

2021: el año de la digitalización

Con la participación de:

Vertiv, Lenovo, Ausape, Compusof, Micro Focus, Trend Micro, Canon,

Arsys, TP-Link, Acer, Samsung, Kaspersky, Watchguard, pfsGROUP e Intersystems



Con

gran energía

conseguimos gran eficiencia

¿Por qué no elegir la mejor protección eléctrica para tus aplicaciones Edge de TI mientras ahorras energía?

Con el nuevo SAI **Vertiv™ Edge** con tecnología line-interactive, lo tienes fácil.

Disponible en formato para rack o en torre, este SAI es altamente eficiente y compacto y tiene súper poderes para proteger tus cargas TI y también tu presupuesto.

- **Gratis: Incluye el software Vertiv™ Power Assist y 2 años de garantía***

What's Your Edge?

[Vertiv.com/WhatsYourEdge](https://www.vertiv.com/WhatsYourEdge)

El X1 Nano es el ThinkPad™ más ligero de su clase

El ThinkPad™ X1 Nano es el ThinkPad que menos pesa de todos, con solo 907 g, lo que abre nuevos caminos en cuanto a rendimiento y funcionalidad con un peso increíblemente ligero. El primer ThinkPad de Lenovo dotado de la plataforma Intel® Evo™ y con procesadores Intel® Core™ de 11ª generación, X1 Nano ofrece una velocidad e inteligencia sin igual, al tiempo que conserva una excelente duración de la batería. Posee una pantalla 2K de 13 pulgadas y bisel estrecho con una ratio de aspecto 16:10, y cuatro altavoces y cuatro micrófonos 360 grados que mejoran las capacidades audiovisuales. Para una experiencia de usuario inmersiva, el X1 Nano es compatible con Dolby Vision y Dolby Atmos®. La conectividad de última generación corre a cargo de WiFi 6 y la opción 5G te brindará una mayor capacidad de ancho de banda y propiciará nuevos niveles de eficiencia y colaboración en conexión permanente en el nuevo entorno laboral híbrido.

También se puede adquirir ya el primer PC plegable del mundo, el ThinkPad X1 Fold. Este equipo ofrece una revolucionaria combinación de portabilidad y versatilidad que define una nueva categoría de informática habilitada por los procesadores Intel® Core™ con Tecnología Híbrida Intel® y que es posible gracias al programa de innovación Project Athena de Intel.

Con 5G opcional, garantiza la velocidad de conexión que estará optimizada allá donde esté disponible, además de contar con las funcionalidades de seguridad ThinkShield.

EL THINKPAD MÁS LIGERO DE LA HISTORIA

Con menos de un kilo de peso, el ThinkPad X1 Nano es el más ligero de la historia. Ofrece uno de los formatos más completos de portátiles ultraligeros disponibles actualmente con un rendimiento, pantalla, sonido y seguridad sobresalientes.



- Equipado con procesadores Intel® Core™ i7 de hasta 11ª generación con gráficos Intel® Iris® Xe, el X1 Nano cuenta con los mejores procesadores del mundo para portátiles finos y ligeros, por lo que facilitan una creación de contenidos hasta 2,7 veces más rápida, una productividad en la oficina más de un 20% más rápida y una velocidad de gaming mayor al 200%, además de streaming en los flujos de trabajo del mundo real en comparación con los productos de la competencia.

- Thunderbolt™ 4 ofrece una conexión rápida y de un solo cable a la red de alimentación, los monitores, el almacenamiento y muchos otros dispositivos externos.

- X1 Nano es el primer ThinkPad que presenta un conjunto actualizado de funcionalidades de seguridad ThinkShield biométricas y con IA. Estas van desde el nuevo reconocimiento de voz y la detección de presencia humana, que permiten el inicio de sesión sin contacto y el bloqueo del dispositivo cuando el usuario se aleja, hasta el conocido lector de huellas dactilares Match on Chip.

- Una pantalla Dolby Vision 2K de 13 pulgadas con una ratio de aspecto de 16:10 ofrece un campo de visión amplísimo y el sRGB 100% garantiza la claridad y la precisión del color. También dispones de opciones con pantalla táctil.

- El sistema de altavoces incluye cuatro altavoces con soporte Dolby Atmos para un sonido envolvente y, combinado con cuatro micrófonos de 360 grados, garantiza que se te escuche alto y claro durante las llamadas de audio y vídeo.

Ultraligero, de alto rendimiento, con pantallas brillantes, un audio impresionante y una conectividad preparada para el futuro, el ThinkPad X1 Nano es perfecto para un entorno laboral híbrido. Por su parte el X1 Fold se enmarca en una categoría informática completamente nueva y redefinirá nuestro concepto y uso de los dispositivos.

EL CAMBIO EN LA INFORMÁTICA PERSONAL

Tras un proceso de creación de cinco años, el ThinkPad X1 Fold es el primero de su clase en una nueva categoría de informática personal que ampliará los límites y redefinirá la forma en que interactuamos con la tecnología. Dimensiones pequeñas, pero todo un mundo de posibilidades. El

ThinkPad X1 Fold se adapta a los nuevos modelos de trabajo en remoto, en la oficina e híbridos, lo que permite a los pioneros adoptar una innovación revolucionaria que potenciará la creatividad, la colaboración y el entretenimiento a medida que se transforma para adaptarse a la perfección a tus necesidades específicas.

Una mirada al futuro en las Sesiones Magistrales AUSAPE



Ingenieros, economistas, matemáticos, periodistas... especialistas de diversas disciplinas se han dado cita en las dos Sesiones Magistrales que AUSAPE ha organizado en los meses

probablemente “los ordenadores cuánticos no van a sustituir a los ordenadores clásicos y el mundo que tendremos será un mundo híbrido”.

A continuación, hubo una Mesa de Debate, en la que Manuel Navarro, Ambrosio Rodríguez, Juan Miguel Revilla y José Luis Pérez abordaron diversos temas, como los países punteros en computación cuántica, las nuevas habilidades necesarias para este nuevo paradigma, la supremacía de la computación cuántica sobre la convencional a corto plazo o la popularización de los ordenadores cuánticos.

