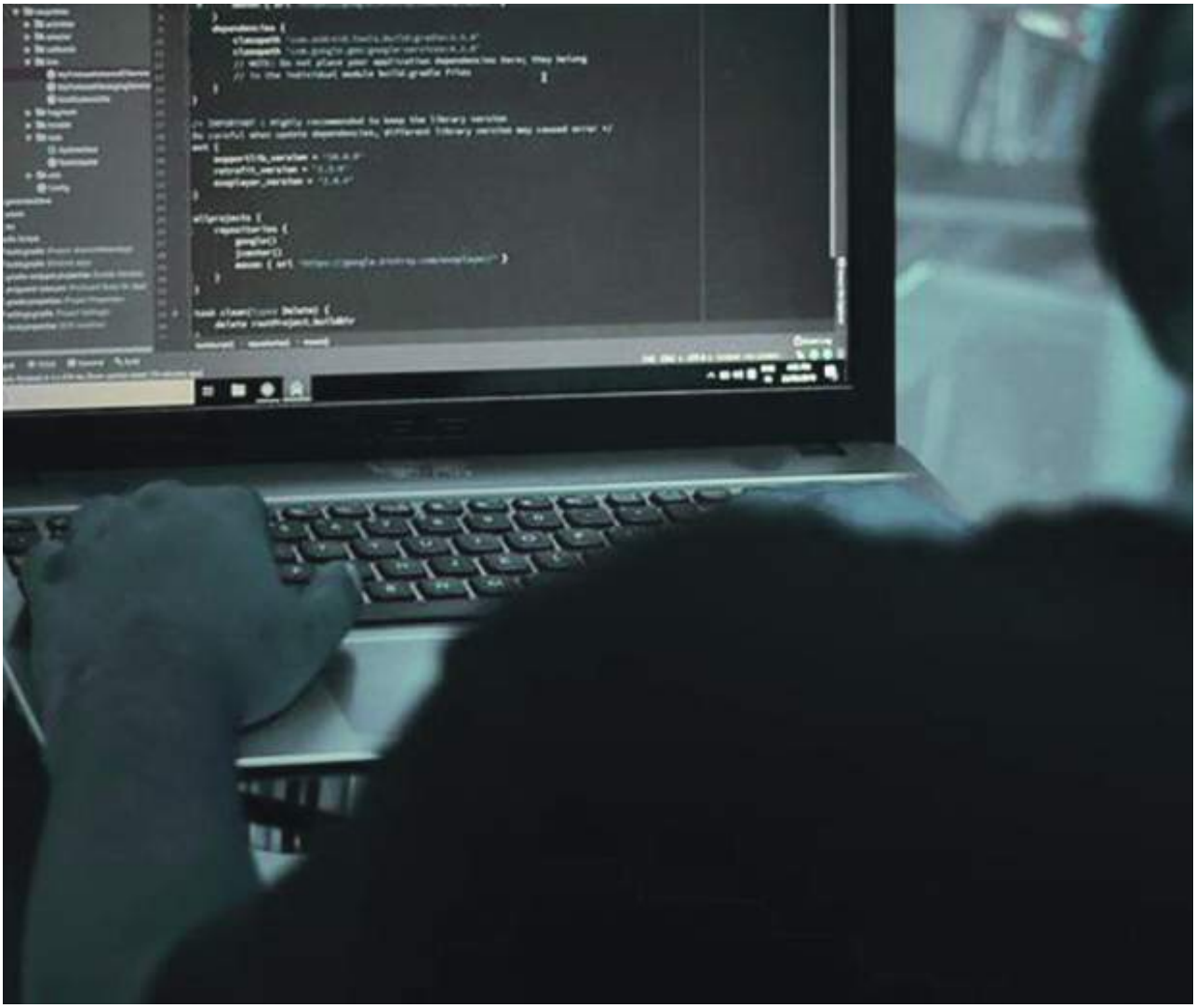
José Miguel Sánchez, Director TICs Aplicadas. Universidad Católica de Valencia

Lo de extraer el valor del dato, ¿supondrá de verdad la evolución de empresas como la suya?
Sí, aunque es un proyecto que solo tiene un pilar tecnológico, y realmente no es el más importante. Lo principal de ese proyecto, y de donde de verdad las empresas pueden sacar beneficios es en la estrategia y en el gobierno de esos datos. Mientras la parte de la empresa que genera y lidera el negocio no esté verdaderamente implicada y crea en él, este tipo de proyectos fracasarán. Nosotros hemos empezado este año con el proyecto y está liderado por alta dirección de la UCV, TI en este caso es un facilitador, no debe ser el protagonista.

