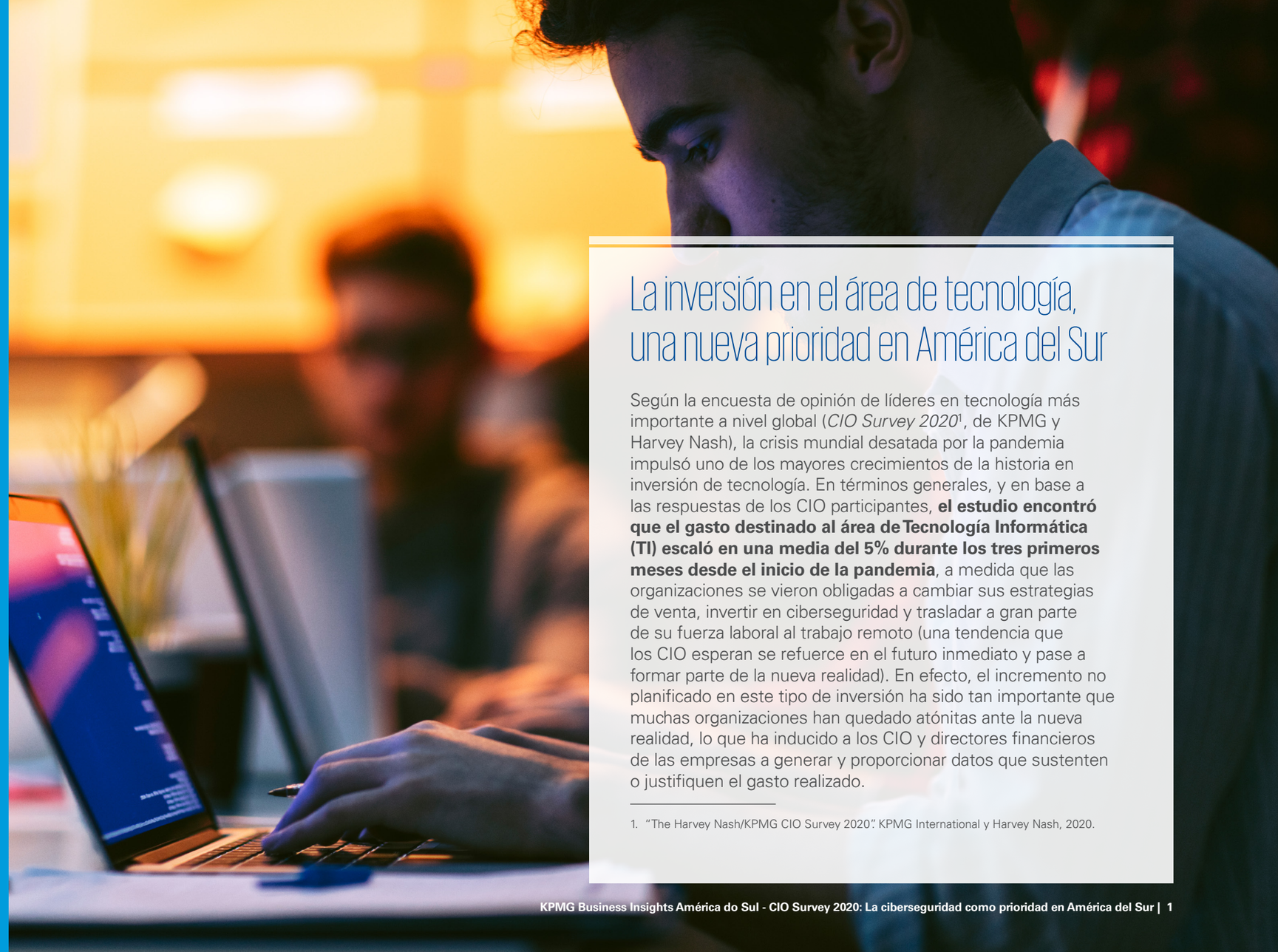
KPMG Business Insights América del Sur

Edición Nº9
CIO Survey 2020

Luis Motta,
socio líder de Tecnologías, Medios y Telecomunicaciones de KPMG en América del Sur.

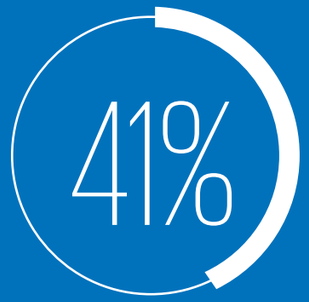
Noviembre 2020



La inversión en el área de tecnología, una nueva prioridad en América del Sur

Según la encuesta de opinión de líderes en tecnología más importante a nivel global (*CIO Survey 2020*[1], de KPMG y Harvey Nash), la crisis mundial desatada por la pandemia impulsó uno de los mayores crecimientos de la historia en inversión de tecnología. En términos generales, y en base a las respuestas de los CIO participantes, **el estudio encontró que el gasto destinado al área de Tecnología Informática (TI) escaló en una media del 5% durante los tres primeros meses desde el inicio de la pandemia**, a medida que las organizaciones se vieron obligadas a cambiar sus estrategias de venta, invertir en ciberseguridad y trasladar a gran parte de su fuerza laboral al trabajo remoto (una tendencia que los CIO esperan se refuerce en el futuro inmediato y pase a formar parte de la nueva realidad). En efecto, el incremento no planificado en este tipo de inversión ha sido tan importante que muchas organizaciones han quedado atónitas ante la nueva realidad, lo que ha inducido a los CIO y directores financieros de las empresas a generar y proporcionar datos que sustenten o justifiquen el gasto realizado.

