



En busca de la conectividad inteligente



it TRENDS



it Digital MEDIA GROUP

Director General

Juan Ramón Melara

juanramon.melara@itdmgroup.es

Director de Contenidos

Miguel Ángel Gómez

miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen

Arancha Asenjo

arancha.asenjo@itdmgroup.es

Directora División Web

Bárbara Madariaga

barbara.madariaga@itdmgroup.es

Directora de IT Digital Security

Rosalía Arroyo

rosalia.arroyo@itdmgroup.es

Director de IT User e IT Reseller

Pablo García

pablo.garcia@itdmgroup.es

Director de Operaciones

Ángel Porras

angel.porras@itdmgroup.es

Redacción y colaboradores

Ricardo Gómez, Alberto Varet,

Hilda Gómez, Arantxa Herranz,

Reyes Alonso, Belén Juárez

Eva Herrero

Favorit Comunicación, Alberto Varet

Ania Lewandowska

Diseño revistas digitales

Producción audiovisual

Fotografía

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

El show debe continuar y la tecnología puede hacerlo posible



No está siendo una época fácil para las organizaciones. El parón provocado por la pandemia está haciendo que muchas hayan visto interrumpidas sus actividades, perdido tiempo en reajustarse a la situación y caer sus negocios. Otras han sabido adaptarse, tener capacidad de resiliencia para absorber el impacto y salir del paso amoldando personal y negocio a los tiempos que corren.

Muy buena parte de esa respuesta ágil se ha debido a las habilidades directivas para organizarse frente a la crisis, pero también la tecnología ha tenido su protagonismo y lo tendrá aún más para devolvernos a esa "nueva normalidad" que va a regir nuestro día a día en los próximos meses y años.

Es el momento de acelerar esa transformación digital de las organizaciones, no solo pensando en el teletrabajo, sino en estrategias tecnológicas que garanticen la conectividad inteligente y ágil de espacios físicos, empleados y otros elementos que intervienen en la toma de decisiones empresariales; que permitan ganar productividad; que garanticen el acceso seguro a las aplicaciones y datos ubicados en la nube; en definitiva, prácticas tecnológicas que, sumadas a las decisiones corporativas, den lugar a organizaciones fuertes y capaces de dar respuesta a las necesidades cambiantes del mercado.

Este trimestre en IT Trends hemos puesto el foco en tres áreas que permiten todo esto. En este número podrás leer ampliamente sobre ello, además de poder ver a sus protagonistas. En el IT Webinars [La era de la conectividad](#), abordamos cómo 5G, WiFi, SD-WAN, el open networking y el acceso remoto seguro, facilitan a las empresas afrontar las más exigentes demandas de

conexión ante un entorno en el que las necesidades se multiplican y los volúmenes de datos a transmitir crecen de manera exponencial. Participaron en la sesión Citrix, HPE, VMware, Sonicwall, Dell Technologies y D-Link.

Uno de los objetivos de las organizaciones es sacar mayor provecho de todo lo que hacen. Las tecnologías de automatización inteligente de tareas lo hacen posible. En las siguientes páginas podrás leer nuestro [Especial RPA: la automatización que te hará ganar agilidad corporativa](#), con las principales claves de esta tecnología ofrecida de la mano de Appian, ABAI Group y Automation Anywhere.

Y por último, la identidad; esa pieza única que debería darnos acceso a redes, datos y aplicaciones para garantizar la total seguridad de la información que manejan las compañías. Empleados, clientes y proveedores juegan un papel fundamental a la hora de blindar esta muralla que debe levantarse entorno a la información. Este fue el tema central del IT Webinars [Autenticación y gestión de identidades, el nuevo perímetro de seguridad](#), en el que participaron CyberArk, Micro Focus, Fortinet, Thales, Check Point, F5 Networks, One Identity, Akamai y SonicWall.

Y no podíamos finalizar el trimestre sin ofreceros los resultados de nuestra encuesta: **Teletrabajo en 2020**, el futuro se hace presente, que [podéis leer aquí](#).

No nos queda más que deseáros una buena lectura (recuerda que tienes cientos de enlaces y vídeos para bucear tanto como quieras en la información) y... ¡un feliz verano! ■

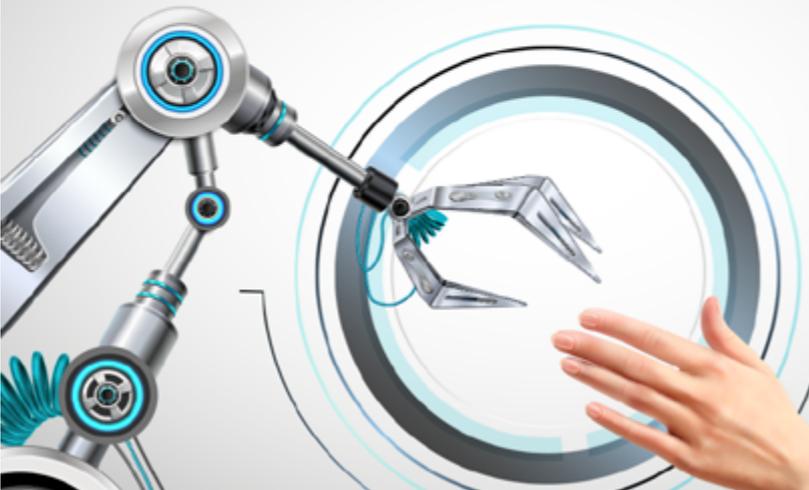
Arancha Asenjo
Directora de IT Trends

www.ittrends.es

Encuentros **it** TRENDS

Inteligencia Artificial
¿cómo lo aplico en mi empresa?

#ITWebinars



23 de septiembre de 2020 · 11:00 h

it TRENDS

La inteligencia artificial (IA) es una rama amplia de la ciencia de la computación que se ocupa de construir máquinas inteligentes capaces de realizar tareas que generalmente requieren inteligencia humana. La IA es una ciencia interdisciplinaria con múltiples enfoques, pero los avances en el aprendizaje automático y el aprendizaje profundo están creando un cambio de paradigma en prácticamente todos los sectores de la industria.

¿Cómo puedo mejorar los procesos empresariales utilizando Inteligencia Artificial?
¿De qué manera puedo sacar provecho para mi organización de las capacidades que esta tecnología propone?

23 de septiembre de 2020 - 11:00 (CET)

REGISTRO



La persistencia del ransomware

#ITWebinars



30 de septiembre de 2020 · 11:00 h

it TRENDS

6 de cada 10 organizaciones fueron víctimas de ransomware en 2019, una cifra que va en aumento año a año debido al incremento en los pagos de rescates. Más de un tercio de las organizaciones experimentaron seis o más ataques exitosos, y el 69% esperan sufrir uno este año.

Aunque inicialmente el ransomware se utilizaba de manera aleatoria, infectando usuarios a los que se pedían rescates de cientos de dólares por recuperar el control de sus ordenadores, los ataques se han hecho mucho más dirigidos y ambiciosos, llegando a colapsar empresas e incluso ciudades. Nadie está a salvo de una amenaza difícil de rastrear.

¿Cómo hacer frente a la amenaza? ¿Por qué no es suficiente con tener un buen backup?
¿Qué sectores están más expuestos? Podrás conocer todas las respuestas en este webinar.

30 de septiembre de 2020 - 11:00 (CET)

REGISTRO



Tecnología, habilitador de la “nueva normalidad”

Durante lo peor de la crisis sanitaria por la COVID-19, las organizaciones han estado utilizando la tecnología para mantener su maquinaria en marcha y, a su vez, minimizar los riesgos para la salud. Esto ha desvelado el gran potencial de la nube, las aplicaciones colaborativas y las comunicaciones de nueva generación, pero también ha revelado la gran brecha digital que afecta a las empresas y sus trabajadores.

Una vez que pase la pandemia, gran parte de la tecnología implementada va a seguir en uso, y los expertos coinciden en que esto transformará para siempre las estructuras empresariales y el propio mercado laboral, en el que las habilidades tecnológicas tendrán más importancia que nunca.

A raíz de la pandemia, las organizaciones han tenido que implementar a marchas forzadas nuevas tecnologías para seguir operando mientras sus empleados se encontraban recluidos en sus hogares. Este cambio ha sido absolutamente disruptivo para ciertas empresas, que hasta ahora no se habían planteado seriamente el uso de nuevas tecnologías ni la necesidad de abordar la transformación digital. Ahora, ante las condiciones de bloqueo impuestas por los gobiernos de los países más afectados, muchas han optado por usar las tecnologías digitales para el trabajo rutinario con aplicaciones empre-

sariales, para habilitar el trabajo colaborativo o para celebrar reuniones a distancia.

Esto está siendo beneficioso en un sentido muy definido, que es el de la modernización de las empresas que se habían mostrado tímidas o indiferentes en cuanto a la transformación digital. Pero a su vez ha puesto de relieve una falta de habilidades digitales entre buena parte del tejido empresarial, y también en los propios trabajadores. De cara al futuro próximo, muchas empresas seguirán utilizando buena parte de las tecnologías que les están permitiendo seguir adelante durante la pandemia, pero para hacerlo correctamente deberán enfrentarse a la brecha digital.

Numerosas organizaciones alertan de los peligros que tiene implementar las nuevas tecnologías sin contar con los conocimientos necesarios en materias como la seguridad cibernética. Como muestra de ello, los últimos estudios revelan que gran parte de las empresas no están preparadas para efectuar el cambio definitivamente, sin antes resolver ciertos problemas básicos. Por ejemplo, en el reciente informe [“Flexibility at Work”](#) realizado por Randstad, los expertos destacan los graves problemas a los que se enfrentan tanto las empresas como los trabajadores españoles para abordar estos cambios en el futuro cercano.

EL TELETRABAJO COMO EJE DEL CAMBIO

Si algo ha demostrado la pandemia es que, a igualdad de condiciones, las empresas con ma-

yor grado de automatización han sido más capaces de mantener las operaciones durante lo peor del confinamiento. Lo mismo se puede decir de aquellas que han podido implementar a tiempo el teletrabajo, permitiendo a sus empleados continuar con la mayor parte de sus funciones sin que se produzcan efectos negativos importantes para el negocio. En este sentido, según la investigación de Randstad, el 42% de las empre-

sas españolas han implantado sistemas de trabajo remoto para seguir funcionando en estos meses de confinamiento. Según este análisis, lo positivo es que, a pesar de verse obligadas a tomar estas medidas, lo que causó una sorpresa inicial y cierta indignación, el 58% de los trabajadores españoles afirma que antes de esta crisis su empleo ya reunía las condiciones propicias para convertirse en un puesto de trabajo remo-

Sólo los profesionales adaptados al cambio digital tendrán éxito cuando la situación se normalice

5 HABILIDADES EMPRESARIALES PARA SALIR REFORZADOS DE LA CRISIS DE LA COVID-19

Las empresas tecnológicas comienzan a recuperar fuerzas

El impacto de la pandemia en las empresas tecnológicas ha sido serio, ya que los clientes han reducido al mínimo el gasto en tecnologías no esenciales, pero a su vez se están generando nuevas oportunidades. Una reciente investigación realizada por la asociación tecnológica CompTIA señala que el ambiente general de los negocios tecnológicos se está estabilizando, con claras señales de mejoría a corto plazo. Esto está motivado por la creciente demanda de servicios de seguridad, computación en la nube y otras áreas que están cobrando importancia para las organizaciones a raíz de la pandemia.

Según indican los datos de este estudio, el porcentaje de empresas tecnológicas que ha experimentado un aumento en las consultas de nuevos clientes y en las oportunidades comerciales fue del 83% en abril y del 84% en junio, un aumento significativo frente al 76% registrado en marzo. Como explica Nancy Hammer, vicepresidenta ejecutiva de relaciones industriales de CompTIA, "sigue habiendo mucha incertidumbre sobre el impacto de la pandemia en el futuro, pero es una señal esperanzadora de que la tecnología se vea como una solución para ayudar a las empresas

a navegar en estos tiempos inciertos". Las principales prioridades de inversión para las organizaciones son los productos y servicios relacionados con la seguridad cibernética, como informa el 42% de las empresas encuestadas. Le sigue el cambio de infraestructura o aplicaciones locales a la nube (42%), los servicios de TI gestionados y subcontratados (40%) y la consultoría general de ayuda para adoptar las tecnologías virtuales (40%). Y también destacan que el área de personal está demandando nuevos servicios tecnológicos para apoyar las estrategias de contratación de cara al futuro.

to. Y el 68% de los trabajadores ya demandaba esta forma de trabajo como medio para mejorar su calidad de vida y su conciliación familiar, pero su empresa lo impedía.

Pero esto se debe mirar con lupa, ya que la realidad es que existe un desconocimiento general muy profundo sobre ciertas cuestiones fundamentales relativas al trabajo remoto en la era digital. Sobre todo, en materia de ciberseguridad, ya que los entornos domésticos y profesionales no se pueden mezclar de forma segura sin seguir ciertas pautas y contar con ciertas tecnologías, algo que desconoce la mayoría. Además, a pesar de sus demandas de teletrabajo, gran parte de la población activa se puede considerar en etapas tempranas de la alfabetización digital, ya que desconocen las características y particularidades de muchas de las tecnologías necesarias para trabajar desde casa.

IMPACTO DE LA AUTOMATIZACIÓN EN EL MERCADO DE TRABAJO

No todos los sectores han podido solucionar los problemas que ha planteado el confinamiento con trabajo remoto, ya que muchas empresas requieren operarios físicos para realizar el trabajo. Por ejemplo, el transporte, la sanidad o la industria manufacturera, y estas empresas ponen sus miras en una estrategia que combine la posibilidad del trabajo remoto con mayores capacidades de automatización.



Y esto significa menos personal humano imprescindible y más automatización a través de maquinaria, robótica y software autónomo.

En estos ámbitos se prevé que la destrucción de empleo podría ser importante en la próxima década, a medida que las fábricas, los almacenes minoristas, o el transporte de mercancías y personas se automaticen más y más. De hecho, muchos fabricantes están planificando la posibilidad de acelerar las próximas etapas del proceso de automatización en el que se han embarcado a largo plazo. Y empresas que no lo consideraban posible, ahora se lo están planteando para prepararse de cara al futuro, tanto por competitividad como por resiliencia frente a situaciones de emergencia como la que estamos viviendo.

Para los expertos en el mercado laboral esto va a tener un impacto radical en el mercado de trabajo,

ya que no solo se reducirá la plantilla en muchas empresas, sino que los requisitos para acceder a los puestos de trabajo estarán cada vez más vinculados a las habilidades tecnológicas, y los trabajadores deberán adquirir nuevos conocimientos y especializarse más. Según la investigación de Randstad Research, en los países de la OCDE el 30% de los empleos se verá modificados tras la pandemia, mientras que el 70% de los trabajos actuales desaparecerá, cifras mucho más desalentadoras que las de investigaciones anteriores.

NUEVOS CONOCIMIENTOS TECNOLÓGICOS PARA CONSEGUIR EMPLEO

Mientras que hasta hace relativamente poco los expertos consideraban que la digitalización y la automatización generarían nuevas y excitantes posibilidades en el mercado laboral, ahora el fu-

turo se percibe con muchas más dificultades para los trabajadores. Los expertos han apoyado la automatización como medio de modernizar la economía, proporcionando puestos de trabajo más dignos y estimulantes a las personas, pero ahora perciben notas más negativas en este avance, ya que la posibilidad de que se repita una situación como la generada por la pandemia de la COVID-19 genera mucho temor e incertidumbre.

Ante esta situación, muchas empresas están buscando en la tecnología una forma de garantizar la continuidad de las operaciones, independientemente de que sus empleados deban quedarse en casa, y esto pasa por una mayor automatización y un aumento del uso de tecnologías digitales en los puestos de trabajo restantes. Así, los empleados del futuro (y no muy lejano), deberán adquirir nuevas habilidades para encajar en la nueva realidad del mercado de trabajo, ya sea que estén en una empresa en proceso de cambio o que quieran acceder a un puesto de trabajo.

Los entornos domésticos y profesionales no se pueden mezclar de forma segura sin seguir ciertas pautas ni tecnologías



Como explica en su informe Valentín Bote, director de Randstad Research, “el teletrabajo no va a ser el único avance tecnológico obligado que nos va a traer la pandemia. La automatización va a ver crecer su protagonismo por la importancia de evitar aglomeraciones, lo cual, lejos de amenazar al empleo, va a generar nuevas oportunidades. Para los profesionales interesados en aprovecharlas, es recomendable seguir de cerca la evolución del mercado laboral y apostar por la formación continua”. Porque un elevado porcentaje de las empresas está teniendo dificultades para encontrar personal cualificado, ya que la brecha digital es muy amplia en general, y es preciso trabajar para reducirla lo antes posible, tanto para los trabajadores en activo como para los futuros profesionales de todas las industrias.

AUMENTA EL RIESGO DE PRECARIEDAD

Los analistas de Randstad prevén que, tras la pandemia, se producirá un movimiento mucho más veloz de lo previsto hacia los empleos a tiempo parcial, las contrataciones temporales, de personal autónomo y a las subcontrataciones a través de ETTs y otras empresas especializadas. Como ejemplo citan el cambio que se produjo en Estados Unidos entre 2005 y 2015, cuando estas modalidades de trabajo pasaron del 10,7% al 15%, una tendencia que se está acelerando peligrosamente y que lo hará aún más a raíz de la pandemia.

Uno de los conceptos que para Randstad va a ponerse más de moda es el de Gig Economy, una modalidad laboral basada en pequeñas tareas o encargos que se pueden llevar a cabo a través de plataformas digitales. Mientras que sus impulsores venden este concepto como una forma de revalorizar el trabajo, en realidad este planteamiento puede esconder un grave problema de precariedad. Porque muchas empresas aprovechan estas plataformas para proponer trabajos puntuales muy mal pagados, por los que una masa creciente de desempleados o trabajadores necesitados compiten, impulsando los salarios a la baja.

Además, en muchos casos esto exige que los trabajadores tengan ciertas habilidades tecnológicas que las empresas dan por hechas, pero que deberán adquirir y costear por sí mismos, en un delicado equilibrio coste-beneficio. Según afirman los responsables de este estudio, el uso de las plataformas de Gig Economy ha aumentado un 30% entre 2016 y 2019, y solo en la Unión Europea esta modalidad de trabajo se ha convertido en la principal fuente de ingresos para el 2% de los adultos.

Aunque el riesgo de precariedad no va a frenar esta forma de microeconomía, más aún teniendo en cuenta que las empresas van a



Muchas empresas seguirán utilizando buena parte de las tecnologías que les están permitiendo seguir adelante durante la pandemia, pero, para hacerlo correctamente, deberán enfrentarse a la brecha digital

apostar por contratar a trabajadores freelance para muchas tareas puntuales, periódicas y específicas. Esto genera oportunidades por las que los trabajadores deberán luchar, y necesitarán contar con nuevas habilidades digitales para poder capitalizarlas, a la vez que luchan por unas condiciones razonables.

GRANDES OPORTUNIDADES PARA LA ROBÓTICA

La automatización suena más que nunca a robótica, ya que las tecnologías implicadas en esta tendencia se basan en una combinación de software y maquinaria cada vez más sofisticada, inteligente y autónoma, que se asemeja cada vez más a los conceptos de robots que la ciencia ficción ha imaginado desde los años 50 del siglo pasado. Ahora hay sectores que pueden sacar partido del impresionante avance que ha dado la robótica, gracias a la combinación de nuevas tecnologías en el campo de la ingeniería mecánica y la automática con la parte de TI. En esta se incluye tanto el hardware de visualización, monitorización y

computación autónoma como el software, donde diversas ramas de la inteligencia artificial han sido absolutamente disruptivas.

Esto está impulsando campos como el de la robótica móvil y la fusión cada vez mayor de las tecnologías de la información con las tecnologías operativas clásicas en las fábricas y en otros entornos. Ahora, además de su tradicional aplicación en las cadenas de montaje de las fábricas, los robots están irrumpiendo en nuevos entornos como el mantenimiento mecánico, los almacenes y centros de intercambio logístico y áreas donde hasta ahora sus aplicaciones eran muy limitadas, como el de la atención médica, donde se han convertido en herramientas fundamentales para la limpieza y la higienización de objetos, superficies y salas completas.

Pero, así como la revolución industrial impulsó un cambio radical en el mercado de trabajo en el siglo XIX, la transformación digital y la automatización a través de la robótica tienen el potencial para generar cambios a gran escala en el mercado de trabajo. Según la investigación de Rands-

tad, la compra de robots ha aumentado un 16% en todo el mundo en la última década. En España, concretamente, hay 157 robots industriales en las fábricas por cada 10.000 trabajadores, con una tasa de robotización del 1,57%, mientras que en Europa este índice es de un 1,06%.

Y se sitúa por delante de otros países fundamentales en la economía de la Unión, como es Francia (1,37%), y de otras economías fuertes como la de Suiza (1,29%) o la propia China (0,97%). Aunque queda bastante por debajo de otras economías fuertes de nuestro entorno, como Alemania (3,22%), Suecia (2,40%) o Dinamarca (2,30%), y de otras economías de primer nivel, como Corea del Sur (7,10%), Singapur (6,58%), Japón (3,08%) o Estados Unidos (2%).