¿Lo del I+D+i, es una leyenda urbana?
En nuestro caso es totalmente una leyenda. En la pandemia se dio un salto en innovación, pero no tanto en TI, pues las herramientas ya existían y estaban a nuestra disposición, sino el avance lo fue en el cambio cultural dentro de la empresa. Por lo general no somos pioneros en la i pequeña, sino que vamos acogiendo tecnologías ya probadas.

¿En la nube u on-premise?
El futuro no tengo ninguna duda que está en la nube, aunque igual no en una nube pura, sino en los entornos híbridos. Un equilibrio entre recursos en nube y infraestructura en local es para mí lo mejor. Con ello no quiero decir tener servicios en un sitio o en otro, sino tener duplicados y sincronizados los servicios.

Dos maneras distintas de luchar contra el crimen financiero



En pleno periodo navideño y en la misma Ley que modificara el delito de Malversación el 23 de diciembre de 2022, se traspuso a nuestro ordenamiento jurídico la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. El fraude y los medios de pago electrónicos son dos elementos que confluyen cada vez con mayor frecuencia y que de manera conjunta se han denominado Crimen Financiero.

Este tipo de conductas, muy vinculadas al blanqueo de capitales suponen grandes retos para las instituciones financieras y otros intermediarios del sistema financiero que se ven obligados a implementar todo tipo de controles para evitar que los defraudadores escojan su entidad para ocultar los activos provenientes del fraude.

OBJETIVOS

Lo que se pretende con esta reforma es dar un paso más para que no queden impunes algunas conductas propias del crimen financiero con una marcada dimensión transfronteriza por el hecho de no encontrarse recogidas en nuestro Código Penal.

El uso de identidades falsas, el robo de credenciales, o la ocultación de los fondos en todo tipo de activos digitales intangibles son algunas de las conductas que habitualmente forman parte de cualquier tipo de fraude, sin embargo, lo cierto es que el constante cambio de las tecnologías utilizadas para la comisión de este tipo de delitos y por lo tanto en las conductas que deben ser juzgadas, generaba grandes dificultades a la hora de encuadrar las mismas en nuestros antiguos delito de estafa y falsedad.

Con esta reforma se incluye una definición amplia del concepto de instrumento de pago distinto del efectivo con el objetivo de evitar que el uso de futuras tecnologías asociadas al fraude quede fuera de la misma. Según el artículo 399 ter de nuestro nuevo Código penal se entenderá por instrumento de pago distinto al efectivo todo aquel instrumento que permita transmitir un valor monetario.

Asimismo, cabe señalar que uno de los objetivos de la Directiva era incluir dentro del Código Penal de todos los estados miembros aquellos delitos que se cometen haciendo uso de medios de pago inmateriales que permiten efectuar transferencias de dinero electrónico, de monedas virtuales y otros criptoactivos, es decir de los Exchanges de criptoactivos. Esta reforma sin embargo no modifica el delito de blanqueo de capitales ni la responsabilidad de las entidades financieras que gestionan los distintos medios de pago.

REFORMA SOBRE EL ANTIMONEY LAUDERING ACT

Pocas semanas después de esa modificación, se aprobaba en los EEUU una nueva reforma sobre el Antimoney Laudering Act que persigue hacer aflorar todos los activos provenientes del crimen financiero cometido dentro y fuera de los EEUU y que utiliza el propio sistema para ocultar los activos de distintas maneras.

La reforma establece el pago de recompensas económicas a aquellas personas que alerten de incumplimientos del denominado BSA (Bank Secrecy Act) cuyo objetivo es obligar a las instituciones financieras a guardar registros de las transacciones superiores a 10.000 $ y reportar aquellas que sean sospechas de fraude, blanqueo de capitales u otro tipo de delito. En concreto el nuevo programa establece una recompensa mínima obligatoria del 10% y de hasta el 30% del capital recuperado a los denunciantes cuya información original de lugar a una acción que permita recuperar fondos de más de un millón de dólares.

INCUMPLIMIENTOS POR PARTE DE LAS INSTITUCIONES FINANCIERAS

En este caso por lo tanto para lograr descubrir actividades ilícitas en el entorno del sistema financiero se pone el foco en los incumplimientos de las propias instituciones financieras y sus empleados necesarios sin duda para que muchos de los crímenes financieros no sean descubiertos.

En un sentido similar llama la atención la sanción de 300.000 $ impuesta por la OFAC hace pocas semanas al conocido Exchange de criptodivisas Kraken por no contar con controles que alertaran del movimiento de fondos con Irán, país sancionado internacionalmente.

