TELEINFOpress
TI & COMUNICACIONES

USAR VPN YA NO ES SUFICIENTE

P.4 - 5

BITDEFENDER PERFILA EXPANDIR SU CANAL DE LA MANO DE COMOL

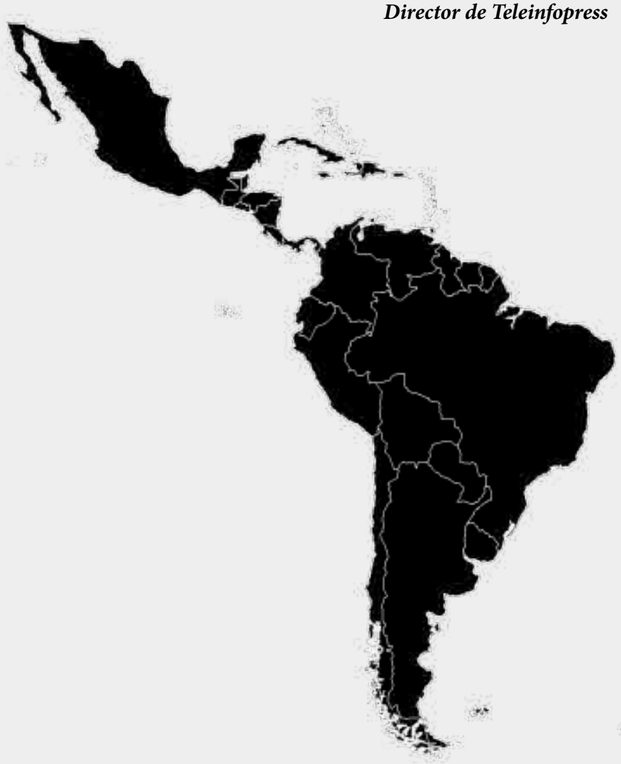
P.6

EN UN NUEVO RETO, SE EXPANDE A BOLIVIA Y PERÚ

P.3

Año 12 / Nº 147 / Noviembre 2021
www.teleinfopress.com

Horacio Romero
Director de Teleinfopress



Director:
Horacio Romero De Lucca
hromero@teleinfopress.com

Directora de Redacción y Edición:
Liliana Almanza A.

Redes Sociales & Página Web:
Miguel Franck

Ventas:
teleinfopress+ventas@telinfopress.com

Prensa:
teleinfopress+prensa@teleinfopress.com

Co-Directora:
Ninoska Azurduy Caso
nazurduy@telinfopress.com

Gerente de Innovación:
Diego Romero A.

Oficina Central:
Santa Cruz, Bolivia
Equipetrol - Sirari
Calle Las Dalias Nº 7 Oeste
Telf. : (591-3) 3429010 - 3429011
Telf. EE.UU: 1-9542828125
teleinfopress@teleinfopress.com
www.teleinfopress.com

Ejemplar de distribución gratuito a nivel nacional a: marcas, mayoristas y canales de distribución del sector de TI y comunicaciones. Además de CEOS, CIOS y Encargados de Adquisisiones de las principales empresas, instituciones y sector gubernamental.

ÍNDICE

Este noviembre XMS compartió la gran noticia de su expansión hacia LATAM con el inicio de sus operaciones en Perú y Bolivia. Lo que le significó a la empresa, ser reiterada una vez más como partner Gold de Microsoft. Emprender este nuevo desafío, llena de orgullo y optimismo a XMS, segura de cumplir con cada expectativa acerca de lo que les depara ingresar a estos dos nuevos mercados.

Para XMS, es un orgullo reconocer que los esfuerzos de su gente son el motor principal de crecimiento que, sumado al compromiso de su equipo directivo, le permite afrontar los desafíos con mayor confianza y la seguridad necesaria para continuar cosechando éxitos.

La demanda y el desafío tecnológico que enfrentan las empresas abre fronteras en Latinoamérica, y Bolivia y Perú no son la excepción.

Es en este nuevo horizonte, en el que las empresas deciden dar un paso adelante para continuar funcionando, abrazando de una vez por todas aquel cambio que siempre se veía "a futuro" para convertirlo en un presente tangible y capaz de mantener a flote las operaciones y objetivos de negocios, la demanda de tecnología requiere una pronta solución.

Milton Díaz, e**n su nuevo rol como Director de Ventas para ambos países**, expresó en entrevista exclusiva a TeleinfoPress: *"América Latina es un mercado de mucho potencial, las compañías en todos los rubros están dispuestas a asumir el reto de dar respuesta ante la creciente demanda tecnológica, innovando y compitiendo para mejorar su rentabilidad, y para esto es indispensable aplicar soluciones de transformación digital y el uso correcto de la tecnología. En este escenario, pienso que XMS tiene muchas oportunidades y mucho potencial de agregar valor al mercado en Latam, con soluciones y servicios que ayudarán a las empresas a implementar sus agendas tecnológicas".*

Ante los objetivos planteados frente a este nuevo desafío, Miltón Díaz resaltó: *"Los objetivos que nos planteamos en primer lugar son el consolidar nuestra presencia en Perú, Bolivia y México; implementar y definir nuestras capacidades de atención y ejecución en estos mercados y definir un roadmap claro de nuestra visión como compañía hasta 2024, esto nos permitirá atender correctamente y exitosamente el mercado de Latam. Actualmente está en ejecución nuestra expansión en Bolivia, Perú y México y pensamos pasar a la fase 2 incorporando Ecuador y Colombia. Por supuesto que debemos construir nuestro centro de atención a clientes de forma regional en términos de delivery de servicios, marketing y operaciones".*

¿Cuáles son las expectativas que tienes en relación al crecimiento en Latam?

Las expectativas sin duda es llegar a ser líder y referente tecnológico en los mercados que pensamos operar en un corto tiempo. Aquí es importante la alianza estratégica con Microsoft que nos permitirá apalancar más rápida y eficientemente nuestro crecimiento en la región.

¿Qué valor agrega XMS en Latam a través de esta expansión?

Sin duda el aporte más importante de esta expansión, es agregar a Latam innovación, experiencia de nuestra gente, alto nivel de calidad en los proyectos que impactarán en una exitosa implementación de las agendas de transformación digital de las empresas en la región.

"Post-pandemia, el conocimiento especializado remoto ahora es tan valioso como la cercanía física, ha habilitado a las empresas a poder buscar los mejores especialistas, es el caso de XMS, una empresa chilena con más de 10 años de experiencia trabajando de la mano con ***Microsoft como Partner Gold,*** *que hoy se propone el desafío de ofrecer soluciones de negocios basadas en productos Microsoft y productos a la medida para satisfacer la necesidad las empresas de contar con especialistas para la correcta adopción de plataformas cloud"* acotó y finalizó Milton Díaz.

Es momento de decir adiós a las VPNs. Las ventajas del Acceso a la Red de Confianza Cero (ZTNA) destacan ante el actual modelo de trabajo remoto, debido a que muchas personas acceden a recursos y aplicaciones críticas desde fuera del perímetro de la red. Los expertos en seguridad, promueven la necesidad de cambiar el paradigma de una red abierta y desarrollada en torno a la confianza inherente a un modelo de confianza cero para conectar de forma segura.

USAR VPN YA NO ES SUFICIENTE

El reciente aumento del trabajo remoto, sacó a la superficie las limitaciones de las redes privadas virtuales (VPNs), aunque las VPNs tradicionales fueron un pilar durante décadas. Hoy las organizaciones buscan alternativas que cumplan mejor con sus planes y con sus objetivos.

Los beneficios de contar con una mayor seguridad, control más granular y mejor experiencia del usuario, a través del acceso a la red de confianza cero (ZTNA), sin duda se presenta como la opción más inteligente para conectar de forma segura la fuerza de trabajo remoto a partir del Home Office en todo el mundo, y más aún en un país como el nuestro.

Durante décadas las VPNs fueron el método de facto para acceder a las redes corporativas, sin embargo, tienen algunos problemas serios, particularmente en términos de **seguridad. Para contar con información precisa sobre este tema primordial ante la imparable evolución de amenazas por la red, entrevistamos a** Esteban Glitman, Gerente Comercial Regional **de** DACAS **y a** Mario Barbosa, Canales Commercial para el Cluster de Bolivia, Venezuela, Paraguay y Uruguay de Fortinet.

Inconvenientes importantes de las VPNs:

Una VPN puede parecer la solución perfecta para muchos de los problemas de privacidad en línea. Como experto referente en seguridad del tema Esteban Glitman nos detalla los tres inconvenientes al confiar en una VPN tradicional para proteger a los trabajadores remotos y las oficinas en casa:

1. Una VPN adopta un enfoque para la seguridad basado en el perímetro.
Los usuarios se conectan a través del cliente VPN, no obstante, una vez dentro del perímetro, con frecuencia tienen amplio acceso a la red, lo cual la expone a amenazas. Cada vez que se confía automáticamente en un dispos

2. Las VPNs no tienen información sobre el contenido que ofrecen.

Las VPNs se utilizan para el acceso remoto cuando se trabaja desde hoteles, cafeterías o desde casa. Debido a que la mayoría de las oficinas en casa se conectan a redes domésticas en su mayoría no seguras, se convirtieron en uno de los objetivos principales para los cibercriminales que buscan un punto de acceso a la red que se pueda aprovechar fácilmente. Debido a que ya no se ocultan detrás de soluciones de seguridad de grado empresarial, se convierten en objetivos más fáciles para las tácticas de ingeniería social y el malware. Las VPNs pueden convertirse en conductos para que el malware regrese a la red.