Otro aspecto que destacan los expertos es la relación entre la robotización y el envejecimiento de la población, y señalan que donde habrá más robots será en los países que envejecen más tarde, sobre todo por el impulso que se dará en el campo de la atención sanitaria a personas mayores.

LOS NUEVOS ENTORNOS DE TRABAJO REQUIEREN NUEVOS PERFILES

A pesar de que las nuevas tecnologías aplicadas a las empresas y las nuevas formas de trabajo remoto, externalización y microempleo están alterando radicalmente el mundo laboral, no todo se ve turbio en el futuro. Con la expansión de las nuevas tecnologías y la popularización de nue-

5G y la nube en el borde, tecnologías clave para la recuperación económica

Desde que dio comienzo el confinamiento, las empresas comenzaron a cambiar su estrategia operativa para dar cabida al teletrabajo, y para automatizar al máximo cualquier interacción con los usuarios y clientes y minimizar el riesgo de contagio. Muchos de estos cambios han llegado para quedarse, porque las empresas están aprendiendo a trabajar de otra forma, que en muchos casos es incluso más eficiente y permite reducir costes tradicionalmente fijos, como los relativos a los puestos de trabajo.

Pero esto también tiene su propio coste, ya que las infraestructuras tecnológicas y las redes empresariales no estaban bien preparadas para una situación como la que estamos viviendo, por lo que muchas organizaciones públicas y empresas han tenido que adoptar soluciones poco ortodoxas para salir del paso. Ahora que los efectos de la enfermedad están mitigándose ya se está comprobando que nada volverá a ser exactamente igual que an-

tes de la pandemia, y mucho menos en las empresas, que ahora deberán escoger si consolidan sus estrategias adoptadas “temporalmente” para superar la crisis o si darán el paso final hacia una transformación definitiva.

Según los expertos de [ABI Research](#), esta segunda opción parece ser la que tomarán buena parte de las empresas, que apostarán por modelos que ya han adoptado parcialmente, y que les aportan beneficios operativos y comerciales. Pero modificar la arquitectura de la red empresarial para ser más flexibles y dinámicos a través del teletrabajo y las nuevas tecnologías exige implementar toda una nueva gama de sistemas, entre los que los expertos destacan las infraestructuras cloud-Edge y las redes 5G.

La consultora pronostica en uno de sus últimos informes que estas dos tecnologías van a ser clave para la recuperación económica, ya que estarán íntimamente ligadas a la transformación digital que buscan

las empresas. Y tendrán un papel aún más importante si se produce lo que muchos temen: un rebrote virulento de la enfermedad, ya sea este mismo otoño-invierno o en temporadas posteriores. Y estas tecnologías no solo impactarán en ciertos sectores, sino que generarán un mercado floreciente en diferentes eslabones de la cadena de suministro tecnológico, e impulsarán grandes beneficios comerciales para industrias como la de telecomunicaciones o las de diferentes categorías de servicios TI.

Como explica en su informe Don Alusha, analista senior de ABI Research, “una combinación de cómputo en la nube y conectividad 5G ultra confiable de baja latencia será la base para impulsar el crecimiento posterior a la COVID-19. Este crecimiento no es solo para las telecomunicaciones, sino también para una multitud de industrias pesadas en activos, que están adoptando los primeros procesos y operaciones digitales”. Con esto se refiere a la

sinergia entre 5G y la computación cloud en el borde, que proporcionará grandes oportunidades a los proveedores de servicios de comunicaciones (CSP), que se enfrentan a un cambio importante en la propia naturaleza de los servicios que demandan sus clientes.

Además, la transformación que ha impulsado la pandemia abarca otros sectores relacionados, como es el de los operadores hiperescala, que ahora deben afrontar sus propios cambios. Según dice Alusha, “los proveedores de hiperescala como Amazon y Microsoft están aprovechando sus operaciones de pequeña escala para lanzar sus ofertas cloud-edge. Tienen la visión de desarrollar capacidades cercanas al límite, pero no necesariamente tienen la penetración y distribución de las capacidades de red que tienen los CSP. Claramente, hay una oportunidad lista para ser abordada por alguien, pero aún no se sabe quién captura qué partes del emergente borde de la nube y el ecosistema 5G”.

vos paradigmas de entorno laboral se generan retos, ya que es imprescindible que los trabajadores cuenten con toda una nueva serie de habilidades. Pero si los profesionales y las empresas trabajan juntos para superar el bache, se abren nuevas oportunidades para la modernización de profesiones tradicionales y para la creación de otras nuevas, impulsadas por la tecnología.

Si actualmente las habilidades tecnológicas son cada vez más determinantes en la cualificación de los trabajadores, tras la pandemia lo serán aún más. De hecho, determinarán casi completamente la capacidad de las personas para obtener y mantener un empleo, así como para progresar en su carrera profesional. Pero actualmente la brecha digital es muy grande, y un 25% de las grandes empresas de los países miembros de la OCDE se ven en dificultades para encontrar trabajadores cualificados para determinados perfiles tecnológicos. Resolver esto no es tarea fácil, pero

las organizaciones empresariales, las instituciones académicas y los gobiernos están impulsando nuevos planes de formación tecnológica más acordes a las necesidades reales de las empresas.

Con ello pretenden reducir lo antes posible la escasez de talento tecnológico, un factor que frena la competitividad de los países y sus industrias en la economía globalizada. Esto irá acompañado de los grandes cambios que ya se están produciendo en la estructura de las organizaciones públicas y privadas, dos complicaciones que al confluir enturbian el futuro del mercado laboral. Para abordar este problema creciente, los expertos de Randstad recomiendan reavivar el diálogo social para involucrar a todos los actores de la sociedad, para conocer tanto la opinión como las necesidades de las personas y de las empresas, y cómo toda la estructura de la sociedad puede aportar su grano de arena para sentar las bases de la futura economía, no solo de las empresas sino de la sociedad. ■



MÁS INFORMACIÓN



[La tecnología cambiará un tercio de los empleos](#)



[Un CEO debe llevar la tecnología en su ADN](#)



[El mercado 5G de consumo se ralentiza, mientras que el empresarial sigue creciendo](#)



[El mercado de robots autónomos en almacenes crecerá con fuerza hasta 2025](#)



[Crece el gasto en soluciones de conferencia basadas en la nube](#)



[Avanzan los planes para crear una nube europea](#)



[Guía mundial de gasto en transformación digital](#)



[Informe Economía Digital en España](#)

Si te ha gustado este artículo,
compártelo



**NUEVO
INFORME**

DOCUMENTO EJECUTIVO

Teletrabajo en 2020:
el futuro se hace presente



ELABORADO POR **itRESEARCH**

Descarga este **documento ejecutivo** de **itRESEARCH**

La era de la conectividad

Las nuevas propuestas de computación requieren mayores velocidades de transmisión y una transformación de los centros de datos y las redes de comunicación. ¿Cuál es el siguiente nivel? Las empresas están construyendo sus infraestructuras de muy diferente manera aprovechando tecnologías como 5G, Wifi, SD-WAN, entornos multicloud; incorporando el IoT; y aumentando la velocidad de conexión. Estas nuevas redes requieren, además, herramientas de monitorización que garanticen la agilidad y productividad, y medidas de seguridad para proteger estas vías de comunicación.

A continuación, puedes leer un resumen de las intervenciones y acceder al vídeo de cada uno de los participantes en el webinar de IT Trends, La era de la conectividad, emitido el pasado junio, o ver la sesión completa en este [enlace](#). Participaron Citrix, HPE, VMware, Sonicwall, Dell Technologies y D-Link. ■



it Nuno Silveiro
Delivery Networks Specialist, Citrix

Nuno Silveiro, Citrix



it Roberto Torres
Global Account Manager Presales, Hewlett Packard Enterprise

Roberto Torres, HPE



it Joaquín Gómez
NSX Sales Account Executive, VMware

Joaquín Gómez, VMware



it Luis Fisas
Director para sur de Europa, Sonicwall

Luis Fisas, Sonicwall



it Gonzalo de Antonio
Sales Executive Iberia, Dell Technologies

Gonzalo de Antonio, Dell Technologies



it Antonio Navarro
Country Manager para Iberia, D-Link

Antonio Navarro, D-Link

NUNO SILVEIRO, DELIVERY NETWORKS SPECIALIST, CITRIX

“SD-WAN conecta con fiabilidad los CPD y las nubes. Aporta una visión amplificada y una capa de seguridad”

Las organizaciones distribuidas necesitan desplegar tecnología que conecte sus diferentes sedes, pero las redes WAN tradicionales tienen ciertas limitaciones de ancho de banda y gestión. La irrupción del concepto de SD-WAN (redes WAN definidas por software) viene a resolver los problemas de fiabilidad y resiliencia de las líneas y mejora la calidad de la experiencia de los usuarios. También resuelven las circunstancias que describía Nuno Silveiro, Delivery Networks Specialist en Citrix durante el IT Webinars [“La era de la conectividad”](#), celebrado en IT Trends. “La mayoría de las empresas se cambian a modelos de negocio digitales porque hay cada vez más competidores”, señaló. Además, las amenazas cibernéticas son una realidad latente en las empresas. “Desde el phishing que busca información oculta hasta la capacidad de los malware de robar datos de los ordenadores de los usuarios. Las compañías han de adquirir sistemas para paliar estos ataques a



NUNO SILVEIRO, DELIVERY NETWORKS SPECIALIST, CITRIX

la vez que optimizan procesos administrativos y de negocio”, prosiguió Silveiro.

Existe una conectividad entre las apps, los datos y la ubicación de los datos. “Están muy distribuidos en aplicaciones SaaS, y en distintas nubes donde los usuarios tienen que conectarse y consumir, lidiando con los retos que hemos identificado previamente. Esto genera un estrés a nivel de conectividad y experiencia del usuario que obliga a las compañías a replantearse un nuevo modo de pensar sobre la conectividad dentro de sus redes en cuanto a optimización y en términos de seguridad”, explicó.

“Abogamos por mantener las aplicaciones con la máxima experiencia de usuario y con seguridad, pero que permitan elegir a las empresas. Queremos que consuman datos en el CPD, en la nube pública, en la nube privada o con multi nubes híbridas, donde ellos quieran, no que tengan solo que centrarse en único producto obligatoriamente”, detalló Silveiro. “Nosotros permitimos a los usuarios que, independientemente de si se conectan por WI-FI o por datos, pueden hacerlo a todas las apps y puedan ser lo más productivos posible. Ahí es donde SD-WAN puede ayudar, ya que se conecta con fiabilidad a los CPD y a las nubes. Tiene una visión amplificada de lo que se produce en el entorno desde un punto de vista central e incluye una capa de seguridad a través de sus conectividades”, comentó este especialista de Citrix. “El objetivo es proveer una buena expe-

riencia de usuario con seguridad y posibilidad de elección para que las empresas se muevan de un entorno a otro y nosotros somos un facilitador de ese cambio. Acompañamos a nuestros clientes sea cual sea su objetivo”, añadió.

Tras la pandemia de la covid-19 y el viraje repentino hacia el teletrabajo de muchas compañías, se ha creado mucho estrés en las organizaciones ya que no tienen centralizada la información. “Han tenido que pensar en la seguridad del acceso y de transporte de todo dispositivo. Nosotros permitimos que los empleados y colaboradores se conecten de un modo efectivo y que se pueda controlar quién accede al sistema y desde dónde accede pues el teletrabajo ya es una realidad”, aseguró Silveiro. “Tenemos que entregar la capacidad de que las empresas tengan seguridad corporativa porque las tradicionales VPN no garantizan la seguridad necesaria pues no controlan ni todos los accesos ni todos los contenidos”, prosiguió.

Y es que, en Citrix, la seguridad es prioritaria. “Hay organizaciones que han migrado escritorios virtuales a la nube sin tener en cuenta que en casa hay más gente que usa la red y puede ser atacada. Hemos desarrollado una solución que permite trabajar en conjunto con la red preinstalada. Es fácil de desplegar y permite un control de la aplicación. Garantiza la política de seguridad al 100%”, concluyó Silveiro.

[Puedes ver aquí la intervención de Citrix.](#) ■



TECNOLOGÍA SD-WAN PARA POTENCIAR EL ESPACIO DE TRABAJO DIGITAL

La tecnología SD-WAN ayuda a las empresas a aprovechar al máximo su inversión, independientemente de que las personas trabajen desde una sucursal o desde una ubicación

remota lejos del centro de datos. Permite utilizar todo el ancho de banda disponible, optimizar el rendimiento para aplicaciones virtuales, Web y SaaS como Office 365, además de otras apps de uso intensivo de ancho de banda como VoIP y garantizar conexiones siempre listas con la mejor calidad posible.



Si te ha gustado este artículo, compártelo



ROBERTO TORRES, GLOBAL ACCOUNT MANAGER PRESALES, HPE

“El empuje de la Industria 4.0 requerirá mayores conexiones y capacidades que 5G puede resolver”

5 G será uno de los motores de movilidad este año. El mercado de infraestructura 5G alcanzará los 4.200 millones de dólares y dos tercios de las empresas desplegarán esta tecnología en 2020 según Gartner. 5G es una alternativa a sus redes actuales con menor latencia y mayor ancho de banda. Esto implica más dispositivos conectados con más capacidades como inteligencia artificial, edge computing o automatización.

“Hay un empuje bestial hacia la industria 4.0 para obtener un mayor rendimiento productivo. La parte VR y AR de realidad aumentada es un caso de uso que va a venir con las nuevas tecnologías de comunicación. Con las gafas de realidad virtual, los empleados se van a poner en frente de las máquinas y leerán el manual de forma virtual”, comenzó Roberto Torres, Global Account Manager Presales en HPE, su intervención en el webinar [“La era de la conectividad”](#), sobre la necesidad de redes



ROBERTO TORRES, GLOBAL ACCOUNT MANAGER PRESALES, HPE

móviles más potentes que den capacidad de comunicación a las nuevas demandas de conectividad.

“Ayudará a que los navegadores de los coches estén conectados entre sí y no solo muestren las líneas verdes o rojas, sino que se verá en tiempo real dónde está el cruce, el semáforo o el peligro y se avisarán unos a otros. Las smart cities con telemetría y sensores ya son una realidad en España. En distintos monumentos se sabe cuándo hay menos personas para limpiar, hacer reformas etc; en sanidad, los doctores usarán esta tecnología para operar en remoto o detectar patologías de manera digital conectando su sistema con el de otros hospitales”, explicó Torres.

Pero, además, 5G traerá cambios fundamentales para las telcos. “Habrá cambios en las funcionalidades. Tiene que cambiar el acceso radio, aunque los teléfonos coexistirán con 4G también. Se producirán modificaciones en las funciones de red de cómo se implementa en el core”, desarrolló Torres. Además, se montarán redes virtuales dentro de la propia red física. “Desde el punto de vista de acceso y movilidad hemos visto la evolución del 1G al 5G. Con 5G se alcanzan velocidades de hasta 10GB por segundo”, prosiguió.

Esta tecnología de 5G convivirá con los equipos Wifi para proporcionar la cobertura necesaria según los casos. “Los dispositi-

vos móviles con imágenes en 4k, cámaras de video con mayor movilidad, más ancho de banda. Hay que evolucionar a microservicios y Kubernetes. Necesitamos crecimiento y la velocidad de despliegue tiene que ser máxima”, señaló Torres. “Las redes de Wifi 6 salen del mismo panel de control de 5G con más dispositivos conectados, más ancho de banda y movilidad entre edificios así que podemos unirlos y ahorrar costes a las grandes telcos”, añadió.

Para este tipo de cliente, HPE propone una línea de servidores rugerizados para el despliegue de redes 5G. “Siempre hemos tenido servidores especializados para el mundo telco. No valen los servidores tradicionales porque hay que llevarlos al Edge. Llevamos tiempo desarrollando equipamientos preparados para aguantar entornos hostiles. Hay mucho polvo y altas y bajas temperaturas, así que hemos tenido que poner equipos especiales. Tenemos la gama tradicional y la Carrier-grade para equipos de telecomunicaciones con despliegues más específicos. Todo es auto programable y definido por el software”, subrayó Torres. “Podemos desplegar entornos de inteligencia artificial, GPUs para desplegarlas en máquinas virtuales o kubernetes donde el IoT pueda orquestar todo este tipo de tecnologías”, concluyó.

[Ve la intervención de HPE en este webinar.](#) ■



LAS VENTAJAS DE LA TECNOLOGÍA 5G

Una red de acceso sólo es posible con un núcleo que sea verdaderamente 5G.

Para HPE es importante la gestión de datos de suscripción y de sesión a través de un entorno de

datos compartidos unificados y centralizados, proporcionar el servicio adecuado para cada caso de uso con una división de la red, acelerar los ciclos de desarrollo a través de una arquitectura abierta de nubes nativas y el enfoque DevOps.



Si te ha gustado este artículo, compártelo



JOAQUÍN GÓMEZ, NSX SALES ACCOUNT EXECUTIVE, VMWARE

“Hemos añadido a la red SD-WAN, el cloud y los usuarios, de manera que tenemos todo en SD-WAN, no solo oficina o campus”

La empresa distribuida y ubicua requiere, de igual manera, redes distribuidas, ubicuas, disponibles para dar servicio, con conexiones fiables y estables y fácilmente gestionables; capaces de interconectar esos entornos de TI híbridos y multicloud donde se alojan las aplicaciones y datos corporativos.

Para VMware, el contexto viene marcado bajo un paradigma de nuevas tecnologías. “Nos estamos moviendo muy deprisa en cuanto a trabajo remoto y dispositivos. Necesitamos muchas más conectividades y de una forma diferente. En VMware nos hemos preguntado dónde está mi red, las apps, y cómo conectarnos de manera óptima”, afirmó Joaquín Gómez, NSX Sales Account Executive, en VMware, durante el IT Webinars [“La era de la conectividad”](#).

“Cualquier dispositivo ha de poder conectarse a tu infraestructura, desde cualquier app y cualquier plataforma. Hay que cambiar cualquier entorno de ejecución porque las apps deben ser



accesibles desde cualquier dispositivo. Todas las operaciones han de ser comunes y la seguridad está embebida en la plataforma”, señaló. Así, la solución de VMware da prioridad a la seguridad y a la migración. “Proponemos diseñar el data center como si fuera cloud (aunque sea en casa). De esta manera, el almacenamiento y las redes serán definidas por software y lo que hago en casa lo puedo hacer en cualquier nube. Después, hay que poner políticas de Zero Trust o políticas de seguridad sobre quién puede hablar con quién dentro de mi centro de datos virtual; también se necesita visibilidad analítica para proteger el contexto y la app en la zona más cercana desde donde se produzca el ataque. Una vez tengo el data center con lo que me interese, lo puedo mover a la cloud aplicando las mismas políticas de segmentación y seguridad”, argumentó Gómez.

En una red cloud, todo está hiperconectado. “Las apps están muy distribuidas. A partir de NSX podemos hacer una infraestructura con piezas pequeñas en diferentes clouds. Esas piezas consiguen eliminar el cerebro de quien ejecuta el trabajo. El cerebro está concentrado en mi data center (en el controller) y hay que poner a trabajadores en diferentes clouds para optimizar, mejorar y acelerar el tráfico de la aplicación poniéndolo cerca de donde se encuentre. Analiza qué usos se hacen en la aplicación, además de prevenir ataques”, explicó Gómez.

“Las redes SD-WAN se han diseñado para conectar oficinas o campus con el data center. Nosotros hemos hecho algo distinto. Hemos añadido a la red SD-WAN, el cloud y los usuarios, de manera que tenemos todo en SD-WAN, no solo oficina o campus. Así se hace una extensión al cloud storage, cloud de seguridad, destination cloud, apps, SaaS, Oracle o cualquier herramienta. Hay muchos tipos de cloud y necesitamos que SD-WAN participe dentro de esta infraestructura, no solo para conectar las ramas de la oficina con el data center, sino también la parte de arriba, es decir, los aplicativos”, comentó Gómez.

En VMware creen que solo puede coexistir seguridad y red a través de la visibilidad. “Tenemos una serie de soluciones con una capa de visibilidad. Hay que ver si el tráfico que va en los diferentes clouds de mi data center, oficinas en el cloud, etc, lo voy a agregar y ver quién habla con quién; después trazo un mapa y lo aterrizo en una solución agregada NSX Intelligent. Con esta solución me voy a conectar con elementos hardware en modo cloud, switches, routers, SD-WAN, etc. Tenemos unos sensores que diferencian los distintos tipos de dispositivos con inteligencia artificial. Para que se conecte todo con seguridad tiene que haber visibilidad y transparencia”, concluyó Gómez.

[Si quieres ver la intervención de VMware, accede en este enlace.](#) ■



EL IMPACTO ECONÓMICO DE CLOUD NETWORKING

Las aplicaciones ahora se ejecutan en todos los puntos de este espectro, y son críticas para la capacidad de las empresas de ganar en mercados hipercompetitivos. Sin embargo, incluso cuando el éxito de los negocios se ha vuelto más dependiente de esta



nueva arquitectura y la cantidad de datos que fluyen a través de las conexiones ha aumentado, muchas organizaciones todavía carecen de un enfoque unificado para la gestión, automatización y seguridad. La Red de Nube Virtual (Virtual Cloud Network) ofrecida en la tecnología NSX, VMware pretende abordar estos problemas, permitiendo a las organizaciones aprovechar una abstracción de software para conectar, operar y asegurar las arquitecturas de extremo a extremo que soportan las aplicaciones donde residan.