La segunda sesión magistral, dedicada a la economía pos-Covid, tuvo lugar el 11 de noviembre, con la presencia de 220 personas, que siguieron las intervenciones del economista Santiago Niño Becerra, como ponente magistral invitado, y el resto de participantes. Ana Campón (CFO de Siemens España), Rufino de la Rosa (Socio de EY Abogados y jefe de Gabinete de la Secretaría de Estado de Hacienda y Presupuestos entre 2009 y 2011), Laurent Arveiller (CFO de SAP España) y Ferrán Llompart (Corporate Treasury Director de Iberostar Group) intervinieron también en el evento, conducido por Sara Antuñano, vocal de Tesorería, Grupos de Trabajo y Delegaciones de AUSAPE.

Niño Becerra habló de que el coronavirus está teniendo un papel acelerador de la puesta en marcha de un nuevo modelo económico y de trabajo, activando procesos y herramientas que ya existían, como el teletrabajo, pero que aún no estaban muy presentes. “El virus nos enseña que las cosas han de hacerse de otra manera”. Asimismo, definió la nueva normalidad como un mundo muy marcado por la tecnología y el poder de las grandes corporaciones.

Pesimista sobre la situación de España, a la que lastra su baja productividad, el economista pronosticó que la caída experimentada en el PIB en 2020 no se recuperará hasta 2024, el desempleo alcanzará un máximo del 17,9% el año que viene y la deuda pública llegará al 124% del PIB en 2022.

En la Mesa de Debate posterior, los ponentes abordaron temas como la tendencia de la Unión Europea a potenciar la tributación indirecta en las transacciones y servicios digitales, la aportación de la tecnología en las nuevas formas de trabajar, el impacto de la pandemia en los sectores industrial y turístico, y los planes de las compañías para el futuro inmediato. La tercera parte de la Sesión Magistral de Economía AUSAPE se dedicó a los asistentes, que pudieron plantear sus cuestiones a los ponentes invitados.

de octubre y noviembre, con la Computación Cuántica y la Economía Pos-Covid como temas de referencia.

La primera de estas sesiones se celebró el pasado 20 de octubre con la participación de Enric Delgado Samper (CTO de IBM España) y Raúl Herrero Calderón de la Barca (Data Management Specialist en Google). Junto a ellos, el director de BYTE, Manuel Navarro; Ambrosio Rodríguez López (director de Computing BPS), Juan Miguel Revilla (redactor especializado en información tecnológica) y José Luis Pérez (director de Operaciones de la consultora Penteo) intervinieron en una sesión moderada por Nacho Santillana, coordinador del nuevo Grupo de Trabajo de Innovación y presidente de AUSAPE en 2018-2019.

El objetivo principal de la sesión, a la que asistieron 175 personas, fue dar a conocer los principios, cualidades y posibilidades de la computación cuántica, una de las tecnologías más prometedoras para las próximas décadas que, sin embargo, todavía es desconocida para el gran público.

Así, Enric Delgado y Raúl Herrero explicaron los principios de superposición, entrelazamiento e interferencia en los que se basa la computación cuántica, además de las características físicas y de hardware de los ordenadores cuánticos. También comentaron los principales tipos de algoritmos y sus aplicaciones: modelado de la naturaleza, simulaciones numéricas, optimización de rutas, y machine learning e inteligencia artificial, que serán de gran utilidad en las industrias farmacéutica, de materiales, financiera o de movilidad como servicio, gracias a su potencia y rapidez y la menor necesidad de recursos.

Enric Delgado concluyó la presentación destacando que “estamos al principio de la computación cuántica”, pero que

Innovar desde la resiliencia digital



Por Moisés Camarero Aguilar.
Director General del Grupo Compusof

Dejamos atrás un año marcado por una pandemia que ha hecho mella en todos los órdenes del panorama social y económico. Ha cambiado el esquema de gestión tradicional de las organizaciones y se ha puesto de manifiesto que la tecnología es el verdadero motor de empresas y administraciones de todos los sectores y ámbitos. Un cambio que será aún más patente los próximos 12 meses tras iniciar la nueva normalidad y en el que asistiremos a una cultura empresarial protagonizada por la innovación, con la certeza de que son los sistemas TIC los que soportan todos los procesos y organizaciones.

A partir de ahora, las tecnologías informáticas tradicionales tendrán que hacer frente al nuevo empuje digital, lo que provocará un cambio en los paradigmas que favorecerá la nube distribuida, la inteligencia artificial y, fundamentalmente, la ciberseguridad como pilar base. Serán tecnologías más adoptables para acomodar nuevos proyectos y experiencias de usuarios y clientes.

A medida que evolucione el Internet de las cosas, las nuevas experiencias tecnológicas proporcionarán diferentes proyectos de negocio y nos adentraremos en nue-

vos planes evolutivos. Y por supuesto, la automatización que dará paso a procesos más orientados a dar respuesta a las necesidades de la era digital. La industria evolucionará, los diferentes sectores de la economía se beneficiarán de nuevos sistemas de ciberseguridad más adaptados a la evolución de los ataques.

Todo ello son aspectos que veremos cómo se van posicionando a lo largo de 2021, si bien es verdad que los CIOs adquirirán un papel de responsabilidad mayor en los resultados operativos de los negocios. La pandemia ha demostrado que éstos pueden impulsar la innovación de toda la organización y su trabajo se acerca cada vez más a la cúspide de la dirección. También veremos un cambio en cómo las personas interactúan en el mundo de los negocios por lo que necesitan procesos digitalizados que le ayuden a constituirse en el centro de sus organizaciones.

Desde nuestra perspectiva de compañía pionera y con casi 40 años de experiencia en el sector, creemos que llega un año en el que la tecnología será la llave de la innovación y el desarrollo. Las empresas están asumiendo que la digitalización es un driver de valor extraordinario. Es la hora de apostar por la tecnología para conseguir negocios más seguros, datos más significativos, que aporten valor y puedan ser almacenados consecuentemente para aprovechar todo su potencial.

No cabe duda, que la nube será el gran aliado, el Edge aportará gran potencial y contaremos con espacios de trabajo más digitales e inteligentes. Lo que antes era una posibilidad, ahora es una necesidad. Las capacidades digitales ya no será una opción, pasan a formar parte de prioridad de los negocios para identificar nuevas oportunidades y asegurar la competitividad. Llega el término “resiliencia digital” que, según IDC, dará la capacidad de respuesta a las empresas para hacer uso de las nuevas posibilidades, incluso un 50% más rápidamente que las que se centran en mantener los niveles de resiliencia empresarial IT existentes.

