KPMG

Algunas consideraciones en ciberseguridad

La innovación tecnológica proporciona grandes beneficios en la jornada de transformación de la industria de Tecnología, Medios y Telecomunicaciones (TMT), pero también plantea nuevos interrogantes y problemas de seguridad que deben ser atendidos.

Marcio Kanamaru
Socio líder de la industria de Tecnologías, Medios y Telecomunicaciones de KPMG en América del Sur

KPMG Business Insights América del Sur
Edición N° 49 | Julio • 2024

No es una novedad

que las empresas de tecnología están continuamente a la vanguardia y en la frontera de la innovación. Este camino de desarrollo no solo conduce a nuevos beneficios que pueden traducirse en ventajas competitivas y comparativas, sino que, al mismo tiempo, conlleva un caudal mayor o diferente de amenazas cibernéticas y compromisos regulatorios frente a los cuales quedan expuestas. Esta es la realidad que viven las empresas de tecnología que, en conjunto a las de medios y telecomunicaciones, están viendo cómo la alta dependencia de los datos y su incidencia casi absoluta en todas las áreas de la organización, implican una necesidad cada vez mayor de blindar la información y privacidad de sus clientes, proveedores y otras partes interesadas, haciendo de la ciberseguridad una máxima prioridad. Y ello no significa poner el foco únicamente en un sistema que proporcione una respuesta rápida frente a las amenazas cambiantes, sino garantizar de forma proactiva que la ciberseguridad y privacidad de los datos estén integrados a la organización para evitar o mitigar la posibilidad de nuevos ataques y aumentar su resiliencia.

Esta es la idea central que motivó la última edición del informe sobre *consideraciones en ciberseguridad para la industria de la tecnología, los medios y las telecomunicaciones* (TMT) de **KPMG** (KPMG, 2024)[1]. El artículo, además de analizar el entorno cambiante de la ciberseguridad y resaltar la necesidad, cada vez mayor, de operar de manera resiliente incorporando la seguridad a todas las áreas de la organización, está centrado en **tres consideraciones fundamentales** que las compañías de esta industria deben tener en cuenta en su camino de transformación y convergencia hacia empresas de tecnología.

En ese sentido, debido a que las empresas de tecnología, medios y telecomunicaciones suelen ser uno de los objetivos más comunes para los ciberdelincuentes, **la incorporación de la ciberseguridad y la privacidad de forma permanente** es la primera de las consideraciones destacadas. Dado que las organizaciones de este sector están desplazando el foco de su negocio hacia un modelo marcado por la transformación digital y la innovación, con las empresas de tecnología realizando fuertes inversiones en inteligencia artificial (IA), y las de medios y telecomunicaciones moviéndose hacia lo digital, la exposición a las amenazas es cada vez mayor. Para contrarrestar tal exposición, los especialistas de **KPMG** proponen adoptar el principio "seguro desde el diseño" en todas las áreas de la empresa, con el objetivo de integrar sin altibajos la seguridad en todo el espectro operativo de la organización. De esta manera, **la ciberseguridad y la privacidad dejan de verse solo como una necesidad para transformarse en auténticos generadores de valor,** al afianzar la confianza digital de los clientes y representar una clara ventaja competitiva. De hecho, los resultados de la última encuesta sobre tecnología realizada por KPMG a 2.100 ejecutivos del sector (KPMG, 2023)[2] mostraron que, debido al aumento significativo que genera en la tasa de éxito, hay una sólida tendencia a la integración de este principio ("seguridad desde el diseño") en la implementación de nuevas tecnologías, sobre todo en países como **Brasil** (donde el 74% de los participantes de ese país así lo aseguró).

En paralelo, teniendo en cuenta que las empresas modernas no funcionan ya como silos autónomos sino como unidades interdependientes dentro de una misma cadena de valor, y que debido a ello existe un aumento en la exposición a nuevas amenazas cibernéticas, la **modernización de la seguridad en toda la cadena de suministro** es otro de los ítems que los especialistas anteponen como prioritarios. Para mejorar la resiliencia operativa dentro de la cadena y combatir esta problemática, que, por otro lado, es propia del desarrollo de la industria y de un entorno

1. Cybersecurity considerations 2024: Technology, media, and telecommunications. Navigating innovation and threats in a hyperconnected world. KPMG, 2024
2.KPMG Global Tech Report 2023. Secure value by navigating uncertainty with confidence. KPMG, 2023

hiperconectado que privilegia la inversión en tecnología, se insta a las empresas a establecer alianzas estratégicas con proveedores que estén focalizados en el seguimiento y gestión de los riesgos, así como a ajustarse a los controles de seguridad, las normativas vigentes, y al estudio exhaustivo de un ecosistema de terceros en constante expansión, especialmente frente al peso que la inteligencia artificial (IA) está adquiriendo como generadora de valor y potenciadora de oportunidades, pero, también, de nuevas amenazas. Con el aumento de las interrupciones en la cadena de suministro, las empresas de la industria TMT que se preocupan en gestionar integralmente los riesgos, necesitan una visión clara y continua del ecosistema en el que se mueven, así como impulsar un esquema de ciberseguridad que abarque tanto a las empresas como proveedores. Y esto no solo es importante a nivel global, sino regional, desde que los ataques a la cadena de suministro representan también una amenaza palpable al crecimiento de las empresas en **Latinoamérica**, sobre todo para una industria pujante y tecnológicamente dependiente como lo es la de TMT.

Finalmente, el artículo señala la importancia de hacer que la **identidad digital sea individual, y no institucional.** Con el aumento en la dispersión de las identidades de los clientes debido al uso de múltiples dispositivos y canales de interacción, los riesgos a la seguridad aumentan exponencialmente. En este escenario, una de las soluciones posibles que la industria está planteando es la de **identidades federadas**, es decir, un mecanismo para la gestión de identidades que permite abordar esta problemática con un enfoque interdependiente, apoyado en la sincronización continua de los datos identificativos y el uso de un mismo usuario y contraseña para acceder a redes de diferentes áreas organizativas o, incluso, empresas. De este modo, las empresas pueden compartir información sin tener que dar a conocer tecnologías de directorio, seguridad y autenticación, como sí lo requieren otras soluciones. Asimismo, los especialistas en tecnología recomiendan el uso de métodos de seguridad del tipo "verificar antes, confiar después", así como aprovechar la IA y el ML para establecer medidas de verificación de identidad basadas en el comportamiento y detectar anomalías o actividades sospechosas en el proceso de autenticación. En **Latinoamérica**, por ejemplo, países como **Argentina, Brasil, México** o **Uruguay**, por mencionar solo algunos, están implementando iniciativas de gobierno con un enfoque basado en identidades digitales, lo que les ha permitido ahorrar millones de dólares en costos administrativos y posibles fraudes[3].

En términos generales, la conclusión es que **las empresas deben ver la ciberseguridad y privacidad de los datos como un activo** que, bien utilizado, ofrece una ventaja competitiva al generar un intangible escaso y altamente valorado en el complejo entorno actual: **la confianza digital de los clientes.** Para ello, la seguridad debe ser incorporada en todas las áreas de la organización y a lo largo de toda la cadena de valor de la industria, abarcando empresas, proveedores y clientes. Solo así, el sector podrá impermeabilizar su resiliencia, estar al día con las regulaciones y avanzar hacia el futuro.

3. *Casos de uso de la Identidad Digital en América Latina.* LinkedIn, 23 de febrero de 2024.

KPMG

Llegó la hora de transformar insights en oportunidades