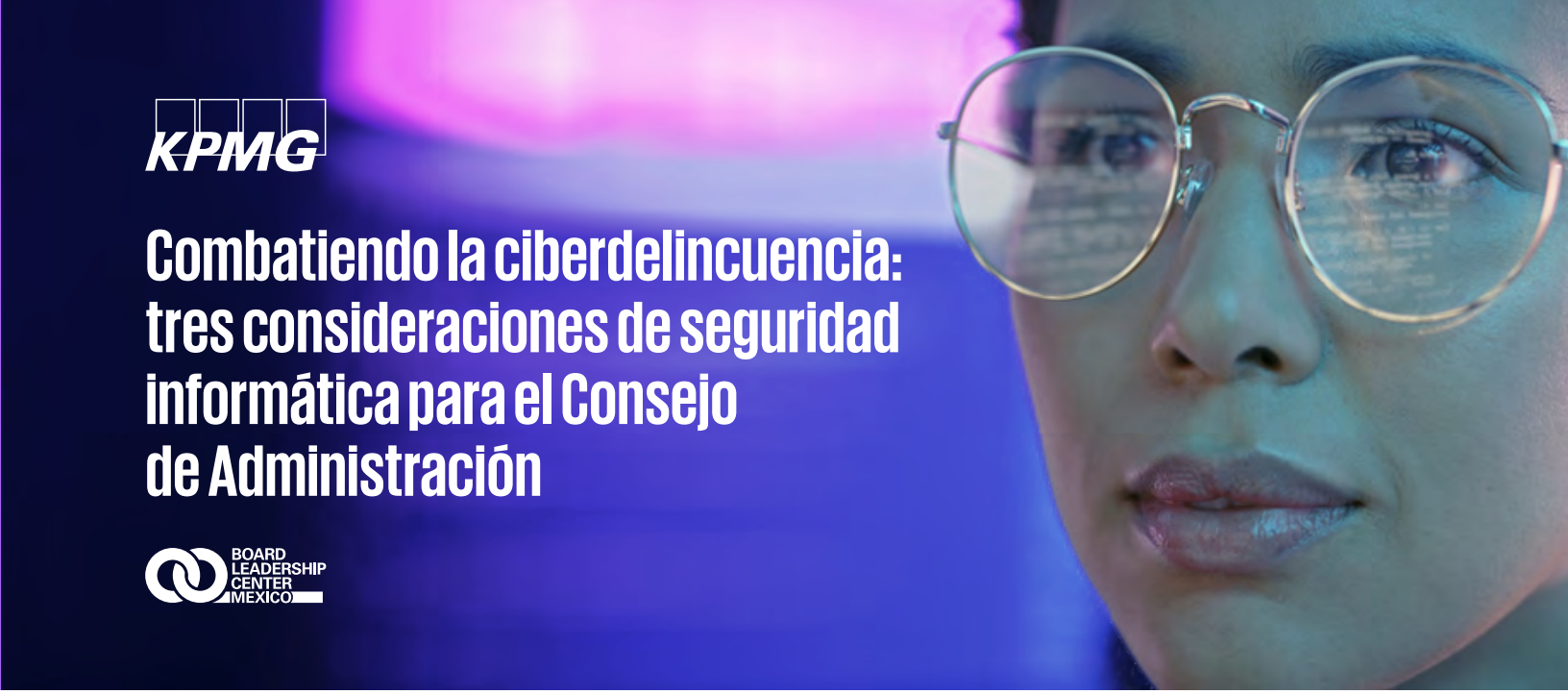
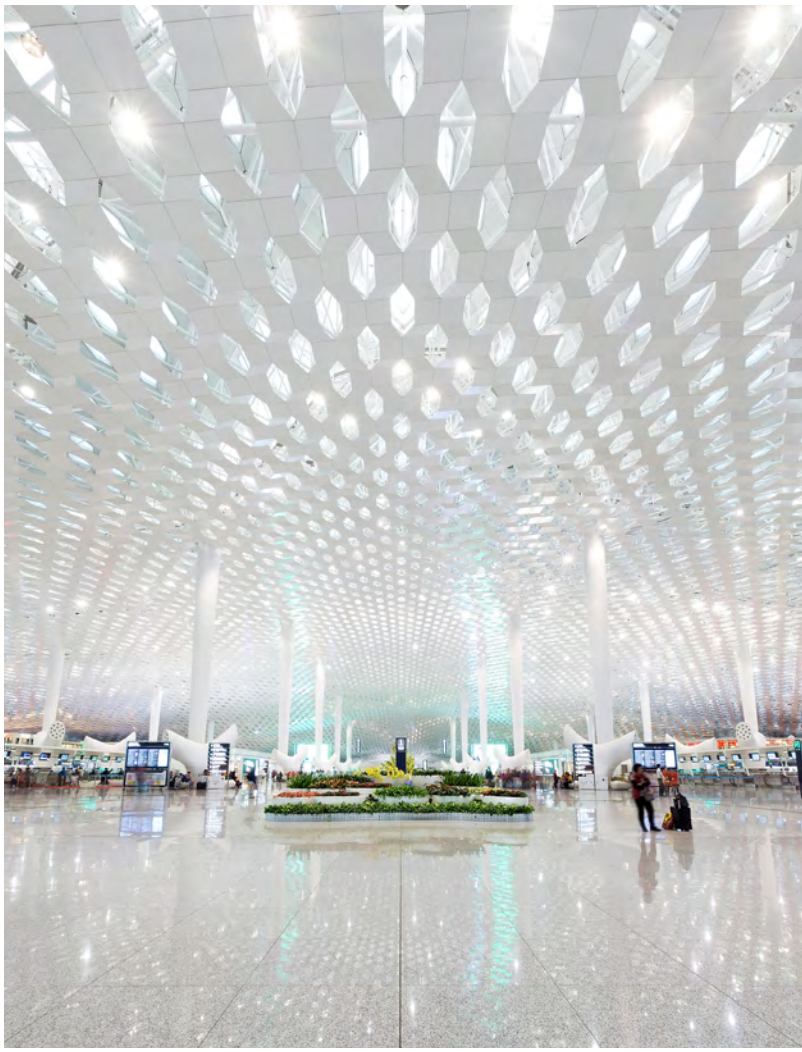