Desde el Grupo Compusof, seguiremos avanzando en esta línea para identificar las necesidades de las empresas y administraciones en el compromiso de ayudar a potenciar sus capacidades. El objetivo no es otro que el de proporcionar a profesionales y ciudadanos la ruta que les acerque a la digitalización para acercar el futuro al día de hoy.

Diga "hola" al futuro con AIOps



Por Luis Colino.
Director de Preventa de
Micro Focus.

En este momento, la pregunta en la mente de todos los líderes empresariales es: ¿cómo superarán las organizaciones esta pandemia y cuántas empresas realmente saldrán adelante al final? Las empresas deben seguir funcionando pero también deben poder adaptarse rápidamente a este nuevo mundo de pandemias, nuevas tecnologías, modelos comerciales innovadores y cualquier otra cosa que les depare el mañana.

En la combinación híbrida actual de servidores locales y virtuales, plataformas de nube pública y privada y dispositivos móviles de todo tipo, es crítico que identificar, resolver y mitigar posibles interrupciones o problemas de rendimiento. Y estos problemas ahora son más difíciles de identificar, y mucho menos de remediar. Tanto el volumen como la variedad de tráfico de redes y aplicaciones que las empresas de datos están generando se han disparado. Para monitorizar y administrar de manera efectiva las operaciones de TI en este nivel de complejidad, las organizaciones están recurriendo a la inteligencia artificial para las operaciones de TI, o lo que se llama AIOps.

AIOps es la abreviatura en inglés de inteligencia artificial para operaciones de TI, término acuñado por Gartner in 2017. AIOps es la aplicación de análisis de big data y aprendizaje automático a los datos de la operación de TI para identificar patrones de manera inteligente y aumentar procesos y tareas comunes.

Los analistas de la industria han definido un conjunto de capacidades que debe proporcionar una solución AIOps. Éstas incluyen:

- **Recopilar datos de muchas fuentes**, como redes, aplicaciones, bases de datos y la nube, así como en una variedad de formas incluyendo métricas, eventos, topología, archivos de registro, transmisión y datos no estructurados como publicaciones en redes sociales y documentos (procesamiento de lenguaje natural).
- **Gestionar los datos**, almacenar los datos en un solo lugar accesible para generar análisis e informes, que también incluya funciones como indexación y fecha de vencimiento.
- **Analizar los datos**, incluida la detección de patrones, la detección de anomalías y el análisis predictivo

- **Llevar a cabo un análisis de causa raíz**, que implica reducir los volúmenes de datos a las pocas (o una) causas probables.
- **Agregar y superponer múltiples herramientas de monitorización y otras inversiones**

¿Por qué se necesita AIOps? Ningún ser humano puede procesar la explosión de datos que se espera que manejen las operaciones de TI, y más cuando incluimos en la ecuación el monitorizar todos los datos provenientes del Internet de las cosas (IoT). Por ejemplo, una locomotora puede producir terabytes de datos durante un viaje. En términos de TI, esta explosión se llama Big Data.

Los beneficios que los usuarios han encontrado al usar AIOps incluyen una carga de trabajo reducida en el personal de operaciones de TI porque la IA está ayudando con el análisis; un análisis de causa raíz (RCA) más rápido porque la IA identifica el problema o reduce la cantidad de elementos que los operadores deben considerar a un conjunto pequeño; evitar problemas antes de que los clientes se vean afectados mediante la detección de anomalías y un tiempo medio de resolución más rápido (MTTR).

La Enterprise Management Associates (EMA) lanzó el pasado 10 de Septiembre su nuevo radar AIOps 2020 en el que analiza las capacidades que las soluciones AIOps deberían aportar, los casos de uso que AIOps está brindando actualmente y un análisis en profundidad de 17 de los principales proveedores de la industria. Micro Focus recibió 4 premios en este informe, destacando el premio especial de "Most balanced user case", gracias a que ofrece fortalezas únicas de AIOps en los tres casos de uso revisados: gestión de incidentes, rendimiento y disponibilidad; Impacto del cambio y optimización de la capacidad; e impacto empresarial y alineamiento de TI con el negocio.

La solución de AIOps de Micro Focus incluye la monitorización de multi-cloud, SaaS, aplicaciones, infraestructura y red, automatización y gestión de la configuración.

- **Operations Bridge**: proporciona la monitorización automática en entornos multi-cloud y on-premise de cualquier dispositivo, sistema operativo, base de datos, aplicación o servicio y aplica AIOps a todos los tipos de datos.
- **Network Operations Management**: la solución de software de gestión de red integral probada en la industria para grandes empresas, MSP y agencias gubernamentales.
- **Operation Orchestration**: permite la automatización de procesos de TI de extremo a extremo con gran agilidad
- **Descubrimiento universal y CMDB universal**: Cree una CMDB que descubra y asigne activos de TI híbridos a través de múltiples nubes, contenedores y TI local.

Para conocer más visite: www.microfocus.com

Más allá del endpoint: por qué las organizaciones eligen XDR



El endpoint ha sido durante mucho tiempo un importante blanco para los atacantes que tienen como objetivo los entornos de TI corporativos. Sin embargo, cada vez más, los responsables de seguridad se ven obligados a proteger los datos de toda la organización, ya sea en la nube, en dispositivos IoT, en el email o en los servidores de la empresa. Por tanto, vale la pena tener visibilidad integral, para detectar y responder más eficazmente. Aquí es donde las soluciones XDR ofrecen una alternativa a las soluciones EDR y de punto. Pero no todos los proveedores son iguales. Trend Micro se distingue del resto al proporcionar capacidades de seguridad maduras en todas las capas, una inteligencia de amenazas líder en el sector y un enfoque analítico impulsado por IA que produce menos alertas de mayor fidelidad.

BAJO PRESIÓN

Los enfoques más avanzados de seguridad han cargado a las organizaciones con muchas herramientas dispares, creando costes adicionales, complejidad de gestión y brechas de seguridad. Esto se suma a la sobrecarga de trabajo de los equipos de seguridad.

Según Gartner, "dos de los mayores retos de las organizaciones de seguridad son contratar y retener personal con conocimientos técnicos, y crear una capacidad operativa de seguridad que pueda configurar y mantener con confianza una postura defensiva, además de ofrecer una capacidad de detección y respuesta rápidas".