Con todo ello, se puede apreciar claramente como hay establecidas dos maneras muy distintas de luchar contra el crimen financiero. La primera de ellas es más propia de un sistema jurídico basado en el positivismo normativo mientras que la segunda de las opciones lo que intenta es la fórmula para buscar y encontrar aquellas soluciones que sean más prácticas, con el fin de conseguir los mismos objetivos que la primera de las fórmulas mencionadas.

César Zárate
socio de Écija Abogados

ASAC mejora la calidad del servicio a sus clientes con Paessler PRTG

Henkel ocupa posiciones de liderazgo tanto en negocios industriales como de consumo: en su cartera incluye productos tan conocidos como Loctite, Wipp Express, Somat o Cucal

TeamViewer, el proveedor mundial de soluciones de conectividad remota y digitalización del lugar de trabajo, ha anunciado que está optimizando el soporte remoto en el departamento informático de la empresa internacional de bienes de consumo Henkel. Gracias al paquete de herramientas de conectividad empresarial segura de TeamViewer Tensor, la empresa con sede en Düsseldorf (Alemania) ha podido simplificar su soporte informático interno global y hacerlo más eficiente.

CONEXIÓN TOTAL

La idea que tenía la multinacional era que todos los miembros del departamento de TI pudieran estar conectados en cualquier momento y sin importanr el dispositivo o el tipo de sistema operativo que estuvieran empleando.

La solución la enconytraron en la propuesta de TeamViewer y gracias a ella, los expertos informáticos de Henkel pueden ahora conectarse a todos los dispositivos de sus empleados, como portátiles, tablets y smartphones (en total 60.000 dispositivos en todo el mundo), independientemente del fabricante o del sistema operativo.

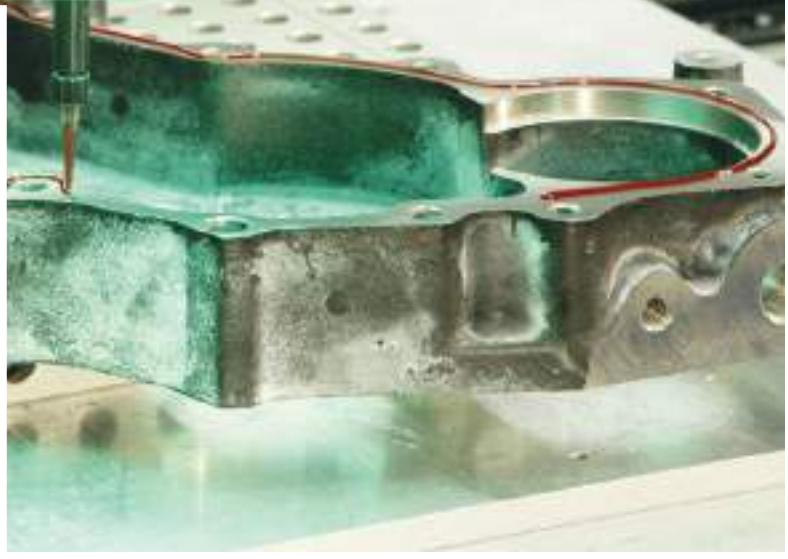
Una de las claves que motivó a Henkel a apostar por las herramientas de TeamViewer es la facilidad con la que se podía implementar la herramientas así como la facilidad de uso. De esta forma, la fácil implementación en los dispositivos, junto con la perfecta integración en el entorno informático existente de Henkel, sumado a las conexiones a ServiceNow, Microsoft Azure y Jamf, entre otros, jugaron un papel clave para decidirse al momento de decidirse por TeamViewer.

Otro de los apartados destacables es el que se refiere a la seguridad, dado que las empresas sufren cada día más ataques. En este sentido, la solución de TeamViewer cumple plenamente con las características de seguridad del sector, como el inicio de sesión único, una gestión de derechos expandible y flexible, y el cifrado de extremo a extremo.

SOPORTE MÁS EFICAZ

En este sentido, Adrian van Zyl, Product Owner Client & Mobility Operations de Henkel, afirma: "TeamViewer Tensor ha hecho que nuestro soporte informático sea mucho más eficiente. Nuestros empleados de todo el mundo utilizan una gran variedad de dispositivos y plataformas, que antes teníamos que gestionar con distintos programas. Ahora, con TeamViewer, tenemos una solución que cubre todas nuestras necesidades de mantenimiento remoto, mejorando así significativamente los flujos de trabajo de nuestros expertos en Tecnologías de la Información. Con esto, nuestro soporte informático central es ahora más seguro, sencillo y rápido". Por su parte, Jan Junker, Vicepresidente Ejecutivo de Ventas y Entrega de Soluciones de TeamViewer, explica: "Hemos adaptado TeamViewer Tensor específicamente a las necesidades de las empresas. La solución se puede modificar según sea necesario y permite acceder a los dispositivos y máquinas de forma rápida y sencilla desde cualquier lugar y en cualquier momento, con el fin de proporcionar soporte y mantenimiento. En tiempos de trabajo flexible, la escasez de competencias y la transformación digital en todos los niveles de la cadena de valor supone un verdadero cambio en las reglas del juego para los departamentos de IT."