3. Las redes ahora están muy distribuidas.

Los recursos y aplicaciones críticos actualmente se distribuyen en centros de datos, sucursales distribuidas y oficinas en casa, así como en entornos de múltiples nubes. La mayoría de las soluciones de VPN no se diseñaron para manejar este nivel de complejidad. Una sola conexión VPN fuerza el backhauling de todo el tráfico a través de un concentrador central para su inspección, lo cual consume muchos recursos y provoca retrasos. El túnel dividido puede solucionar esto, pero crea su propio conjunto de desafíos, ya que el tráfico se dirige directamente a Internet sin pasar por un firewall.

Entendiendo los 3 inconvenientes descritos por Esteban Glitman, **pedimos a** Mario Barbosa**, como Regional Canales Commercial de la marca referente en ciberseguridad** Fortinet, **nos pueda proveer información sobre la solución alternativa ZTNA, propuesta como una mejor opción:**

A diferencia del enfoque tradicional basado en la VPN, que supone que se puede confiar en cualquier persona o cualquier cosa que pase los controles del perímetro de la red, el modelo de confianza cero adopta el enfoque opuesto: no se puede confiar en que algún usuario o dispositivo acceda a nada hasta que se demuestre lo contrario.

Incluso si se le otorga a un usuario permiso para acceder a un área de la red o una aplicación, esto no supone que el usuario sea de confianza en otras áreas. Para implementar una estrategia integral de confianza cero en un entorno muy distribuido, los administradores de la red deben controlar quién puede acceder a qué aplicaciones sin importar dónde se encuentren esos usuarios o aplicaciones. Este enfoque de “privilegios mínimos” requiere controles de acceso rigurosos que abarquen la red distribuida para que los dispositivos, los usuarios, el endpoint, la nube, el software como servicio (SaaS) y la infraestructura estén protegidos.

Cinco ventajas de ZTNA:
Afortunadamente, existen soluciones que permiten a las organizaciones implementar una estrategia efectiva de confianza cero sin tener que hacer una gran renovación de la red. Las soluciones de ZTNA ofrecen múltiples ventajas sobre las VPNs.

1. Las organizaciones pueden extender el modelo de confianza cero más allá de la red. A diferencia de una VPN, la cual se enfoca exclusivamente en la capa de la red, ZTNA escala una capa para proporcionar seguridad de manera efectiva a las aplicaciones independientemente de la red.

2. ZTNA funciona de forma transparente en segundo plano, lo cual mejora la experiencia del usuario. Un usuario hace clic en la aplicación que desea y, detrás de escena, el agente cliente hace todo el trabajo. Se hacen conexiones seguras y se aplican los protocolos de seguridad y la inspección para garantizar una experiencia óptima. A diferencia del uso de una VPN, los usuarios no tienen que preocuparse por configurar una conexión ni por la ubicación de una aplicación.

3. Cada usuario y dispositivo se verifica y se valida antes de que se le otorgue acceso a una aplicación o recurso. Este proceso incluye una revisión de postura que verifica que el endpoint ejecute el firmware correcto y un programa de protección del endpoint que verifica que sea seguro conectarse a la aplicación. La verificación es granular, por sesión con la misma
política de acceso, ya sea que un usuario acceda a recursos locales, ubicados en una nube virtual o en una nube pública. La misma política también controla quién puede acceder a esa aplicación con base en el perfil del usuario y del dispositivo que se autentican.

Contando con información precisa que ayudará a las empresas y a usuarios a entender las necesidades que exige la seguridad de los datos, lograr una mayor seguridad, control más granular y mejor experiencia del usuario, a través del acceso a la red de confianza cero (ZTNA), Esteban Glitman **explica la mejor forma de contar con un acceso remoto más seguro.**

Mejor acceso remoto: 4. Debido a que ZTNA se enfoca en el acceso a las aplicaciones, no importa en qué red se encuentre el usuario.
Simplemente ofrece conexiones automáticas seguras a las aplicaciones, sin importar dónde pueda estar el usuario mediante la verificación de la postura del usuario y del dispositivo para cada sesión de la aplicación, incluso cuando los usuarios están en la oficina.

5. ZTNA reduce la superficie de ataque al ocultar a Internet las aplicaciones críticas para el negocio. La conexión segura se realiza sin dificultades con solo hacer clic en la aplicación. Una conexión segura se establece sin tener que exponer públicamente el enlace de la aplicación.

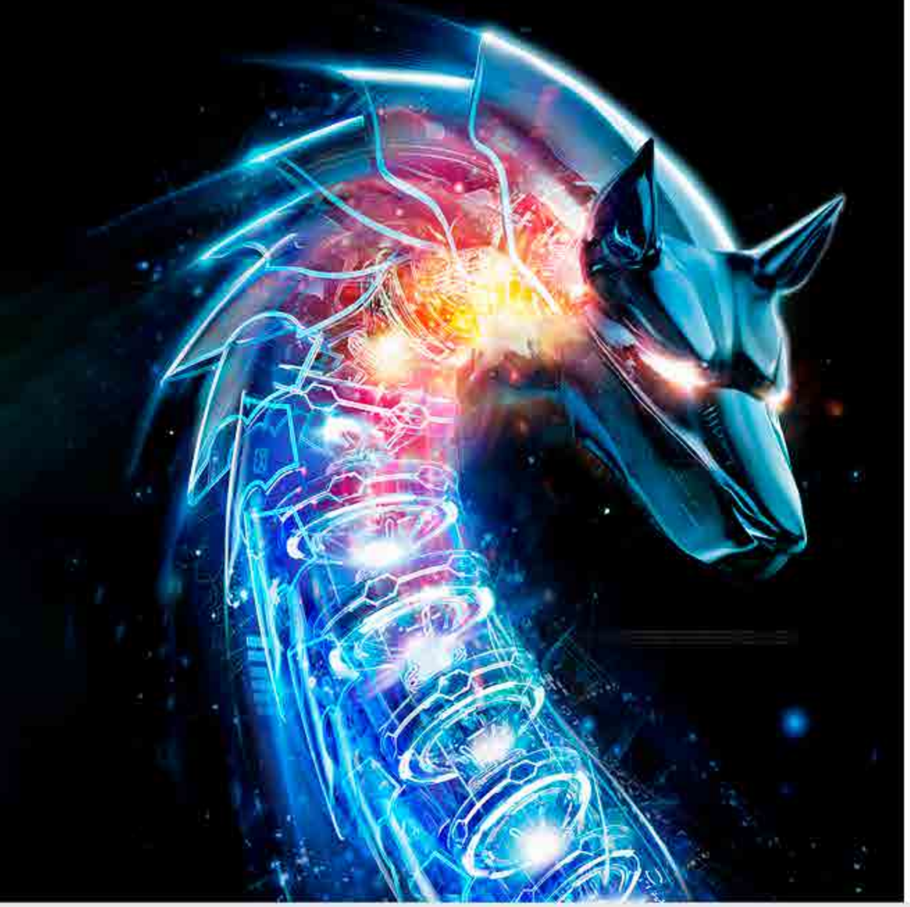
Contando con información precisa que ayudará a las empresas y a usuarios a entender las necesidades que exige la seguridad de los datos, lograr una mayor seguridad, control más granular y mejor experiencia del usuario, a través del acceso a la red de confianza cero (ZTNA), Esteban Glitman **explica la mejor forma de contar con un acceso remoto más seguro.**

Mejor acceso remoto:
Cada vez son más las organizaciones que reconocen la necesidad de dejar de utilizar las VPNs tradicionales. ZTNA está demostrando ser una mejor solución, más fácil de utilizar, con el beneficio extra de que se agrega seguridad de aplicaciones a una solución de acceso remoto. Las organizaciones deben tener el cuidado de seleccionar soluciones ZTNA que se integren con su infraestructura existente. El desarrollo de una solución de acceso a la red de confianza cero requiere una diversidad de componentes, que pueden incluir un cliente, un proxy, autenticación y seguridad, los cuales se podrían utilizar para aplicar ZTNA a usuarios remotos, sin importar dónde estén.

Para mayor información:
consultas@dacas.com
- www.dacas.com

BITDEFENDER PERFILA EXPANDIR SU CANAL DE LA MANO DE COMOL

La estratégia desde COMOL, Mayorista de Bitdefender en Bolivia, permitirá al Canal de Venta de la marca vender sus soluciones y servicios avanzados de ciberseguridad para la prevención, detección y respuesta de amenazas. Presenta una arquitectura multinivel con beneficios crecientes a medida que los partners realizan mayores ventas, proporcionando distintos niveles de acceso a fondos de marketing, servicios de soporte comercial y asistencia técnica.