XDR es atractivo para a las organizaciones que luchan con-

tra todos estos desafíos, así como para aquellas que no pueden obtener valor de, o que no tienen los recursos para invertir en, soluciones SIEM o SOAR. Entonces, ¿qué implica?

QUÉ BUSCAR

Como indica Gartner, todas las soluciones XDR deberían fundamentalmente lograr lo siguiente:

- Mejorar la protección, detección y respuesta
- Aumentar la productividad general del personal de seguridad operativa
- Menor coste total de propiedad (TCO) para crear una capacidad efectiva de detección y respuesta

Sin embargo, el analista invita a pensar antes de elegir el proveedor en el que invertir, pues en algunos casos, la inteligencia de amenazas subyacente puede tener poca potencia, y los proveedores tienen lagunas en su cartera de producto que podrían crear peligrosos puntos ciegos de TI. La eficacia será una métrica clave. Según Gartner, "tiene que responder a la pregunta de si encuentra cosas, y también a la de si realmente encuentra cosas que sus herramientas actuales no encuentran".

UN LÍDER EN XDR

Aquí es donde Trend Micro XDR sobresale. Ha sido diseñado para ir más allá del endpoint, recogiendo y correlacionando datos de toda la organización, incluyendo email, endpoint, servidores, cargas de trabajo cloud y redes. Con este contexto mejorado y el poder de los algoritmos de IA y los análisis de seguridad expertos de Trend Micro, la plataforma identifica las amenazas con mayor facilidad y las contiene de manera más efectiva.

Forrester reconoció recientemente a Trend Micro como líder en la detección y respuesta empresarial, diciendo de XDR: "Trend Micro tiene un enfoque con visión de futuro y es una excelente opción para las organizaciones que desean centralizar los informes y la detección con XDR, pero tienen menos capacidad para realizar una "caza" de amenazas de forma proactiva".

Según Gartner, menos del 5% de las organizaciones emplean actualmente XDR. Esto significa que hay una gran necesidad de mejorar la protección en toda la empresa. Trend Micro XDR ofrece a las organizaciones globales una valiosa oportunidad de minimizar para exposición al riesgo empresarial a la vez que se maximiza la productividad de los equipos de seguridad.

Consolidar la digitalización, el gran reto empresarial de 2021



El conjunto de aprendizajes con el que finalizamos este año tan incierto nos da pie a empezar 2021 con el foco mucho más claro. La aplicación de la digitalización en las empresas ha pasado de ser progresiva a llegar abruptamente y de forma acelerada tras el confinamiento. Ahora es momento de mirar al futuro y reflexionar acerca de cómo afrontar 2021, el año en el que se consolidará definitivamente la digitalización empresarial.

Los nuevos modelos de trabajo que hemos atisbado este año han llegado para quedarse. Algunas compañías mantendrán un modelo de teletrabajo completo, mientras que otras apostarán por formatos híbridos de trabajo. Sea cual sea la modalidad por la que opten, lo que debemos tener claro los partners tecnológicos es que estas nuevas fórmulas laborales requieren una adaptación e integración digital completa, un proceso en el que nuestra responsabilidad es estar al lado de los clientes y asesorarles en todo momento.

El ámbito de la impresión y la gestión documental no escapan a esta realidad, en la que es necesario contar con las mejores herramientas, productos y soluciones que garanticen la máxima eficacia y productividad y ayuden a las empresas a consolidar la digitalización en 2021.

CONECTIVIDAD, SEGURIDAD Y CLOUD: TRES SERVICIOS ESENCIALES PARA LA DIGITALIZACIÓN EN EL SECTOR DE LA IMPRESIÓN

La deslocalización geográfica de los trabajadores ha tenido como consecuencia un cambio en las necesida-

des de impresión y gestión documental. Las empresas necesitan equipos que les proporcionen la opción de imprimir en Cloud, desde cualquier ubicación y con total seguridad. Los dispositivos imageRUNNER ADVANCE DX de Canon incorporan tecnologías de vanguardia que dan respuesta a estas necesidades y que integran sistemas de automatización inteligente con los que se reduce el tiempo a la hora de gestionar documentos o flujos de trabajo.

La seguridad es otra de las principales preocupaciones de las empresas en este entorno digital. Estos equipos de Canon están preparados para proteger al máximo la información, gracias a funcionalidades como el sistema de borrado automático de datos después de cada tarea, el cifrado de los mismos y el hardware antimanipulación que protege las contraseñas y claves de los usuarios del dispositivo.

Además de los mecanismos de seguridad, es imprescindible contar con un software de gestión de impresión que aproveche las ventajas que reporta la nube. El software uniFLOW Online Express de Canon, incorporado en estos dispositivos, amplía la elevada gama de opciones de seguridad y conectividad que ofrecen los equipos de Canon, al tiempo que permite una interoperabilidad entre ellos.

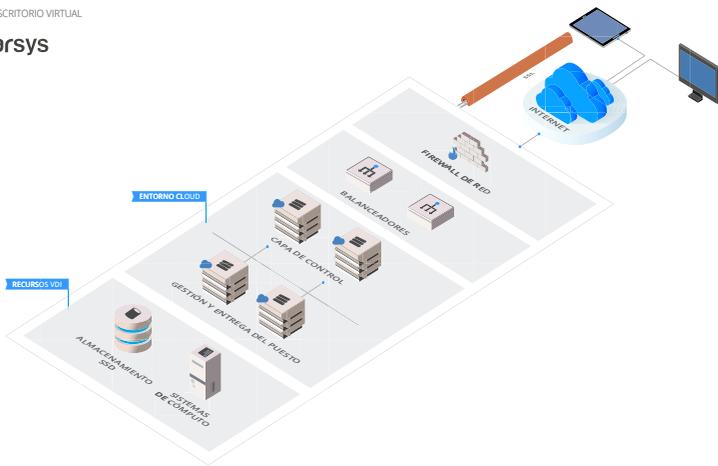
La digitalización en el ámbito de la impresión no solo implica adaptarnos a las nuevas necesidades de los clientes desde el punto de vista de los productos. También los servicios están cambiando, siendo la externalización de los mismos una opción cada vez más recurrente para muchas empresas. Por ello, en Canon continuamos reforzando también esta área continuamente, incorporando cada vez más facilidades para que los clientes puedan centrarse en su core de negocio sin preocuparse por integrar la digitalización en todo tipo de procesos.