LOCTITE



Cuatro claves para que el CIO evite la pérdida de datos

La democratización de los datos se ha convertido en un elemento indispensable para asegurar la competitividad de las compañías. Y es que, las empresas data driven obtienen un 70% más de ingresos por trabajador.

Para profundizar en el tema, Denodo ha elaborado un listado con cuatro claves que permiten a las empresas democratizar sus datos sin afectar a la gobernanza.

"La gobernanza y la privacidad de los datos se volverán excesivamente complejas, a menos que las empresas empiecen a tomar medidas desde ahora. Sin una visibilidad y un control adecuados de los datos existe el riesgo de perder ingresos y productividad", declara Jaume Brunet, Sales Director para Iberia y Latinoamérica en Denodo.

DEMOCRATIZACIÓN DE DATOS

Estas son las 4 claves para democratizar los datos:

- **Basar el acceso en roles.**

La premisa de la democratización de los datos es muy conveniente para las empresas, ya que se pueden agilizar los procesos. Sin embargo, hay datos que no deberían ser visibles para todos. Con una plataforma de virtualización de datos, las organizaciones pueden configurar controles de acceso basados en roles (RBAC) en una capa central. Esto significa que pueden especificar exactamente qué roles pueden acceder a qué datos. De este modo, las empresas pueden garantizar que los empleados solo accedan a los datos que correspondan a su función y nivel.

- **Controlar el uso de los datos.**

No solo es importante controlar a qué registros tienen acceso los empleados, sino que también es imprescindible entender el uso que van a hacer. Las empresas están obligadas a hacer una correcta gestión y utilización de sus datos y el monitoreo permite tener una visión general de quién usa o cambia qué datos, cuándo y cómo. Las plataformas de virtualización de datos van un paso más allá siendo capaces de recomendar conjuntos de datos a los usuarios que mejor se adaptan a sus propósitos. Además, la capa semántica en la virtualización de datos garantiza que todos los registros sigan una taxonomía y una práctica de nomenclatura comunes, y proporciona a los empleados estos registros virtuales estandarizados, evitando que las diferentes definiciones de datos generen confusión o incluso caos.

- **Asegurar los sistemas backend.**

Si todos los empleados pueden usar los datos de la empresa se puede conducir a una sobrecarga de los sistemas backend (por ejemplo, ERP). Para evitar esto, la virtualización ayuda a la definición de restricciones específicas para las consultas, limita cuántas consultas se pueden realizar simultáneamente, cuánto tiempo puede tardar la consulta antes de que finalice automáticamente o cuántas filas puede tener el resultado, entre otras cosas.

- **Filtrar las consultas de datos.**

Con la ayuda de una plataforma de virtualización de datos, las empresas no solo pueden limitar cómo las consultas afectan a los sistemas backend, sino también cómo los empleados pueden realizarlas. Para ello, hay filtros disponibles que restringen el área consultada evitando que los empleados accedan a toda la base de datos de la empresa. Este dato es muy importante, además, porque la democratización de los datos también implica que muchos empleados realicen consultas sin ningún conocimiento técnico y este sistema de filtrado puede ser una solución efectiva para otorgar acceso a los datos sin tener que temer que los sistemas se sobrecarguen y los costes se disparen.

Las empresas quieren rentabilizar la nube: FinOps, la megatendencia

Las compañías continúan escalando en su transformación digital, siendo la nube la base de la digitalización que otorga a la empresa la agilidad y flexibilidad que demanda hoy el mercado, pero el incesante incremento del coste de la nube hace que los CIOs tengan entre sus prioridades la revisión de los planes cloud en 2023.

Nos encontramos en una situación hiperinflacionista, lo que está provocando que muchas empresas estén poniendo en marcha planes para buscar la rentabilidad a corto plazo. Entre las acciones de estos planes, el ahorro en costes operativos suele ser uno de los principales puntos de acción y los departamentos de TI no se libran.

Distintos informes en los que se trata de evaluar el verdadero éxito de las adopciones cloud llegan a afirmar que únicamente un 20% de los proyectos alcanza el éxito, entendiendo como éxito el aprovechar realmente las ventajas que un entorno cloud proporciona; y de ellos únicamente un 9% realmente consigue un ahorro de costes IT.