Si te ha gustado este artículo, compártelo



LUIS FISAS, DIRECTOR PARA SUR DE EUROPA, SONICWALL

“Políticas de acceso muy permisivas, no autenticar con doble factor, passwords muy sencillas o antivirus basados en listas o firmas, son los fallos más comunes al proteger la red”

La red empresarial está sometiéndose a un constante cambio y evolución. El perímetro se está perdiendo de manera acelerada sumando a marchas forzadas a los hogares. Se incorporan los dispositivos IoT y nos conectamos a la cloud. El rendimiento de la red y su expansión son críticos y los ciberataques se están multiplicando.

Luis Fisas, director para sur de Europa en Sonicwall, evalúa en su intervención en el IT Webinars [“La era de la conectividad”](#), la realidad que vivimos: “Disponemos de más de un millón de sensores en todo el mundo que recopilan información en tiempo real. Existe un crecimiento del ransomware de un 56% frente al año pasado y la covid-19 ha provocado un aumento de ataques que se focalizan en documentos de PowerPoint y PDF”. Además, el 70% de lo que circula por internet está encriptado. “Esto produce que no sea fácilmente analizable por un firewall normal y provoca que las empresas adopten nuevas tec-



 Luis Fisas
Director para sur de Europa, Sonicwall

 **LUIS FISAS, DIRECTOR PARA SUR DE EUROPA, SONICWALL**

nologías para descryptar y encriptar este tráfico. Solo un 5% de los clientes están inspeccionando este tráfico así que es un peligro para el 95% de empresas restantes”, añadió Fisas.

Por otra parte, el teletrabajo ha cambiado la manera de plantearse la seguridad de las empresas. “En dos meses hemos implementado un plan de trabajo en remoto que se iba a ir desarrollando en siete años. Ahora los puntos de entrada a los servidores no están en un edificio sino en múltiples sitios, lo que amplía el riesgo de ciberataque”. Fisas ejemplifica el momento actual con un símil: “Hemos pasado de tener un castillo con una muralla a un modelo aeropuerto donde entra y sale todo el mundo”.

Es un nuevo paradigma. “Las empresas han de saber si la persona es quien dice ser y que no está suplantando la identidad de otra. El dilema es la autenticación, pero gracias a una plataforma de capture cloud con dispositivos y elementos de ciberseguridad, distinguimos si los dispositivos que se conectan son correctos”, afirmó Fisas.

En Sonicwall enfocan este desafío en tres áreas: asegurando el acceso remoto o móvil, protegiendo el acceso a las aplicaciones cloud y salvaguardando los dispositivos en el puesto de trabajo. “Lo hacemos a través de equipos SMA que defienden estas credenciales”, añadió el directivo. Además, “invertimos en sistemas de autenticación y protección de los correos como

Google Suite, Office 365 y para clouds como One Drive o Dropbox. Después hay que proteger el PC analizando el comportamiento de las apps. Además, el gran peligro de los malware no son los que ya existen, sino los que no conocemos porque se están desarrollando. Conviene tener sistemas de protección con inteligencia artificial puesto que el nivel de desarrollo y variación es rápido y de gran volumen”, dijo Fisas.

Las empresas se ven abocadas a cambiar su infraestructura, pero a veces, cuando se hace de manera rápida, se cometen errores. “Políticas de acceso muy permisivas, no autenticar con doble factor, nivel de las passwords muy sencillos o antivirus basados en listas o firmas y no análisis de comportamiento son los fallos más comunes”, destacó.

Lo que está claro es que después del confinamiento, el teletrabajo ha venido para quedarse. “Hemos pasado de un 20% a un 100% de trabajadores en muchas empresas y algunos clientes se plantean cerrar o reducir el espacio en oficinas porque no van a necesitar tanto espacio. Muchas empresas ofrecerán el 50% del tiempo de trabajo en remoto, lo que permitirá más flexibilidad laboral y otras van a ofrecer remoto siempre. Los sistemas de seguridad de muchas empresas han de cambiar y ser más robustos para garantizar su propia protección”, concluyó Fisas. [Para ver la intervención de Sonicwall, accede aquí.](#) ■



¿SON SUS OFICINAS REMOTAS UNA PUERTA ABIERTA A LOS CIBERATAQUES?

Los investigadores de amenazas de Capture Labs de SonicWall registraron 9.900 millones de ataques de malware en 2019. Durante los últimos cinco años, los ciberdelincuentes han atacado a las organizaciones con un ingente volumen de ataques. Su objetivo era sencillo: lanzar una red lo más grande posible y recoger los frutos. Las soluciones SD-Branch son una de las herramientas ideales para una seguridad sin límites en entornos empresariales distribuidos.



Si te ha gustado este artículo, compártelo



GONZALO DE ANTONIO, SALES EXECUTIVE, DELL TECHNOLOGIES

“El open networking garantiza protección, velocidad en la inversión y agilidad en las empresas”

Uno de los conceptos que ha venido a revolucionar las redes es el open networking que describe una red que utiliza estándares abiertos y hardware commodity, es decir, que tiene la capacidad de ser abierta en términos de compatibilidad de componentes, tanto software como hardware. “Las redes son piezas de la infraestructura que están ancladas en el pasado, pero el open networking viene a renovar la industria con una aproximación totalmente abierta frente a los modelos que han regido tradicionalmente dicha infraestructura”, señaló Gonzalo de Antonio, Sales Executive en Dell Technologies en el IT Webinars [“La era de la conectividad”](#). “Nosotros viramos al open networking hace 6 años. Es una transformación de distribuciones propietarias o arquitectura tradicional o de un solo fabricante, a un modelo en el que cada componente puede ser fabricado en una compañía distinta. Esto garantiza protección, velocidad en la inversión y agilidad en las empresas”, prosiguió.



“Dell diseña el hardware del servidor, pero se puede desplegar software de otras compañías como Linux o Microsoft. Esto ha sido una revolución en el mundo del cómputo y cambió el mercado. Se ha producido una desagregación total de la infraestructura: hay diferentes proveedores y diferentes capas”, señaló de Antonio, cuya compañía está convencida de que el open networking es el futuro de las redes. “La separación de capas la llevamos a la práctica con distintos proveedores de chips. De ahí diferentes puertos; diferentes CPU, diferentes memorias, etc”, comentó este especialista de Dell Technologies. “Si somos nosotros los que desplegamos y vendemos un software, garantizamos el soporte y garantía de la solución. De esta manera vamos al mercado con una aproximación diferente según las necesidades de cada cliente – se le proporciona hardware, un sistema operativo o soporte, pero también podemos suministrar software solo, pero dando un soporte total”, añadió.

“Las ventajas son la arquitectura abierta, la posibilidad de elección, estandarizar hardware, bajar los costes porque si se quiere cambiar el hardware no se tiene por qué renovar el software y viceversa y eso se traduce en un ciclo de vida más largo y una mayor protección de cada inversión”, matizó. Bajo este principio, Dell Technologies cubre todos los componentes de la red involucrados en una infraestructura moderna para cualquier empresa. “Damos una

solución completa definida por software que puede integrarse fácilmente en el entorno existente. Huimos de cuando las empresas dicen: deshágase de su infraestructura legacy”.

Toda la red se conforma y trata como un único elemento lógico, aunque haya centenares de elementos en la red. “Se pueden tratar y gestionar fácilmente. Ese elemento lógico puede estar distribuido en diferentes localizaciones, pero se puede gestionar desde un único punto de gestión, no hay que conectarse a cada uno de los switches. De esta manera facilitamos las operaciones y la gestión”, comentó de Antonio, quien continuó detallando las capacidades de la propuesta de Dell en el mercado: proveer de forma automática los puertos a los que se conectan las máquinas virtuales; ser inteligente e identificar los flujos de tráfico que entran y aplicar políticas diferenciadas de segmentación; o proporcionar información a la empresa para identificar problemas y resolverlos sin usar herramientas externas. “Sabemos lo que ocurre a tiempo real y lo que ocurrió en el pasado. Es decir, si un servidor se cayó o no funcionaba bien”, añadió.

La compañía también dispone de soluciones de SD-WAN para sedes remotas, asegurando la calidad de la experiencia del usuario. “La solución es completa. Las redes han de cómo los paracaídas: funcionan mucho mejor cuando están abiertas”, concluyó. [Para ver la intervención de Dell Technologies, accede en este enlace.](#) ■



OPEN NETWORKING PARA ACELERAR LA AGILIDAD DE LAS EMPRESAS

La infraestructura de red en muchas empresas está envejeciendo y se ha quedado obsoleta. Sus componentes propietarios y las interfaces que utilizan pueden obstaculizar los planes de una empresa para avanzar. La red está de alguna manera bloqueada, o cerrada por el hardware y software propietarios del fabricante desplegado, lo que limita el ritmo de la innovación en comparación con el rápido avance de los entornos informáticos de computación abiertos.



Si te ha gustado este artículo, compártelo



ANTONIO NAVARRO, COUNTRY MANAGER IBERIA, D-LINK

“Necesitamos mayor ancho de banda a nivel LAN e inalámbrico. Habrá que aumentar los gigas; apostamos por conexiones de 1GE y 10GE”

La transformación digital ha incrementado la importancia de la red, especialmente en el extremo donde clientes, empleados, aplicaciones cloud y dispositivos IoT se conectan a la empresa. “En D-Link creemos que la transformación digital es una oportunidad de negocio porque necesitamos dar acogida a miles de dispositivos conectados y eso necesita infraestructuras de red. Necesitaremos mayor ancho de banda a nivel LAN e inalámbrico. Habrá que aumentar los gigas. Lo mismo en wireless. Necesitaremos movilidad y escalabilidad ilimitada; llegan tecnologías como 5G. El PoE, las Smart cities, y las industrias 4.0 necesitan soluciones específicas que nosotros abordaremos”, expuso Antonio Navarro, Country Manager para Iberia de D-Link, sobre las claves del presente y futuro de la tecnología de conectividad en el webinar [“La era de la conectividad”](#) de IT Trends.

Para solventar estas necesidades, desde el proveedor apuestan, dentro de la tecnología de



conmutación, por las conexiones 1GE y 10GE. “Tenemos que dar cabida a esas velocidades. Democratizar que una PYME pueda tener una conexión a gran velocidad y una empresa grande, incluso un nivel mayor”. El crecimiento tiene dos vertientes. “Primero en soluciones como data center y core de red de alto rendimiento de 10, 25, 40 o 100 GB. Por otro lado, vamos a presentar un switch no gestionable puramente de 10 GB”, dijo Navarro. Junto a estas propuestas, el director general de D-Link en Iberia apuntó estas otras tendencias en conectividad.

❖ **PoE (Power over Ethernet):** Es una subtecnología que cada vez cobra mayor importancia. “Es la que más crece por los puntos de acceso, cámaras IP o telefonía IoT. Antes estaba limitado a 100 metros de distancia, pero ahora alcanza hasta 250 metros. Es muy importante para la videovigilancia exterior porque se ahorran costes y así, no se depende de equipos intermedios”, explicó Navarro.

❖ **Switching industrial.** “Se usa para todo lo relacionado con digital signage, transporte, industria 4.0, video vigilancia y Wireless exterior porque necesitaremos resistencia a altas o bajas temperaturas y esto lo aportan los equipos robustos”.

❖ **Wi-fi:** “cubrimos el Wireless de tres maneras: a nivel tradicional con controladores Wireless, a través de gestión de proyectos de control mediante plataformas basadas en software o con una plataforma pura en cloud.

Con estos sistemas tenemos diferentes velocidades y dispositivos específicos para hoteles, por ejemplo. Permite gestionar la política de seguridad, los escenarios multi-side, la gestión del ancho de banda, hotspots etc”.

❖ **Cloud:** “nuestra solución tiene una escalabilidad ilimitada y ventajas como equipos que se auto provisionan y permiten un ahorro de costes de desplazamiento. Damos gestión cloud centralizada tanto en la parte inalámbrica como en la cableada y tenemos más de siete modelos a los que iremos sumando más a lo largo del año”.

❖ **Gateways SD-WAN:** “Es nuestro complemento porque vamos a ver cada vez más entornos críticos en cloud. Controla y asegura el tráfico de red, se dota de muchas funcionalidades a nivel seguridad, servicios VPN, firewall, DPI, etc. Con esta tecnología sabemos lo que está pasando, y cómo controlarlo en cada momento”.

Asimismo, en la sesión, Navarro hizo referencia a la convivencia de Wifi 6 y 5G. “Van a cohabitar y se van a ayudar mutuamente. Sacaremos equipos en todas las plataformas. Estas tecnologías tienen ventajas muy parejas: mayor velocidad, mucha menor latencia, mucha mejor gestión de usuarios concurrentes, mayor densidad de usuarios por celda y mucho menor consumo”, concluyó Navarro.

[Si quieres ver la intervención de D-Link, puedes acceder en este enlace.](#) ■

it whitepapers **SOLUCIONES DE CONMUTACIÓN PARA EL CENTRO DE DATOS**

D-Link
DATACENTER Switching eBook

DataCenter Network Architectures
Leaf-Spine / VxLAN
3-Tier (Core/Aggregation/Access)
Kover Campus
Business Development Manager D-Link Spain & Portugal

Este ebook repasa las principales arquitecturas de red para el data center y las soluciones de switching que dan respuesta a las demandas actuales del CPD.

Si te ha gustado este artículo, compártelo



Autenticación y gestión de identidades, el nuevo perímetro de seguridad

La identidad se ha convertido en el nuevo perímetro de seguridad. Saber quién accede, desde dónde, con qué dispositivo y a qué recursos es uno de los pasos más complicados de la migración a la nube.

La manera de afrontarlo pasa por la autenticación basada en contexto y de múltiples factores, una autenticación no sólo de las personas, sino también de las aplicaciones y dispositivos, y de una manera centralizada.

No nos olvidemos de la gestión de cuentas privilegiadas, un aspecto muy importante teniendo en cuenta que, según Forrester, el 80%

de las violaciones de datos tienen una conexión con credenciales privilegiadas comprometidas, como contraseñas, tokens, claves y certificados.

Las empresas necesitan mejorar la protección de las identidades, amenazadas por una gestión poco hábil de las contraseñas, un panorama digital en constante cambio o una gran rotación de los empleados, lo que genera la necesidad de gestionar el aprovisionamiento y el desaprovisionamiento de credenciales. Desde una perspectiva de capacidad de administración y cumplimiento, esto representa

una gran amenaza para proteger los datos de su empresa

Dentro de las actividades trimestrales de IT Trends, el pasado abril se emitió la sesión online **Autenticación y gestión de identidades, el nuevo perímetro de seguridad**, a cuya sesión completa puedes acceder [aquí](#), con la participación de CyberArk, Micro Focus, Fortinet, Thales, Check Point, F5 Networks, One Identity, Akamai y SonicWall. También puedes pinchar, en la siguiente página, en cada una de las imágenes de los portavoces para acceder a sus intervenciones en nuestra web. ■





it
televisión

Carlos Luaces de Santiago
Sales Engineer Iberia, CyberArk

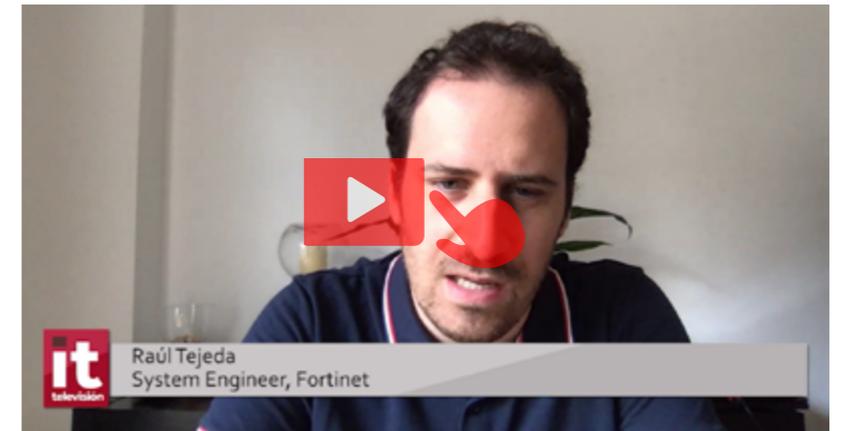
Carlos Luaces de Santiago, CyberArk



it
televisión

Ramsés Gallego
Security International Director, Micro Focus---

Ramsés Gallego, Micro Focus



it
televisión

Raúl Tejeda
System Engineer, Fortinet

Raúl Tejeda, Fortinet



it
televisión

Guillermo Martín Soto
Regional Sales Manager Iberia & North Africa Cloud Protection & Licensing Identity and Access Management, Thales

Guillermo Martín Soto, Thales Iberia y Magreb



it
televisión

Eusebio Nieva
Director Técnico, Check Point

Eusebio Nieva, Check Point



it
televisión

Daniel Varela
Solutions Engineer Security, F5 Networks

Daniel Varela, F5 Networks



it
televisión

Raúl D'Opazo
Solution Architect, EMEA Sales Consultant, One Identity

Raúl D'Opazo, One Identity



it
televisión

Enric Mañez
Enterprise Security Sales, Akamai

Enric Mañez, Akamai



it
televisión

Sergio Martínez
Director General, SonicWall Iberia

Sergio Martínez, SonicWall Iberia

NO SOMOS SOLO FIREWALLS.

SonicWall ofrece ciberseguridad sin límites para la era hiperdistribuida y una realidad laboral en la que todo el mundo teletrabaja con múltiples dispositivos en un entorno poco seguro.

La plataforma en la nube SonicWall Capture Cloud integra la seguridad, la gestión, el análisis y la inteligencia de amenazas en tiempo real en la cartera de productos de redes, correo electrónico, dispositivos móviles y de seguridad en la nube de la empresa.



Firewalls físicos y virtuales



Sandbox multi-motor en la nube



Seguridad en la nube pública y privada



Antivirus de nueva generación



Correo electrónico seguro



Seguridad Cloud



SD-WAN



Acceso Remoto Seguro



Wifi Seguro



Visibilidad e informes unificados



El teletrabajo ha llegado para quedarse Trabajamos como vivimos



Santiago Campuzano,
Country Manager
de Citrix Iberia

Y por fin llegó la calma. Parece que, muy lentamente, la situación generada por la crisis del coronavirus se estabiliza en toda la sociedad, tanto en el plano personal como en el profesional. Han sido unos meses muy duros que, especialmente en España, no se olvidarán y que han supuesto un reto muy difícil de superar. Desde el punto de vista profesional y, en concreto, en el ámbito de la tecnología ha sido un reto enorme para las organizaciones mantener la capacidad productiva a través del plan de continuidad de negocio, con grandes retos en las áreas de infraestructuras, comunicaciones y movilidad extrema, con implementación de programas de teletrabajo.

Un reto para todos, aunque mayor en empresas donde ni existía la posibilidad tecnológica ni la cultura o el liderazgo para llevarlo a cabo. Después de ser participes en proyectos con la mayoría de las grandes empresas y organizaciones públicas, podemos decir que la continuidad de negocio ha sido muy exitosa y con una fuerte implementación de los modelos de acceso remoto. Y digo

modelos de acceso remoto y no teletrabajo porque evidentemente lo que estamos viviendo en estos días no es un modelo de teletrabajo y, mucho menos, de smartworking. Sin embargo, se ha demostrado que la tecnología y las personas están sobradamente preparados para aceptar que, probablemente, el teletrabajo ha llegado para quedarse. Aunque quedan muchas tareas pendientes para que pueda ser efectivo y beneficioso para las personas, las empresas y la sociedad.

Desde el punto de vista de las personas quizás nos hemos llevado lo peor del teletrabajo y ninguna de sus ventajas. Entre otras vicisitudes hemos vivido unas jornadas de trabajo interminables, escasa comunicación dentro de la organización informal, falta de medios para tener un espacio físico de trabajo mínimamente preparado, tener que adecuar el hogar para que todo el mundo pudiera cumplir con sus obligaciones o formativas, carencias en las comunicaciones, problemas para conciliar el entorno profesional y el familiar o, en algunos casos, incluso llevar el ordenador físico

desde la oficina a casa. Visto así, sinceramente no es un panorama muy halagüeño. Después de haber vivido prácticamente toda mi carrera profesional en entidades que permitían y fomentaban el teletrabajo, esto no es teletrabajo.

En el plano personal los beneficios, en un entorno bien gestionado, son muchos. Facilidad en la conciliación familiar, mayor productividad personal al evitar las horas punta de tráfico o mejora en algunos hábitos de vida como la alimentación o el deporte. En definitiva, un modelo motivador en casi todos los aspectos, ofreciendo ventajas profesionales y personales. Para las empresas ha sido una lucha contrarreloj y, en muchas ocasiones, sin un destino muy claro. Evidentemente los objetivos de los planes de continuidad de negocio eran conocidos, sin embargo, más allá del puro ámbito tecnológico. Pero si bien se ha demostrado que tecnológicamente es un reto superado, desde el punto de vista cultural y desde el liderazgo quedan aún tareas pendientes. Para empezar, el teletrabajo supone un ejercicio de responsabilidad bidireccional.