Consolidar la digitalización constituye un procedimiento muy camaleónico, en el que confiar en socios tecnológicos especializados es fundamental para implementarla, tanto desde un punto de vista técnico como dentro de la cultura corporativa empresarial.

Por M^a Jesús Arroyo,
Product Manager, Canon España

La virtualización de escritorios, la mejor opción para el teletrabajo

ESCRITORIO VIRTUAL
arsys



El Desktop as a Service (DaaS) externaliza la informática empresarial y ofrece movilidad, rendimiento, costes predecibles y máxima seguridad para el puesto de trabajo.

El coronavirus nos ha obligado a adaptarnos a una crisis sin precedentes. Para muchas empresas, el impacto en su negocio ha sido devastador, aunque el Cloud Computing ha sido uno de nuestros grandes salvavidas y nos ha facilitado las comunicaciones, el ocio y la actividad profesional.

El teletrabajo se ha consolidado como una de las herramientas más poderosas de la Nube y aquellas empresas que fueron capaces de llevar a término su transformación digital y consiguieron cambiar el chip de su cultura operativa han conseguido sobreponerse a la adversidad.

Actualmente, Arsys aloja más de 3.000 escritorios virtuales (VDI, Virtual Desktop Infrastructure) en su centro de datos, que se han convertido en una alternativa realista, y de disponibilidad inmediata, para muchas de las empresas que tuvieron (y tienen aún) que apostar por el trabajo no presencial. “Esta es una de sus ventajas, pero también son muchas las

compañías que entienden esta tecnología como una forma de externalizar su informática, con independencia de sus posibilidades para el trabajo en remoto”, explica Susana Juan, responsable de las soluciones VDI en Arsys.

Estamos ante una tecnología que responde a las necesidades tangibles de las organizaciones: movilidad, rendimiento y costes predecibles en pago por uso. Esto significa llevar a todas las personas de una misma empresa, sea cual sea su localización, ciudad, país o punto de conexión remota, a una misma oficina virtual de dimensiones infinitas y, por tanto, también de posibilidades infinitas. Y con absolutas garantías de seguridad, pues la plataforma está protegida por diferentes capas de protección física y lógica que configuran un entorno absolutamente blindado.

Además, como también se eliminan los servidores (que se virtualizan junto a los escritorios remotos) y la informática local se reduce a la mínima expresión, las empresas se benefician de un ahorro importante, entre otras cosas, en mantenimientos y licencias de software, pero también en electricidad asociada al consumo de los equipos on premise o de los sistemas de refrigeración.

Además de las cualidades inherentes a la tecnología, “en Arsys no queremos olvidarnos del servicio y acompañamos a las empresas en la consultoría o durante el despliegue de la solución. Entendemos que muchas empresas no cuenten con personal técnico especializado pero con nosotros ninguna compañía va a renunciar a la tecnología por ese motivo”, concluye Susana Juan.

PRINCIPALES CARACTERÍSTICAS

- Informática siempre actualizada. Escritorios virtuales de alto rendimiento y sin mantenimiento.
- Sin inversión, en pago por uso.
- Movilidad total. Acceso a todas las aplicaciones y documentos desde cualquier dispositivo, con un consumo máximo de 100 KB por usuario.
- Control informático (IT). Unifica la gestión y reduce las incidencias en un 70%.
- Flexibilidad. Incorporaciones inmediatas de sedes o usuarios con recursos adaptables a cada puesto.
- Seguridad extrema. Alta disponibilidad, backup, encriptación SSL, antimalware, redundancia y SLA (Acuerdo de Nivel de Servicio)
- Administración sencilla y centralizada

Omada SDN



La pandemia ha conseguido que grandes cambios se hagan patentes en el trabajo diario en la mayoría de empresas. En un nuevo mundo de trabajo marcado por el teletrabajo y los modelos semipresenciales en las oficinas, sin duda hace imprescindible contar con las herramientas necesarias para subirnos a la ola de la transformación digital.

Las redes están en todas partes hoy en día, transmitiendo información las 24 horas del día. No somos conscientes de hasta qué punto vivimos conectados y menos aún de cómo exigimos cada vez más de esas conexiones. La pandemia no ha hecho más que acelerar este proceso. Este crecimiento desenfrenado puede acabar desbordando la capacidad de los sistemas y las personas responsables de su mantenimiento.

Por ejemplo, hoy en día no es raro que el responsable de administrar una red de una empresa u organización tenga que lidiar no sólo con una red, sino con varias, y lo que es peor es que muchas veces tiene que además estar pendiente de todas a la vez y al mismo tiempo. No es raro que en estas circunstancias se cometan fallos o se ignoren brechas de seguridad.

Si la tecnología existe para hacernos la vida más fácil, ¿acaso no tiene sentido hacer lo mismo para aquellos que tienen que gestionarla?

Ahí es donde entran las redes definidas por software (en inglés Software Defined Networking, SDN). Se entiende por tecnología SDN a aquel conjunto de técnicas usadas en redes computacionales con el objetivo de facilitar la

implementación e implantación de servicios de red para que sean más fáciles de manejar, de esta manera se facilita la gestión del administrador de red. Una red SDN tiene un sistema de software controlador en su núcleo para implementar automáticamente servicios de red y distribución de datos, esto ayuda a la implementación e implantación de servicios de red de una manera mucho más fácil y cómoda.

TP-Link entiende mejor que nadie la importancia de una buena conexión de red y su correcta gestión, especialmente en entornos empresariales.

La solución empresarial Omada SDN está formada por una gama de productos (puntos de acceso wi-fi, switches, y routers) que conforman una completa solución Cloud inteligente y altamente escalable diseñada para la implementación de redes empresariales Wi-Fi más potentes, seguras y sencillas de gestionar, todo ello controlado a través de una plataforma de gestión centralizada. Además, con la implementación de Zero Touch Provisioning (configuración o provisionamiento desatendido o con mínima asistencia) los administradores podrán implementar y configurar de forma remota redes de múltiples sitios. La gestión remota a través de la nube, del software gratuito Omada o desde un controlador físico, es 100% centralizada, lo que garantiza el control de todos los productos TP-Link desde una única interfaz, en cualquier lugar y en cualquier momento, con el correspondiente ahorro de costes y posibles incidencias.