Actualmente, se desperdicia más del 30% del creciente gasto en software y servicios en la nube. Las principales razones son la falta de una visión completa y entendimiento de todos los servicios que la nube ofrece así como el no abordar el cambio cultural que supone una adopción cloud.

NUBE: FINOPS, MEGATENDENCIA EN 2023

"Re-evaluar" y maximizar la rentabilidad de la inversión en cloud -responsable del mayor gasto destinado a TI según Gartner- es uno de los principales desafíos para el CIO este año. En este escenario, adoptar una estrategia FinOps -un marco operativo que integra las áreas de tecnología, finanzas y negocio- puede ayudar a la empresa a tener una visión macro de las soluciones en la nube utilizadas en la operación y, así, reducir gastos con servicios innecesarios, e impulsar la responsabilidad financiera a todos los niveles de la organización.

ESTABLECIENDO EL MODELO

Establecer un modelo de FinOps además de visibilizar el gasto permite que las empresas puedan optimizar los costes y tener una planificación basada en datos actualizados a medio-largo plazo. En definitiva es rastrear de forma "efectiva" el gasto en la nube para detectar posibilidades de ahorro.

El término FinOps, dada su naturaleza, no va a estar en boca de los usuarios finales, por lo que, a nivel generalista, esta tendencia que marcará el 2023 no va a tener la misma relevancia mediática que otras, pero es seguro que va a estar muy presente en todas las empresas durante este año.

El consumo y la inversión en la nube continuará en ascenso. A pesar del incremento de precios que está suponiendo la inflación, el gasto en la nube no se está reduciendo, sino que, en el caso de la nube pública, se está incrementando. Según la consultora Gartner, se estima que para el próximo año 2023 la inversión crecerá en todo el mundo un 20% más que en 2022, lo que la llevará a superar los 591.000 millones de dólares.

Las empresas siguen apostando por la transición digital y la modernización de las TI, pero tendrán entre sus objetivos la minimización del riesgo y la optimización de los costes con un marco operativo FinOps.

Óscar Ferrer,
equipo de Goodly en Paradigma Digital

Cuando se trata de ransomware más vale engañar que curar

A medida que las ciberamenazas siguen apareciendo en los titulares, las organizaciones de todos los sectores se enfrentan al riesgo de estrategias de ataque más elaboradas y engañosas. Tomemos como ejemplo los continuos problemas que presenta el ransomware, que sigue imponiendo enormes costes a las empresas que deciden pagar con la esperanza de recuperar sus datos cifrados.

Sin embargo, un informe publicado por la Red para la Represión de Delitos Financieros de Estados Unidos revela que, solo en el sector bancario, el número y el coste de los ataques es cada vez más preocupante. De hecho, los bancos de dicho país procesaron 1.200 millones de dólares en pagos sospechosos de ransomware durante 2021, un 188% más que el año anterior.

A nivel organizativo, estos problemas se manifiestan de diversas maneras. Por ejemplo, el 88% de los encuestados en un reciente estudio que realizamos afirmaron que la prevención de daños a los datos es una de sus principales preocupaciones a la hora de proteger los datos y reaccionar ante amenazas y ataques. Además, al 72% de los profesionales de TI les preocupa la recuperación tras un ataque y minimizar el tiempo de inactividad.

Una de las principales inquietudes es que muchos equipos de TI no disponen actualmente de herramientas que puedan detectar adecuadamente los ataques de ransomware en una fase suficientemente temprana del proceso como para evitar que tengan éxito. En el mismo estudio, sólo el 12% de las organizaciones informaron de que sus herramientas de detección de ransomware eran adecuadas y también podían cubrir el creciente patrimonio de datos, independientemente de dónde residan.

El ransomware y el ciberriesgo, en general, están redefiniendo la forma en que las organizaciones deben mejorar su capacidad para proteger su infraestructura y sus activos de datos y, al hacerlo, reducir el riesgo empresarial. Los profesionales de TI deben ir un paso por delante e invertir en tecnología proactiva que mejore su capacidad de recuperación. Como resultado, combinar la protección de datos y la ciberseguridad es la nueva normalidad.

En este entorno extremadamente desafiante, la prioridad actual para la mayoría de las empresas es fortificar sus defensas perimetrales para evitar las intrusiones por completo. En particular, se necesita un enfoque multicapa para proteger los datos de forma integral, entre otras cosas porque no basta con hacer backup. Evitar encontrarse en un escenario de recuperación es, después de todo, mucho más deseable para mitigar la interrupción del negocio.