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE

Por parte de los miembros del equipo tienen que ser capaces de gestionar su tiempo, sus actividades y sus objetivos; y, por parte de los managers se deben fijar medidas de control basadas en KPI's, al tiempo que se huye del micromanagement.

A decir verdad, todos los equipos tienen que entender que la situación vivida, a pesar de estar con una teórica mayor disponibilidad, requiere una mayor flexibilidad con menor carga de reuniones virtuales y, sobre todo, ayudando a proteger el individuo dentro de su espacio y fuera de la organización no funcional de la empresa. En definitiva, garantizar la productividad global sin sobrecargar a las personas porque exigir resultados no tiene que ver con controlar el trabajo. Además, existen ahorros relevantes en los gastos asociados a los edificios e infraestructuras, se producen reducciones significativas del absentismo y, en la sociedad multigeneracional en la que vivimos, supone un factor importante de atracción de talento.

Más que nunca el trabajo es lo que se hace, no donde se hace. Por último, desde el punto de vista social también el teletrabajo tiene un impacto relevante. Aparte de permitir reducir el tráfico general, con la consecuente reducción de la contaminación, también ahorra tiempo a todos los trabajadores que se ven afectados por la reducción del tráfico en la hora punta. Por supuesto, también se disminuyen los incidentes y accidentes de tráfico en el tiempo de desplazamiento al lugar de trabajo. Más allá de hacer demagogia acerca de modelos de

transformación digital, que en muchos casos poco tienen que ver con el teletrabajo o el smartworking, debemos ser pragmáticos en entender por qué la llamada nueva normalidad va a afectar también a la forma en la que las personas trabajan.

Como consecuencia de la revolución socio-tecnológica de los últimos años nuestra forma de entender el uso de dispositivos y aplicaciones ha cambiado, siendo una parte intrínseca casi de nuestra naturaleza humana actual, por ello adaptarnos a usarlo no ha sido complicado, aunque sí gestionarlo en la situación vivida. Ahora más que nunca trabajamos como vivimos.

Sin embargo, también es cierto que la experiencia digital se ha convertido en un componente, diríamos, que intrínseco a nuestra forma de vida. Por ello, la selección correcta de la tecnología es si cabe más crítica que nunca. Ya que no en vano buscamos de forma nativa una experiencia digital óptima, que ayude a satisfacer las expectativas del usuario, permita entornos flexibles y dinámicos desde el punto de vista de IT y, por supuesto, lo haga en un entorno de seguridad.

Nuestra experiencia nos ha permitido a ayudar a que más de medio millón de personas trabajen desde sus casas en estos días y creemos que únicamente es viable con una visión holística del proceso, por ello, cuando hablamos de los espacios de trabajo inteligentes o digitales y de la transformación del puesto, pensamos en una forma de acceso única que no cambie la experiencia del



CÓMO TRANSFORMARSE EN UN ESPACIO DE TRABAJO DIGITAL

Ya no es suficiente almacenar de forma segura sus archivos. Debe poder trabajar con esos archivos en tiempo real con sus compañeros, clientes y partners. Su espacio de trabajo digital debe extenderse más allá del uso compartido de archivos para apoyar una plataforma de colaboración de contenido que se centre en la seguridad, los flujos de trabajo y la movilidad y productividad de los usuarios.



cliente con la máxima seguridad, independientemente del dispositivo y de donde esté el usuario y adaptándose a ese contexto; y, lógicamente, acompañado del modelo adecuado de infraestructura, ya sea cloud u on premise en función de la estrategia de la organización. ■

Si te ha gustado este artículo, compártelo



La urgente necesidad de proteger las credenciales privilegiadas

Anastasia Sotelsek,
Principal Sales
Engineer de
CyberArk Iberia



Si mejorar la seguridad de credenciales privilegiadas no es una de las prioridades principales de los responsables de seguridad, debería serlo. Los atacantes externos y los intrusos malintencionados actúan constantemente sobre cuentas privilegiadas para robar información confidencial, fingir ser una persona de confianza o interrumpir aplicaciones y servicios críticos para el negocio.

Según el último Informe de CyberArk, Global Advanced Threat Landscape, menos de la mitad de las organizaciones tiene implementada una estrategia de seguridad de acceso privilegiado para DevOps, IoT, RPA y otras tecnologías que son fundamentales para las iniciativas digitales. Esta debilidad facilita que los atacantes asalten el acceso privilegiado que les permita moverse lateralmente a través de una red para avanzar en su ataque.

Las cuentas privilegiadas son ubicuas. Existen en sistemas, bases de datos y aplicaciones;

residen en las instalaciones y en la nube, y son utilizadas por personas, aplicaciones, procesos automatizados, máquinas y bots. Las organizaciones deben localizar y proteger cientos, o incluso miles, de cuentas privilegiadas dispersas en la red.

Para mitigar el riesgo, estas credenciales deben protegerse con fuertes medidas de seguridad de acceso privilegiado. Implementar un programa efectivo de gestión de acceso privilegiado (PAM) es un desafío para muchas organizaciones, ya que el panorama de amenazas es amplio, complejo y en constante evolución.

LA UBICUIDAD CONDUCE A LA VULNERABILIDAD

A medida que las organizaciones migran a plataformas en la nube y adoptan nuevas tecnologías como la automatización de procesos robóticos (RPA), el número de identidades no humanas, de servidores y de aplicaciones en

cada organización aumenta exponencialmente. Las organizaciones deben adaptar continuamente sus sistemas y prácticas PAM para seguir el ritmo de esta innovación, así como la evolución paralela del panorama de amenazas.

CONOCER NUESTRO GRADO DE EXPOSICIÓN

Muchas organizaciones confían en procesos manuales ineficientes para asignar y monitorizar credenciales de cuentas privilegiadas. Las contraseñas y las claves a veces permanecen sin cambios durante meses, o incluso años, después de su creación. Los ex empleados, integradores y fabricantes a menudo mantienen el acceso a aplicaciones y sistemas críticos mucho después de su salida de la empresa, exponiéndolas a violaciones de datos y ataques maliciosos.

Los empleados descontentos o los atacantes externos pueden actuar sobre cuentas inactivas o contraseñas sin cambios para realizar ataques sofisticados. Una vez que un atacante inteligen-

te obtiene acceso a credenciales de cuentas privilegiadas, puede moverse lateralmente y acceder a otros recursos empresariales críticos en solo minutos. Los adversarios pueden pasar de penetrar un puesto de trabajo a obtener derechos de administrador completos en un controlador de dominio en menos de 20 minutos.

Al pensar como si fueran un atacante, las organizaciones pueden defenderse de las técnicas que estos suelen usar para acceder a cuentas privilegiadas, robar datos y eliminar sistemas.

PLANIFICAR CON ÉXITO LAS ACCIONES PAM

Tener un marco de seguridad priorizado por fases para alinear las iniciativas PAM con la posible reducción de riesgos, ayuda a las organizaciones a abordar sus responsabilidades lo más rápido posible.

Los responsables de seguridad deben seguir estos pasos:

1. Identificar las cuentas privilegiadas, las credenciales y los secretos más críticos, y enfocarse en las cuentas que podrían poner en peligro la infraestructura de misión crítica o exponer datos confidenciales desde una perspectiva de riesgo de la organización.

2. Desarrollar un plan priorizado para reducir las vulnerabilidades y fortalecer la seguridad. Establecer qué acciones son las más importantes, qué elementos se pueden lograr

rápidamente y con recursos mínimos, y cuáles requieren un tiempo y esfuerzo significativos.

3. Una vez que el plan esté implementado, debe ser reevaluado y mejorado continuamente para abordar las amenazas en evolución y las nuevas tecnologías.

APROVECHAR AL MÁXIMO LA INVERSIÓN

Los atacantes perfeccionan continuamente sus habilidades, encontrando nuevas formas de penetrar en las redes y evitar ser detectados. Los equipos de TI y seguridad pueden superar estos desafíos y minimizar los riesgos de acceso privilegiado al observar cómo los atacantes vulneran el acceso privilegiado, y preguntarse: ¿cuáles son los vectores de ataque de acceso privilegiado más comunes y cómo piensa y se comporta el perpetrador en cada caso?

Para evitar el robo de credenciales, las organizaciones deben discontinuar los procesos desarticulados manuales de gestión de secretos y credenciales, introducir un repositorio digital (Vault) seguro, para almacenar y monitorizar de forma centralizada las credenciales de cuentas privilegiadas, y rotar automáticamente las contraseñas y las claves según las políticas de seguridad.

Siguiendo estas recomendaciones, las organizaciones pueden fortalecer su estrategia de seguridad, reducir riesgos y aprovechar al máximo sus inversiones en tecnología. ■



LAS CINCO GRANDES RAZONES PARA DAR PRIORIDAD A LOS PRIVILEGIOS

El acceso privilegiado es una puerta de entrada a los activos más valiosos de una organización y la base de casi todas las filtraciones graves de seguridad.



Las organizaciones deben contar con una estrategia tanto para gestionar y supervisar el acceso privilegiado como para detectar y responder a amenazas si quieren reducir el riesgo de convertirse en el blanco de los ataques avanzados que existen en la actualidad.

Si te ha gustado este artículo, compártelo





ASEGURE ACCESO REMOTO A SISTEMAS INTERNOS CRÍTICOS

Acceso Zero Trust, Autenticación Multifactor
Biométrica y Aprovisionamiento Just-in-time
con CyberArk Alero.

[SOLICITE UNA DEMO](#)



Las redes son fundamentales en el desarrollo de la seguridad intrínseca y las aplicaciones modernas, pero las empresas necesitan simplificarlas



Sergio Oropeza,
Senior Manager
Solution Engineer de
VMware Iberia

La seguridad se ha vuelto increíblemente compleja. Habiendo tantos productos disponibles, desde la seguridad del end-point hasta la seguridad de las aplicaciones, pasando por la seguridad de la red, hay mucho para tener en cuenta. Siendo las redes una de las herramientas más potentes para la ciberseguridad de una empresa, ya sea como canal para garantizar la seguridad o como instrumento que posibilita la oferta y la disponibilidad de las aplicaciones necesarias para que las empresas mantengan la competitividad, no estaríamos equivocados si afirmáramos que la seguridad de red es crítica. Ahora bien, ¿quién es el máximo responsable de la seguridad de red?

Las redes se han transformado en un conductor crítico, que crea la conectividad expansiva ne-

cesaria para transferir los datos desde la fuente hasta el usuario final. Las redes conectan el centro de datos, las múltiples nubes y los sensores de IoT en el perímetro, es decir, todos los componentes de una empresa en el mundo de hoy. No sería desacertado afirmar que las redes son fundamentales para una redefinición moderna de la seguridad informática. Y, sin embargo, esto solo ha sido posible gracias al surgimiento de las redes definidas por software.

Teniendo esto en cuenta, puede sonar alarmante que, de acuerdo con un nuevo estudio de IDC, un 60% de los responsables de TI en España consideren que obtener visibilidad de red de extremo a extremo es todo un reto. Al menos, parecen reconocer que es un problema: casi la mitad de los encuestados por IDC

piensa que la falta de visibilidad es motivo de preocupación. Asimismo, el 41% opina que la falta de visibilidad ha derivado en divergencias entre los equipos de seguridad y de TI, mientras que, según una nueva encuesta de alcance mundial llevada a cabo por VMware y Forrester, un tercio 35% de los encuestados no está pensando en implementar una estrategia integral de TI y seguridad.

Las empresas están empezando a ocuparse de esta cuestión, reconociendo que la transformación de redes es cada vez más importante para garantizar los niveles de resiliencia y seguridad requeridos por las empresas de hoy. De acuerdo con el estudio de IDC, el 43% de las empresas europeas la considera una de sus prioridades para el período 2019-2021.

El mundo de hoy es una olla a presión: las empresas tienen que adaptarse a las condiciones del mercado a un ritmo vertiginoso, y para ello dependen de sus aplicaciones, es decir, del desarrollo, la ejecución y la administración de aplicaciones en toda la red, desde el centro de datos a cualquier dispositivo, pasando por todos los entornos de nube. Es fundamental poder aprovechar el potencial de estas aplicaciones, pero la posibilidad de protegerlas, junto con los datos asociados y los usuarios, es un reto cada vez más difícil de cumplir.

Entonces, y dado que no pueden darse el lujo de fracasar, ¿cómo pueden las empresas aprovechar el potencial de las redes para proteger los datos en todos los puntos de la organización, desde el origen hasta el usuario final?

LA DIFICULTAD DE DAR PRIORIDAD A LAS REDES

En primer lugar, si existe alguna posibilidad de una estrategia integral y un enfoque cohesionado, la colaboración entre los equipos involucrados es de vital importancia, si bien la convergencia y la coordinación de equipos es uno de los principales obstáculos que deben sortear las organizaciones.

A día de hoy, solo un tercio de los equipos de redes participa en el desarrollo de estrategias de seguridad, pese a que el 47% de dichos equipos forman parte de su ejecución. Esto in-

dica que los equipos de redes no desempeñan el mismo papel que otros actores de TI o de seguridad a la hora de hablar de ciberseguridad. Derribar estos muros y eliminar la fricción entre los equipos interesados debería ser una prioridad fundamental: en el mundo de hoy, la seguridad debe verse como un deporte de equipo, pues el complejo panorama de amenazas contemporáneas solo puede enfrentarse si se aúnan fuerzas y se adopta un enfoque holístico.

UN ENFOQUE INTRÍNSECO PARA SUPERAR DESAFÍOS CADA VEZ MÁS COMPLEJOS

En segundo lugar, necesitamos que la seguridad vuelva a ser simple. Los enfoques tradicionales, pensados para un mundo distinto pero aplicados a un escenario de amenazas infinitamente más desalentador, han traído aparejada una complejidad disfuncional e inmanejable, que depende de demasiados productos específicos. Estas supuestas soluciones, que típicamente se centran en bloquear amenazas en el perímetro de la red, tienden a actuar por reacción y dependen de la capacidad de reconocer el software malicioso, lo que es inútil frente a las más de 300.000 amenazas de día cero que surgen cada día. Son soluciones completamente inadecuadas para el mundo de hoy, en plena transformación digital, en el que el flujo de información es ubicuo y la infraestructura tiene

que ser ágil y estar en condiciones de mutar y ajustarse a escala en forma continua.

Creemos que es posible simplificar la seguridad si se la armoniza con las aplicaciones y los datos, se la ofrece a través de la red y se la vuelve intrínseca a todos los componentes de la infraestructura (en lugar de hacerlo solo en el perímetro de la red). En un mundo definido por software, es posible integrar sin fisuras la seguridad en cada una de las capas de los cimientos digitales de una empresa, con lo que se reduce significativamente la superficie expuesta a los ataques maliciosos. Se trata de un enfoque más proactivo, en el que ya no es necesario ser capaz de reconocer cómo es una amenaza. En lugar de sumar complejidad, simplifica las cosas, utilizando la infraestructura de software y los terminales existentes, y permitiéndoles incorporar la seguridad en las aplicaciones y los datos en origen. Así, las empresas logran pasar de un modelo de seguridad heredada, en el que se reacciona ante lo malo y se intenta bloquearlo o perseguirlo, a un enfoque más robusto en el que lo “bueno conocido” se aplica rigurosamente.

DESARROLLOS CON EL FOCO EN LAS APLICACIONES MODERNAS

Con el fin de garantizar una experiencia de cliente cada vez mejor, el ritmo del desarrollo y despliegue de aplicaciones se ha acelerado considera-

blemente. En este mundo feliz, la tecnología empresarial ya no puede ser un entorno dominado por silos operativos e inconsistencias en las herramientas de redes y seguridad en redes públicas, privadas y del perímetro. Hoy en día, el éxito comercial exige una mayor automatización, una infraestructura uniforme y la capacidad de conectar y garantizar marcos de aplicaciones modernas en los despliegues de centro de datos y cloud.

Las empresas, tanto grandes como pequeñas, están atravesando una transformación de aplicaciones que les permite advertir esto y anticiparse a la competencia. La modernización de aplicaciones mediante el uso de contenedores y microservicios se ha consolidado como el enfoque dominante de desarrollo de software y Kubernetes, como la plataforma natural para la orquestación de contenedores.

Por todo ello, un enfoque centrado en el software a través de una red virtual en la nube (VCN, por sus siglas en inglés) es la apuesta mínima para las empresas que quieren avanzar a pasos agigantados. Dejemos atrás las redes y los productos de seguridad añadidos y aislados. Imaginemos, en cambio, una capa de red continua y segura, definida por software, que vaya del centro de datos al perímetro, pasando por la nube.

Una VCN es una capa de software que abarca toda la infraestructura del centro de datos y más allá, desde los servidores físicos hasta las nubes privadas y públicas y el perímetro. Confíere a la

red una agilidad, una flexibilidad y una simplicidad automáticas, lo que le permite facilitar los resultados de negocios en lugar de ser un centro de coste compartimentado. Garantizando una conectividad segura y ubicua, con la velocidad y la capacidad de automatización del software, una VCN permite cumplir la promesa de desterrar los silos y las oportunidades perdidas, y mejorar considerablemente la gestión de las cuestiones de seguridad en la empresa. La seguridad de red contribuye positivamente a la competitividad de la empresa y deja de ser un centro de coste cada vez más ineficiente.

Todo esto parece ir contra el sentido común, y en especial contra las prácticas de seguridad más extendidas, pero, en materia de seguridad intrínseca, menos es más. Utilizando menos soluciones específicas en todo el entorno de TI (redes públicas y privadas, dispositivos y aplicaciones), las empresas pueden incrementar su visibilidad y eficiencia, y reducir costes.

Las redes son la plataforma universal que impulsa la conectividad, la seguridad intrínseca y el suministro de aplicaciones. Garantiza una conectividad uniforme y ubicua, y seguridad en las aplicaciones y los datos, estén donde estén. Las empresas no pueden permitirse esperar más tiempo para reconocer que las redes son el ADN de toda estrategia moderna de seguridad, cloud y aplicaciones. Deberían verse como un arma estratégica y no como un simple conducto. ■



LAS EMPRESAS ESPAÑOLAS ACEPTAN LENTAMENTE LOS DESAFÍOS DE LA CIBERSEGURIDAD (Informe Forbes Insights)

Este informe de VMware y Forbes Insights realizado entre grandes empresas europeas, entre ellas 35 españolas, explora el estado de la ciberseguridad en esta región. Las

conclusiones obtenidas en España frente a las europeas difieren en algunos aspectos significativos, como una gran brecha en la concienciación en ciberseguridad de los niveles directivos y los técnicos. El documento también proporciona algunas recomendaciones sobre cómo las organizaciones en España pueden mejorar la protección de sus operaciones.



Si te ha gustado este artículo,
compártelo



El impacto de la era Exascale en nuestro modo de vida y trabajo



Adriano Galano,
AI and HPC sales
specialist en HPE

Cada segundo en la tierra se producen cantidades gigantescas de datos en todos los ámbitos de la vida. Los datos son hoy la energía que mueve la economía de cualquier país. Toda decisión debe estar soportada por los datos y gracias a los datos somos capaces de predecir y anticiparnos a cualquier evento o necesidad futura. Para 2025, IDC predice que, en todo el mundo, los datos crecerán hasta 175 zettabytes, y será fundamental convertir estos datos en conocimientos accio-

nables, utilizando combinaciones de modelado, simulación, análisis de datos, aprendizaje automático e inteligencia artificial (IA). Los conocimientos prácticos impulsan los negocios.

Pero ¿están nuestras organizaciones preparadas para tratar y analizar estas bastas fuentes de información? Los sistemas exascale son capaces de dar respuesta y muchas de las innovaciones que estamos desarrollando en esos grandes sistemas muy pronto la llevaremos a sistemas de cualquier tamaño, lo que

permitirá a la supercomputación, el HPC y el IA a organizaciones de cualquier tamaño:

- ❖ Dar respuesta a la “explosión cámbrica” en las tecnologías de cómputo: una mayor diversidad de tipos y modelos de computación: procesadores, aceleradores, FPGA, de propósito específicos.

- ❖ A las nuevas tendencias en sistemas de almacenamiento y memoria. Permitiendo realizar la visión que esbozamos hace algunos años ya sobre el “Memory Centric Computing”

“Los sistemas exascale son capaces de dar respuesta y muchas de las innovaciones que estamos desarrollando en esos grandes sistemas muy pronto la llevaremos a sistemas de cualquier tamaño”

❖ Sistemas de interconexión como CRAY Slingshot, que aporta los beneficios de el alto rendimiento y baja latencia de las redes de comunicación, pero soportado en estándares del mercado como Slingshot. Y la evolución a los sistemas de interconexión fotónicos y nuevos estándares que romperán las fronteras de los centros de datos tal y como los conocemos hoy.

❖ Seremos capaces de dar soluciones a los datos allí donde se originen, desde el extremo (Edge) hasta los grandes supercomputadores.

❖ Y todo con los elementos de software que permitirá a los clientes tener la potencia de un supercomputador con la experiencia de usar un Cloud.