El gran valor que Omada SDN ofrece al canal y a los clientes es su gran flexibilidad, además de ser muy robusta y fiable. La misma gama de productos sirve tanto para instalaciones pequeñas como muy grandes, con mucho o poco tráfico. Es ideal para el mundo de empresarial, educación, restauración, Hospitality y en cualquier negocio que necesite una alta densidad de conexión ya que ofrece como atractivo una red potente y estable desde el momento de su puesta en marcha. El cliente puede cubrir múltiples necesidades con una sola línea de productos, reduciendo considerablemente el tiempo de aprendizaje.

La principal ventaja adicional que nos diferencia respecto de la competencia es que TP-Link España pone a disposición de sus clientes y partners equipos especializados de ingenieros preventa y postventa ubicados en España, para todos los proyectos.

Además, actualmente se están desarrollando certificaciones exclusivas de Omada SDN. Por supuesto, la formación y la certificación de aquellas empresas que deseen ser partners será crucial a la hora de tener acceso.

Alfa Romeo vuela con Acer



Alfa Romeo Racing ORLEN cuenta con unos componentes extremadamente resistentes y rugerizados para mantenerse por delante en cada carrera incluso en las situaciones más difíciles. La nueva línea Acer ENDURO ofrece soluciones reales para los retos que tienen lugar en un ambiente tan difícil como las carreras y en boxes. Portátiles y tablets potentes con resistencia de grado militar que ofrecen la fuerza, precisión y acceso inmediato cuándo y dónde sea para lograr el objetivo de : crear el coche de carreras más veloz del mundo. Estas son las razones por las que confiar en los dispositivos ENDURO.

RESISTENCIA DE GRADO MILITAR

Los dispositivos Acer ENDURO ofrecen al equipo de carreras Alfa Romeo el hardware que necesitan. Los portátiles y tablets equipan potentes procesadores Intel y soluciones tecnológicas avanzadas para un rendimiento y usabilidad sin precedentes en cualquier condición. Para una resistencia fiable, todos los dispositivos Acer ENDURO vienen con certificación MIL-STD-810G e IP65. Esto significa que todo el equipo puede confiar en la protección contra caídas, golpes, derrames, vibraciones, polvo, líquidos y mucho más.

VELOCIDAD SIN PRECEDENTES

En un espacio de trabajo tan exigente, como en boxes, un portátil con suficiente potencia para rendir al máximo en todo momento es algo imprescindible. El portátil ENDURO N3 equipan un procesador Intel® Core™ i7 de décima generación, una gráfica discreta opcional NVIDIA® MX230, hasta 32GB de memoria DDR y una unidad SSD NVMe Gen 3 de hasta 512GB. Con esos componentes, el equipo puede estar seguro de conseguir sus objetivos con total tranquilidad.

EL RENDIMIENTO QUE EXIGES

En el mundo de las carreras, el rendimiento lo es todo. Esa es la razón por la que el equipo de carreras de Alfa Romeo con-

fiar en su portátil Acer ENDURO N7 con suficiente potencia para conseguir sus objetivos con rapidez. Con una CPU quad-core Intel® Core™ i5 de octava generación, los ingenieros cuentan con la suficiente potencia y rapidez que necesitan. Todas sus tareas como configurar la parada de boxes o hacer pruebas de velocidad en el circuito pueden completarse mucho más rápido que antes.

SACA BRILLO A TUS CARRERAS

Diseñado para una vida ligada a los garajes y las carreras, el portátil Acer ENDURO N7 está equipado con una pantalla que funciona muy bien en interiores y exteriores. Para potenciar la visibilidad en condiciones de mucha luz su pantalla ofrece 700 nits de brillo. Esto permite a los ingenieros trabajar a pleno rendimiento incluso en condiciones de luz natural, pudiendo ver con claridad las condiciones del coche, rastrear su velocidad y cualquier otra tarea sin sacrificar la batería del dispositivo.

¡NUNCA TE QUEDES SIN COMBUSTIBLE

No importa el entorno, en las carreras cualquier equipo informático está funcionando en todo momento. Esta es la principal razón por la que el equipo de carreras de Alfa Romeo se enorgullece de trabajar con el portátil Acer Enduro N7 el cual no solo viene equipado con una batería de alta capacidad (10 horas de uso) adaptable, sino también otra batería extra de refuerzo. Los ingenieros pueden hacer uso del mismo dispositivo durante varios desplazamientos sin tener que apagarlo.

CONECTADO EN CUALQUIER LUGAR

Diseñado para ser más delgado y ligero que otros modelos similares, Alfa Romeo también puede tener la seguridad de permanecer conectado gracias a la consistente señal inalámbrica que ofrece su antena wireless WiFi 5 (802.11ac) convenientemente colocada. Y el chipset GPS integrado permite a los miembros del equipo conectar automáticamente sus datos a la localización de las pruebas.

LA POLE POSITION EN SEGURIDAD

En el mundo de las carreras profesional, todos los datos relacionados con el rendimiento y la configuración tienen que permanecer a salvo. Alfa Romeo ha escogido los dispositivos ENDURO porque tratan cualquier aspecto relacionado con la seguridad con la importancia que merece. Su sistema TPM 2.0 es un potente chip resistente a manipulaciones externas que comprueba si existen signos de intrusión mientras se enciende el equipo. El sistema Acer Enduro Manageability Suite (AEMS) protege el dispositivo y acelera el despliegue de servicios y la configuración del sistema a través de varios dispositivos.

Descubre todas las soluciones Enduro en acer.es

Tecnología y talento, las claves para afrontar 2021



Por David Alonso,
director del área B2B de Samsung

La crisis del COVID-19 ha cambiado totalmente nuestras vidas y ha complicado nuestra situación económica. Los ERTE y el cese de actividad en algunos negocios han afectado de lleno al tejido empresarial de nuestro país, que está conformado por pymes en un 99%. Incluso el aprendizaje se ha transformado, dando paso al e-learning, que se extendió en muchos hogares durante el confinamiento; pero que ha puesto de manifiesto una brecha digital: 683.000 alumnos en España no han tenido acceso a dispositivos móviles para continuar con su educación mientras estaban en casa.

Por lo tanto, tanto empresas como instituciones públicas han visto este año que la digitalización no es una posibilidad. Se trata de una necesidad urgente, que debe realizarse en un momento complicado, donde también contamos con muchas oportunidades y recursos para llevarla a cabo con todas las garantías. La Agenda Digital 2025 y las ayudas de la Unión Europea son una base para poner en alza el talento de muchos profesionales que van a liderar esta transfor-

mación, desde múltiples disciplinas y sectores en nuestro país.

