# KPMG Business Insights América del Sur

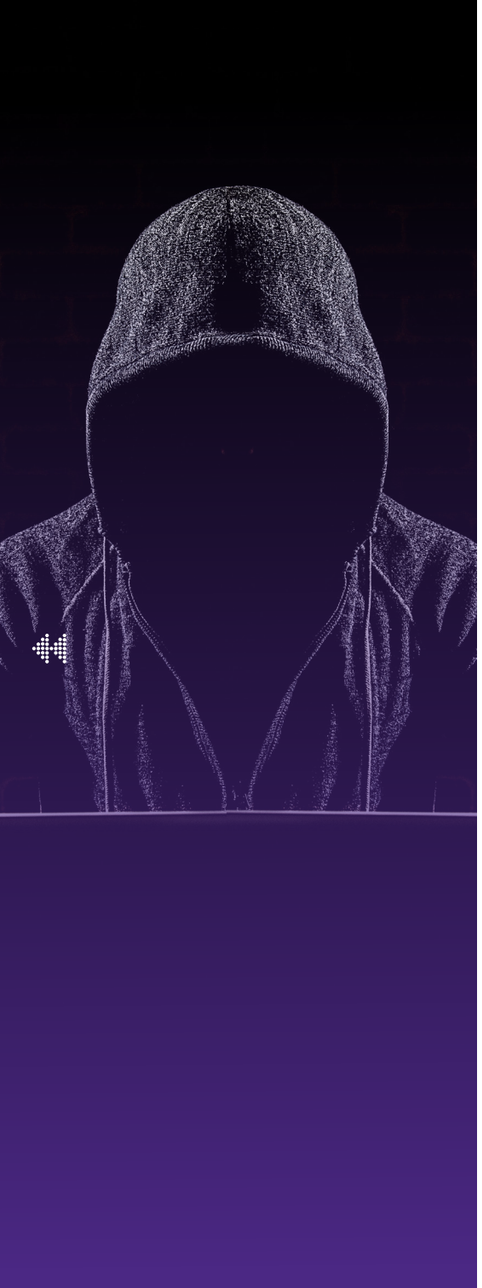
**Edición N°15**
**Ciberseguridad**

**Leandro Augusto,**
socio líder de Ciberseguridad
de KPMG en América del Sur.

**Mayo 2021**

## Ciberseguridad: principal riesgo para el crecimiento y una prioridad en América del Sur.

La pandemia ha cambiado radicalmente nuestras vidas. Desde cómo trabajamos y compramos productos, hasta cómo nos entretenemos y socializamos. Y como resulta lógico, estos cambios trajeron aparejada la transformación de los modelos de negocio de las empresas y sus estrategias comerciales, volcando la mayor parte de su actividad hacia lo digital. Asimismo, la ruptura provocada por la crisis sobre las cadenas de distribución y suministros, antaño dependientes de la intermediación y de los flujos comerciales provenientes de otros países, han sesgado su foco en el último año hacia lo doméstico, con el objetivo de que las empresas que los conforman puedan ejercer una suerte de mayor control sobre su funcionamiento, y sin la dependencia estricta de los grandes mercados globales. En síntesis: **los empleados continúan trabajando desde sus hogares, las instalaciones y oficinas permanecen cerradas, las cadenas de suministro cambian su enfoque, y la omnicanalidad trae consigo grandes migraciones hacia los canales digitales.**



Pero lo antedicho no es solamente una sensación individual o la opinión bien formada de quien escribe, sino que forma parte de un cambio de paradigma reforzado por los datos y las opiniones de los líderes empresariales de todo el mundo, y que, en última instancia, son quienes deben afrontar esta nueva realidad con acciones, recursos y nuevas inversiones destinadas a adaptar sus organizaciones a las nuevas demandas y modelos de negocio. En particular, la última encuesta de KPMG a líderes ejecutivos de todo el mundo (**CEO Outlook Pulse Survey 2021**)[1] arrojó algunos resultados que llamaron mucho la atención y que permiten, al menos en parte, dilucidar cuál ha sido el alcance y los efectos de la pandemia en los negocios. En ese sentido, vale la pena destacar que mientras la mitad de los CEO que participaron de esta encuesta afirmó esperar un regreso a la "normalidad" durante el 2021, uno de cada cinco de los mismos aseguró que sus negocios no volverán a ser los mismos y que, al contrario, han cambiado para siempre. Asimismo, el cambio de paradigma en las operaciones y en el comportamiento de los consumidores han acelerado los procesos de transformación tecnológica y digitalización **convirtiendo a una gran parte de las organizaciones en unidades productivas altamente dependientes de la tecnología y la infraestructura que la respalda**. Y, ciertamente, durante 2020 han abundado los ejemplos de empresas que experimentaron una tasa acelerada de adopción tecnológica –en algunos casos, generando transformaciones que hubieran llevado años en llevarse a cabo–, y cuyos efectos terminaron derramándose sobre toda la cadena de valor en la que están insertas. Desde empresas que habían dedicado más de 2 años a impulsar la adopción de *Skype* entre sus empleados y fueron capaces de hacer lo mismo con *MS Teams* en tan solo 3 semanas (y con una tasa de adopción del 100%), hasta el impacto de las nuevas tendencias en materia laboral y de consumo, que promueven el uso de las videoconferencias para las reuniones laborales, las sesiones de colaboración en línea, o una mayor interacción con los clientes a través de los canales digitales. Y es probable que esto tenga un impacto permanente, desde que alrededor del 61% de los ejecutivos que respondieron la mencionada encuesta global anual de KPMG **aseguró que seguirá aprovechando las funcionalidades de las herramientas digitales de comunicación mucho más allá de la pandemia**. Y como resulta lógico, estas tendencias también han tenido su impacto en la región de **América del Sur**. Ya en la encuesta del año pasado[2] podía detectarse hacia dónde estaban dirigiéndose las empresas de la región en materia tecnológica, **desde que alrededor del 61% de los ejecutivos sudamericanos habían asegurado que estaban destinando una gran parte de sus recursos al financiamiento de la innovación y la adquisición de nuevas tecnologías**, preparando sus organizaciones para la nueva realidad.