Todo esto lo llevaremos a los clientes de modo ágil, simple, flexible. Con la libertad de elección que nos da el mundo híbrido y con modelos de

pago por uso y fórmulas financieras que garantizarán que toda esta innovación sin barreras pueda llegar a las organizaciones y la sociedad.

Concluyendo, se espera que la computación a exascale resuelva problemas que antes estaban fuera de nuestro alcance, con avances en nuevas soluciones energéticas, asistencia sanitaria, predicción meteorológica, ciencia de los materiales y mucho más. Permittiéndonos crear una industria más competitiva, con empresas más ágiles centradas en el dato y sociedades más resilientes, capaces de mitigar los desastres v centrado en los seres humanos. ■

Si te ha gustado este artículo,
compártelo



GUÍA DE PLANIFICACIÓN DE VIRTUALIZACIÓN DE CLIENTES HPE SIMPLIVITY

Hewlett Packard Enterprise ha probado implementaciones de escritorios virtualizados a gran escala usando las soluciones VMware y Citrix® en la infraestructura hiperconvergente HPE SimpliVity. Los resultados han sido validados y publi-

cados en forma de varios informes técnicos sobre arquitecturas de referencia y rendimiento. Estos documentos proporcionan un proyecto para diseñar e implementar infraestructura hiperconvergente altamente resiliente y escalable para implementaciones de virtualización de clientes.



HPE DISCOVER VIRTUAL EXPERIENCE

HERE TO HELP

Únete a la gran experiencia virtual

A partir del 23 de junio en directo y bajo demanda



→ **REGÍSTRATE HOY GRATIS**

No consolidar la infraestructura de ciberseguridad plantea desafíos al 99% de las empresas del mundo

Mario García,
director general de
Check Point para
España y Portugal



La pandemia de la COVID-19 ha provocado un cambio en la cultura de trabajo, puesto que los efectos han sido globales, rápidos y generalizados donde evaluar las inversiones en ciberseguridad es más necesario que nunca. Como norma general, en ciberseguridad no hay segundas oportunidades, pero ahora más que nunca, es fundamental dar un paso adelante y contar con una estrategia de seguridad adaptada a los nuevos tiempos. Los datos de una encuesta que hemos llevado a cabo recientemente reflejan que el 69% de las empresas de todo el mundo está de acuerdo en que dar prioridad a la consolidación de los proveedores llevaría a una mejor seguridad IT, dejando una conclusión muy clara: la era de la consolidación de las estrategias e infraestructuras de protección en el mundo digital también ha llegado para quedarse.

Todavía hoy, muchas empresas establecen su estrategia de ciberseguridad de entornos y dispositivos corporativos desde la falsa premisa de que un mayor número de productos se traduce en una mayor seguridad, aunque se tiende a olvidar los retos que esto supone: mayor complejidad para establecer una estrategia óptima, dificultades técnicas, posibles puntos sin protección, etc. Sin embargo, en esta situación, es fundamental que se produzca un cambio de enfoque por parte de los responsables de ciberseguridad, que, sin duda, deben apostar por la simplicidad. En ocasiones como esta, la frase de “menos es más” adquiere un significado trascendental para el bienestar de todos los activos corporativos, y por ende, de la salud de cualquier modelo de negocio. Contar con una solución de ciberseguridad consolidada que permita a las

empresas reforzar y centralizar sus defensas, así como agilizar los tiempos de respuesta a la hora de hacer frente a cualquier tipo de amenaza cibernética, se ha convertido en un aspecto clave.

LA EXPANSIÓN DE LA SUPERFICIE DE ATAQUE, UN RETO MAYÚSCULO PARA LA CIBERSEGURIDAD

A medida que el panorama de amenazas evoluciona y los ciberataques se hacen cada vez más sofisticados, el 99% de las empresas que utilizan múltiples soluciones de distintos proveedores afirman que esto ha planteado nuevos desafíos a su organización. Como consecuencia del teletrabajo, se ha producido un cambio de tablero de juego, ya que se ha pasado de un foco central de desarrollo de actividad profesional (oficina) a múltiples ubicaciones. Esto ha derivado

en un aumento de los dispositivos y redes personales que se utilizan para trabajar, lo que se traduce en una mayor superficie de ataque y, por tanto, más y mayores riesgos para la seguridad corporativa.

En este sentido, la ecuación es muy sencilla: cuantos más dispositivos hay que securizar, mayor es el número de potenciales objetivos para los atacantes y menor es la confianza en su nivel de ciberseguridad. La nueva realidad de trabajo mixto ha supuesto un examen para muchos CISOs, puesto que proteger una red de dispositivos cada vez más amplia es un reto para 9 de cada 10 empresas. A esto, además, hay que sumarle el factor añadido de que equipos como los smartphones, tabletas e incluso ordenadores portátiles apenas cuentan con medidas de seguridad instaladas, por lo que son un objetivo fácil para los ciberdelincuentes y una puerta abierta que da acceso a toda la red de datos y dispositivos de una empresa.

La sensación de urgencia y cambio constante en la que se encuentran muchas compañías en la actualidad les ha hecho optar por soluciones en las que se implementan nuevas herramientas de seguridad para proteger estos equipos. Nuestros datos indican que casi la mitad de las empresas utilizan entre 7 y 40 productos de seguridad distintos en su día a día, lo que aumenta de manera exponencial la complejidad a la hora de gestionar de todos estos recursos y servicios. Estas prácti-

cas hacen que, lejos de aumentar sus niveles de protección, las empresas tengan nuevos focos de vulnerabilidades o brechas de seguridad.

LA VISIBILIDAD, EL ENEMIGO A BATIR EN LA NUEVA ERA DE LA ESTRATEGIA DE SEGURIDAD CONSOLIDADA

Ante este escenario, no cabe duda de que consolidar y centralizar la estrategia de ciberseguridad se ha convertido en una necesidad, por lo que uno de los principales obstáculos a solventar es la falta de visibilidad. Tener alto nivel de visibilidad garantiza la eficacia necesaria para hacer frente y evitar los ciberataques más sofisticados por lo que, sumado a la gestión unificada, completan la arquitectura de seguridad.

La realidad es que la práctica totalidad de las empresas de todo el mundo utilizan múltiples plataformas de gestión de herramientas y productos de ciberseguridad, lo que dificulta la visibilidad. Además, para casi 8 de cada 10 profesionales de ciberseguridad, trabajar con varios proveedores supone un reto, puesto que actividades como el mantenimiento, las actualizaciones de las diferentes versiones, la renovación de los contratos y otras acciones relacionadas con el cuidado y la provisión de una solución de seguridad exigen un tiempo y unos recursos muy valiosos.

No tener una visión integral de la situación de las amenazas de una empresa complica la res-

puesta ante incidentes, lo que aumenta el grado de vulnerabilidad y, por tanto, la posibilidad de que los ataques de un cibercriminal tengan éxito y afecten a los datos, infraestructuras o dispositivos. Además, reducir proveedores proporciona un mayor nivel de ciberseguridad, puesto que hay una mayor integración y se minimizan las brechas entre producto, así como una reducción en el tiempo, el coste y los recursos de los sistemas de reparación de incidentes.

LA ESCALABILIDAD, ELEMENTO CLAVE EN LA CONSOLIDACIÓN DE LA ESTRATEGIA DE CIBERSEGURIDAD

No cabe duda de que el primer paso que deben dar las empresas consiste en reconocer cuál es el reto que tienen ante sí. Sin embargo, este no es el único obstáculo, puesto que todavía tienen que dar algunos pasos más en el camino hacia una nueva realidad cibersegura. En este sentido, es evidente que deben elegir una postura y una herramienta de protección que permita unificar y simplificar la gestión de toda la infraestructura de ciberseguridad, sobre todo en estos momentos en los que la movilidad y accesibilidad a los datos en remoto son un pilar fundamental para el desarrollo de las tareas profesionales.

Ante este nuevo escenario, la propuesta que hacemos desde Check Point se centra en un concepto clave: la escalabilidad. Las redes de las empresas son cada vez más extensas y cuentan

con un mayor número de dispositivos conectados, por lo que es necesario contar con herramientas que puedan crecer e hiperescalar a la misma velocidad que lo hacen las infraestructuras corporativas. En nuestro caso, contamos con productos como Check Point Maestro, la primera solución de seguridad de red realmente hiperescalable de la industria. una nueva arquitectura hiperescalable que ofrece a los negocios de cualquier tamaño, la potencia y flexibilidad de las plataformas de seguridad de nube y la posibilidad de expandir sus pasarelas de seguridad existentes hasta una capacidad de hiperescalar sin interrupciones (seamless).

Asimismo, también contamos con nuestra solución Infinity NEXT, una arquitectura de seguridad cloud nativa consolidada que está diseñada para proteger cualquier punto dentro de una red corporativa en cualquier lugar gracias a la innovativa tecnología de nanoagentes y un completo panel de más de 60 soluciones y servicios de protección y prevención de amenazas. Infinity NEXT, además, ofrece protección sin interrupciones y actualizaciones constantes para cualquier red, dispositivos móviles, así como entornos IoT y cargas de trabajo multi-cloud. De esta forma, las empresas pueden elegir entre utilizar la totalidad de las tecnologías disponibles en la suite de Infinity Next o implementar aquellos módulos específicos que se adaptan a sus necesidades inmediatas

con total flexibilidad y facilidad de manejo desde un único panel de control.

Soluciones como estas llegan para dar respuesta a las demandas y necesidades actuales de las empresas que, en condiciones normales, cambian a una gran velocidad, pero que en la nueva realidad que nos toca vivir varían de forma vertiginosa. La combinación de ambas herramientas llega para ofrecer a las compañías de cualquier tamaño lo que verdaderamente necesitan: productos que reducen procesos, minimizan costes y simplifican las tareas relacionadas con la protección de los entornos y activos corporativos. Asimismo, ayuda a consolidar la estrategia de ciberseguridad de las empresas, ofreciendo estabilidad y aportando las medidas necesarias para hacer frente a los nuevos retos que surgen como consecuencia de la nueva realidad de trabajo mixta.

En resumen, la transformación digital empodera a las organizaciones, pero no deben perder de vista el enfoque de ciberseguridad adecuado, puesto que, de lo contrario, expone a las empresas a una gran variedad de amenazas. La pandemia del Covid-19 ha supuesto un cambio radical para las empresas, que han visto cómo tenían que implantar una serie de cambios significativos en su forma de trabajo para poder hacer frente a la situación actual. El teletrabajo es sin duda uno de ellos, pero para que pueda instaurarse de forma definitiva, es imprescindible hacerlo de forma segura. Por tanto, nos en-



CHECK POINT CLOUDGUARD SAAS, MÁS QUE UN CASB

Como explica el documento, CloudGuard SaaS es la solución de prevención más efectiva para malware y ataques zero-days en aplicaciones SaaS. Utiliza la tecnología SandBlast de Check Point y bloquea las amenazas zero-day antes de que lleguen a los usuarios, ofreciendo contenido seguro en segundos, utilizando emulación avanzada de amenazas y tecnología de extracción.



contramos en las etapas iniciales de una nueva era centrada en consolidar las estrategias de ciberseguridad corporativas. ■

Si te ha gustado este artículo, compártelo





CHECK POINT INFINITY

SECURE YOUR EVERYTHING™

Más información



Aprovechando el potencial del 5G con la SD-WAN segura

José Luis Laguna,
Director Systems
Engineering Fortinet
España y Portugal



Las redes 5G de alta velocidad y baja latencia tienen el poder de transformar los negocios. Sin embargo, esta transición hacia una cobertura 5G a gran escala no se producirá de la noche a la mañana. Incluso aunque esté disponible, todavía hay pocos dispositivos que soporten 5G, y escasas aplicaciones que requieran el nivel de rendimiento proporcionado a través de estas redes. Esto significa que las empresas deben mantener todas las opciones abiertas en lo que respecta a la conectividad, incluso si la tecnología 5G ya está a su disposición.

Con todas las opciones sobre la mesa, la gestión y la seguridad de las conexiones de red se

complica aún más. Las organizaciones no solo deben proporcionar el tipo de conexión adecuada a un dispositivo específico utilizando una determinada aplicación, sino que también, deben reconocer cuándo cambian los requisitos de conectividad o si una conexión comienza a fallar. Además, deben ser capaces de realizar cambios rápidos de conectividad sin que afecte al rendimiento o cause interrupciones.

Al mismo tiempo, debe haber estrategias de seguridad que eviten la exposición del tráfico sensible al riesgo cuando estas conexiones cambien. Para lograr este nivel de seguridad se necesitan redes inteligentes que puedan tener en cuenta las decisiones que se toman a

nivel de red/conectividad, que puedan evaluar las capacidades de rendimiento de los usuarios finales, los dispositivos del perímetro o de IoT, y que comprendan los requisitos de rendimiento de una aplicación. Por lo tanto, no solo debe ser capaz de asignar estos requisitos a la mejor conexión posible y cambiar las conexiones cuando sea necesario, sino también de mantener la seguridad como una parte integrada de este proceso para garantizar que todo se ajuste simultáneamente.

Este es un desafío complejo que pocos proveedores saben cómo abordar. Y es esencial tener en cuenta que incorporar 5G a la lista de opciones disponibles no es tan simple como

“A medida que la tecnología 5G se abre camino, es más relevante que nunca el papel crítico de la red SD-WAN segura en cualquier estrategia de conectividad remota”

tener otra opción de conectividad. Al contrario, añadir más opciones a un sistema construido sobre múltiples partes móviles puede agravar de forma exponencial el reto de seleccionar, supervisar y gestionar las conexiones, superando en última instancia la capacidad y las posibilidades de gestión de los routers tradicionales basados en el perímetro.

SD-WAN ALLANA EL CAMINO HACIA EL 5G

Dado que los routers WAN tradicionales nunca fueron diseñados para las complejidades de conectividad que demandan las delegaciones de hoy en día, cuando las organizaciones empiecen a considerar su transición a 5G, también deberían considerar adoptar una solución SD-WAN. Además de estar ya diseñadas para soportar y gestionar las conexiones 5G, estas soluciones pueden determinar automáticamente los requisitos necesarios para establecer la conexión apropiada para cualquier aplicación o servicio dado. Independientemente del número de usuarios que se conecten a los diferentes servicios, las soluciones SD-WAN pueden propor-

cionar la flexibilidad necesaria para establecer y modificar las conexiones en función de los requisitos de ancho de banda, calidad y coste. Si una conexión se deteriora debido a la latencia o a la pérdida de paquetes, estas soluciones también deberían ser capaces de permutar dinámicamente dicha conexión por otra. Además, una solución SD-WAN segura, es capaz de mantener la seguridad como un componente integrado del proceso de gestión de la conectividad. Al aprovechar SD-WAN, las organizaciones pueden garantizar que todos los dispositivos tengan las mejores tasas de conexión posible en todo momento sin comprometer la flexibilidad, la visibilidad o la protección.

A pesar de los beneficios que ofrece, SD-WAN, al igual que cualquier solución, no es perfecta. Al hacer el cambio de un router WAN a una solución SD-WAN tradicional, las organizaciones pierden las protecciones asociadas con el tráfico de retorno a través del centro de datos. Aunque la mayoría de las soluciones SD-WAN proporcionan algunas herramientas muy básicas para reemplazar las funciones completas

de seguridad, como una VPN y un firewall, no son lo suficientemente buenas.

Para soportar los requisitos de conectividad y ancho de banda de las organizaciones actuales y sus aplicaciones, las organizaciones necesitan una solución SD-WAN segura capaz de gestionar y asegurar eficazmente en tiempo real los entornos en continuo cambio. Si esto no es así, habrá dificultades para mantener la seguridad actualizada a medida que cambien los requisitos de conexión y de las aplicaciones, lo que dará lugar a brechas que abrirán la puerta para que los ciberdelincuentes exploten las redes.

A los desafíos habituales asociados con la seguridad de SD-WAN, cuando entra en la ecuación la tecnología 5G las complejidades aumentan. Para seguir el ritmo de las velocidades que ofrece 5G y evitar que la seguridad se convierta en un cuello de botella crítico al realizar tareas esenciales como la inspección del tráfico cifrado, la seguridad tendrá que actuar más rápido que nunca. De hecho, más rápido que la mayoría de los productos de seguridad disponibles actualmente. Además, a medida que aumenta el volumen de tráfico cifrado (que actualmente constituye más del 70% del tráfico de la red), también lo hace la tasa de adopción de TLS 1.3. Teniendo en cuenta estos cambios, garantizar que la seguridad pueda soportar velocidades de 5G sin interrumpir comunicaciones críticas para el negocio es más esencial que nunca.

Alcanzar este nivel de seguridad puede ser más fácil de decir que de hacer. La inspección del tráfico cifrado tiene un gran impacto en el rendimiento de los firewalls de nueva generación (NGFW), tanto que muchos proveedores se niegan incluso a publicar sus valores de rendimiento. Lo que significa que la inspección activa del volumen cada vez mayor de tráfico cifrado (especialmente cuando se utiliza TLS 1.3 para asegurar las conexiones 5G) tendrá un impacto cada vez más negativo tanto en el firewall como en la conectividad SD-WAN al aumentar las expectativas de rendimiento. Amenazando, en última instancia, a una de las principales razones por las que se adoptó inicialmente la tecnología 5G.

Para cumplir con estos nuevos requisitos de rendimiento e ir al compás de tareas como la inspección del tráfico cifrado, las organizaciones deben adoptar una solución SD-WAN segura diseñada desde el principio para ofrecer alto rendimiento. Al aprovechar los ASIC de seguridad propios, en contraposición a los procesadores comerciales, la solución Secure SD-WAN de Fortinet es el único dispositivo diseñado para gestionar las funciones de seguridad críticas mientras se mantiene el rendimiento a estas velocidades de conexión.

La seguridad también debe integrarse perfectamente del lado de la red SD-WAN para

garantizar que cuando sea necesario cambiar una conexión, ambas piezas respondan como un sistema único y consolidado. Además, una interfaz de gestión unificada garantizará que cualquier cambio dentro del entorno de la red SD-WAN sea visible y se controle fácilmente desde un único panel de gestión. Fortinet es el único proveedor de SD-WAN que proporciona estas capacidades esenciales.

A medida que la tecnología 5G se abre camino, es más relevante que nunca el papel crítico de la red SD-WAN segura en cualquier estrategia de conectividad remota. Las ofertas SD-WAN construidas alrededor de una infraestructura de servicio que integra la red y la seguridad en una única solución, combinadas con hardware diseñado para ofrecer el rendimiento y la escalabilidad que requieren las redes alimentadas por 5G, son las soluciones perfectas para las organizaciones en transición a 5G. Con las funcionalidades avanzadas de su lado, las organizaciones pueden mantener los riesgos a raya y avanzar en su camino hacia el 5G. ■

Si te ha gustado este artículo,
compártelo



LOS CENTROS DE DATOS HÍBRIDOS DISTRIBUIDOS REQUIEREN CAPACIDADES ADICIONALES DE NGFW

La evolución de los modernos centros de datos ha llevado a que las aplicaciones y los datos se distribuyan cada vez más a través de infraestructuras hí-



bridadas. Si bien esto contribuye a permitir una mayor agilidad para los flujos de trabajo críticos para el negocio, simultáneamente amplía la superficie de ataque de la organización a la vez que complica la visibilidad e inhibe los controles.