Combatiendo la ciberdelincuencia: tres consideraciones de seguridad informática para el Consejo de Administración

BOARD LEADERSHIP CENTER MEXICO

Los especialistas en tecnología se preparan ante futuros ataques cibernéticos

De acuerdo con una encuesta recientemente realizada por KPMG, ocho de cada diez ejecutivos expertos en la industria de tecnología, medios y telecomunicaciones (TMT) prevén un aumento de los riesgos cibernéticos durante 2023. No obstante, solo 39% (en México únicamente 8%) de los encuestados afirman que su empresa tiene la capacidad de identificar una vulneración o un ciberataque una semana después de que este haya sucedido, y solo 21% (5% en México) tiene la capacidad de contenerlo dentro de ese mismo plazo, a partir de su descubrimiento.[1]



Con los riesgos de vulneraciones, ataques de *ransomware*, *malware*, entre otros, las compañías de TMT tienen mucho que perder en caso de ocurrir un evento de este tipo: control sobre propiedad intelectual, información de clientes, infraestructura de red, acceso al centro de datos, su posición competitiva en el mercado y, principalmente, utilidades.

Si limitamos el alcance específicamente a las compañías tecnológicas, los riesgos operativos, reputacionales, regulatorios y financieros se vuelven aún mayores. Con estos intereses en juego, prevenir y, en su caso, mitigar el riesgo de ciberataques jamás había sido un factor tan esencial como ahora.

A partir de conversaciones con integrantes del Consejo de Administración de empresas de tecnología, así como del Comité de Auditoría y de la Administración, identificamos tres medidas clave que el Consejo debe tener en cuenta para mitigar de manera efectiva los riesgos cibernéticos.