En efecto, si bien la crisis sanitaria global y el impulso que ésta proporcionó sobre la inversión en tecnología han transformado nuestras vidas, **lo cierto es que trae aparejado otra realidad menos alentadora: el ciberdelito**. Como era de suponer, el crimen organizado ha demostrado agilidad y creatividad para explotar el temor y la incertidumbre que la pandemia trajo consigo. Los ataques por *ransomware*, el *fraude por correo electrónico* y el *ciber-espionaje* han ido prosperando durante los últimos 12 meses a medida que los atacantes iban tropezando con distintas brechas y debilidades susceptibles de ser explotadas, especialmente en un entorno de impulso en la modalidad de trabajo remoto, pero sin las medidas de seguridad que este cambio lógicamente demandaba. Por ende, no resulta sorpresivo que, según la encuesta citada, **el riesgo asociado a la seguridad cibernética haya calificado entre las principales preocupaciones para los CEO** (incluso por encima de las preocupaciones regulatorias y fiscales, o las relacionadas a la cadena de suministro), **y como uno de los principales riesgos que enfrentarán en los próximos 3 años para asegurar el crecimiento organizacional**. Sin embargo, y a pesar de que esto pueda parecer algo sorpresivo para el resto del mundo, no es algo nuevo para los líderes **sudamericanos**. Tanto en la encuesta realizada el año pasado por KPMG a CEO de empresas[3], como en otra más reciente que profundizó en las inquietudes de los CIO[4], puede apreciarse que la preocupación en materia de ciberseguridad se ha disparado en paralelo a la mayor dependencia tecnológica. En efecto, mientras la ciberseguridad ya aparecía como uno de los principales riesgos detectados por los ejecutivos locales en los resultados publicados en 2020, **también era destacada como fuente de preocupación entre los CIO sudamericanos**, especialmente si se tiene en cuenta el crecimiento observado durante 2020 en los ataques de *phishing, malware* y DDoS.

Este es un resultado por demás interesante, desde que la mayoría de los ejecutivos, lejos de sentir que sus organizaciones están protegidas y preparadas para lidiar con los incidentes cibernéticos, **reconocen finalmente la disipación de esa "ilusión de seguridad" de la cual se jactaban algún tiempo atrás**, y deciden prepararse para enfrentar esta nueva realidad.

**61%**

De los ejecutivos que respondieron la mencionada encuesta global anual de KPMG **aseguró que seguirá aprovechando las funcionalidades de las herramientas digitales de comunicación mucho más allá de la pandemia.**

Puede apreciarse que la preocupación en materia de ciberseguridad se ha disparado en paralelo a la mayor dependencia tecnológica.

1 "CEO Outlook Pulse Survey 2021", KPMG International, 2021.
2 "CEO Outlook Sudamérica 2020: Edición especial COVID-19". KPMG en América del Sur, agosto de 2020.
3 Ibidem, página 2.
4 "The Harvey Nash/KPMG CIO Survey 2020". KPMG International y Harvey Nash, 2020.

En ese sentido, la mayoría de los ejecutivos (52% en la encuesta de KPMG de este año) aseguró que sus compañías buscarán mejorar las inversiones en medidas que refuercen la seguridad de los datos, las tecnologías centradas en el cliente, las comunicaciones digitales y, también, la inteligencia artificial. No obstante, también es importante señalar que, además de las inversiones destinadas a estos elementos, las empresas deberán poner un ojo en las capacidades y talentos tecnológicos, especialmente las competentes en ciberseguridad, que se ha transformado en uno de los *skills* más requeridos a nivel global, pero también regional, desde que la mayor parte de los líderes en tecnología sudamericanos sostiene que, como resultado de las nuevas condiciones reinantes tanto en el contexto comercial como laboral, la superficie factible de ataques quedará, de aquí en más, mucho más expuesta frente al cibercrimen.

En adelante, las organizaciones exitosas no solo incorporarán la seguridad cibernética como parte fundamental de su estrategia de negocios, sino que, al mismo tiempo, buscarán generar y apoyar la confianza de sus clientes tanto en su nivel de resiliencia cibernética, como así también en la seguridad con la que gestionan y protegen los datos personales y en la transparencia de su enfoque. **Dado que esa "confianza" se ha convertido en un claro determinante del éxito**, una implementación efectiva de la seguridad cibernética puede desempeñar un papel fundamental y vital para la organización; y más aún en un mundo que se acerca, cada vez más, a la supremacía digital.

KPMG

# Ser especialista transforma negocios

En un mercado en constante movimiento, buscar lo nuevo es prepararse para el éxito en el futuro.

#KPMGTransforma

Disponible en App Store

DISPONIBLEE N Google Play