Además del talento, la tecnología va a ser el gran catalizador de este cambio, desde tres puntos de vista. El primero, que afecta a cualquier tipo de negocio, es la tecnología que ayuda en la eficiencia de los procesos, en el ahorro de costes y, por consiguiente, en la competitividad del negocio. La segunda afecta a las personas, que hemos modificado nuestros hábitos para adaptarlos a una nueva realidad: para comunicarnos, comprar y entretenernos de forma digital; y que también afecta a las organizaciones, que deben adoptar una relación digital con los clientes y ciudadanos. Y el tercero es la responsabilidad digital, que debe existir para controlar los riesgos de este cambio.

Esta evolución debe llevarse a cabo sin ningún tipo de brecha, en empresas e instituciones. En todas ellas habrá un factor que permitirá que el cambio de desarrolle de forma fluida: el 5G. En Samsung creemos que las redes de próxima generación son un elemento de diferenciación tecnológica y un impulsor del cambio. En nuestro caso, disponemos de un ecosistema completo: desde el chip hasta las antenas. Por lo tanto, podemos asegurar una gran fiabilidad y seguridad en el desarrollo de 5G. Somos líderes en todo el mundo, tanto en infraestructura como en dispositivos.

Otro factor transversal en esta transformación es la ciberseguridad; para que todos los servicios públicos y privados puedan funcionar de forma digital y sin fisuras. Gracias a Samsung Knox, nuestra plataforma de seguridad móvil de extremo a extremo, nuestros dispositivos son los más seguros del mundo, así lo confirma Gartner desde hace varios años. También colaboramos activamente con el INCIBE, referente mundial en materia de seguridad, y somos el único fabricante de móviles certificado por el CCN en España.

En resumen, el próximo año 2021 debe ser el año donde la digitalización nos transforme como país. Nos encontramos ante una oportunidad única para posicionarnos en un nuevo ámbito competitivo, donde es fundamental la cooperación público-privada, el uso de la tecnología y el talento de los profesionales. Las pymes y las Administraciones públicas no están solas, y en Samsung vamos a acompañarlos en este proceso para conseguirlo.

Desafíos de ciberseguridad en tiempos de pandemia



Alfonso Ramírez,
director general de Kaspersky Iberia

2020 ha sido un año complicado, aunque al mismo tiempo interesante para todos aquellos que nos dedicamos a la ciberseguridad. La pandemia ha desencadenado un aumento del cibercrimen a todos los niveles. Cibercriminales y grupos organizados aprovecharon los meses de desconcierto global para desplegar nuevos métodos y vectores de ataque. Las cifras hablan por sí solas: en marzo los ciberataques relacionados con el Covid-19 alcanzaron el pico de un millón al día y se produjo un aumento del 30.000% en phishing, sitios web maliciosos y malware dirigido a usuarios remotos.

Y es que el escenario cambió inesperadamente y de forma abrupta. Si a principios de año las empresas estaban inmersas en el reto del IoT y en cómo conectar los distintos elementos en sus infraestructuras, de forma repentina, en marzo, tuvieron que hacer frente al reto del teletrabajo. De un plumazo las organizaciones vieron borrado su perímetro, lo que puso de manifiesto múltiples carencias: equipos desactualizados o no protegidos, conexiones no seguras, escasez de protocolos básicos de ciberseguridad y de concienciación de los usuarios.

Todo ello ha generado una mayor necesidad de protección de las actividades de negocio. Y, a pesar de que debido al impacto económico de la pandemia se ha recortado el gasto de TI en general, nuestros datos señalan que la ciberseguridad seguirá siendo una inversión prioritaria para las empresas.

De hecho, el 67%¹ de las organizaciones europeas espera aumentar en los próximos tres años su presupuesto en este ámbito.

Y es que 2021 traerá nuevos desafíos para los que las organizaciones deberán estar preparadas. Es probable que la crisis por el Covid-19 provoque una ola masiva de pobreza, lo que invariablemente se traduce en que un mayor número de personas recurran a la delincuencia (incluida la cibernética). En el ámbito de las ciberamenazas financieras, las más peligrosas puesto que afectan al bienestar económico de las víctimas, surgen nuevas tendencias. El desplome de algunas economías y monedas hará mucho más atractivo el robo de bitcoins. Deberíamos esperar más fraudes dirigidos principalmente a BTC debido a que esta criptomoneda es la más extendida.

Asimismo, pronosticamos un crecimiento aún mayor de los intentos de extorsión, ya sea a través de ransomware, ataques DDos o incluso ambos. Se consolidarán y utilizarán exploits avanzados como zero-day – vulnerabilidades aún no encontradas por los desarrolladores- o N-days para atacar a las víctimas. Los grupos de ransomware con más fondos resultado de los ataques cometidos con éxito en 2020, podrán adquirirlos en el mercado negro para escalar y aumentar así la efectividad de los ataques. Esto resulta especialmente crítico para aquellas compañías más sensibles a la pérdida de datos, que habrán de pasar por un proceso agotador de recuperación de datos y la interrupción de sus operaciones online.

Veremos también un cambio en los métodos utilizados por muchos cibercriminales para exigir el pago. Es probable que se utilicen otras criptomonedas de mayor privacidad, como Monero, como primera moneda de transición, y que los fondos se conviertan más tarde en otras criptomonedas cifradas, incluyendo Bitcoin, para cubrir las huellas de los cibercriminales.

Estos son sólo algunos ejemplos de lo que podemos esperar en 2021. Vivimos tiempos complejos, que ponen de manifiesto la necesidad de colaboración entre las instituciones públicas y el sector privado para compartir inteligencia y redoblar los esfuerzos en ciberseguridad. Existen ya iniciativas llevadas a cabo con éxito en este sentido. Por ejemplo, el proyecto NoMoreRansom, del que Kaspersky es fundador, ha logrado evitar el pago de 643 millones de euros. Es un paso, pero aún queda mucho camino por recorrer. Unidad de acción y transparencia serán factores clave para afrontar los nuevos desafíos en materia de seguridad TI.