LA NECESIDAD DE TECNOLOGÍA DE ENGAÑO

Con el fin de lograr la postura de seguridad más sólida para proteger los datos contra los ataques de ransomware, las organizaciones necesitan herramientas multifacéticas que funcionen en cada fase de la cadena de ataque. Aunque generalmente infrautilizadas, las modernas tecnologías de engaño desempeñan un papel cada vez más importante en la detección temprana de amenazas invisibles y de día cero que sortean con éxito las herramientas de seguridad convencionales. Pero, ¿qué son estas tecnologías y cómo funcionan?

El engaño cibernético es una estrategia de seguridad proactiva que funciona embaucando a los malos actores y los ataques maliciosos. Las soluciones de ciberengaño más avanzadas en la actualidad empiezan donde terminan las herramientas de seguridad convencionales, utilizando un proceso de dos pasos para ralentizar y hacer emerger amenazas desconocidas y de día cero. Por ejemplo, utilizando señuelos y sensores de amenazas, los malos actores o el malware intrusivo pueden ser desviados hacia activos convincentes pero falsos. En este punto, se envían inmediatamente alertas de alta confianza a los principales interesados y a los sistemas de seguridad, notificándoles la presencia de amenazas en curso antes de que puedan comprometer los sistemas o datos reales.

A diferencia de los honeypots, que están diseñados para examinar y aprender de los atacantes y sus intentos, los sensores de amenazas están diseñados para enfrentarse activamente a los malos actores en cuanto se inicia un ataque. Utilizando una arquitectura eficiente, similar a la de los servicios web, estos sensores de amenazas están diseñados para imitar cualquier activo del usuario, inundando sus entornos con activos digitales falsificados que son indistinguibles para los atacantes. Sin afectar a las operaciones normales de la red, atraen a los atacantes con señuelos que los desvían y engañan durante el reconocimiento, el descubrimiento, el movimiento lateral y mucho más. Y como los sensores de amenazas sólo son visibles para el atacante, las empresas se benefician de notificaciones extremadamente precisas sobre falsos positivos, lo que les permite conocer la actividad, las rutas de ataque y las técnicas desplegadas.

Este enfoque permite a las organizaciones ofrecer una defensa multicapa contra amenazas como los ataques de ransomware, dotando a los usuarios del poder de identificar y desviar inmediatamente las amenazas maliciosas antes de que los datos sean robados, dañados o comprometidos. En la situación actual, en la que el ransomware ha evolucionado rápidamente hasta convertirse en un motor masivo de la ciberdelincuencia en todo el mundo, está claro que las tecnologías existentes no pueden por sí solas impedir que se produzcan todos los ataques ni garantizar que las víctimas puedan recuperarse rápidamente.

En su lugar, las organizaciones deben centrarse en crear soluciones más eficaces diseñadas para abordar los riesgos específicos que plantean el ransomware y otras tácticas sofisticadas de la ciberdelincuencia. Utilizando el engaño como estrategia de protección proactiva, pueden situarse en una posición mucho más fuerte para frustrar a los malos actores antes de que tengan la oportunidad de pedir un rescate.

César Cid de Rivera, Vicepresidente Internacional de Ingeniería de Sistemas de Commvault

PEDRO ZALDÍVAR MARTÍNEZ, DIRECTOR DE LA UNIDAD DE NEGOCIO DE CLOUD DE NUNSYS

"Para tener éxito en la gestión de datos es importante tener una estrategia clara"

Gestión de los datos y apuesta por la nube híbrida son prioritarias para las empresas. Conscientes de ello, Nunsys ha apostado por plataformas as a Service como GreenLake de HPE para que puedan afrontar estos retos. Hablamos con Pedro Zaldívar sobre ello.

En general, ¿cree que las empresas están ejecutando de forma correcta sus procesos de transformación digital?
A día de hoy, no todas las empresas que están inmersas en un proceso de transformación digital están maximizando el rendimiento que les ofrece la digitalización. Los principales problemas que veo son la falta de liderazgo y alineación estratégica por parte de la cúpula directiva, la resistencia al cambio por parte de algunos empleados y la necesidad de saber gestionar la simbiosis entre la complejidad tecnológica y el aumento de los riesgos de seguridad de información que las implantaciones de algunas soluciones pueden conllevar.

Una de los elementos más importantes en las estrategias de digitalización es el que se refiere a la gestión de los datos, ¿se está realizando una correcta gestión de los mismos?
Es una realidad que la gestión eficiente de datos es crítica para el éxito de cualquier proceso de digitalización. Además, la capacidad de almacenar, procesar y analizar ingentes cantidades de datos en tiempo real es fundamental para el correcto funcionamiento de tecnologías como la IA, IoT o el análisis predictivo. Los principales problemas que nos encontramos en la gestión del dato en las empresas se basan en 2 puntos fundamentales: la calidad y la seguridad del dato. Por un lado, la falta de limpieza y validación de datos incide negativamente en la eficacia de la transformación digital y por otro, la falta de medidas adecuadas, en cuanto a seguridad de los datos, puede exponer a la empresa a riesgos de ciberseguridad y perdida de información clave para la compañía. Para tener éxito en la gestión de datos es importante tener una estrategia clara, asegurar la calidad de los datos y protegerlos.