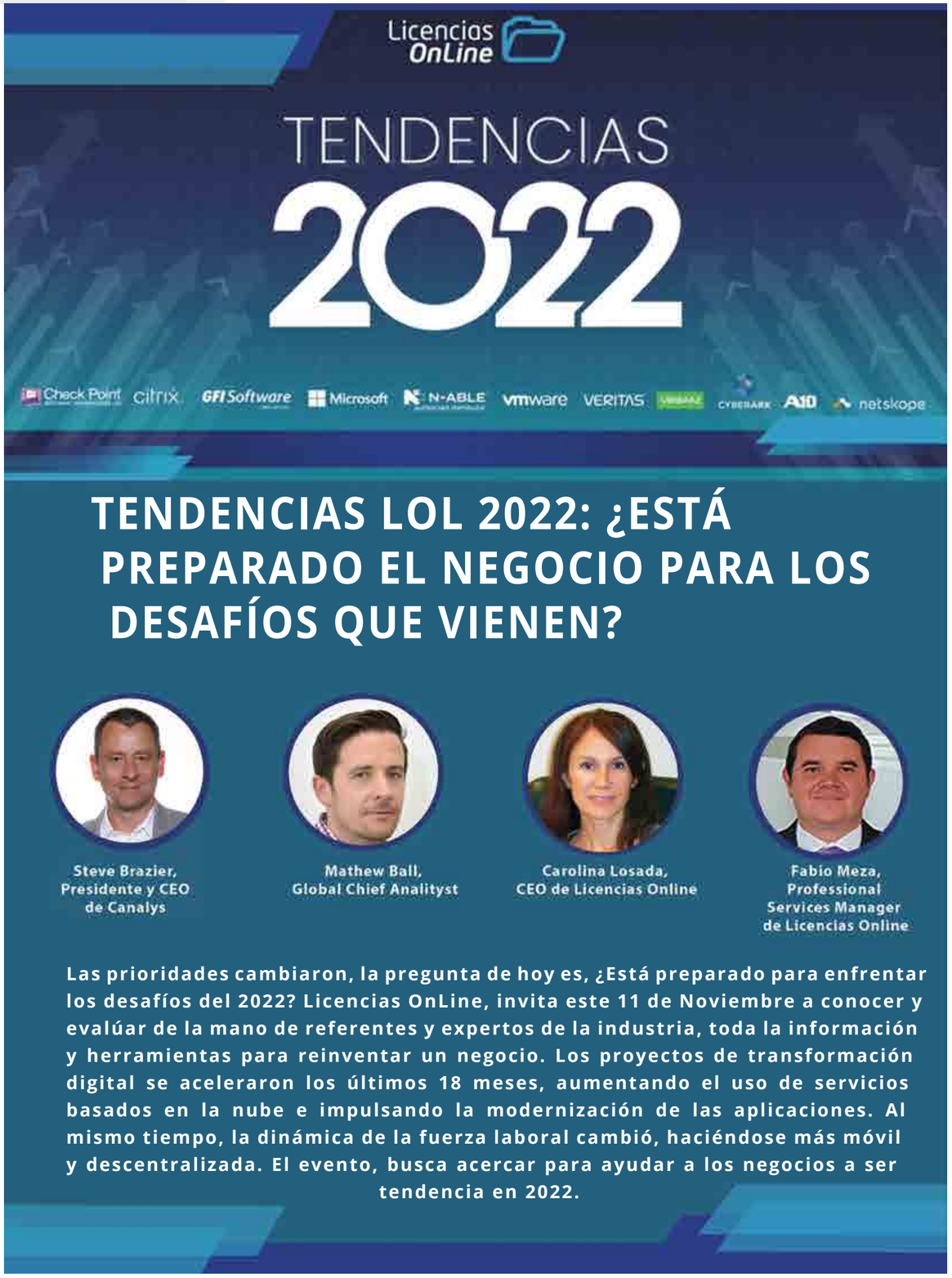
Bitdefender, reconoce el potencial de la industria tecnológica boliviana y busca expandir su Canal de Venta en el país a través del mayorista COMOL SRL., poniendo foco en su estrategia de canales locales.

"Hoy, mi principal objetivo es ampliar la red del Canal de Venta de Bitdefender, identificar a los mejores partners y por supuesto potenciar la relación con este canal, con el fin de mejorar el posicionamiento y consolidación de la marca en el mercado de Bolivia. Y para alcanzar esto, me apoyaré en la estratégia de optimizar las oportunidades de negocio de los socios y hacer que Bitdefender se posicione como la mejor solución de seguridad informática más innovadora que predice, previene, detecta y repara incluso las amenazas digitales más recientes" indicó Rene Molina, Gerente General en COMOL SRL.

Bitdefender, contra el ransomware y el malware

A pesar del tiempo online que demanda la actual realidad y que nos expone a numerosos ataques informáticos, la protección de varias capas de Bitdefender mantiene los documentos, imágenes y vídeos a salvo de todas las amenazas conocidas y emergentes, incluidos el ransomware y el malware utilizando inteligencia artificial avanzada y otras tecnologías revolucionarias para anticipar, detectar y bloquear instantáneamente las amenazas, antes de que estas puedan causar daños a su valiosa información.

Bitdefender ha tenido la mejor tasa de detección del sector durante los últimos cinco años. Prueba de ello, es que cientos de millones de sistemas ejecutan el software de seguridad de Bitdefender en todo el mundo.



Licencias Online llevará a cabo un evento con foco en Partners y empresas usuarias de tecnología con el objetivo de compartir un anticipo de lo que será el mercado IT de cara al próximo año.

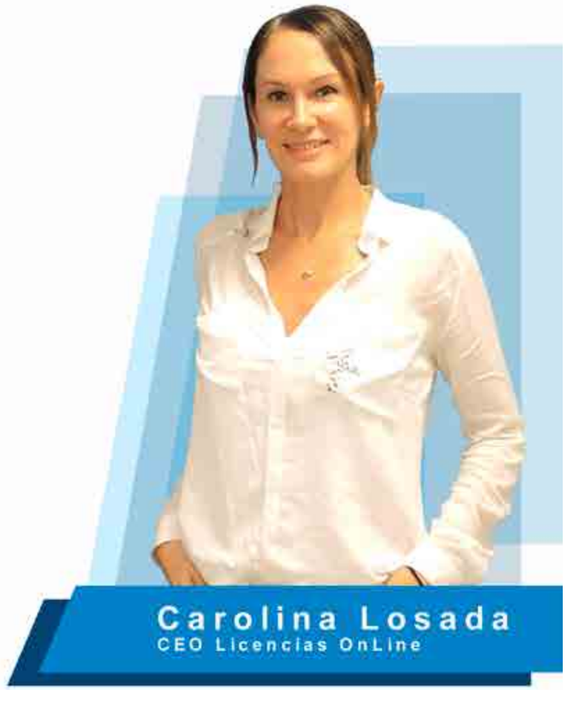
La nueva normalidad ha impuesto desafíos a los que los usuarios y empresas han tenido que enfrentar. **Los proyectos de transformación digital se aceleraron durante los últimos 18 meses, aumentando el uso de servicios basados en la nube e impulsando la modernización de las aplicaciones.** Al mismo tiempo, la dinámica de la fuerza laboral cambió, haciéndose más móvil y descentralizada.

Para abordar estos retos el mayorista de valor agregado invita a participar de **un evento exclusivo online el próximo jueves 11 de noviembre, liderado por expertos de la industria, quienes brindarán toda la información y las herramientas necesarias potenciar el negocio en el 2022.**

"Todos los años **nos proponemos dar contenido de valor a nuestros partners y a sus usuarios finales para apoyarlos en**

Carolina Losada

los desafíos que se les presenten durante el año. *En esta ocasión, dado el contexto actual de alta transformación digital, decidimos adelantarnos para mostrar las oportunidades que se presentarán en 2022 a partir de lo que conlleva la adaptación a convivir con la pandemia de forma más controlada"*, manifiesta ***Carolina Losada, CEO de*** Licencias OnLine. ***"Nos acompañarán referentes globales de la industria como Steve Brazier, CEO de Canalys, y su equipo de analistas que nos van a contar qué oportunidades ven en Latinoamérica para el año próximo*** *producto de la aceleración en la adopción de tecnología del último año y medio".*



"*Creemos que va a ser un evento muy interesante para el mercado", sigue la vocera. "Por un lado,* Martina Rúa, *periodista y escritora que llevará adelante el evento, nos dará su visión del rol de la innovación durante la transformación digital de las empresas. Además, junto al apoyo de Canalys* ***tendremos una perspectiva de lo que se viene en el mercado basado en los pilares de Infraestructura, Cloud y Seguridad, y el impacto que la tendencia de trabajo híbrido tendrá en la adopción de tecnología en las empresas como de los usuarios".***

Tendencias LOL 2022 Se abordarán temas como: la innovación en el mercado TI; tendencias y oportunidades del mercado para 2022; desafíos del trabajo híbrido en empresas y usuario final. Además, habrá un espacio de preguntas y la posibilidad de interactuar con los líderes presentes.

Tendencias LOL 2022 contará con la participación de **Steve Brazier**, **Presidente y CEO de** Canalys; Mathew Ball, **Global Chief Analityst Canalys**; Carolina Losada, **CEO de** Licencias Online; y Fabio Meza, **Professional Services Manager de Licencias Online.**

VMware se separa oficialmente de Dell Technologies, la compañía de software de virtualización y gestión de entornos “cloud” vuelve a ser una empresa independiente. VMware, pasó a formar parte de Dell cuando esta compró EMC en 2016. Ahora, como dos empresas oficialmente separadas, se espera que tanto VMware como Dell Technologies puedan beneficiarse de una mayor capitalización bursátil y que reciban el apoyo de los inversores, que hará que ambas puedan trabajar con nuevos clientes y expandir sus tecnologías, mientras siguen manteniendo lazos muy cercanos entre ellas.

FINALMENTE VMWARE Y DELL SE INDEPENDIZAN

Después de que el 14 de abril de 2021, Dell y VMware anunciaran en una carta abierta a clientes y socios, que llegaron a un acuerdo por el que la segunda volvería a ser una compañía independiente a finales de este año, finalmente se confirma su separación, VMware y Dell son ya oficialmente dos empresas independientes.

La escisión también tiene impactos financieros, ya que Dell Technologies se deshará del 81% de las acciones que tiene de VMware, que cotiza en bolsa. De esta manera nacerá una empresa de software independiente de Dell con un valor de mercado cercano a los 64.000 millones de dólares. Las operaciones de hardware de Dell, con las que se queda, tienen un valor de alrededor de 33.000 millones de dólares, según el último precio que tenían sus títulos.

Aproximadamente dos tercios de los ingresos de VMware salen todavía de las divisiones de software más tradicionales de la compañía, esto es, servicios de mantenimiento y licencias. Pero la compañía está dando pasos firmes hacia un modelo de negocio basado en la nube, y espera que para finales de su año fiscal que termina en enero de 2025, el 40% del total de sus ingresos venga de suscripciones.