FORTINET®

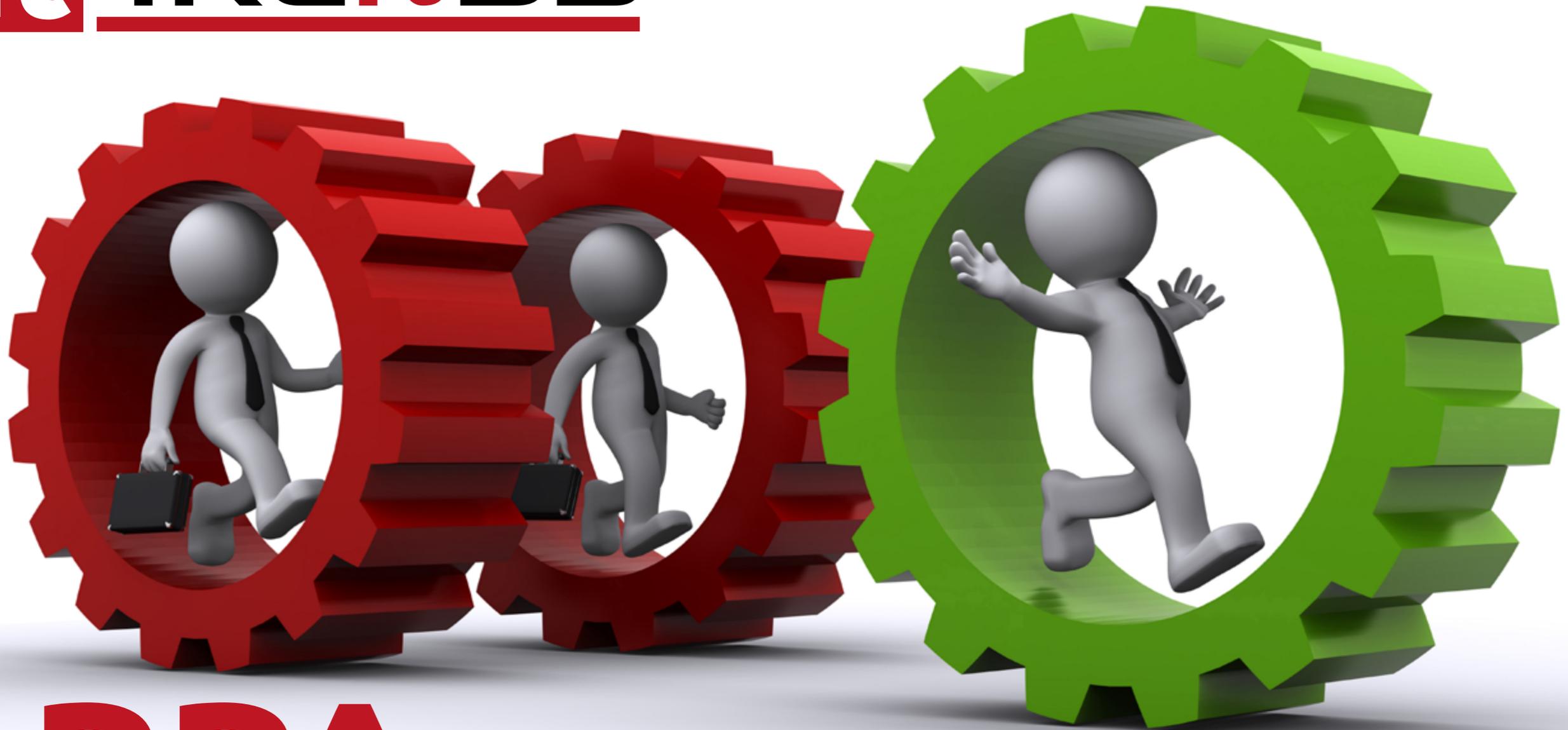


DISEÑADO PARA EL TELETRABAJO SEGURO

Poder adoptar el teletrabajo rápidamente es crítico para la continuidad del negocio y la seguridad. Las soluciones de Fortinet para el teletrabajo ayudan a las organizaciones a garantizar un acceso remoto seguro para todos sus empleados en cualquier ubicación.

SABER MÁS





RPA: la automatización que te hará ganar agilidad corporativa

Patrocinadores:



Uno de los anhelos de las empresas es seguir avanzando en sus procesos de Transformación Digital con el objetivo de incrementar su eficiencia y su productividad y, para ello, no sólo se necesitan herramientas y conocimientos, sino transformar todos los procesos del negocio y la relación con los clientes. Una de las claves para poder digitalizar los procesos es la automatización, que aporta no sólo esa eficiencia deseada, sino también la eliminación de los errores humanos en estos procesos, permitiendo, además, liberar este valor que aportan los profesionales a labores más productivas para el negocio.

Automatizar para una transformación de los procesos eficiente y productiva



Las siglas RPA responden al concepto Robotic Process Automation, Automatización Robótica de Procesos, que, aunque el nombre puede llevar a alguno a pensar en un mundo poblado por robots de apariencia futurista y cinematográfica, es tecnología orientada a la automatización de tareas vía software para reducir las interacciones e intervenciones humanas en el uso de las herramientas informáticas, sobre todo cuando se trata de tareas repetitivas en las que el talento humano no aporta un valor diferencial. Estos robots de software nos permiten, por tanto, reducir el posible error por intervención humana y aumentar la eficiencia y efectividad de los procesos de los que estemos hablando.

Pero ¿es RPA un concepto nuevo? La verdad es que no. No se trata de una tendencia surgida en este momento, pero lo cierto es que en los últimos tiempos ha vivido una evolución importante y, como han adelantado algunos expertos, el gasto generado alrededor de este tipo de herramientas y procesos automatizados denota su creciente papel en el engranaje de las operaciones empresariales.

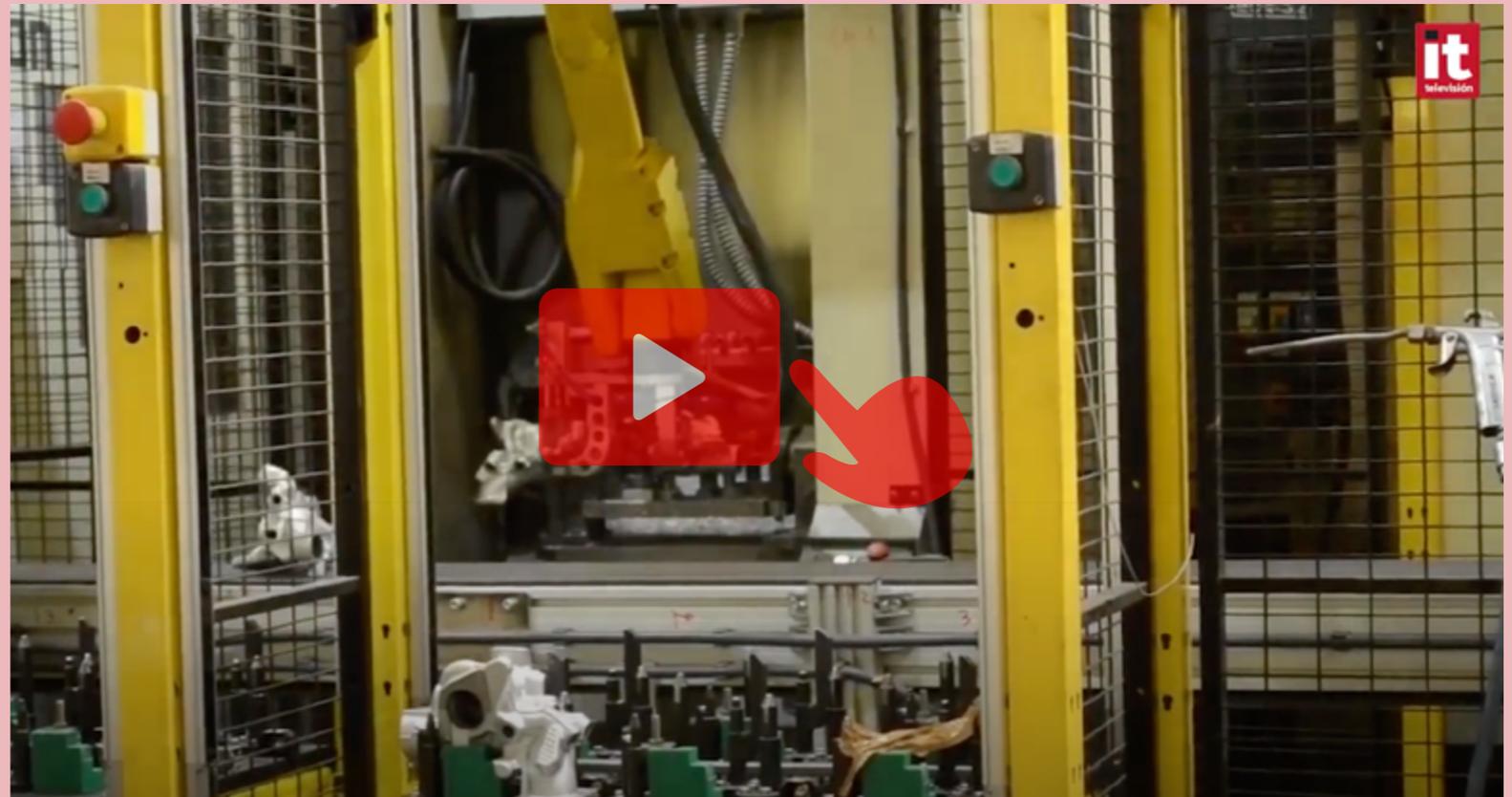
EL MERCADO DE SOFTWARE RPA CRECE DE FORMA EXPLOSIVA

Durante el año 2018, el mercado mundial de software de Automatización Robótica de Procesos ya creció más de un 63%, dando un impulso sin precedentes al sector, que se está viendo reforzado hoy por la gran demanda de los nuevos modelos

de negocio digital y la necesidad de dar continuidad a los negocios. Y en ello está teniendo mucha influencia la creciente sinergia con otras tecnologías de automatización, como la Inteligencia Artificial o el reconocimiento de texto y voz.

Según Gartner, en su [informe sobre el mercado de RPA](#) hace dos años los ingresos alcanzaron los 846 millones de dólares, y se esperaba que durante 2019 la tendencia continuara, hasta elevar la cifra a unos 1.300 millones (los datos

confirmados de 2019 todavía no se han publicado). Como señaló en su momento Fabrizio Bisconti, vicepresidente de investigación de Gartner, “el mercado de RPA ha crecido desde nuestro último pronóstico, impulsado por las demandas de los negocios digitales a medida que las organizaciones buscan un procesamiento directo. La competencia es intensa, con nueve de los 10 principales proveedores cambiando la posición de participación de mercado en 2018”.



RPA: beneficios y retos de la automatización de procesos basados en robótica

Una situación que define mucho este campo es que los cinco principales proveedores acapararon el 47% del mercado de RPA en 2018, aunque es destacable que los que ocupaban la sexta y séptima posición vieron un crecimiento de ingresos de tres dígitos, lo que indica que

los puestos del ranking mundial no están garantizados y, según Biscotti, esto se extiende a los cinco primeros de la lista.

Como señalan los expertos de Gartner, aunque las soluciones RPA se pueden encontrar en todas las industrias, sus principales clientes

son los bancos, las aseguradoras, las empresas de telecomunicaciones y las de servicios públicos, ya que pueden integrar con efectividad esta tecnología en sus numerosos sistemas heredados, lo que les permite avanzar mejor en la Transformación Digital.

Cinco mejoras que RPA está aportando al sector público

El camino hacia una mayor automatización ha comenzado tanto en las empresas privadas como en las administraciones y empresas públicas. Y la RPA está demostrando ser la tecnología que más rápido encuentra su lugar en las organizaciones. En el caso del sector público está contribuyendo de forma decisiva a agilizar los procesos, sobre todo los que involucran burocracia y que tradicionalmente han obligado a tener plantillas muy numerosas, compuestas por trabajadores que realizaban tareas repetitivas.

1 Pero ahora, gracias a la adopción de RPA, este panorama está cambiando de forma radical y, a pesar de que existen muchos miedos sobre la pérdida de empleos asociada a esta tecnología, los expertos opinan que se trata más bien de un cambio de las tareas asignadas. De hecho, pensando en el sector público, los cinco benefi-

cios más positivos e importantes, con un mayor impacto en los próximos años son, primero, **mejor servicio al ciudadano**, ya que, gracias a la automatización robótica de procesos, determinados servicios que las administraciones públicas solo ofrecían en horario comercial podrán prestarse durante las 24 horas, algo que los ciudadanos demandan cada vez más. Esto se lograría integrando robots y chatbots, lo que permitirá a la infraestructura responder automáticamente a los mensajes y las consultas de los ciudadanos.

2 En segundo lugar, **más rapidez en el procesamiento de consultas**, y es que la burocracia en el sector público lastra las operaciones a niveles que generan una gran frustración a los ciudadanos. Con la introducción de RPA se puede lograr un salto enorme en agilidad y en nivel de servicio

a los ciudadanos. Empleando robots y otros sistemas automatizados se pueden escanear documentos automáticamente, validar los datos, verificar las características de un demandante y su idoneidad para acceder a un servicio... acelerando procesos sin que tengan que intervenir los funcionarios y trabajadores.

3 Tercero, **más precisión en la entrada de datos**, porque mediante RPA es más fácil que la información sea verificada en cada paso, sin que se produzcan errores en la recopilación de datos. Además, los ciudadanos y los propios empleados de la administración cuentan con más herramientas para verificar que la información es correcta, como portales web, aplicaciones de soporte o escritorios remotos, y la resolución de problemas por errores en los datos puede hacerse mucho más deprisa.

4 Cuarto, **integración de sistemas de bajo coste**, debido a que las herramientas de RPA pueden ayudar a una mejor integración de los sistemas heredados con las nuevas tecnologías, facilitando la gestión de la información y la transferencia de datos entre distintos sistemas. Este es un problema constante para las empresas del sector público, organizaciones donde el gasto en TI es contenido y donde el personal no siempre cuenta con las capacidades necesarias para implementar nuevas tecnologías y trabajar con ellas.

5 Por último, **mejoras de conciliación y presentación de informes**, debido a que RPA proporciona una agilidad sin igual para el trabajo con los datos necesarios para elaborar esos informes, como la verificación de cuentas y saldos en los sistemas, y la localización y administración de las discrepancias e inconsistencias en la información.

Un tema que considerar, y al que Gartner da mucha importancia, es que este entorno va a cambiar mucho en los próximos años, porque las grandes empresas como IBM, Microsoft y SAP, que dominan el mercado tecnológico, están buscando asociarse con otras empresas del sector o adquirirlas, para aumentar su conocimiento, sus clientes y su impulso. Pero, a su vez, las nuevas compañías están adaptándose con más agilidad a las nuevas demandas de los clientes de la era digital, añadiendo capacidades como el procesamiento de eventos y el análisis en tiempo real, lo que atrae a clientes de diferentes ámbitos y escalas.

Estas estrategias harán que, según Deloitte, el mercado de soluciones de automatización crezca a un ritmo anual del 20%, alcanzando los 5.000 millones de dólares en 2024. A nivel general, 2020 va a ser un gran año para estas tecnologías, ya que las compañías se encuentran en plena adopción de automatizaciones inteligentes.

RPA + INTELIGENCIA ARTIFICIAL

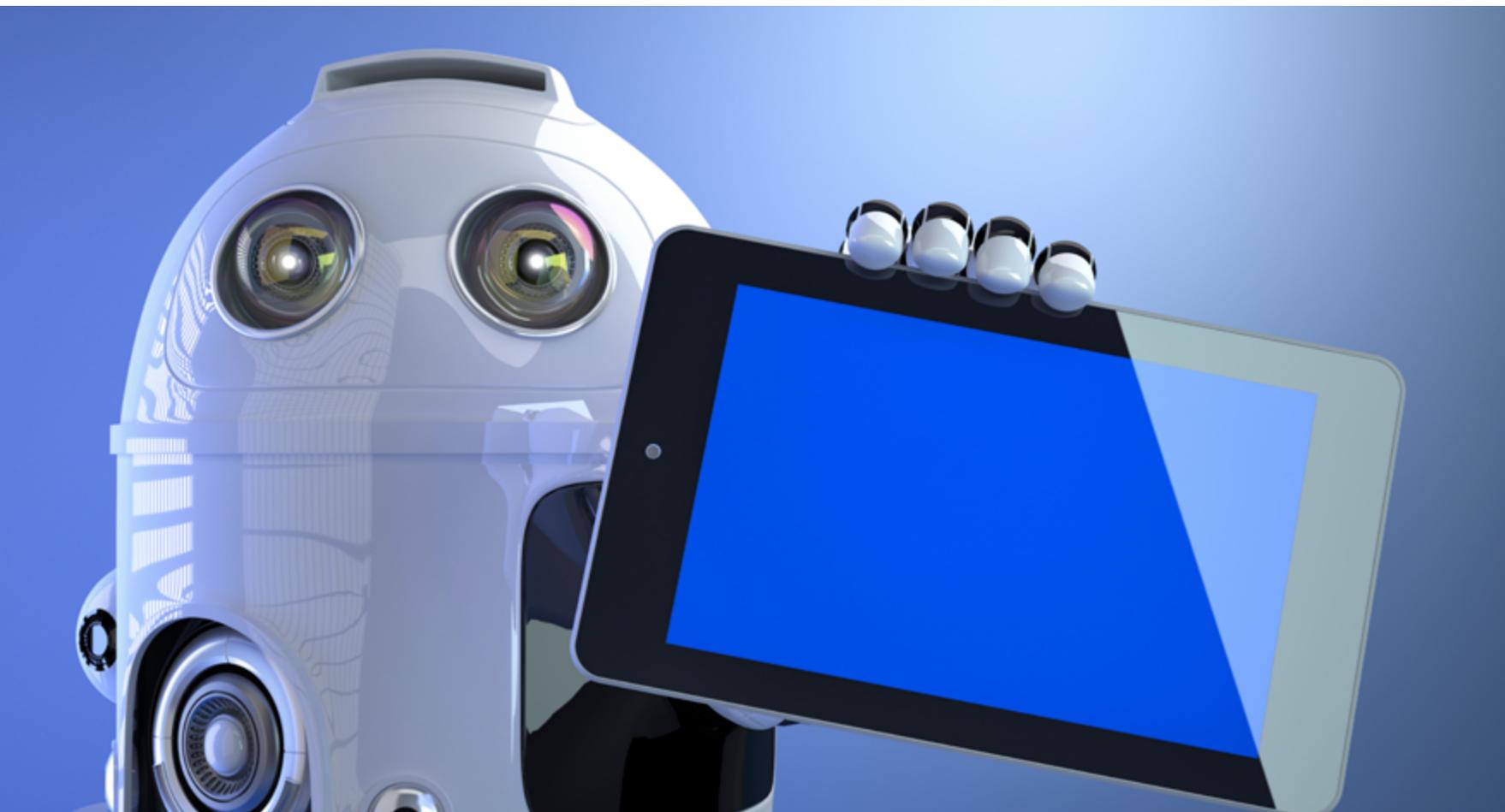
El estudio [Automation with intelligence. Reimagining the organisation in the Age of With](#), pronostica un crecimiento sólido no solo de las soluciones de automatización robótica de procesos, sino que las automatizaciones que

se produzcan serán inteligentes e integrarán Inteligencia Artificial.

Según los datos, extraídos de entrevistas a 523 directivos de compañías de 26 países de todo el mundo, el 47% afirma que combina RPA con Inteligencia Artificial como parte de su estrategia de implementación de automatización inteligente. Además, están consiguiendo buenos resultados, ya que organizaciones que combinan estas dos tecnologías reportan un incremento del 9% en sus ingresos, frente al 3% que registran aquellas que sólo emplean RPA.

Por tanto, concluye Deloitte que la implementación de procesos de automatización inteligente sigue superando las expectativas. Además, las organizaciones que emprenden pruebas piloto perciben de media un retorno alrededor de los 15 meses tras su incursión, mientras que las que se encuentran en fase de escalada lo registran ya de media a los nueve meses. Según Santiago Gómez Rebollo, socio de consultoría de la firma, “2020 será el año clave para la automatización inteligente, a medida que las organizaciones combinen la automatización de procesos con robots con Inteligencia Artificial y otras tecnologías que permitan nuevas maneras de trabajar”.

En su opinión, las automatizaciones trascenderán de la rutina a la innovación, desde recolectar información a predecir datos, analizando y apoyando para la toma de decisiones. “Las empresas que reconfiguren su manera de trabajar, que tomen ventaja de la combinación



El sector financiero, pionero en aprovechar la automatización que le ofrece la RPA

Según el informe elaborado por la firma de investigación Juniper Research, la RPA en el sector financiero tendrá un crecimiento espectacular.

Esta industria ha sido una de las primeras en identificar el gran valor que puede aportar la automatización robótica de procesos a sus operaciones, y los analistas afirman que entre 2018 y 2023 la adopción de es-

tas soluciones crecerá un 400% entre estas empresas, generando unos ingresos que pasarán de los actuales 200 millones de dólares a 1.200 millones al final del período. Las regiones más importantes en este mercado serán Norteamérica y Europa Occidental, que ahora mismo abarcan casi el total del mercado.