[1] *Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook*, KPMG LLP, 2022. https://advisory.kpmg.us/articles/2022/kpmg-2022-fraud-outlook-tmt.html

Incrementar la supervisión y el grado de preparación que la Administración aplica para afrontar la creciente complejidad de las amenazas

El Consejo muestra el gran avance que ha logrado en cuanto al monitoreo y la efectividad del sistema de ciberseguridad dentro de la Administración. De acuerdo con el documento *Agenda del Consejo de Administración 2023*, el Consejo opera con una mayor experiencia en cuestiones de Tecnología de Información (TI), perfeccionando su enfoque en la forma en que la Administración implementa las herramientas de información, como reportes de paneles específicos de la compañía y la línea de negocio, a fin de identificar los riesgos y oportunidades críticos, evaluar el talento en materia de ciberseguridad, escenarios que simulen diversos ataques, entre otros.[2]

A pesar de estos avances, las amenazas se hacen cada vez más complejas, lo cual ha obligado a las compañías y al Consejo a operar en un estado continuo de recuperación. Este fenómeno se encuentra particularmente presente en el sector de tecnología, así como en el área de medios y telecomunicaciones, en donde 83% de los ejecutivos han señalado ser testigos de un aumento en la frecuencia de al menos un tipo de ciberataque durante 2021.[3]

Como sucede en diversos sectores, las empresas de tecnología son propensas a incidentes de suplantación de identidad y estafas. Sin embargo, también son especialmente vulnerables a cierto rango de ataques informáticos más complejos. De acuerdo con *KPMG 2022 Fraud Outlook*, era más probable que los ejecutivos de TMT reportaran un crecimiento en ataques de *malware* (30% en comparación con el 22% del promedio), hackeo social (23% respecto del 17% promedio) e inyección SQL[4] (18% frente al 11%), que los ejecutivos de otros sectores.

Entonces, ¿qué es lo que hace que las empresas, específicamente de tecnología, sean más vulnerables? ¿No deberían ser las compañías tecnológicamente avanzadas las más preparadas para los ciberataques? No necesariamente. Por un lado, las empresas de tecnología no solo están recolectando, almacenando y gestionando datos, sino que también los generan. Estas compañías se mantienen como líderes gracias a una innovación constante, pero ello, a su vez, las hace objeto de agentes que buscan perjudicarlas. Esto representa un conflicto a nivel de industria, ya que los delincuentes cibernéticos apuntan a múltiples compañías tecnológicas a la vez, para ver en dónde pueden instalarse antes de lanzar su ataque.

[2] *Agenda del Consejo de Administración 2023*, KPMG Board Leadership Center en México, 2023.

[3] *Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook*, KPMG LLP, 2022.

[4] Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

La vulnerabilidad en la cadena de suministro también es una cuestión clave. Las empresas de tecnología se enfrentan a una mayor responsabilidad respecto a la seguridad de sus productos, independientemente de que se trate de *software*, *hardware* o de otro tipo, a lo largo de toda la cadena de suministro, desde el desarrollo inicial de la tecnología hasta cada punto de contacto con el cliente.

En otras palabras, la responsabilidad de mitigar los riesgos informáticos no se detiene en el punto de venta. Después de todo, si un cliente compra una nueva computadora, desea tener una garantía razonable de que la compañía que se la vendió se mantendrá alerta sobre cualquier vulnerabilidad informática durante el transcurso de vida del dispositivo. Este es solo un ejemplo de cómo la protección de la cadena de suministro debe ser un factor prioritario para la Administración.

En este sentido, 79% de los ejecutivos de tecnología que respondieron la encuesta de KPMG opinan que la protección de su ecosistema de socios comerciales y la cadena de suministro son factores tan importantes como la construcción de las defensas informáticas de su propia organización.[5]

Vivimos en una época en la que las compañías se encuentran bajo un intenso escrutinio en cuanto a la forma en que protegen y utilizan los datos de sus clientes. Todos los grupos de interés, desde compradores hasta reguladores y autoridades responsables se han encargado de decirles a las compañías tecnológicas más grandes que "el hecho de que lo puedan hacer no significa que lo deban hacer". La repercusión que un ciberataque tiene en la reputación puede, incluso, sobrepasar las afectaciones de carácter financiero.