1. "The Harvey Nash/KPMG CIO Survey 2020". KPMG International y Harvey Nash, 2020.



Y 46% de los líderes en tecnología globales y sudamericanos, respectivamente, aseguró haber experimentado un incremento sustancial en la cantidad de ataques cibernéticos durante el brote de coronavirus.

En **América del Sur**, región en la que más de los 260 CIO participantes de la encuesta se identifican con empresas que destinan un presupuesto de TI no mayor a los US$ 9 millones anuales, el crecimiento del gasto en activos tecnológicos también fue significativo e, incluso, según la misma encuesta, mayor al promedio global (11% en promedio). De hecho, esta tendencia quedó también reflejada en los resultados de otra importante encuesta que KPMG realiza anualmente: el *CEO Outlook 2020*[2]. Según ésta, el 61% de los ejecutivos **sudamericanos** y el 67% de los CEO pertenecientes a las principales economías del mundo aseguraron estar destinando la mayor parte de sus inversiones a la compra de tecnología, tanto como parte del proceso de transformación que deben realizar ante las condiciones impuestas por la nueva realidad, como de reorientación en su estrategia de desarrollo.

Como resulta lógico, **la preocupación de las organizaciones en materia de ciberseguridad se ha disparado en paralelo a la mayor dependencia tecnológica**. A pesar de que el cibercrimen ya había sido destacado por diversos organismos como una de las principales amenazas globales antes del inicio de la pandemia de COVID-19 –el *World Economic Forum* (WEF), por ejemplo, en la última edición de su estudio anual sobre riesgos globales[3] acentuó el rol de los ciberataques como uno de los principales riesgos a enfrentar, junto a otros importantes tales como los desastres naturales y climáticos, o los políticos–, el peso de esta preocupación y la inversión que impulsa en materia de ciberseguridad en la fase de recuperación económica posterior al brote se ha transformado en algo prioritario para la mayoría de las organizaciones, sin importar el sector que éstas atiendan. Esta realidad, incluso, se ha hecho más evidente cuando se aprecian los resultados de la encuesta *CIO Survey 2020*, desde que el **41% y 46% de los líderes en tecnología globales y sudamericanos**, respectivamente, aseguró haber experimentado un incremento sustancial en la cantidad de ataques cibernéticos durante el brote de coronavirus, especialmente en la forma de *phishing, malware* y DDoS (*denial of service attack*).

Producto de este contexto, o de la "nueva normalidad", el incremento en la demanda de profesionales calificados en ciberseguridad no tiene precedente, transformando a este *skill* o capacidad en una de los más requeridas a nivel global, pero también regional, desde que el 87% de los líderes en tecnología **sudamericanos** aseguró estar "de acuerdo" o "muy de acuerdo" en que, como resultado de las nuevas condiciones reinantes tanto en el contexto comercial como laboral, la superficie factible de ataques quedará más expuesta frente al cibercrimen. Tal vez por esta razón la mayoría de los CIO, tanto a nivel global como **regional**, pronosticó un incremento sensible en la cantidad de empleados capacitados en el área de TI, como así también que, en los próximos 5 años, los nuevos roles laborales terminarán compensando aquellos puestos que sean cubiertos por la automatización; un augurio que es compartido por el 70% de los CIO globales y el 81% de los CIO **sudamericanos**. Sin embargo, es importante señalar que, según la misma encuesta, persiste un elevado nivel de escasez en "talentos y capacidades tecnológicas". En ese aspecto, además de las capacidades relacionadas a la seguridad cibernética, las siguientes tres habilidades tecnológicas más escasas a juicio de los CIO son la gestión del cambio organizacional, la arquitectura empresarial, y la arquitectura técnica y el análisis avanzado de datos (*advanced analytics*). A nivel regional, alrededor del 60% de los líderes entrevistados en **América del Sur** observaron, tanto antes como luego del inicio de la pandemia, una notoria falta de capacidades tecnológicas que, en definitiva, podrían afectar la fase de recuperación de las empresas y su crecimiento futuro esperado.

Solo el 48% de los líderes en tecnología espera un incremento del presupuesto durante el próximo año, cuando, antes del brote de COVID-19, esa cifra era del 57%.