Tres prácticas recomendadas para prevenir ataques de ransomware



Por Carlos Vieira, Country Manager de WatchGuard para España y Portugal

El número de ataques de ransomware se ha disparado en los últimos años, y la situación de la pandemia lo ha fomentado, infectando a millones de equipos y costando a las empresas millones de pérdidas. Recomendamos tres prácticas óptimas que todas las organizaciones, independientemente de su tamaño y sector, deberían aplicar.

1. Educación y concienciación

Detestamos decir esto, pero el mayor activo de su empresa es también su eslabón más débil y su principal vector de ataque. Muchos de sus empleados nunca han oído hablar de phishing o de un ataque man-in-the-middle, y los hackers lo saben. Es esencial educar a los empleados sobre los métodos de ataque más comunes y cómo evitarlos. Aquí hay algunos consejos básicos que puede darles:

- No pinchar nunca en los links proporcionados en un correo electrónico. Escriba o copie la dirección en el navegador para evitar abrir inadvertidamente un enlace que enmascarado un sitio web malicioso.
- Tener cuidado al abrir los archivos adjuntos de los correos electrónicos. Este es el método más común de ataque por ransomware.
- Cuando se acceda a un sitio web, hay que prestar atención a la URL. Los sitios maliciosos comunes incluyen URL con direcciones IP al principio o un supuesto sitio seguro que no utiliza HTTPS.
- Las direcciones de correo electrónico clonadas son otro método para adquirir información confidencial. Nunca se debe enviar información personal por correo electrónico. ¡Es mejor utilizar el teléfono!
- Nunca se debe dar la contraseña a nadie por correo electrónico. Las compañías legítimas nunca solicitan credenciales de acceso por email.

2. Backup. Backup. Backup.

Hay una solución fácilmente evitable para los ataques de ransomware: tener varios juegos de copias de seguridad. Los dispositivos NAS no son copias de seguridad, son simplemente grupos de almacenamiento que contienen datos que ofrecen formas convenientes de acceder y manejar esos datos. Y esto no es suficiente. Es vital tener backups adicionales, en la nube o, preferiblemente, en copias de seguridad offline. Sí, backups offline. Después de todo, el ransomware moderno puede encontrar y cifrar el almacenamiento en red. Una buena copia de seguridad manual en un horario regular ayudará a asegurar que tenemos la última copia de nuestros datos listos para usar en caso de que se produzca un ataque.

Igualmente, es importante automatizar las copias de seguridad siempre que sea posible. No hay que dejar que un error humano haga que la compañía pierda un backup.

3. Defensa en profundidad

Los ataques de ransomware intentan aprovechar todos los posibles vectores de ataque. Cuantas más capas de seguridad existan, mayores serán las posibilidades de evitar un ataque que otra capa podría haber dejado pasar. Estos tipos de ataque pueden convertirse en algo único, desviándose de los métodos tradicionales de detección basados en firmas. Estas son algunas de las capas de seguridad críticas que cualquier organización debería tener:

- Proteja su red. El ransomware no solo utiliza la red para conectarse a un servidor malicioso y obtener la clave de cifrado, sino que también utiliza la red para propagar el ataque en una organización.
- Aproveche el entorno de sandboxing para mitigar las amenazas zero-day. El entorno sandboxing es una excelente herramienta para prevenir el malware desconocido sin arriesgar la seguridad del dispositivo.
- Obtenga visibilidad en dispositivos endpoint. Los ataques de ransomware a menudo comienzan en los dispositivos endpoint. Tener visibilidad de la actividad de estos dispositivos permite detectar y remediar las amenazas antes de que se produzcan daños.
- Conecte los puntos entre la red y el endpoint. La correlación de los datos de los eventos de red y del endpoint proporciona una evaluación global y exhaustiva de amenazas.

Automatización inteligente de procesos con ReexDoc



Por Diana Argudo Alcolado, directora de desarrollo de negocio en pfsTECH, by pfsGROUP

Nuestro reto como líder de la transformación eficiente consiste en analizar los procesos operacionales de nuestros clientes e identificar posibles ineficiencias para, a través de la automatización con RPA (Robotic Process Automation) e IA (Inteligencia Artificial), generar modelos de negocio más rentables, sostenibles y productivos.

Para conseguir este reto en pfsTECH centramos el foco en la automatización inteligente como vía para lograr eficiencias y reducción de costes, así como la búsqueda de nuevas vías de interacción y colaboración entre empleados y proveedores para poder llegar con una propuesta de valor diferencial al cliente.

Como palanca de automatización inteligente disponemos de ReexDoc, una potente plataforma diseñada para el Reconocimiento y Extracción de información en Documentos de forma automatizada, a través de técnicas de IA.

ReexDoc es una solución de pfsTECH, pensada para transformar y convertir en más eficientes los procesos de extracción y gestión de documentos, que a su vez

permite integrarnos vía API con otros fabricantes líderes del mercado de RPA como UiPath, Automation Anywhere, Blue Prism o Help Systems.

Con la suma de ReexDoc + RPA podemos conseguir la automatización inteligente de un proceso, end to end, de principio a fin, dejando la responsabilidad de toma de decisiones y analítica a nosotros, los humanos, un modelo híbrido en donde se integran procesos manuales y procesos digitales existentes.

La automatización inteligente de procesos potencia las capacidades de las personas, aumentando su productividad y su aporte de valor de negocio, ideas, estrategias, reduciendo su tiempo dedicado a tareas de poco valor para conseguir mayor agilidad, productividad y calidad. La cantidad de procesos que pueden ser automatizados con esta combinación de tecnologías

es muy elevado a día de hoy: contabilización de facturas, procesamiento de pedidos, gestión de albaranes, partes médicos, tramitación de prestaciones/pagos, extracción de movimientos bancarios, reporting, procesos de atención en contact centers, alta de empleados, etc.

Un caso de uso muy demandado y claro en las organizaciones viene a ser el procesamiento de facturas, desde su recepción por email hasta su contabilización extremo a extremo.

Los procesos de backoffice son buenos candidatos para la automatización inteligente, en donde toda la parte tediosa de extracción de datos recae en ReexDoc y las acciones a realizar con esos datos recae en RPA.

Impulsar la automatización inteligente en las organizaciones y adoptar este cambio aumenta la competitividad de las empresas, potencia las capacidades de sus empleados, incrementa la eficiencia y mejora la agilidad y productividad.



ADELANTARSE A LOS
CAMBIOS **IMPORTA.**



Las principales empresas
del mundo confían en
InterSystems para resolver
sus retos más difíciles.