Pero, según indican ciertas voces de la industria, esta evolución se enfrenta a determinadas trabas, ya que la adopción de las herramientas RPA está en sus fases iniciales en muchas de las empresas del sector. Esto supone que no existe una gran comprensión de esta tecnología, lo que retrasa la obtención de

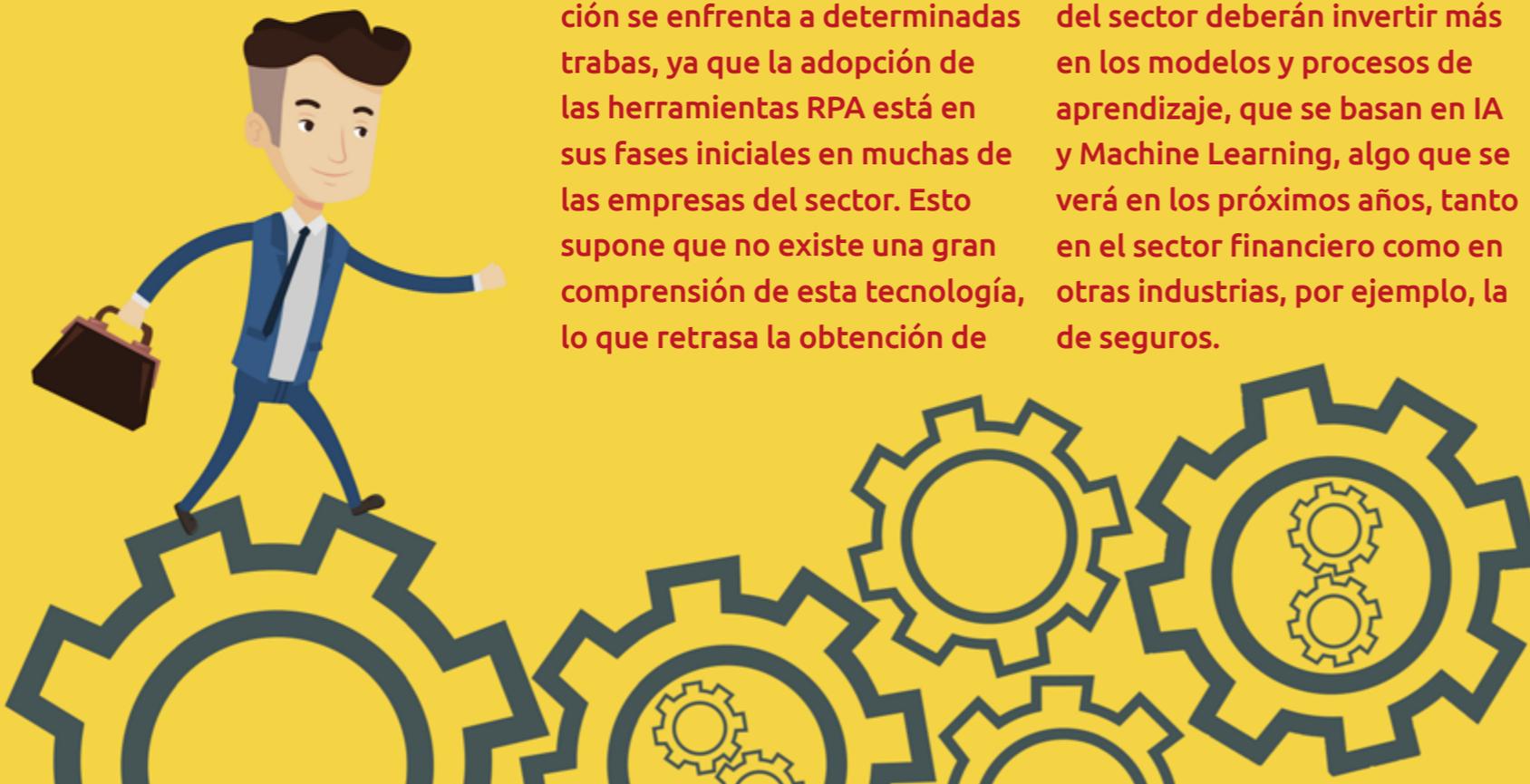
beneficios en estas inversiones. Por ahora, las aplicaciones RPA que más se han adoptado en la industria financiera son los chatbots, que prometen una interacción más ágil, intuitiva y sencilla para el usuario, lo que mejorará la experiencia del cliente. Pero todavía necesitan pulir su funcionamiento y mejorar su inteligencia para alcanzar todo su potencial. Para ello, las empresas del sector deberán invertir más en los modelos y procesos de aprendizaje, que se basan en IA y Machine Learning, algo que se verá en los próximos años, tanto en el sector financiero como en otras industrias, por ejemplo, la de seguros.

entre las personas y las máquinas ejecutando nuevos procesos, y que tengan las habilidades y el conocimiento para impulsar la automatización inteligente serán las mejores posicionadas para aprovecharse de las oportunidades que esta tecnología les puede aportar”, añade.

LA INVERSIÓN ESPAÑOLA EN RPA CRECERÁ MÁS DE UN 35% HASTA 2022

Esta evolución en los datos globales tiene su reflejo en nuestro país. La consultora IDC, en colaboración con Microsoft, presentaba recientemente [un informe en el que analizan cómo optimizar las operaciones de las empresas y la manera de satisfacer mejor a clientes y empleados](#). Y son varias las conclusiones, como el hecho de que el año próximo la mitad de los ingresos de las compañías tendrán su origen en la transformación de modelos de negocios digitales, basados, además, en economías de plataforma y monetización de datos. Una cifra que ascenderá hasta el 80% en 2023.

Según se desprende de esta investigación, las organizaciones deben evolucionar hacia una plataforma tecnológica que pase a ser un núcleo inteligente, que debe estar definido por capacidades cognitivas como la analítica avanzada, la Inteligencia Artificial o Machine Learning. Todo ello apoyado en despliegues en la nube. Es fundamental que la relación entre las organizaciones y sus clientes sea a tiempo real. Al hilo de este informe, ahora, con la Inteligencia Artificial, se añe-



de valor a cada una de las capas de análisis de datos, permitiendo automatizar tareas específicas y mejorar las actividades relacionadas y el proceso general de apoyo a la decisión. De hecho, la inversión en automatización de procesos en Europa crecerá a una tasa del 35% hasta 2022 según IDC. En España, incluso por encima de esta tasa.

Otra investigación, ésta de [Kaizen Institute](#), destaca dos cifras muy importantes y que generan mucha controversia. La primera es que, con las tecnologías actuales, solo el 5% de los trabajos en Europa pueden ser completamente

automatizados. Y la segunda es que en el 60% de los empleos se pueden automatizar hasta un 30% de las actividades que desarrollan los trabajadores, principalmente las tareas repetitivas y de poco valor añadido para los trabajadores.

La implementación de estas tecnologías comenzó en las grandes corporaciones y en determinados sectores, pero actualmente la Automatización Robótica de Procesos ha calado hasta otros niveles de la economía, llegando a las pequeñas y medianas empresas. Un ejemplo de ello es España, donde el 53% de las PYMES ya ha aplicado

RPA a sus procesos como parte de su estrategia de digitalización, de acuerdo con dicho estudio.

Los analistas han puesto énfasis en los enfoques actuales de RPA, que solo requieren instalar un software en las máquinas de cada empleado y llevar a cabo una configuración sencilla, que resulta muy intuitiva para casi cualquier perfil de trabajador. Gracias a esto, el proceso resulta rápido (generalmente menos de seis meses) y requiere una inversión mínima, lo que ha permitido llevar esta tecnología a empresas de menor tamaño en un tiempo bastante corto.



Aunque las soluciones RPA se pueden encontrar en todas las industrias, sus principales clientes son bancos, aseguradoras, empresas de telecomunicaciones y de servicios públicos, ya que pueden integrar con efectividad esta tecnología en sus numerosos sistemas heredados (Gartner)

Otra ventaja de RPA es que resulta más flexible y escalable que otras estrategias.

En palabras de Javier Langa, manager de Kaizen Institute para Europa Occidental, “aunque sigue existiendo cierto temor en la sociedad a la pérdida de puestos de trabajo ligado a la automatización, la realidad es que el avance de nuevas tecnologías genera un saldo total positivo de puestos de trabajo, y permite sacar mucho más potencial de los trabajadores, liberándoles de las tareas tediosas de poco valor añadido para las que no es necesario el potencial del cerebro humano y enfocarse en proyectos que involucren un proceso creativo”.

EL RECELO DEL TRABAJO AUTOMATIZADO

Pese a las promesas empresariales de ahorro de costes, eficiencia, o productividad, existe entre los empleados el temor a la pérdida de su puesto de trabajo. El último estudio de Ipsos sobre [el progreso de la automatización en España](#) muestra que el temor a la automatización y la consiguiente pérdida del empleo es mayor en los mercados emergentes.

Como ya hemos mencionado anteriormente, tecnologías como la Inteligencia Artificial y el aprendizaje automático están abriéndose paso en el entorno empresarial, proporcionando nuevas formas de abordar las tareas diarias, especialmente de carácter administrativo, que suelen ser más repetitivas y tediosas. Pero poco a poco, de la mano de esos nuevos asistentes digitales, las

En España, el 53% de las PYMES ya ha aplicado RPA a sus procesos como parte de su estrategia de digitalización

tecnologías de automatización van a poder aplicarse a trabajos de otro nivel, como a ciertas tareas relacionadas con la organización y la gestión. Porque la IA y el ML ofrecen numerosas posibilidades en el ámbito de las empresas, muchas de ellas todavía por descubrir. Claro, que esto va a tener un impacto importante en el mercado laboral, ya que muchos trabajos actuales van a desaparecer o van a transformarse hasta el punto de ser irreconocibles en unos años.

Según la encuesta de Ipsos, realizada en 28 países distintos, un 35% de la población ve probable que su puesto de trabajo sea automatizado en los próximos 10 años. Mientras tanto, un 54% piensa que es poco probable que esto se produzca y un 11% no está seguro de lo que sucederá.

En opinión de Vicente Castellanos, director de estudios sociales de Ipsos España, “la digitalización supone automatizar cada vez más los puestos de trabajo. Del estudio de IPSOS se desprende que cuanto mayor parte de nuestro trabajo se dedique a la toma de decisiones, menos nos sentimos

amenazados por la digitalización, y aceptamos de mejor grado que la toma de decisiones se base en herramientas que nos ayuden a decidir mejor”.

Como conclusión, el 69% de los entrevistados durante esta investigación opinan que podrán mantener su empleo a pesar de los cambios que traerá la automatización. En el caso de España, el 66% se siente seguro de tener las habilidades necesarias para que su puesto de trabajo deba mantenerse.

LA IA Y LA AUTOMATIZACIÓN REQUERIRÁN PERSONAL CON MÁS INTELIGENCIA EMOCIONAL

Lo que está claro es que la introducción de la IA y la RPA demandarán nuevas habilidades, pues para trabajar con Inteligencia Artificial y con la automatización hacen falta profesionales con cualificación técnica, pero también con otras habilidades transversales, como es la inteligencia emocional (IE). Según una investigación de la firma [Capgemini](#), la demanda de estas competencias se multiplicará por seis en los próximos 3 a 5 años.

Este estudio, denominado [Emotional Intelligence – The essential skillset for the age of AI](#), tiene como objeto analizar cómo están introduciéndose capacidades humanas como requisitos fundamentales para el trabajo en entornos de automatización e Inteligencia Artificial. Uno de sus principales pronósticos es que la demanda de inteligencia emocional para este tipo de empleos se multiplicará por seis en los

El mercado de soluciones de automatización crece a un ritmo anual del 20% y se espera que alcance los 5.000 millones de dólares en 2024 (Deloitte)

próximos 3 a 5 años. Pero, sin embargo, menos de una de cada cinco empresas está formando a los trabajadores que no tienen funciones de supervisión en este campo.

Esto es un freno importante para alcanzar la cualificación necesaria para la automatización dentro de las organizaciones, dada la opinión de empleados y directivos, que creen que la inteligencia emocional es una capacidad clave, junto con la conciencia de uno mismo, la autogestión, la conciencia social y la gestión de las relaciones. Y creen firmemente que esto se convertirá en un requisito fundamental para tener éxito en los próximos años.

Pero, según las respuestas obtenidas en esta investigación, la inmensa mayoría de las organizaciones no ha modificado sus procesos de selección y formación de personal para implementar este enfoque. Y esto impedirá que se pueda aprovechar el potencial de la inteligencia emocional para mejorar la satisfacción del

empleado, reducir la rotación de personal, generar más ingresos y reducir costes.

Entre las principales conclusiones de este informe destaca que el avance de la automatización y de la IA en las empresas propiciará un cambio de percepción sobre el valor que habilidades como la inteligencia emocional tienen en la organización. Esto será importante para el trato con el cliente, ya que las tareas rutinarias automatizadas dejarán espacio para que los empleados dediquen más tiempo al trato personal, como opina el 76% de los directivos encuestados. Y otros tantos creen que los empleados deberán asumir tareas que requieren competencias emocionales. Por ello, para el 61% de encuestados la IE se va a convertir en una competencia clave en un plazo de 1 a 5 años.

Otro asunto importante en este sentido es que los trabajadores se muestran preocupados por la introducción de la Inteligencia Artificial y la automatización, y ven peligros para su puesto de trabajo. Esto pone el foco en otras habilidades que permitirán progresar en la organización a largo plazo, como son este tipo de soft skills. Esta idea se ve reforzada por los datos, ya que las organizaciones con una plantilla más dotada en materia de IE ya están percibiendo beneficios. Por ejemplo, un 60% de ellas afirma estar consiguiendo unos resultados un 20% mejores en diversos factores de negocio, como la productividad, la satisfacción del empleado, la cuota de mercado o la atención al cliente. ■



MÁS INFORMACIÓN



[Beneficios de la monitorización de red para la automatización industrial](#)



[Beneficios empresariales de la automatización y la orquestación](#)



[Impacto de la automatización en las operaciones de IT](#)

Si te ha gustado este artículo, compártelo



Convierta Desafíos En Oportunidades

Impulse La Continuidad Del Negocio Con
Una Fuerza De Trabajo Digital Inteligente

No todas las tecnologías de automatización robótica de procesos (RPA) son iguales. Cuando se producen cambios, necesita una solución que se adapte e implemente rápidamente. Automation Anywhere ofrece la única plataforma RPA con inteligencia artificial integrada, creada para la nube y con un interfaz web para satisfacer las necesidades de hoy y prepararlo para las incertidumbres del mañana.

automationanywhere.com/la/products/enterprise/a2019



La automatización de procesos, motor de la eficiencia en las empresas españolas

España está inmersa en el proceso de desescalada. Tras más de dos meses de confinamiento, la nueva normalidad empieza a hacerse notar y con ella, los cambios en las empresas para ser 100% seguras y eficientes. Y es que, si hay lecciones aprendidas de esta situación vivida, además de demostrar que el teletrabajo es factible en nuestras organizaciones, entre ellas figura la necesidad de automatizar procesos para que nuestras empresas sean más ágiles, productivas y eficientes.

Dicha necesidad puede cubrirse desde varios frentes, pero desde hace unos años, el concepto de RPA o automatización robótica de procesos, está sonando en las organizaciones con mayor fuerza como esa tecnología que les permitirá alcanzarlo. “Permite automatizar tareas manuales y repetitivas, de gran volumen y basadas en reglas, que no aportan generalmente valor a la empresa pero que suelen tener un elevado coste al necesitar de la intervención humana”, explica Víctor Ayllón, Vicepresidente RPA COE de Appian Corporation.

Por su parte, Óscar Martínez, Regional Sales Director de Automation Anywhere, apunta que se trata de una tecnología intuitiva y fácil de usar: “es capaz de interactuar con cualquier sistema o aplicación a través de la interfaz de usuario, lo que permite a los



usuarios de negocio construir automatizaciones o bots por sí mismos y obtener un retorno de la inversión en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías donde se requiere una inversión inicial mayor y más recursos técnicos”.

Generalmente se suele asociar la automatización con la destrucción de puestos de trabajo. Sin embargo, ABAI Group quiere desmarcarse de esa idea. “La RPA es un medio para un fin con más transcendencia. El ser humano aporta una función de valor que nunca podrá ser sustituida por robots porque aporta creatividad, juicio y empatía. Lo que queremos potenciar son esas habilidades hacia un automatismo para mejorar la experiencia del empleado, pero sin perder el foco de la máxima eficiencia y mínimos costes”, agraga Carlos Fernández, responsable de soluciones de negocio de ABAI Group.

UNA PROPUESTA EN ALZA

La automatización robótica de procesos es una tendencia global y organizaciones de todas las industrias y regiones ya han automatizado al menos alguno de sus procesos de negocio. Aunque las cifras pueden ser dispares (un informe de HfS Research señala que en 2021 el volumen de negocio de este sector será de 12.700 millones de dólares, mientras que Morgan Stanley aumenta la cifra a 54.000 millones), lo cierto es que hay un gran interés. En España, según IDC, el 58% de los CIO considera que la automatiza-

ción de procesos y la IA serán la principal prioridad de inversión. La consultora señala, también, que el mercado de RPA en nuestro país se duplicará en los próximos años.

“Entre los sectores más avanzados en la automatización inteligente, destacan Banca y Servicios Financieros, BPO, Utilities, IT y Manufacturing. No obstante, el contexto actual, en el que las organizaciones necesitan combinar la continuidad del negocio con la particularidad impuesta por la COVID-19 de evitar la interacción física y ser más ágiles a la hora de dar respuesta al cliente, está favoreciendo la aceleración de proyectos de automatización en todas las industrias, convirtiéndola en una necesidad. En este sentido, existe interés y necesidad en prácticamente todos los sectores, como el sector sanitario, la banca, las compañías aseguradoras, las operadoras de telecomunicaciones, el sector de la energía, el retail, la Administración Pública e, incluso, en el ámbito turístico”, asegura Ayllón.

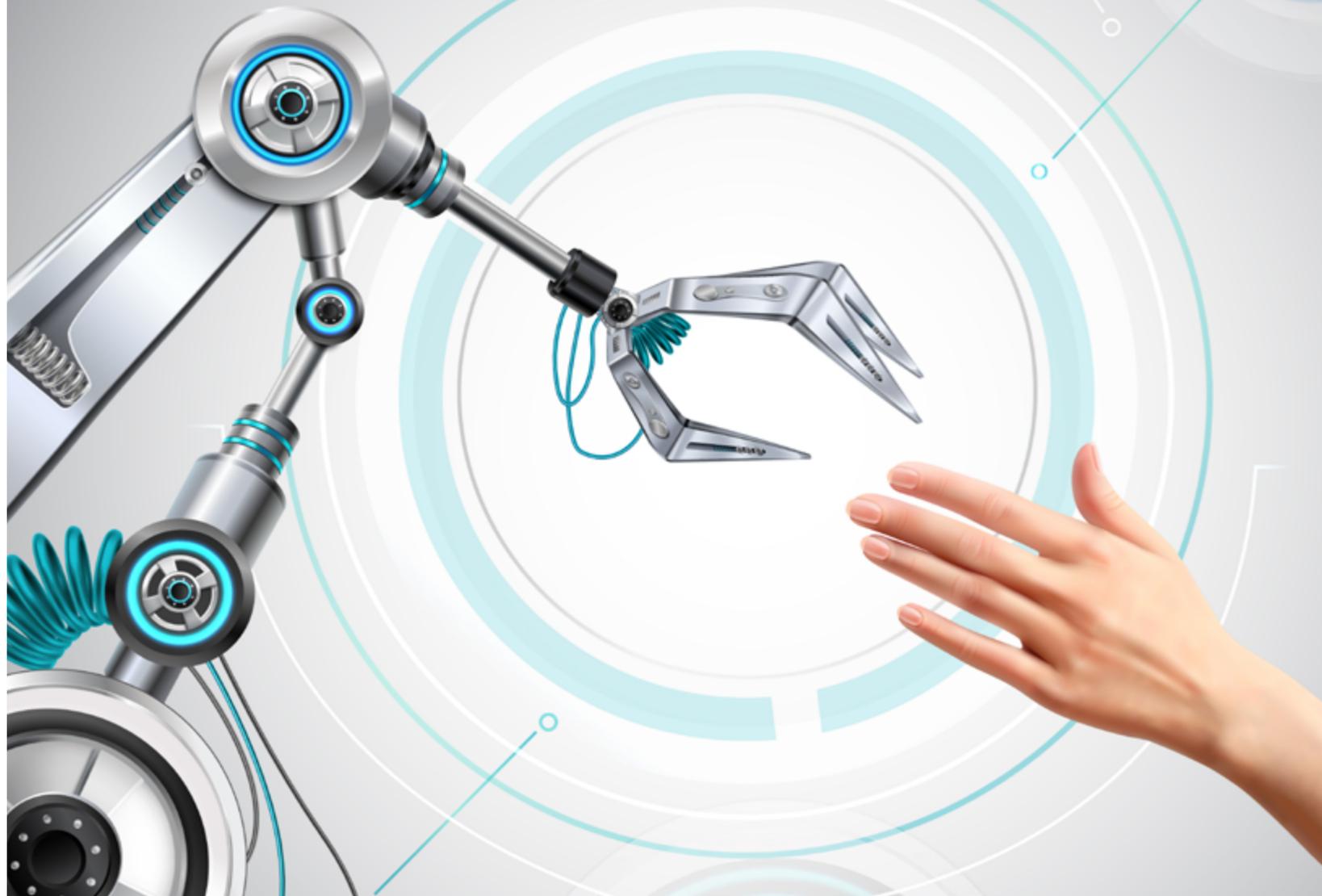


“La crisis por la pandemia pone de manifiesto que las compañías deben estar preparadas para el cambio y garantizar la continuidad de su negocio. Las plataformas de automatización son sus aliadas para enfrentarse a este nuevo escenario”

VÍCTOR AYLLÓN, APPIAN

Automation Anywhere coincide. “En los últimos años, hemos visto una gran adopción de nuestro software por parte de empresas de servicios financieros, que han conseguido mejorar la eficiencia, reducir el fraude y reforzar el cumplimiento, reduciendo los costes operativos. También existen importantes implementaciones en otros sectores como las compañías de seguros, que mejoran la evaluación de riesgos y la gestión de siniestros para ofrecer una mejor experiencia a sus clientes; o las organizaciones farmacéuticas y de salud, que optimizan sus tiempos de procesamiento y mejoran los servicios a los pacientes. Otro gran mercado desde nuestro punto de vista son las empresas manufactureras e industriales, con larga tradición en robots físicos y que pueden ganar eficiencias en todo lo que tiene que ver con operaciones, cadena de suministro y back office”.