A pesar de revelar un incrementó drástico en el gasto destinado a tecnología durante la pandemia, los resultados de la encuesta también dejaron entrever que los presupuestos del área de TI de las empresas podrían sufrir alguna presión o quedar comprometidos durante el próximo año, desde que el porcentaje de CIO que esperaba algún incremento en el presupuesto de su área en los próximos 12 meses cayó del 51% al 43% con el inicio de la crisis sanitaria. En **América del Sur**, en tanto, la tendencia se replicó, desde que solo el 48% de los líderes en tecnología espera un incremento del presupuesto durante el próximo año, cuando, antes del brote de COVID-19, esa cifra era del 57%.

Finalmente, **la encuesta detectó un claro aumento en los niveles de influencia de los CIO en las decisiones de las empresas**. Aun cuando para el 61% de los encuestados la participación de los líderes en tecnología en los directorios sigue mermando, casi dos tercios de la muestra global (61%) y el 77% de los CIO **sudamericanos** afirmó que la pandemia aumentó considerable y permanentemente su influencia; un resultado que podría estar sugiriendo que los líderes globales en tecnología están hallando otras formas de incrementar su relevancia, sin la necesidad de participar en el board de las empresas.

2. "CEO Outlook 2020". KPMG International, agosto de 2020.
3. "The Global Risks Report 2020". World Economic Forum (WEF), 2020.

La nueva realidad interpela a los países de la región a reconocer la importancia de la ciberseguridad como elemento crucial para impulsar su desarrollo. Si bien queda mucho por hacer, la mayoría de las organizaciones están adoptando diferentes estrategias para impulsarla y priorizarla en sus agendas, destinando una mayor cantidad de recursos al perfeccionamiento de esta "práctica" y a tasas consideradas "inusitadas" para los últimos diez años (decisión que no solo incluye una mayor inversión en tecnología, sino también en la captación y retención de talentos). En ese sentido, tal vez resulte interesante desglosar algunas de las principales consideraciones o tendencias emergentes en ciberseguridad que *KPMG* abordó en un estudio[4] realizado con anterioridad al inicio de la pandemia (pero que no por ello ha perdido vigencia), y que podría funcionar como "hoja de ruta" para entender desde dónde deben partir tanto el sector privado como el público de la región para abordar exitosamente sus preocupaciones en materia de seguridad. Entre las principales pueden destacarse "la alineación de los objetivos empresariales a lo imperativo en materia de seguridad" (como principio básico para determinar el nivel óptimo de gasto en este aspecto), "la optimización de la experiencia digital del consumidor" (que implica reducir los obstáculos que generalmente impone una mayor ciberseguridad) y, entre otras consideraciones, "la necesidad de dar más espacio de desarrollo al equipo de seguridad", una decisión que implica no solo un incremento en la participación de sus profesionales en las decisiones de las empresas, sino en su nivel de influencia (una realidad que ya estamos presenciando tanto a nivel global como regional, según revelan algunos de los resultados comentados previamente).

Asimismo, y aun cuando los indicadores de desarrollo tecnológico de la región (como el nivel de penetración de internet, la cantidad de computadoras por hogar y la cantidad de suscripciones a líneas móviles, entre otras variables), alcanzan valores que, en promedio, son menores a los registrados en otros mercados o regiones más avanzadas; ha existido una mejora gradual en materia de inversión en infraestructura tecnológica y un incremento sustancial de las iniciativas destinadas a apuntalar la ciberseguridad en casi todos los países **latinoamericanos** en los últimos años. Estas "necesidades", que ya eran evidentes frente a los nuevos estándares impuestos por una economía globalizada y altamente dependiente de la tecnología, solo ha quedado exacerbada en la "nueva normalidad" y, especialmente, en la fase de recuperación económica posterior a la pandemia. En paralelo, y como destaca un informe del *Banco Interamericano de Desarrollo*[5], también resulta importante que los gobiernos de la región "eduquen" a sus ciudadanos sobre los riesgos asociados a la conectividad y la alta dependencia tecnológica, como así también en lo que atañe a la relevancia que adquieren la ciberseguridad y, especialmente, el usuario (como primera línea de defensa) en este contexto. Este tipo de iniciativas permiten incrementar la conciencia sobre los riesgos cibernéticos y fomentar el desarrollo de soluciones que mejoren la resiliencia de un país frente a la nueva realidad. Al mismo tiempo, deben continuar los esfuerzos por integrar al marco legal vigente las normas referidas al cibercrimen. Este elemento resulta crucial en un proceso social que reconoce el problema, pero principalmente para habilitar los recursos y medios necesarios para combatir efectivamente el ciberdelito. Finalmente, resulta estimulante que el tema de la ciberseguridad esté ocupando un lugar de privilegio en las agendas de los países de la región, los cuales se encuentran plasmando esa relevancia en medidas que apuntan de manera directa a establecer economías hiper conectadas, pero también más seguras y resilientes.

---

4. "All hands on deck: Key cybersecurity considerations for 2020". KPMG, 2020.
5. "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?", Banco Interamericano de Desarrollo, Observatorio de Ciberseguridad en América Latina y el Caribe, pág. 115, 2016.