[5] *Technology companies lean on cyber to go faster and gain trust*, KPMG LLP, 2022.

A la luz de los retos descritos, el Consejo de Administración de las empresas de tecnología, así como su Comité de Auditoría, deben mejorar el control que llevan a cabo dentro de cierto número de áreas críticas, incluyendo:

- Qué tan sensible es la Administración a las señales oportunas de advertencia de ataques cibernéticos
- La medida en que la Administración incorpora las consideraciones en materia de ciberseguridad dentro del proceso de diseño de nuevos productos y sistemas internos
- Si el plan de respuesta de la compañía es sólido en caso de crisis y se encuentra listo para operar, teniendo en cuenta la pérdida potencial de la infraestructura esencial, así como los centros de datos
- La calidad de los procesos y controles establecidos en la gestión de ciberdelitos y si están a la par con el panorama de amenazas que evoluciona constantemente
- Los riesgos informáticos que plantea la cadena de suministro de la compañía
- Si tuviera lugar un ciberataque o cuando este ocurre, la capacidad de la Administración para identificar el origen del incidente en forma oportuna, eficiente y efectiva (es decir, la existencia de un defecto en los controles internos) y establecer nuevos procedimientos para evitar incidentes futuros

Al respecto, el estudio *Perspectivas de la Alta Dirección en México 2023. Capitalizar la experiencia para lograr el crecimiento* de KPMG en México, señala que la Alta Dirección considera que los ataques cibernéticos constituyen el principal riesgo de negocio que podría ocasionar impactos relevantes (tanto cualitativos como cuantitativos) en la organización con 51% (45% en 2022).

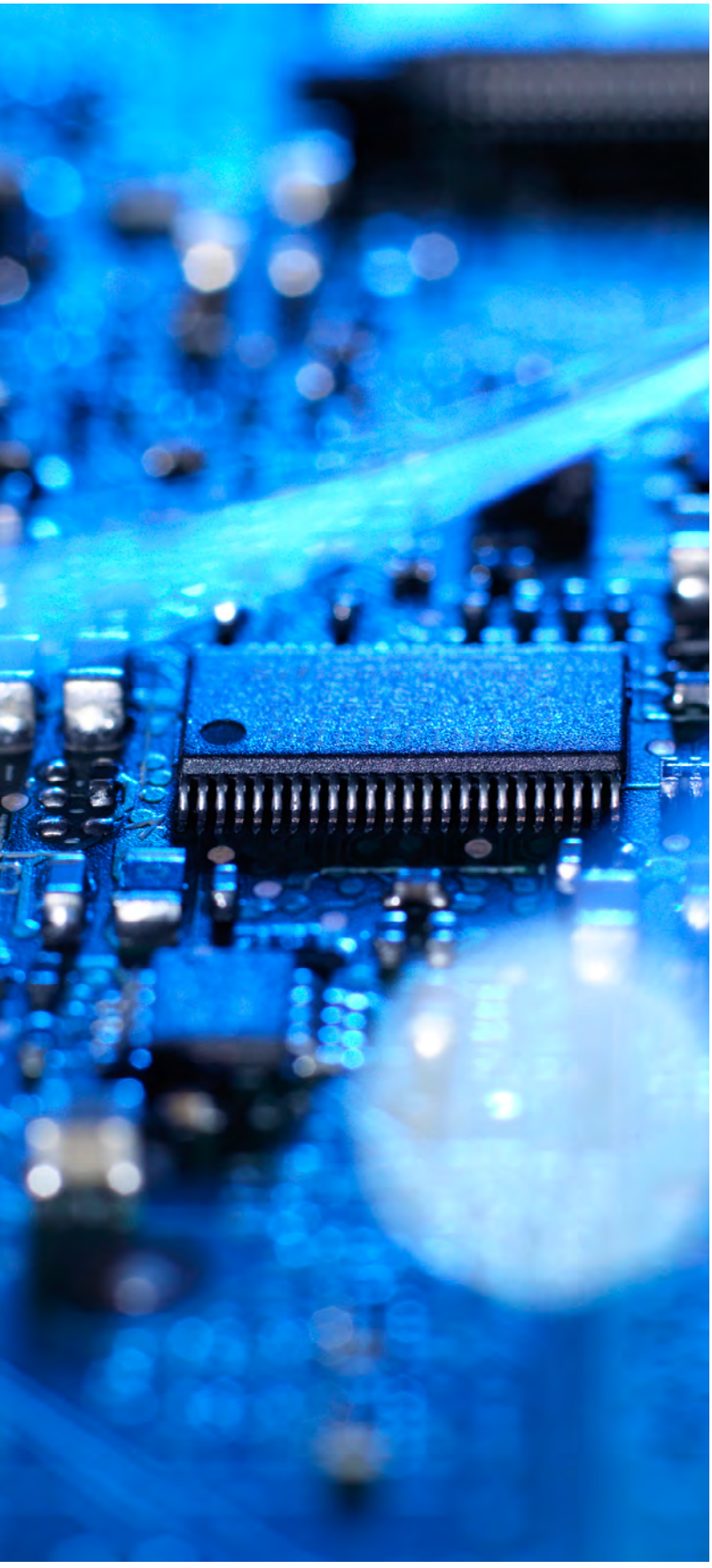
Vigilar de cerca el entorno reglamentario y realizar la planeación pertinente