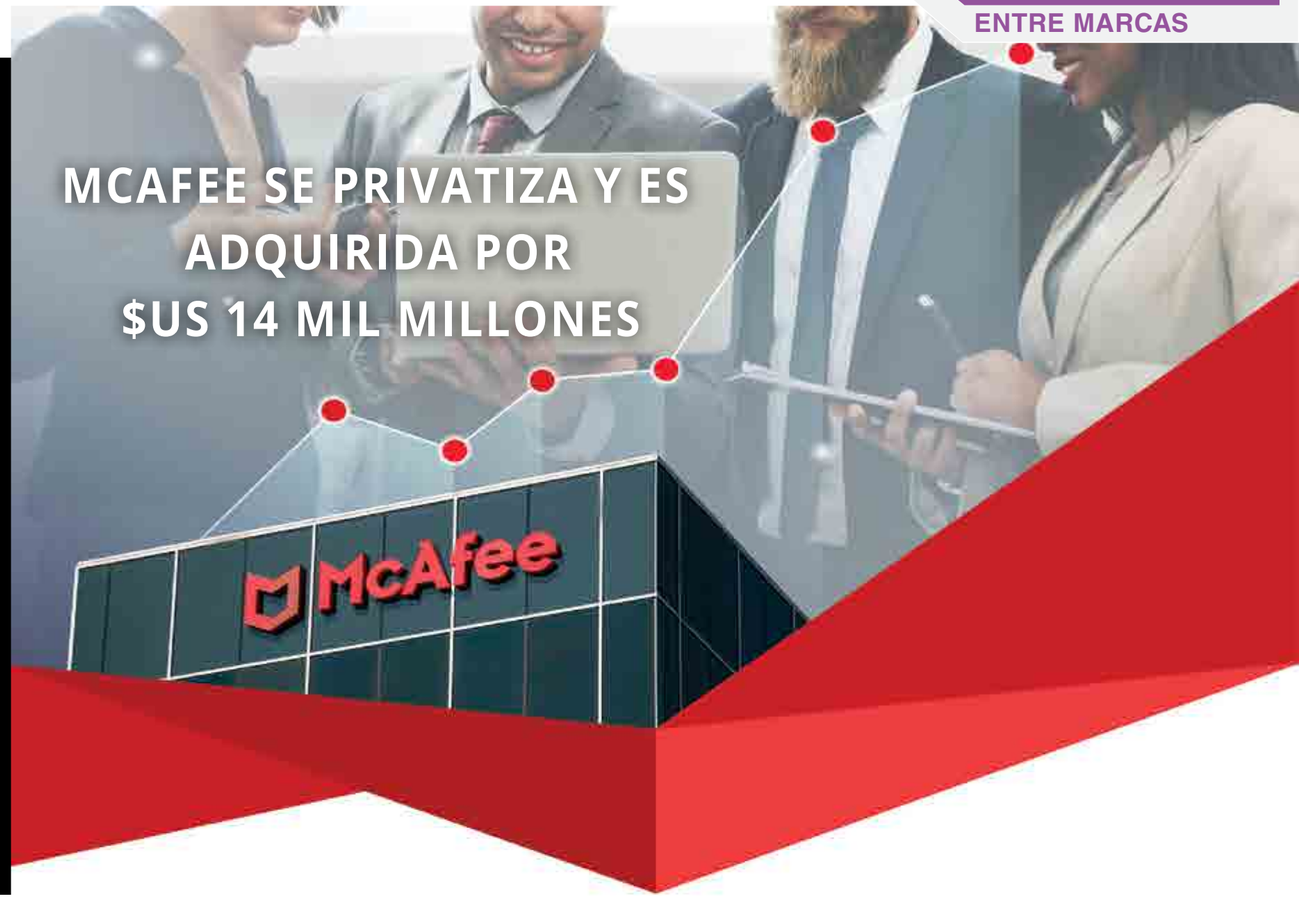
Ambas compañías esperan que la división en dos empresas independientes dará a ambas la flexibilidad financiera suficiente para avanzar mientras sigue creciendo su colaboración de desarrollo de negocio, que es muy estrecha. Eso incluye servicios como **VMware Cloud en Dell EMC**, que combina la integración del software de red, así como la computación y almacenamiento de VMware, con la Infraestructura hiperconvergente (HCI) de Dell.

Por otro lado, todo apunta a que ambas empresas seguirán trabajando juntas en diversos sectores, como el edge, las telecomunicaciones y el 5G. Además cuentan con un compromiso para seguir impulsando los ingresos de VMware a través del canal de ventas de Dell, así como de que VMware siga ofreciendo los Servicios financieros de Dell.

El CEO de VMware, **Raghu Raghuram**, también expuso una opinión, la empresa será más flexible para asociarse de manera más profunda con proveedores cloud y en local, además de contar con *“más flexibilidad para usar acciones para completar compras futuras, lo que los ayudará a seguir siendo competitivos. El paso de hoy reforzará nuestra misión para ser la Suiza del sector cloud, con un posicionamiento único para proporcionar a nuestros clientes la mejor combinación de opciones a medida que hacemos crecer nuestro robusto ecosistema de partners”.*

Michael Dell, que además de ser el Presidente y CEO de Dell seguirá formando parte de la Junta Directiva de VMware, ha manifestado que *“hoy se da un paso importante para Dell Y para VMware. Desbloqueamos un valor significativo para los accionistas, al mismo tiempo que se mantiene nuestro sólido acuerdo en ventas, soporte e innovación para nuestros clientes. Avanzamos a toda velocidad, solucionando los problemas de los clientes, impulsando el progreso y capturando oportunidades en sectores como el multicloud, el edge y las telecomunicaciones”.*

VMware ha distribuido también un dividendo especial en metálico de 11.500 millones de dólares a todos los accionistas de VMware. Entre ellos está Dell Technologies, que ha recibido 9.300 millones, y que utilizará los fondos recibidos para reducir deuda.



MCAFEE SE PRIVATIZA Y ES ADQUIRIDA POR $US 14 MIL MILLONES

McAfee alcanza un acuerdo de privatización de 14.000 millones de dólares con un grupo de inversores que incluye a Advent International Corp. y a Permira Advisers y Crosspoint Capital Partners, privatizándola y apoyando el desarrollo e incremento de nuevas medidas de ciber seguridad enfocadas al consumidor. La compañía indicó que se espera que el acuerdo anunciado el lunes 8 de noviembre, concluya el cierre en la primera mitad de 2022.

La empresa de software de seguridad **McAfee,** será adquirida por un grupo de inversores internacionales en **14 millones de dólares**. Según anuncio la marca, en el acuerdo se acordó pagar 26 dólares en efectivo por cada acción. Como empresa privada, siguiendo el objetivo de este grupo de inversores, la compañía será enfocada puramente a los consumidores.

Recordemos que en 1987, **John McAfee** fundo la compañía dándose a conocer por su software antivirus informático. El fundador, dejó a McAfee en 1994, siendo adquirida por **Intel** en 2010 por $ 7,68 mil millones. En 2014, Intel anunció que gradualmente McAfee sería eliminada y absorbida por Intel, siendo renombrada como “Intel Security”.

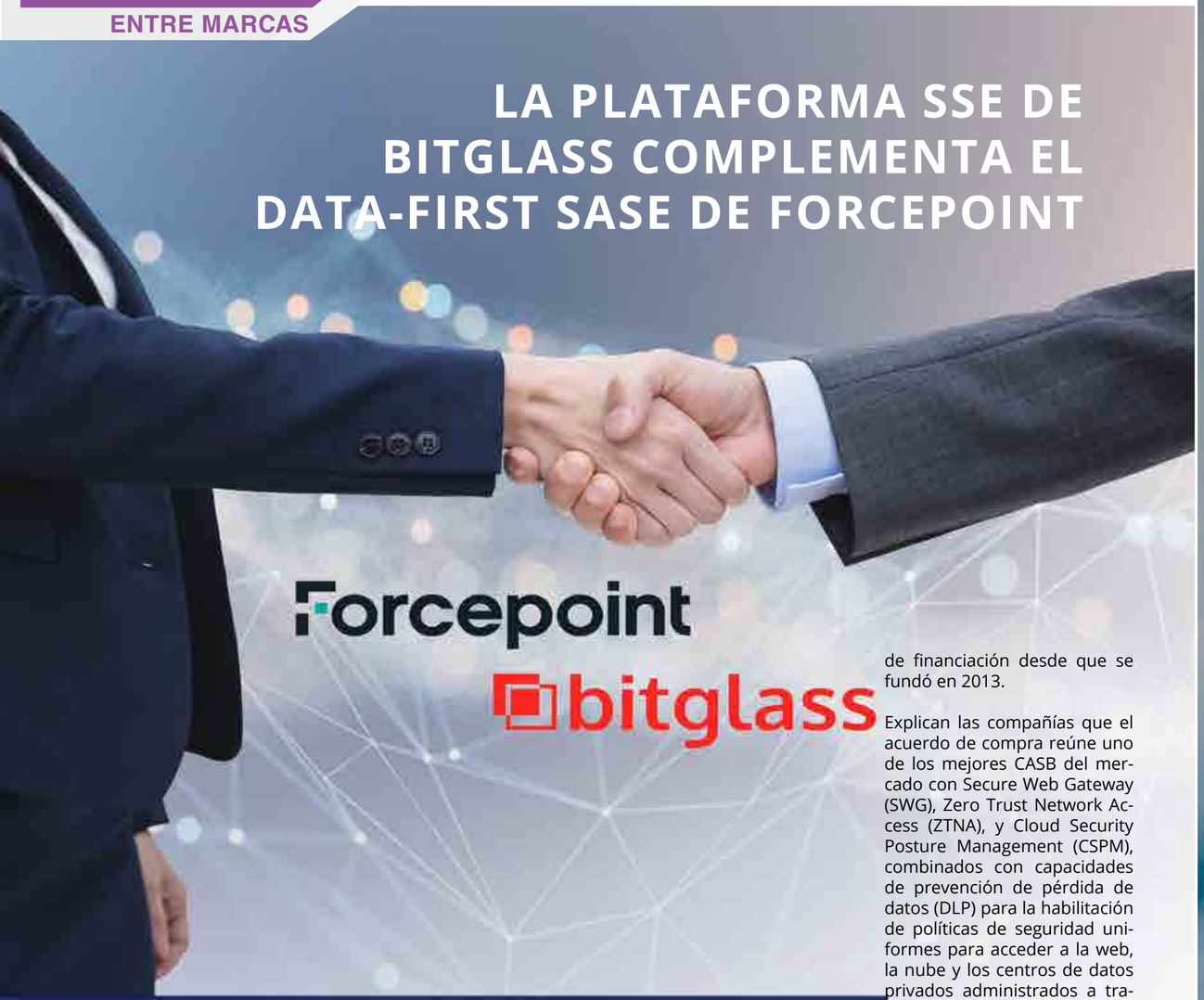
En esta nueva adquisición, Advent International Corporation, junto a otros como **Permira**, Crosspoint Capital, **CPP, GIC** y una **subsidiaria de la Autoridad de Inversiones de Abu Dhab**i (ADIA), es el grupo inversor que marcará el nuevo rumbo de McAfee al privatizarla, por lo que contara con un importante aporte de recursos financieros y operativos con el que busca mejorar aún más su oferta para el consumidor y acrecentar soluciones para la gran demanda de los consumidores de servicios de protección digital.