¿Qué tipo de soluciones recomendaría para llevar una gestión eficiente de los datos? ¿Qué proporcionan esas soluciones?
Nos encontramos en la era de la información, para las empresas uno de sus principales activos son los datos. El tratamiento que hacemos de los mismos y la facilidad de acceso a ellos para la toma de decisiones aportan una ventaja competitiva en un mercado cada vez más globalizado. Con la finalidad de ayudar a las empresas a afrontar estos nuevos retos, ofrecemos soluciones de Cloud Hibrida para los centros de datos mucho más flexibles que se adapta a las necesidades de cada empresa. Apostar por una estrategia de Cloud Hibrida nos permite decidir cuál es lugar más idóneo para almacenar los datos en función del uso que vayamos a hacer de ellos o bien desde donde va a ser consumida esta información.
Otro aspecto fundamental en la gestión eficiente de los datos son los mecanismos que implementamos para salvaguardar y proteger la información de los ciberdelincuentes. En este sentido, HPE GreenLake permite acceder a todas estas tecnologías en un modelo as a Service. El Datacenter debe ser un medio que permita a las empresas llevar sus productos al mercado a la mayor velocidad posible, garantizando el Time to Market.

Nunsys, a través de su Datacenter Nunsys Cloud, ofrece servicios como Virtual Datacenter. ¿Qué ventajas ofrece?
Nunsys Cloud es un datacenter de proximidad TIER III+. Entre los Servicios que ofrecemos principalmente se encuentran los Servicios de Infraestructura como Servicio Virtual Datacenter (IaaS), Backup as a Service (BaaS), Disaster Recovery as a Service (DRaaS), Hosting y Housing entre otros. Nunsys Cloud soporta prácticamente cualquier carga de trabajo de las que está demandando el mercado como por ejemplo poder soportar cargas de trabajo para SAP. Una de las principales ventajas que ofrece Nunsys Cloud es la operación del servicio. Este servicio se ofrece por un equipo humano altamente cualificado. Las empresas además de los Servicios de Cloud nos demandan todo un conjunto de Servicios gestionados que permitan sacar el máximo partido a sus sistemas de información. Nunsys con un equipo humano de más de 1600 personas a lo largo de todo el territorio nacional, estamos especializados en Comunicaciones, Cloud, Seguridad de la Información, Aplicaciones de Negocio y Servicios IT. Esto nos permite cubrir 360º en el ámbito de la tecnología convirtiéndonos así en un socio tecnológico estratégico para nuestros clientes.

La práctica totalidad de empresas parecen decantarse por un modelo de cloud híbrida. Ustedes se apoyan en la plataforma GreenLake de HPE. ¿Por qué eligen esa plataforma?
HPE GreenLake se adapta a la perfección a nuestro modelo de negocio. Permite crecer de forma ilimitada. El coste del servicio es predecible para evitar un impacto en la cuenta de resultados. Puedo elegir la tecnología y la arquitectura más adecuada para cada solución y la localización de cada una de las cargas de trabajo. En definitiva aúna lo mejor de la nube publica y de la nube privada. Con HPE GreenLake, el cliente tiene libertad de elección cosa que no ofrecen otras nubes públicas. Otro aspecto diferenciador es que no hay que sobredimensionar los centros de datos para atender a picos ya que es lo suficientemente flexible para adaptarse a estos picos.

¿Cuál es la propuesta de valor de Nunsys?
Nuestra propuesta de valor se centra en ofrecer a las empresas un amplio porfolio de servicios que permita cubrir todas sus necesidades. Buscamos la diferenciación y esto lo conseguimos gracias a nuestros productos propios. Nunsys Cloud es un claro ejemplo de ello. Aportamos por la excelencia y la incorporación a nuestros productos de la última tecnología como por ejemplo la Inteligencia Artificial.

No-Code: ¿oportunidad o peligro?

Javier Placer,
socio y cofundador de Cibercotizante.

Las tecnologías de propósito general que precipitarán el acelerón de la humanidad hacia mejores maneras de vivir son la solar, la biotecnología y el aprendizaje automático (conocido popularmente como Inteligencias Artificiales aunque no lo son porque las máquinas no son inteligentes). Son desarrollos de Machine Learning, Aprendizaje Automático.