Dado que las compañías de diversos sectores se enfrentan con un panorama de ciberseguridad en constante evolución, entender el impacto de los distintos riesgos informáticos en la posición financiera de la compañía resulta una misión crítica. Los incidentes en materia de ciberseguridad pueden derivar en gastos adicionales (incluyendo un aumento en las primas de seguro y responsabilidades legales), pérdidas en ingresos y una reducción en los flujos de efectivo a futuro.[6] Asimismo, no contar con controles adecuados incrementa el riesgo de procesos de litigio a largo plazo, además de los consiguientes daños reputacionales, afectando así a la compañía más allá del ejercicio actual.[7]

Los reguladores trabajan constantemente para dar mayor claridad a la relación entre el riesgo cibernético y la información financiera. De acuerdo con lo previsto en la normativa de 2018, emitida por la Comisión de Bolsa y Valores de EE.UU. (SEC), se espera que las compañías que han sufrido algún ciberdelito ofrezcan un aseguramiento razonable, sobre todo de que la información sobre el rango y la magnitud de los impactos financieros derivados del evento en cuestión se han incorporado en la información financiera de forma oportuna, a medida de que los datos estén disponibles.[8] Esto también incluye efectos futuros, tales como una reducción de ingresos, aumento en costos de litigios, ciberseguridad y costos de seguro, así como la posibilidad de que los activos se vean perjudicados.[9]

En marzo de 2022, la SEC adoptó una postura aún más firme, al proponer nuevas normas en relación con los requisitos de gestión de riesgos cibernéticos, estrategia, gobierno y revelación para compañías del sector público.[10] De ser promulgadas, las normas aumentarían la importancia de revelar la información requerida respecto a los incidentes de ciberseguridad en cierto número de presentaciones corporativas, incluyendo presentaciones anuales. También requerirían la revelación de estos eventos dentro de un plazo de cuatro días, contados a partir de la fecha en que el incidente adquiera el carácter de importante, junto con la información más detallada sobre las políticas y procedimientos de seguridad informática de las compañías, la función de la Administración en el gobierno de ciberseguridad y el nivel de control y conocimientos del Consejo.[11]

[6] *Defining Issues: SEC Issues Guidance on Cyber Security,* KPMG LLP, 2018.
[7] *Mitigating Risk in an Increasingly Digitized World,* KPMG LLP, 2022.
[8] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures,* U.S. Securities and Exchange Commission, 2018.
[9] *Defining Issues: SEC issues guidance on cyber security,* KPMG LLP, 2018.
[10] *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies,* U.S. Securities and Exchange Commission, 2022.
[11] *SEC on ESG: Proposed enhancements to cybersecurity disclosures,* KPMG LLP, 2022.