“Estamos encantados de contar con el apoyo de empresas de primer nivel, con verdadero conocimiento del panorama de la ciberseguridad y tienen un historial probado de éxito”, indicó Peter Leav, P**residente y CEO de McAfee.**

“Esta transacción es un testimonio del liderazgo de McAfee en soluciones de protección en línea y de nuestros talentosos empleados, clientes y socios destacados” adjuntó Leav. *“Estamos muy agradecidos con nuestros empleados por su arduo y continuo trabajo y su compromiso con nosotros”* recalcó.

Esta operación llega el momento adecuado, cuando los **ataques cibernéticos** se han incrementado y por consiguiente existe una mayor demanda de soluciones de seguridad para proteger las nuevas infraestructuras de trabajo remoto impulsadas por la pandemia.

LA PLATAFORMA SSE DE BITGLASS COMPLEMENTA EL DATA-FIRST SASE DE FORCEPOINT



Forcepoint compra Bitglass y refuerza su propuesta SASE. Forcepoint utilizará la plataforma SSE de Bitglass para complementar su arquitectura SASE que prioriza los datos para acelerar sus esfuerzos y lograr que las tecnologías avanzadas de protección contra amenazas y seguridad de datos sean más fáciles de implementar para las organizaciones.

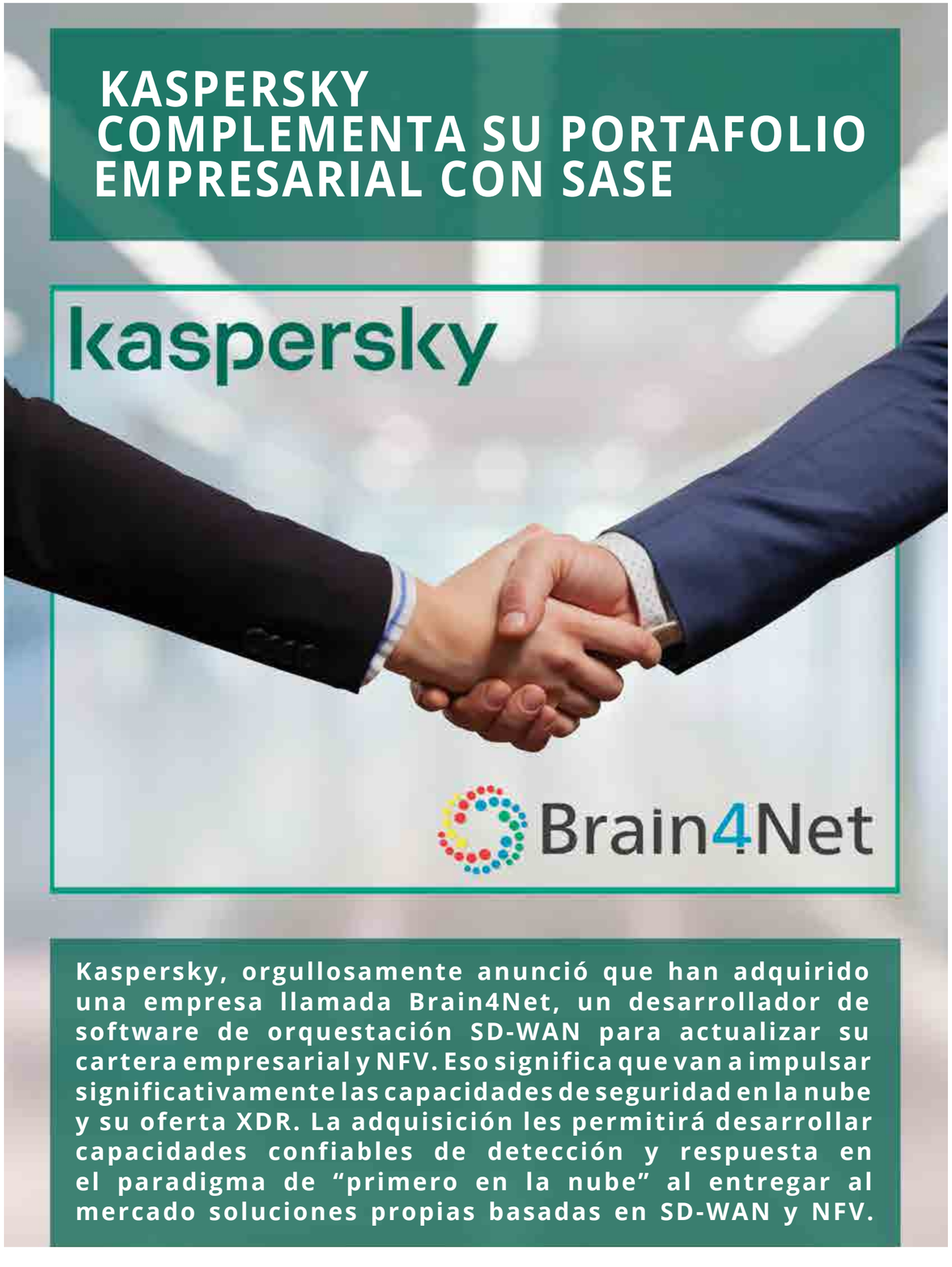
Dos empresas nacidas bajo el impulso del CASB consiguieron mantenerse independientes, y ambas han apostado por convertirse en líderes de **SASE (Secure Access Service Edge)**. Una de ellas es Netskope, y la otra Bitglass, ambas en el impulso de aprovechar al máximo los hiperescaladores modernos que van más allá de simplemente ser accesible en Internet, ampliarse para manejar cargas crecientes y proporcionar la resistencia que los clientes necesitan para garantizar un acceso permanente a las aplicaciones y los datos.

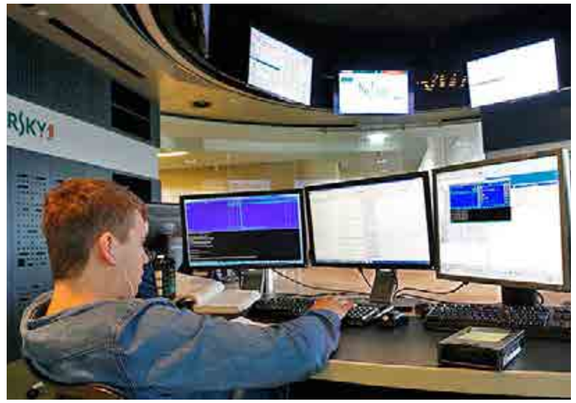
Forcepoint, acaba de firmar un acuerdo definitivo para adquirir Bitglass. Empresa que ofrece la una plataforma SSE integrada y nativa de la nube del sector para asegurar el acceso a y el uso de información, a medida que las organizaciones migran la nube. Los detalles financieros del acuerdo no se han dado a conocer aún, pero debe tenerse en cuenta que Bitglass ha recaudado 150 millones de dólares en 4 rondas de financiación desde que se fundó en 2013.

Explican las compañías que el acuerdo de compra reúne uno de los mejores CASB del mercado con Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), y Cloud Security Posture Management (CSPM), combinados con capacidades de prevención de pérdida de datos (DLP) para la habilitación de políticas de seguridad uniformes para acceder a la web, la nube y los centros de datos privados administrados a través de una única consola.

La plataforma SSE de Bitglass complementa la arquitectura SASE Data-first de Forcepoint y "acelerará los esfuerzos de esta última para hacer que la seguridad de datos avanzada y las tecnologías de protección contra amenazas sean más fáciles de implementar y usar para las organizaciones".

La de Bitglass es la tercera adquisición de Forcepoint este año después de la de Deep Secure en junio y Cyberinc en mayo. Esta oleada de compras se produce después de que Raytheon vendiera Forcepoint a la firma de capital privado Francisco Partners por 1.100 millones de dólares.





Para comenzar, hablemos sobre el fortalecimiento de la cartera de soluciones de **Kaspersky** con las capacidades de Secure Access Service Edge.

En el mercado desde 2015, Brain4Net pasó seis años desarrollando soluciones para la automatización de TI y construyendo redes definidas por software. Ahora, el equipo pasa a ser parte de Kaspersky para crear una solución convincente de Secure Access Service Edge (SASE), agregando experiencia y desarrollos que ayudarán a crear una plataforma unificada al agregar una capa de seguridad de red a las experiencias en seguridad de esta clase. El uso de un único lago de datos y una única herramienta de investigación en los datos de ´endpoint, nube y red` acelera significativamente las operaciones de los equipos de seguridad en la detección y respuesta de amenazas.