En ABAI Group creen que la RPA actualmente está presente en la gestión de ventas, back



“RPA interactúa con cualquier sistema o aplicación, permite a los usuarios de negocio construir bots por sí mismos y obtener un ROI en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías”

ÓSCAR MARTÍNEZ, AUTOMATION ANYWHERE

office y unificación de bases de datos. Sin embargo antes de que llegue 2025 va a ampliarse el nicho. “Nuestro día a día está lleno de tareas repetitivas. Envío de informes, datos de hojas de cálculo, recordatorios, evaluaciones de ratios etc. El cómputo de ese tiempo no es una cuestión menor y es que la RPA no solo cubre la capa básica de las tareas, sino que puede ampliarse a todas las actividades de procesos mecánicos que aportan poco valor”, afirma Fernández; “cuando las empresas midan los tiempos se darán cuenta del poco valor que les sacamos a las cualidades de nuestros empleados”.

“Entre nuestros clientes hay varias empresas del IBEX 35 -entre otros Santander Consumer- en las que estamos implementando proyectos junto con la ayuda inestimable de nuestro canal, gran cantidad de multinacionales con oficinas en España y que tienen como plataforma de automatización Automation Anywhere y un número importantes de oportunidades en diversos sectores”, apunta el responsable de ventas de la compañías, quien destaca, en estos momentos, la oportunidad que la aplicación de RPA tiene para hacer frente a los efectos de la COVID-19, y al uso que gobiernos y empresas están haciendo de sus robots RPA para combatir los desafíos que presenta la pandemia. No es un caso de nuestro país, pero puede servir de ejemplo: “colaboramos con varios hospitales, como el Hospital General de Northampton en Londres, para automatizar la monitorización

constante del suministro de oxígeno del centro médico, reducir el riesgo de errores y apoyar el tratamiento de pacientes con COVID-19”.

También desde Appian están obteniendo grandes referencias de clientes en nuestro mercado. “Los principales bancos españoles como Santander o Bankia utilizan nuestra aplicación y la administración pública está empezando a incorporar esta tecnología en sus procesos”, añade Ayllón, quien destaca también el Centro de Excelencia Robotics de Deloitte, “donde se han automatizado más de 100 procesos robóticos con Appian RPA, con más de 41.000 horas de uso en un año. Han amplificado sus capacidades de automatización de procesos a gran escala, con un importante impacto, tanto en operaciones internas de su área Business Process Outsourcing (BPO) como en procesos críticos para clientes de diferentes industrias”.

Por su parte, Fernández destaca que, “en ABAI Group implementamos RPA en telco, utilities y logística. El objetivo es separar el tiempo de gestión del tiempo de relación con el cliente. La automatización alivia sistemas, aplicaciones y tiempos de espera”.

AUTOMATIZACIÓN DE PROCESOS, COMBINACIÓN DE TECNOLOGÍA Y CAPACIDAD HUMANA

Además de generar oportunidades para las empresas, y en contra de la leyenda negra que acarrea la automatización, la RPA no significa destrucción

de empleo. Aún más, según el World Economic Forum (WEF), las profesiones emergentes resultantes de la automatización podrían representar 6,1 millones de empleos en todo el mundo entre 2020 y 2022. “La robotización puede potenciar las habilidades humanas y generar nuevas oportunidades laborales”, destacan desde Appian.

La creación de estas plataformas de software para la automatización de procesos se ha venido enriqueciendo en los últimos años sumando tecnologías. “Nuestros esfuerzos en I+D van encaminados a permitir a toda organización automatizar de forma integral sus procesos, de extremo a extremo. Para ello, combinamos diferentes tecnologías bajo una única plataforma que ayuden a nuestros clientes en todos los pasos de la automatización en sí: descubrir, analizar, diseñar, automatizar, medir, monitorizar y reevaluar; un concepto que va más allá de la RPA y que se conoce como hiperautomatización”, afirma Óscar Martínez.

“Nuestro día a día está lleno de tareas repetitivas y el cómputo del tiempo que empleamos en realizarlas no es una cuestión menor. La RPA puede ampliarse a todas las actividades de procesos mecánicos que aportan poco valor”

CARLOS FERNÁNDEZ, ABAI GROUP

Bajo este precepto, la solución de Automation Anywhere ofrece una propuesta en la nube, con un interfaz web, que se implementa en cuestión de minutos y es accesible desde cualquier dispositivo. Su plataforma combina RPA, inteligencia artificial, aprendizaje automático y análisis de datos en tiempo real, para ayudar a las organizaciones a iniciar rápidamente su proyecto de automatización de procesos y luego poder escalarlo fácilmente y de forma ilimitada. “Nuestra propuesta permite el uso de la automatización desde las aplicaciones más comunes como Salesforce, Excel o G Suite y, por tanto, solventa uno de los problemas de la automatización que, según Gartner, es el número limitado de procesos automatizados en las implantaciones existentes”.

Por parte de Appian, “entendemos la automatización de procesos como una manera de repensar los trabajos para combinar de la for-



ma más eficiente capacidades humanas, inteligencia artificial y robots, entendiendo cada una de estas piezas como “trabajadores” de un mismo workflow”. En base a ello, han construido una plataforma con la que “hemos conseguido un mayor control de la base instalada de bots así como la posibilidad de desplegar bots más sofisticados para tareas más complejas. La capacidad de orquestar fácilmente la próxima generación de mano de obra combinada: personas, software, robots e IA en flujos de trabajo sin fricción (incluso en ausencia de API), nos da una potente administración de robots para aumentar la escala y el rendimiento, y ejecutamos Appian Cloud, segura y disponible a nivel mundial”, relata Ayllón, quien destaca, además, la incorporación de Novayre Solutions SL, desarrolladores de Jidoka RPA, como un punto de

inflexión en su oferta. “Con la incorporación de este activo, Appian ha conseguido permitir a los clientes la opción de utilizar la funcionalidad de automatización full-stack (iBPMS, RPA, AI y gestión de caso) a través de Appian Cloud con la expectativa de que estas soluciones mantengan su rápido y fácil desarrollo y entrega, así como un ROI elevado y plazos muy cortos para recuperar la inversión”.

En el caso de ABAI Group, la compañía ha diseñado su solución RPA junto a su partner White Pass. “Ofrecemos un portfolio integral. Para ello hemos diseñado aplicaciones de negocio personalizables que sirven como interfaz entre las personas y el robot. Queremos reducir a cero el tiempo de petición y tramitación. Además, los robots no son infalibles y menos en procesos complejos, así que para ofrecer esa experiencia

integral cubrimos esos procesos haciendo que las gestiones no finalizadas se envíen a los especialistas. Es un marco digital sin carga y descarga de ficheros y sin tiempos vacíos por procesos manuales”, explica Fernández.

La oportunidad de la automatización está ahí. Hoy más que nunca las organizaciones deben estar preparadas para el cambio, para repensar sus negocios, para ganar agilidad. Y las cifras esperadas del mercado de automatización indican que están en el camino de querer y poder aprovechar las capacidades que esta propuesta tecnológica les brinda para seguir avanzando en su transformación. ■

MÁS INFORMACIÓN

-  [Entrevista completa con Óscar Martínez \(Automation Anywhere\)](#)
-  [Entrevista completa con Víctor Ayllón \(Appian\)](#)
-  [Entrevista completa con Carlos Fernández \(ABAI Group\)](#)

Si te ha gustado este artículo,
compártelo

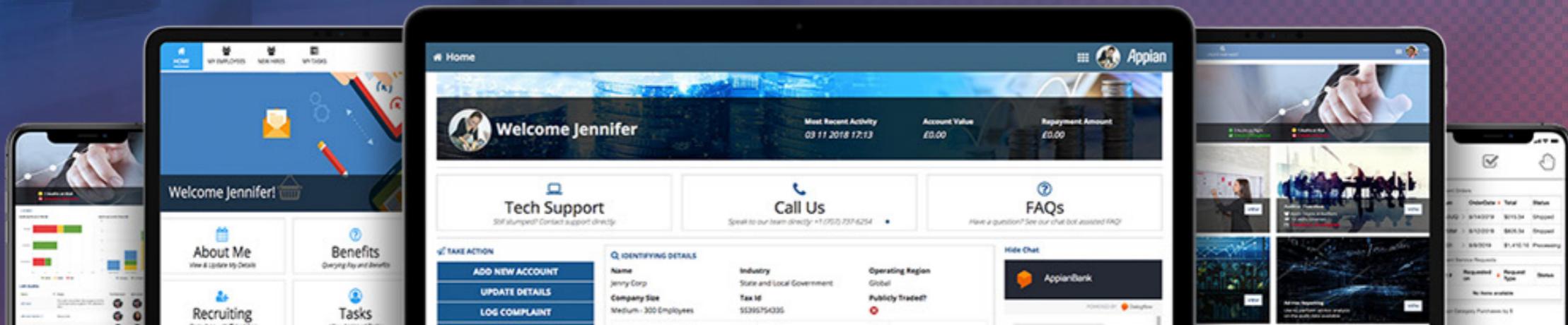


Automatizar las tareas.
Mejorar la productividad.
Todo con una plataforma potente.

Prueba hoy el RPA de Appian

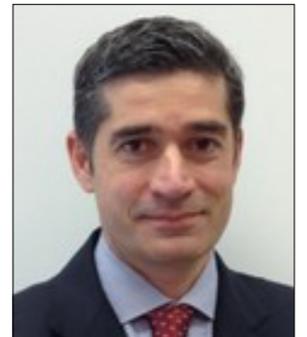


Appian



Automatización inteligente para acelerar la transformación digital

ÓSCAR MARTÍNEZ,
Regional Sales
Director de
Automation Anywhere



Según Gartner, en los dos últimos años, la Automatización Robótica de Procesos o RPA ha sido el segmento de software de más rápido crecimiento. Para finales de 2023, el 90% de las organizaciones grandes o muy grandes habrán implementado alguna forma de RPA como pieza clave de sus iniciativas de transformación digital, en comparación con el 55% que ya lo hacían en 2019.

La Automatización Robótica de Procesos (RPA) es una forma de automatización no invasiva, intuitiva y fácil de usar, que interactúa con cualquier sistema o aplicación involucrada en un proceso a través de la interfaz de usuario. Permite a los usuarios construir bots para auto-

matizar tareas comerciales basadas en reglas al imitar las actividades de un usuario y en general es más fácil de implementar, de forma que se obtiene un retorno de la inversión en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías donde se requiere una inversión inicial mayor y más recursos técnicos.

Además, un gran número de organizaciones aplica ya diferentes tecnologías de Inteligencia Artificial para complementar y aumentar las posibilidades de la RPA (un 80% de las empresas para 2022, según Gartner), como por ejemplo en el procesamiento inteligente de documentos (IDP), donde se utiliza inteligencia

artificial para procesar datos no estructurados de correos electrónicos, contratos, documentos escritos a mano, etc.

En Automation Anywhere creemos que todo proceso que puede ser automatizado dentro de una organización debería ser automatizado para desbloquear el potencial humano, liberar a los empleados de esas tareas tediosas y repetitivas, y que así se puedan centrar en las cosas que sólo los humanos pueden hacer: como el pensamiento crítico y la creación de valor a través de la innovación.

Automation Anywhere es la única plataforma de RPA que democratiza el uso de la automatización de procesos con una combinación de

“Todo proceso que puede ser automatizado dentro de una organización debería ser automatizado para desbloquear el potencial humano”

facilidad de uso y la fiabilidad necesaria para acelerar las iniciativas de transformación digital de cualquier empresa.

Entonces, si el camino más rápido hacia la transformación digital es la automatización, ¿por qué es todavía tan difícil para muchas organizaciones hoy? La razón se debe a que la mayoría de las empresas tienen sistemas y aplicaciones informáticas tanto en front como en back office que trabajan en silos y nunca fueron diseñados para trabajar juntos. ¿Cuál es la principal ventaja de las empresas nativas digitales más exitosas? Estas empresas modernas nacieron ya en un mundo dominado por procesos digitales e integran las herramientas de front y back office y las aplicaciones de productividad que usan todos los empleados para obtener una ventaja significativa en términos de costes y velocidad de ejecución.

Hoy en día, las empresas tradicionales no solo se enfrentan a la competencia de estas compa-

ñías nativas digitales, sino también a otros factores externos como la reciente pandemia de COVID-19. RPA puede ayudar, es el equalizador entre la empresa tradicional y las organizaciones nativas digitales.

Si bien ciertas soluciones de automatización puntuales pueden ayudar con ciertos pasos del proceso en el front o back office, solo una solución completa de automatización permitirá derribar los silos. De esta forma, las organizaciones pueden comenzar con cualquier proceso sabiendo que puede llegar a ser en una empresa totalmente automatizada y cerrar la brecha entre el front office, el back office y todos los empleados.

Esta transformación digital por medio del uso de la Automatización Inteligente a través del front y back office, permite a las empresas obtener las siguientes ventajas competitivas:

- ❖ Tomar medidas más rápidas bajo la restricción de recursos reducidos

- ❖ Mantener la continuidad del negocio con una fuerza laboral digital 24/7
- ❖ Preservar la conexión con todas las partes interesadas a través de múltiples sistemas
- ❖ Asegurar una buena atención al cliente durante picos en el volumen de llamadas
- ❖ Ayudar a proteger las funciones y operaciones comerciales más críticas durante los actuales momentos de incertidumbre

Automation Anywhere ofrece la única plataforma de automatización inteligente con una arquitectura diseñada para la nube y con un interfaz web, por lo que se implementa en cuestión de minutos y es accesible desde cualquier dispositivo. Combina RPA, inteligencia artificial, aprendizaje automático y análisis de datos en tiempo real, para ayudar a las organizaciones a iniciar rápidamente su proyecto de automatización de procesos y luego poder escalarlo fácilmente y de forma ilimitada. ■

Si te ha gustado este artículo,
compártelo



El equipo de Rainbow y Extel CRM somos ahora

ABAI GROUP
YOUR BUSINESS PARTNER

ABAI Group es una compañía de servicios de relación con clientes y externalización de procesos

Para más información sobre nuestras soluciones de gestión omnicanal, Back Office, RPA, Text&Speech Analytics, Chatbot y Big Data consulta nuestra web

www.abaigroup.com



RPA: de necesidad empresarial en confinamiento a ventaja competitiva frente al cambio



VÍCTOR AYLLÓN,
Vicepresidente RPA
Centro de Excelencia
de Appian Corporation

La automatización no es un fenómeno nuevo. Ha estado presente a lo largo de la historia como una oportunidad para generar más valor a partir del equilibrio del paradigma clásico de personas, procesos y tecnología. Sin embargo, no ha sido hasta hace unos años, cuando los “robots software” RPA empiezan a ganar tracción a un ritmo acelerado en el tejido empresarial español, sobre todo, en el sector TIC, Industria, Banca y Utilities. Prueba de ello, son los datos que ofrece IDC. La consultora revela que en España la inversión en automatización de procesos se duplicará hasta 2021.

La capacidad que tiene el RPA de liberar a los trabajadores de tareas de gran volumen, repetitivas y lineales, que requieren un elevado esfuerzo manual, y traspasarlas a una “plantilla digital” de robots software, aportando rapidez

y precisión a los procesos, permite a las organizaciones evolucionar rápidamente hacia un paradigma más productivo, ágil y eficiente. Es por ello que RPA está ganando tracción a un ritmo acelerado, siendo, según la consultora Gartner, la categoría de software empresarial de más rápido crecimiento en los últimos años.

Aun así, en la mayoría de los procesos aún hay tareas “robóticas” que se ejecutan de forma manual y que requieren una elevada dedicación humana, restando recursos a actividades de mayor valor. Según los expertos, el mercado RPA aún tiene mucho margen de crecimiento y un largo recorrido por delante.

COVID-19, CATALIZADOR DEL CAMBIO

Antes del COVID-19, Deloitte vaticinaba que, en 2020, el 72% de las entidades habría empe-

zado a adoptar esta tecnología. Sin embargo, el coronavirus ha acelerado esta tendencia al evidenciar que la automatización robótica de procesos es una necesidad para todas las empresas en pleno confinamiento.

El aislamiento social impuesto como medida para frenar la propagación del virus ha paralizado organizaciones de sectores como el aéreo o el turístico y ha puesto bajo presión a las de sectores como el sanitario o el comercio electrónico, que se han visto obligadas a buscar nuevas fórmulas para continuar operativas al tiempo que protegen la salud de sus trabajadores. En ambos casos, RPA ha permitido dar respuesta a estos desafíos. Para las primeras, la automatización es una forma de reducir costes en un momento de inactividad y para las segundas, una necesidad para escalar su ca-

pacidad operativa. La repentina dispersión de los equipos de trabajo ha dejado claro que los procesos de negocios deben poder ser operados, gestionados y coordinados de forma similar independientemente de dónde se encuentren los trabajadores.

Con este panorama, muchas organizaciones pisan el acelerador para abordar proyectos de automatización. Estamos observando como los directivos precipitan sus inversiones en automatización como consecuencia del COVID-19, principalmente porque, además de los beneficios mencionados, esta tecnología presenta particularidades que hacen factible una adopción generalizada en un momento como el actual. Hablamos de su versatilidad para automatizar procesos muy diferentes, su rápida implementación o su desarrollo, que no interfiera con sistemas corporativos ya implantados.

Hay muchas empresas que están aprovechando la coyuntura para empezar a construir ahora lo que serán los procesos en la época post COVID-19, convencidas de que la automatización robótica de procesos les aportará una ventaja competitiva clave.

La pandemia del COVID-19 ha dejado patente que vivimos un momento repleto de incertidumbres por un virus que se manifiesta y propaga de manera caprichosa y que la relajación de las medidas de confinamiento nos devolverá a una normalidad en la que nada volverá a ser como antes. En este escenario, la única certeza es que

RPA será un valor diferencial para que las compañías estén preparadas para el cambio.

RPA INTELIGENTE Y EN EL CLOUD

Con el objetivo de dar respuesta a un entorno empresarial repleto de interrogantes y rápidamente cambiante, se abordarán despliegues de RPA en el Cloud que, además de proporcionar conectividad a los procesos y dotar de continuidad al negocio, permitirá dimensionar la capacidad de ejecución con rapidez y agilidad en función de las necesidades del mercado. También se le dotará de inteligencia artificial (IA) con el objetivo de identificar, diseñar, medir y administrar procesos automatizados en toda la empresa.

Tradicionalmente y de forma equívoca, se ha pensado que la automatización reemplazaría a los humanos. Superada esta asociación y demostrado que, lejos de eliminar puestos de trabajo, genera nuevas oportunidades laborales- según el World Economic Forum (WEF), las profesiones emergentes resultantes de la automatización podrían representar 6,1 millones de puestos de trabajo entre 2020 y 2022-, la automatización robótica de procesos se convierte en una pieza fundamental en la transformación digital de la empresa.

DEL RPA 1.0 A LA HIPERAUTOMATIZACIÓN

La tecnología RPA muestra sus mayores ventajas y rentabilidad en procesos mecánicos,

basados en reglas, con una entrada y una salida bien definida, aunque no todos los casos de uso pueden ser abordado como proyectos “puros” de RPA. Gartner recientemente ha introducido el término “Hiperautomatización” que es la confluencia de tecnologías RPA, BPM e Inteligencia Artificial para poder ofrecer una automatización de procesos que sea efectiva y que aborde procesos complejos y completos.

En este contexto, RPA desarrolla todo su potencial para proporcionar la adaptabilidad y la resiliencia necesaria para que las organizaciones sean competitivas en una economía globalizada en la que también la capacidad de innovación se “contagia”.

Estamos inmersos en una imparable revolución tecnológica: la forma de operar de las empresas y el papel del trabajador humano está evolucionando rápidamente. Y la actualidad deja claro que, hoy más que nunca, las compañías deben estar preparadas para el cambio. La automatización de procesos, que combina el potencial de RPA con las tecnologías de IA y las capacidades humanas, es un aliado fundamental para enfrentarse a este nuevo escenario. ■

Si te ha gustado este artículo,
compártelo



RPA automatización y agilidad corporativa



Especial
it TRENDS

¡DESCÁRGALO AQUI!



Diálogos itTRENDS



“La inteligencia del espacio de trabajo está ligada a la productividad y a las interrupciones”
(Mar García, Citrix)



“HPE propone IA y alta computación para acelerar la búsqueda de la cura de la COVID-19”
(Fran Yañez, HPE)



“Los atacantes utilizan todo lo que está a su alcance para sofisticar sus ataques, y sabemos que la IA no es una excepción” (José Luis Laguna, Fortinet)



“La monitorización de las funciones serverless es fundamental” (Eusebio Nieva, Check Point)



“El ADC se necesita siempre, la gran diferencia es cuándo y cómo necesito balancearlo”
(Joaquín Gómez, VMware)



“Por cada empleado puede haber hasta 10 cuentas privilegiadas” (Albert Barnwell, CyberArk)

Diálogos **it** **TRENDS**



EVO Banco plasma en una hipoteca digital su filosofía tecnológica

El sector de la banca ha hecho tradicionalmente un uso intensivo de las tecnologías para procesar sus datos, gestionar las transacciones, estudiar los cambios en el mercado, poner la atención en los usuarios y generar nuevos productos como la hipoteca digital de EVO Banco. En IT Trends, hablamos con Javier González, Director de Innovación Digital y Big Data de EVO Banco, sobre las tecnologías que se esconden tras este producto, así como tras la TI corporativa de la entidad.