Dado que la resolución definitiva de la SEC respecto a la norma propuesta se espera para la primavera de 2023, las compañías de los diversos sectores junto con el Consejo necesitan estar preparadas. Para el Consejo de Administración de empresas tecnológicas, esto debería impulsar un mayor enfoque en aspectos clave de la compañía:

- **Normas de ciberseguridad y privacidad dentro del contexto de la información financiera.** El Comité de Auditoría debe tener una función clave, al supervisar el impacto que tenga una vulneración u otro evento informático sobre los estados financieros

- **Inventario de todas las relaciones de terceros.** Los programas de aseguramiento dedicados pueden verificar los protocolos de ciberseguridad, reforzar las relaciones con los proveedores y maximizar el cumplimiento regulatorio relacionado a lo largo de toda la cadena de suministro[12]

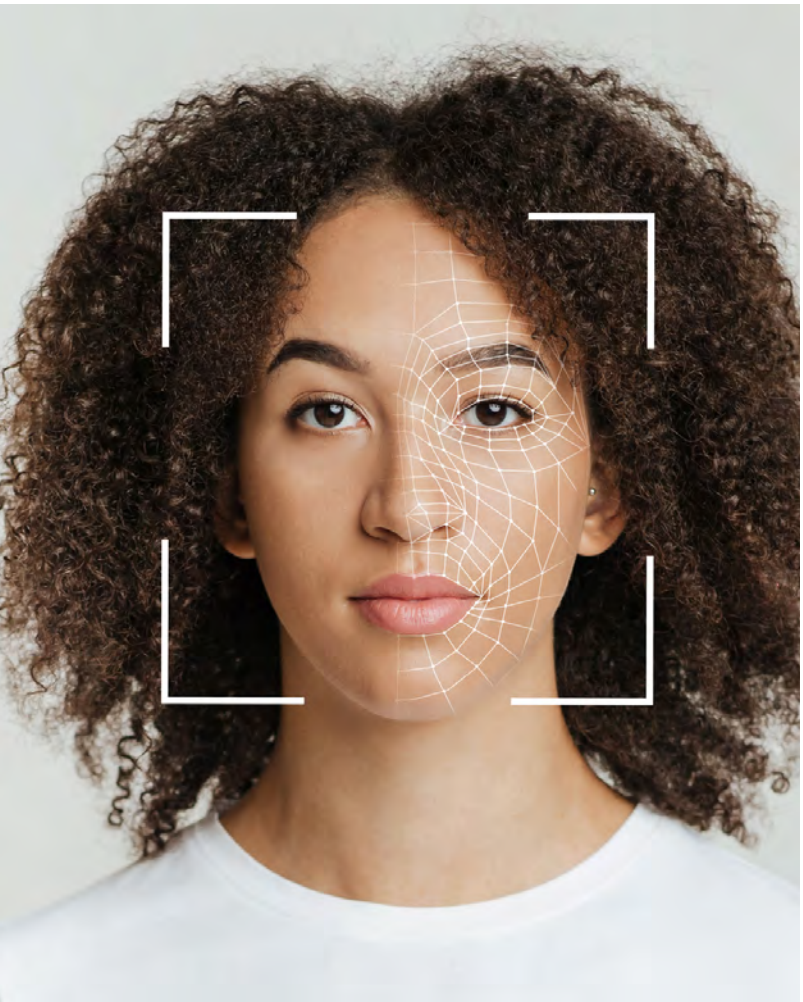
- **Evaluación de la forma en que una futura regulación informática podría impactar en el negocio.** Aunque las empresas tecnológicas ya están sujetas a una legislación exhaustiva en materia de privacidad de datos, también deben tener en cuenta el impacto de la promulgación de cualquier reglamento futuro por parte de la SEC u otro organismo gubernamental para las operaciones, estrategia y la presentación de información

- **Comprensión de quién asumirá la mayor parte del trabajo en materia de cumplimiento regulatorio.** El Consejo puede utilizar los nuevos requisitos de presentación de información de la SEC como indicador para evaluar la composición del Comité de Revelación de la compañía, asegurándose de incluir a los líderes funcionales adecuados (es decir, a la Dirección de Cadena de Suministro, Dirección de Seguridad de la Información, entre otros).[13] También pueden determinar, a nivel interno, las personas que se encargarán de monitorear el cumplimiento. Tradicionalmente, el Comité de Auditoría tiene a su cargo el control de riesgos cibernéticos; sin embargo, el aumento en la carga de trabajo para la presentación de informes de la SEC podría requerir una expansión de directores y comités adicionales[14]

[12] *Mitigating risk in an increasingly digitized world,* KPMG LLP 2022, 2022.
[13] *Agenda del Comité de Auditoría 2023,* KPMG Board Leadership Center en México, 2023.
[14] *Agenda del Consejo de Administración 2023,* KPMG Board Leadership Center en México, 2023.