Kaspersky presentara su oferta SASE

En resumen, con la adquisición de Brain4Net, Kaspersky pretende llevar al mercado una oferta SASE completamente nueva que combina las soluciones y tecnologías de seguridad de Kaspersky con las capacidades y experiencia en orquestación y control de redes de Brain4Net. Y gracias a este movimiento estratégico, ofrecerán a clientes corporativos tanto servicios de seguridad como de conectividad.

La arquitectura de TI distribuida es la nueva normalidad

Una infraestructura de TI empresarial típica, solía incluir la sede con un centro de datos central, así como sucursales que dirigían todo su tráfico a través de la sede. Con el tiempo, las empresas comenzaron a migrar su infraestructura a la nube. Sin embargo, desde que comenzó la pandemia de COVID-19, la velocidad de la migración se ha disparado y la tendencia de trabajar desde cualquier lugar está haciendo que los enfoques tradicionales de la infraestructura de TI sean prácticamente obsoletos.

Una forma de reducir los gastos y optimizar las operaciones de TI distribuidas es adoptar tecnologías de red de área amplia definida por software (SD-WAN). El uso de una SD-WAN, permite la construcción de redes de área amplia (WAN) sobre los principios de las redes definidas por software (SDN). Las soluciones SD-WAN permiten el enrutamiento del tráfico a través de varias partes de las redes corporativas de manera eficiente al tiempo que brindan un único punto para la administración y el monitoreo, que crean superposiciones virtuales utilizando todo tipo de redes existentes (basadas en MPLS, banda ancha de Internet, LTE, 5G o similar), y son menos costosas y más fáciles de implementar y administrar que las WAN tradicionales basadas en MPLS. En el lado de la TI, SD-WAN, brinda alto rendimiento, visibilidad y agilidad de la red corporativa, y también reduce los costos de mantenimiento.

Más en concreto, la futura oferta SASE prevé incluir Agente de Seguridad para el Acceso a la Nube (CASB), pasarela web segura en la nube (SWG), Plataforma de protección de cargas de trabajo en la nube (CWPP), gestión de la postura de seguridad en la nube (CSPM), acceso a la red Zero Trust (ZTNA), entre otros servicios.

En las ventajas de contar con su propia SD-WAN, el cambio llevará a Kaspersky a un nuevo territorio que agudiza su objetivo de convertirse en un proveedor único de seguridad empresarial tanto para terminales como para redes.

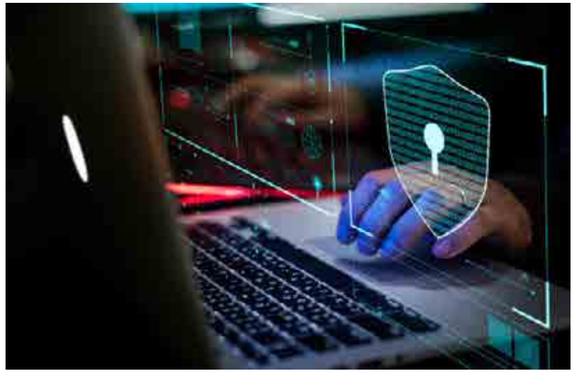
En un ecosistema para la seguridad corporativa

ecosistema de seguridad corporativa

Todos estos componentes formarán parte de un ecosistema único, que responde a la visión de Kaspersky sobre el futuro de la ciberseguridad corporativa. El elemento central de este ecosistema es Kaspersky Open Single Management Platform. Se convertirá en una única plataforma tecnológica cloud nativa para construir Kaspersky XDR y utilizará una arquitectura de despliegue agnóstica. De este modo, la plataforma podrá utilizarse en la nube pública, la nube privada o incluso en modelos on-premise.

“Estamos encantados de unir fuerzas con el equipo de Brain4Net, que ya ha construido tecnologías y servicios maduros mundialmente reconocidos para la orquestación y el control de la red. Estoy seguro de que sus conocimientos y experiencia, combinados con las tecnologías de seguridad más premiadas de Kaspersky y su reconocida experiencia en materia de amenazas, encajarán perfectamente con nuestra visión de la seguridad corporativa, mientras que las nuevas ofertas ayudarán a los responsables de seguridad a acelerar la detección, investigación y reparación de las amenazas, reduciendo el tiempo medio de respuesta”, afirma **Andrey Efremov, Chief Business Development Officer de Kaspersky.**

Max Kaminskiy, CEO, co-fundador de Brain4Net, añadió: *“Estamos encantados de unirnos al equipo de Kaspersky. La expansión de la tecnología SD-WAN necesita un escenario de negocio sólido, que es Kaspersky XDR, y la elección de las tecnologías de Brain4Net confirma el alto nivel de los productos y las competencias de la compañía. Juntos seguiremos haciendo del mundo un lugar más seguro y confortable”.*



IA, METAVERSO E HIPERCONECTIVIDAD EN UN MUNDO HÍBRIDO

Microsoft Cloud en Ignite 2021, está introduciendo más de 90 nuevos servicios y actualizaciones. Donde en el centro de estos nuevos anuncios, se encuentra el compromiso de abordar las tendencias y explorar formas innovadoras de conectar a personas, a organizaciones e ideas, creando inteligencia ambiental sobre entornos digitales que responden y son conscientes de las necesidades de un usuario.

La nube de Microsoft proporciona un conjunto completo de recursos diseñados para impulsar las capacidades de metaversos -IoT que permiten a los clientes crear "gemelos digitales" de objetos físicos en la nube; utilizar Microsoft Mesh para crear un sentido compartido de presencia en los dispositivos; y el uso de recursos impulsados por IA para crear interacciones naturales a través de modelos de aprendizaje automático de voz y visión.

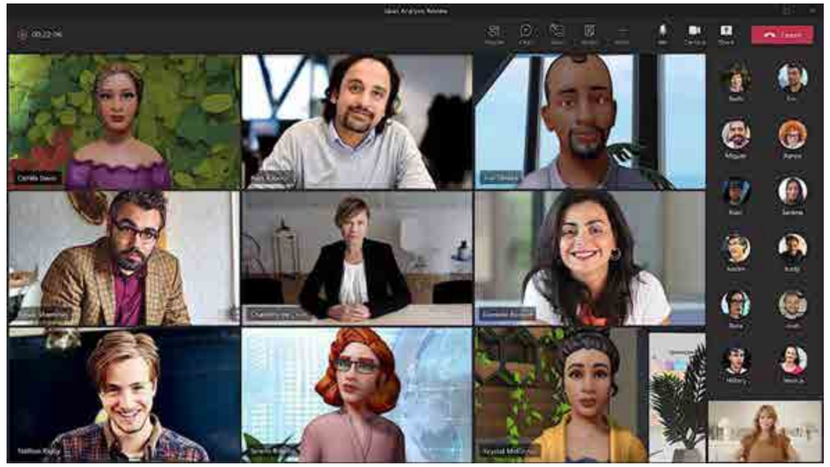
Frank X. Shaw, Vicepresidente corporativo de Microsoft Communications, publicó que *"Microsoft y Microsoft Cloud están a la vanguardia en ayudar a las organizaciones y a sus empleados y clientes a navegar por las principales tendencias de este nuevo tiempo. La nube de Microsoft es utilizada por organizaciones grandes y pequeñas, desde nuevas empresas emergentes hasta las de Fortune 500. Potencia la capacidad digital de una organización, al tiempo que proporciona las garantías necesarias para mantener la confidencialidad y la seguridad de los datos".*

En Ignite, Microsoft hará dos anuncios importantes que continúan la evolución del metaverso:

1.- Dynamics 365 Connected Spaces: Ahora en versión preliminar, este producto proporciona una nueva

Dynamics 365 Connected Spaces perspectiva sobre la forma en que las personas se mueven e interactúan con casi cualquier espacio, desde el comercio minorista, almacenar en la fábrica y cómo gestionan la salud y la seguridad en un entorno de trabajo híbrido.

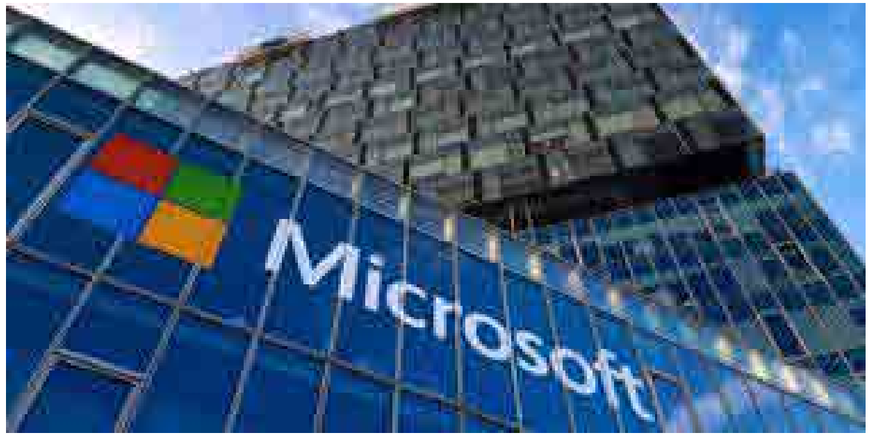
2.- Mesh para Microsoft Teams: Este puente de métodos de comunicación hace que la presencia humana sea la conexión definitiva. Ahora, todos en una reunión pueden estar presentes sin estar físicamente presentes utilizando avatares personalizados y espacios inmersivos a los que se puede acceder desde cualquier dispositivo, sin necesidad de equipos especiales.