Al hacerse disponibles masivamente con herramientas Nocode, se está revolucionando la forma en que se crean aplicaciones y su software. Ejemplo de ello es el chat sobre modelos de aprendizaje automático de lenguaje GPT-3 de OpenAI, que ha facilitado la forma en que se entiende y se utiliza el aprendizaje automático.

Sin embargo, hay algunas culturas que todavía muestran reticencias a otorgar los adicionales grados de libertad que este tipo de herramienta facilita. Tienen una idiosincrasia y una tradición que les impide aceptar cambios y avances tecnológicos y menos si genera cosas nuevas sin permiso de la idiocracia. En lugar de aprovechar las oportunidades que la tecnología ofrece, fuerzan la protección de su forma de hacer las cosas para seguir utilizando herramientas rancias.

Pero, ¿están justificadas estas reticencias? ¿Es justificable prohibir el uso de nuevas herramientas? En mi opinión, no. La tecnología proporciona herramientas que nos permiten mejorar nuestras vidas. Es demasiado casual que haya solo una correlación entre mejoras sostenibles en calidad de vida y la aplicación masiva de herramientas en toda la historia conocida. Si bien es cierto que algunos aspectos de la idiosincrasia y la tradición deben ser protegidos -entrénese usted con RHL su modelo para proteger los aspectos que le dan ventaja competitiva- también es importante no perder de vista las oportunidades que la tecnología nos ofrece. Además, permite a personas que antes no tenían acceso a estas herramientas crear aplicaciones y software sobre los temas que sí son expertas. Esto significa que la tecnología puede ser utilizada para mejorar de manera más amplia y desde abajo la vida de las personas y fomentar el progreso en todo el mundo.

A mi juicio, es esencial facilitar el uso de herramientas Nocode como ChatGPT3 o youchat, indeleblemente combinadas con otras como BigML que permiten asegurar la solvencia de un proceso, ya que estas combinaciones de herramientas pueden contribuir al avance y mejora de la vida de la mayoría de las personas.

Lo importante no es saber multiplicar o dividir sino resolver el problema adecuado. La división aritmética de la distancia por la velocidad para saber el tiempo es lo más fácil, entender y aplicar la ecuación lo complicado. ¿También se van a prohibir las calculadoras?

Pueden ayudar a ahorrar tiempo, reducir los costes de desarrollo de aplicaciones, generar ventajas competitivas sostenibles y resultar en mejoras de la productividad. Si se prohíbe su uso, muy probablemente tendrá un efecto negativo en la productividad, sobre todo relativa a otras culturas construidas sobre bases que dan más peso a la variable libertad en sus algoritmos. Y es muy asimétrico con el cuchillo jamonero, que sí es legal.

nexica | econocom

Nexica Hybrid Cloud

nexica cloud

Nexica Hybrid Cloud integra soluciones y servicios en:

NEXICA CLOUD
en centros de datos TIER3 en Barcelona y Madrid

MICROSOFT AZURE
en el AZURE STACK HUB de Nexica Cloud o en un DC de Microsoft

AWS
con interconexión directa desde su nube

Y otros clouds públicos o privados

Con **NEXICA HYBRID CLOUD, hibridamos?**

Econocom Nexica
C/ Acer, 30, 1º 4ª | 08038 Barcelona
C/ Cardenal Marcelo Spínola, 4 | 28016 Madrid
T. 900 800 296 | hola@nexica.com

30 edición

Seguimos innovando
Seguimos avanzando

ASLAN 30 Ed 2023

22 y 23 MARZO MADRID

congreso.aslan.es

DATA MANAGEMENT | CYBER SECURITY | DIGITAL WORKSPACE | CLOUD DATACENTER | INTELLIGENT NETWORKS

Todo cambia.

La innovación digital está siendo esencial para desarrollar nuevos servicios y empresas más competitivas, más seguras y más inteligentes. El Congreso ASLAN2023 es una oportunidad para conocer nuevas tendencias tecnológicas, compartir experiencias en digitalización y crear sinergias para aprovechar los fondos europeos.

Juntos, aceleramos la transformación digital.

GLOBAL SPONSORS

aws | DELL Technologies intel | econocom | eset Digital Security Progress. Protected. | Hewlett Packard Enterprise | JUNIPER NETWORKS | PURESTORAGE

EVENT SPONSORS

A10 | Acronis | AnyDesk | Cambium Networks | CLOUDFLARE | DARKTRACE | dynatrace | Extreme | getronics | hp | JOTELULU | kaspersky | MICRO FOCUS | NetApp | NUTANIX | SAP | SCC | SOPHOS Cybersecurity evolved. | zoom

El gran evento anual en España organizado por la Asociación nacional de la industria tecnológica

@aslan Aceleramos la Transformación Digital