Desde un punto de vista de los clientes: Los modelos de inteligencia artificial a gran escala ahora se están convirtiendo en plataformas, creando inteligencia ambiental: entornos digitales que responden y son conscientes de las necesidades de un usuario. Estos avances de IA pueden ser utilizados por las organizaciones de diversas maneras, desde la implementación de agentes inteligentes para ayudar en el servicio al cliente hasta la extracción de información de volúmenes de datos no estructurados.

Mesh para Microsoft Teams *"Hace solo cinco años, anunciamos la primera computadora de IA a hiperescala. Ahora, tenemos la supercomputadora de IA más poderosa del mundo, con clientes que utilizan la infraestructura para abordar problemas importantes. AMD, por ejemplo, lo utilizó para diseñar procesadores de próxima generación. Investigadores en los Países Bajos lo utilizaron para simular cómo el Covid-19 puede propagarse por partículas de aerosol en áreas altamente pobladas",* agregó FrankX. Shaw.

En Ignite, Microsoft anunció el servicio Azure Open AI, que inicialmente estará disponible solo por invitación. Esto dará a los clientes acceso a los potentes modelos de Open AI, además de la seguridad, confiabilidad, cumplimiento, privacidad de datos y otras capacidades de nivel empresarial integradas en Microsoft Azure. Asimismo, está ofreciendo a los clientes de Azure Open AI Service, herramientas para garantizar que los resultados que proporcionan los modelos sean apropiados para el negocio y estamos monitoreando cómo las personas emplean la tecnología para garantizar que se use correctamente.



QUE SIGNIFICA UNA IMPLEMENTACIÓN DE REDES 5G EN AMÉRICA LATINA

Según el reporte de 5G Américas, se sostiene que el 5g puede producir un beneficio acumulado de más de un trillón de dólares a las economías latinoamericanas. Sin embargo apenas se está en una fase de crecimiento, mientras que LTE es la tecnología de banda ancha móvil predominante. Tanto la iniciativa privada y los gobiernos han presentado de manera pública pruebas 5G para aplicaciones masivas e industriales que dan cuenta de las oportunidades que estas redes ofrecen, por lo que es crucial establecer políticas adecuadas para promover inversiones que incentive el entorno tecnológico de 5G.

5G Americas publicó su reporte **"Implementación de redes 5G en América Latina",** donde presenta las recomendaciones para fomentar su despliegue que recopila mejores prácticas y políticas públicas para el desarrollo de infraestructura de telecomunicaciones móviles, partiendo de barreras identificadas en la región.

El reporte, en sí muestra una transformación digital más profunda con el entorno tecnológico de 5G y la adopción de mejores prácticas para el despliegue de infraestructura móvil que contribuirían a que las economías latinoamericanas obtengan beneficios económicos duraderos.

Específicamente, resumiendo el tema del reporte, **diferentes ramos industriales podrán implementar soluciones 5G que ya se conocen para promover eficiencias y mayor productividad en algunos de sus procesos.** Por lo tanto, la obtención de los beneficios económicos duraderos con 5G requiere de un desarrollo industrial robusto en los países.

Se destaca que a nivel internacional, distintas proyecciones sobre las aportaciones económicas atribuibles a 5G difieren en los montos estimados, hay coincidencias en que las contribuciones económicas se explicarían por la adopción de este entorno tecnológico por varios sectores industriales, como complemento de los servicios al público masivo.

"Para las administraciones nacionales, las políticas que incentiven la evolución de las redes móviles serán importantes para aportar elementos a una recuperación económica en el contexto de la pandemia de Covid-19, pero también para sentar las bases de una infraestructura digital más robusta. Es importante detectar en los distintos niveles de gobierno normas obsoletas o procesos que pueden ser sujetos a mejora para establecer criterios consistentes con los objetivos de cierre de la brecha digital y calidad de los servicios", mencionó José Otero, **Vicepresidente de 5G Americas para América Latina y el Caribe.**

Entre los ejemplos que describe el reporte se encuentran normas ágiles para instalación de small cells, mimetización de antenas, homologación de reglamentos de instalación en gobiernos locales y silencio administrativo positivo.

Los mecanismos de asignación del espectro, como licitaciones, concursos, subastas, también son un elemento en el que se pueden presentar barreras para el desarrollo de infraestructura, dado que es un insumo esencial para las redes inalámbricas. Destaquemos que Licitaciones con altos precios o compromisos excesivos pueden desalentar la participación y el aprovechamiento de este bien escaso.

VUELVEN LAS FAKE NEWS Y LAS CAMPAÑAS DE DESINFORMACIÓN

En las predicciones globales de ciberseguridad 2022 de Check Point Software Technologies publicados en su reciente Informe, se detalla los principales retos de seguridad a los que se enfrentarán las empresas en 2022 ante los crecientes ataques de los ciberdelincuentes, que siguen encontrando nuevas oportunidades de ataque con las deepfakes, las criptodivisas, los wallets y mucho más.

Las Fake News, los ataques a la cadena de suministro, a dispositivos móviles vulnerables, criptomonedas y el aumento notable del ransomware son solo algunas de las predicciones de **Check Point Software** para el año que viene entre los aspectos más destacados del **Informe sobre Predicciones Globales de Ciberseguridad 2022:**

- **Vuelven las Fake News y las campañas de desinformación:** a lo largo de 2021, se difundió información errónea sobre la pandemia de la COVID-19 y la correspondiente vacunación. En 2022, los grupos de ciberdelincuentes seguirán aprovechando las campañas de noticias falsas para ejecutar diversos ataques de phishing y estafas.

- **Los ciberataques a la cadena de suministro siguen aumentando:** los ataques a la cadena de suministro serán cada vez más comunes y los gobiernos comenzarán a legislar para hacer frente a estas amenazas y proteger las redes, así como a colaborar con los sectores privados y otros países para identificar y atacar a más grupos de amenaza a nivel mundial.

- **La "guerra fría" cibernética se intensifica:** la mejora de las infraestructuras y de las capacidades tecnológicas permitirán a los grupos terroristas y a los activistas políticos impulsar sus programas y llevar a cabo ataques más sofisticados y de mayor alcance. Los ciberataques se utilizarán cada vez más como conflictos indirectos para desestabilizar

actividades a nivel mundial.

- **Las filtraciones de datos son de mayor escala y más costosas:** las filtraciones de datos se producirán con mayor frecuencia y a mayor escala y su recuperación costará más a las empresas y a los gobiernos. En mayo de 2021, el gigante estadounidense de los seguros pagó 40 millones de dólares en rescates a los ciberdelincuentes. Esto fue un récord, y es de esperar que los rescates exigidos por los atacantes aumenten en 2022.

- **La criptodivisa gana popularidad entre los ciberdelincuentes:** cuando el dinero se convierta en puro software, la ciberseguridad necesaria para protegerse de los atacantes que roban y manipulan bitcoins y altcoins cambiará de forma inesperada.

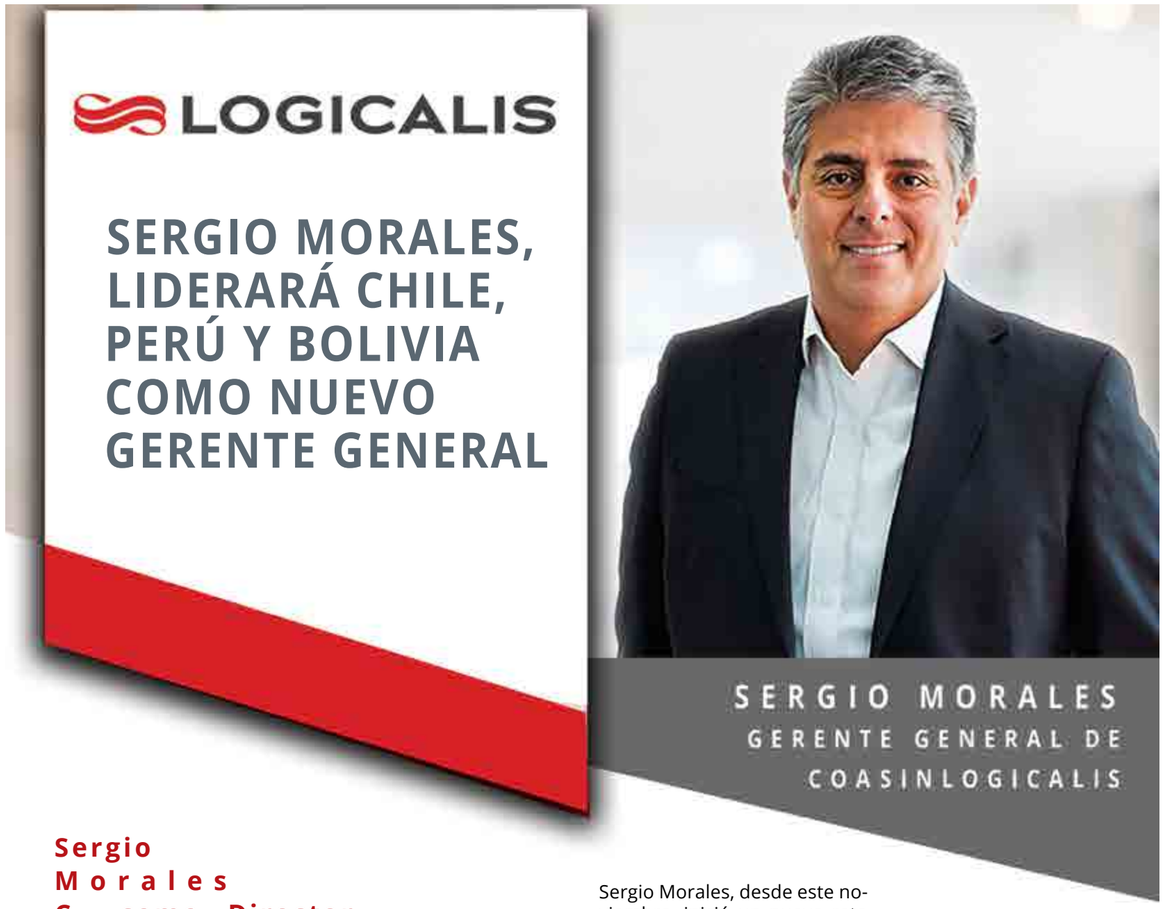
- **Dispositivos móviles en el punto de mira:** a medida que los monederos móviles y las plataformas de pago por móvil se utilicen con más frecuencia, los ciberdelincuentes evolucionarán y adaptarán sus técnicas para explotar la creciente dependencia de los dispositivos móviles.

- **Los ciberdelincuentes aprovecharán las vulnerabilidades de los microservicios:** con la arquitectura de microservicios adoptada por los proveedores de servicios en la nube (CSP), los ciberdelincuentes están utilizando las vulnerabilidades encontradas en ellos, para lanzar ataques a gran escala contra los CSP.

- **La tecnología deepfake se convierte en un arma para los ataques:** las técnicas de video o audio falsos son ahora lo suficientemente avanzadas como para ser un arma y utilizarse para crear contenido dirigido a manipular opiniones, cotizaciones bursátiles o para obtener permisos y acceder a datos sensibles.

- **El ransomware sigue haciendo su agosto:** a nivel mundial en 2021, 1 de cada 61 empresas experimenta un ransomware cada semana. Los ciberdelincuentes seguirán atacando a las compañías que puedan permitirse pagar un rescate, y la sofisticación del ransomware aumentará en 2022. Veremos cómo utilizan cada vez más herramientas de penetración para personalizar los ataques en tiempo real y vivir y trabajar dentro de las redes de las víctimas.

Gery Coronel, Country Manager para la Región Sur de América Latina de Check Point Software, comentó que *"De cara al futuro, las empresas deben ser conscientes de los riesgos y asegurarse de que cuentan con las soluciones adecuadas para prevenir, sin interrumpir el flujo normal de la empresa, la mayoría de los ataques, incluidos los más avanzados. Para adelantarse a las amenazas, las organizaciones deben ser proactivas y no dejar ninguna parte de su superficie de ataque sin proteger o supervisar, o corren el riesgo de convertirse en la próxima víctima de complejos ataques dirigidos"* e indicó que durante el 2021, los ciberdelincuentes adaptaron su estrategia de ataque para explotar temas de actualidad como vacunación, las elecciones y el cambio al trabajo híbrido, para atacar las cadenas de suministro y las redes de las empresas con el fin de lograr la máxima disrupción. Gery Coronel, alertó también que la sofisticación y la escala de los ciberataques seguirán batiendo récords y podemos esperar un enorme aumento en el número de ransomware y ataques móviles.

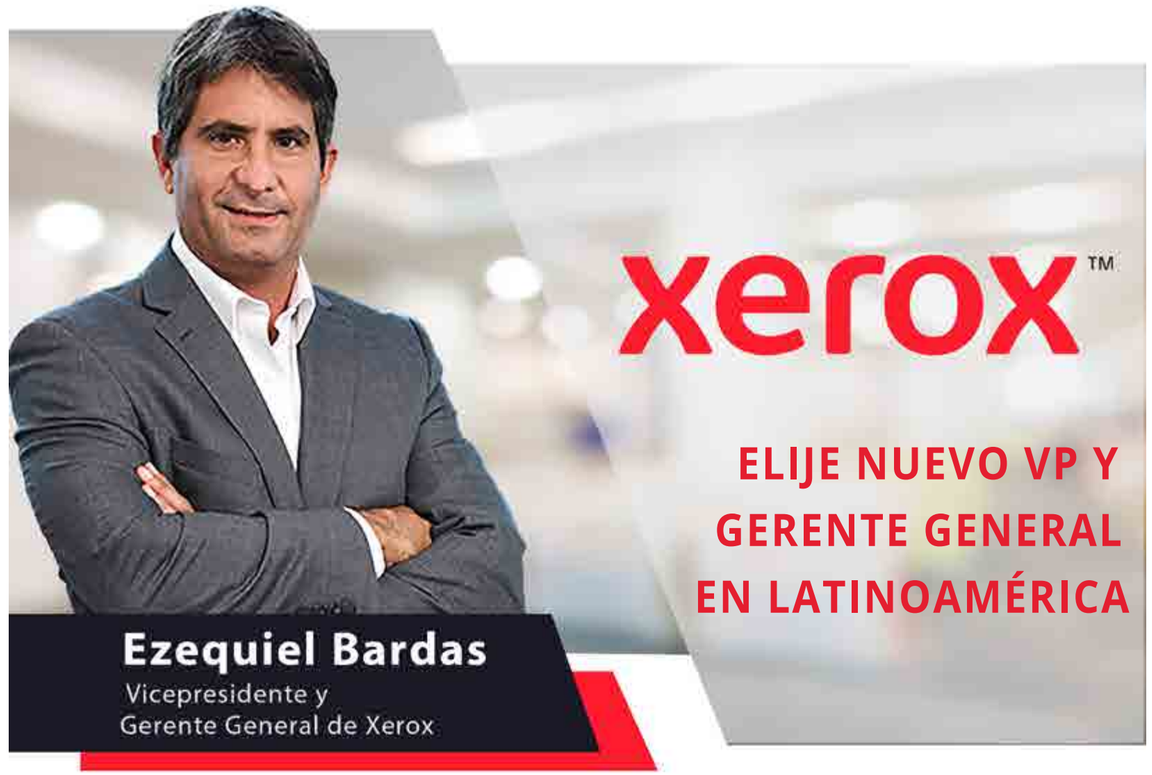


Sergio Morales C., como Director de Operaciones de ventas indirectas en Unisys Latin America, ya demostró sus aptitudes para manejar el sector IT, y lo reafirmó como Gerente Corporativo del mercado empresarial en Telmex y Director (VP) de Telecomunicaciones para el mercado corporativo en el grupo América Móvil, y por último en su última experiencia, antes de sumarse este noviembre a Coasin Logicalis como el nuevo Gerente General de la Región para Chile, Perú y Bolivia, se desempeñó anteriormente como Gerente General de Adexus Latam.

Sergio Morales, desde este noviembre, inició un nuevo reto al asumir como Gerente General de la Región de Chile, Perú y Bolivia de Logicalis Latam; y además mantendrá su puesto como profesor adjunto del Centro de Transformación Digital de la Universidad del Desarrollo, miembro de la Junta Directiva del Centro de Estudios Futuros de la Universidad de Santiago de Chile (USACH) y miembro del Consejo Empresarial del Departamento de Ingeniería Industrial de USACH.

"Estoy muy feliz de sumarme al equipo de CoasinLogicalis ya que es un gran actor dentro del mercado nacional, cuyo rol fue transformándose a lo largo de los años hasta convertirse en un arquitecto del cambio, apoyando los procesos de negocios necesarios para llevar a sus clientes a la era digital. Desde mi rol buscaré potenciar nuestro capital humano y ecosistema de partners, apoyando comprometidamente al desarrollo del país, aportando innovación y experiencias internacionales", señaló Morales.

En sus estudios, egresó de licenciado en Ingeniería Civil Industrial y Licenciado en Ciencias en Ingeniería por la Universidad de Santiago de Chile. Actualmente es reconocido en el mundo empresarial como un profesional con fuertes habilidades en estrategias de negocios y ventas, con amplia experiencia en servicios y operaciones TIC y enérgica inclinación por estrategias de planificación orientadas a resultados.



Ezequiel Bardas es a partir de este noviembre el nuevo Vicepresidente y Gerente General de Xerox para Latinoamérica, encargado de encabezar la estrategia de negocio en toda la región con el objetivo de continuar con el crecimiento de la marca.

Xerox anunció el nombramiento de **Ezequiel Bardas como Vicepresidente y Gerente General de Xerox** para Latinoamérica. Le reportan directamente los Gerentes Generales de las filiales de Xerox en: Brasil, México, Xerox XMLA (Conformada por Argentina, Chile, Ecuador y Perú), y el grupo de Distribuidores que atienden el resto de América Latina (XDG).

Con el objetivo de continuar con el crecimiento, cuya finalidad es que la compañía se posicione como referente y líder indiscutible en los sectores de servicios, soluciones y tecnología, Ezequiel Bardas, seguirá en el impulso que inició en enero de 2018 desde su anterior posición, como Presidente y Director General de Xerox en México, ahora para toda Latinoamérica. Gestión en la que logro un importante crecimiento que destaca la implementación de la estrategia y cobertura del mercado corporativo y una línea de negocios adicional para el sector gráfico.

"Ezequiel y su equipo impulsarán iniciativas enfocadas en la transformación digital de los negocios, el desarrollo de ingresos sostenibles y el crecimiento de las ganancias. Estas iniciativas incluyen implementar una estrategia de producción en la región, diversificar nuestra cartera con más soluciones de valor agregado y mejorar el enfoque en el canal, logrando el incremento de nuestra participación en el mercado", sostuvo **Mike Feldman, Vicepresidente Ejecutivo y Presidente de Operaciones en las Américas y Ofertas de Servicios Globales en Xerox.**

El ejecutivo, inició en Xerox como Director General de Xerox Argentina, con sede en Buenos Aires, cargo que ocupó desde el 2012, siendo responsable del liderazgo y la gestión organizativa de una filial con grandes retos en el ámbito económico.

Bardas es Licenciado en Mercadotecnia y Negocios (UADE) y posee también una Maestría en Administración de Negocios (IAE, Argentina). Seguirá dirigiendo las operaciones de México hasta que se nombre a su reemplazo.

TELEINFOpress