Reconocer el vínculo entre la ciberseguridad y la gobernanza de datos

El riesgo informático, que antes era responsabilidad independiente del Comité de Auditoría, comienza a visualizarse bajo el marco más amplio de la gobernanza de datos. Las empresas están construyendo estrategias sólidas en materia de gobernanza de datos desde el Consejo, a fin de identificar y abordar los riesgos asociados con la ciberseguridad, privacidad y ética de datos, así como higiene digital e inteligencia artificial. Si bien, históricamente, los riesgos informáticos han sido responsabilidad del Comité de Auditoría, y claramente tiene una función continua en el control de dichos riesgos, la creciente complejidad del panorama ha ocasionado que la supervisión alcance cada vez más puntos en la agenda del Consejo. El lugar exacto donde se aborda el tema de la ciberseguridad y la importancia que tiene en el Comité depende de varios factores, como la naturaleza del negocio, el nivel actual de preparación y ciberseguridad de la empresa, el alcance de los comités del Consejo y el conjunto de habilidades únicas de los consejeros y consejeras.[15]



Para las empresas de tecnología, esta consolidación significa que el Consejo y el Comité de Auditoría deben estar dispuestos a analizar, discutir y monitorear el riesgo cibernético dentro del contexto de cuestiones más amplias de gobernanza de datos. Por ejemplo, las nuevas tecnologías, que probablemente requieran un mayor enfoque del Consejo y el Comité, que incluyen:

- ***Software* de reconocimiento facial**: ¿cómo se recolectan los datos de reconocimiento facial? ¿Dónde se almacenan? ¿Cuáles son los conflictos de privacidad asociados y cómo los está mitigando la Administración?

- **Inteligencia artificial y aprendizaje automático**: ¿cuáles son las consideraciones éticas? Conforme la tecnología avanza y se adapta, ¿qué sesgos se encuentran implícitos y cómo los aborda la Administración? ¿Qué riesgos de cumplimiento regulatorio y de reputación se generan debido al uso de esta tecnología por la compañía?

En última instancia, la forma en que el Consejo y la Administración colaboran para abordar los conflictos de gobernanza de datos constituye la base para la certidumbre digital: la confianza que los grupos de interés tienen en la capacidad de la organización para aprovechar la tecnología digital a fin de proteger sus intereses y preservar las expectativas de los socios.[16] Como lo hemos visto en incontables ocasiones, a escala nacional y global, el no poder preservar la confianza digital trae repercusiones perjudiciales a nivel financiero, reputacional, legal, entre otros.

[15] *Oversight of cybersecurity and data governance,* KPMG LLP, 2021.
[16] *Cyber trust insights 2022,* KPMG LLP, 2022.

La responsabilidad y la mitigación son factores esenciales

Hoy en día, las empresas de tecnología deben permanecer alerta para detectar vulnerabilidades. Los riesgos cibernéticos, informáticos, de privacidad, así como otros relativos a la gobernanza de datos, causan estragos a lo largo de todo el sector. Independientemente de que surjan en las etapas iniciales de innovación de producto o durante la recolección y almacenamiento de datos de los clientes, durante el aprendizaje automático o a lo largo de la cadena de suministro, los integrantes del Consejo de las organizaciones tienen mucho trabajo por delante, a fin de anticipar y colaborar con la Administración para mitigar estos riesgos.

El Consejo debe asegurar que la Administración asuma la responsabilidad por la acción o falta de acción, y deberá ayudar a que la función de liderazgo envíe y refuerce el mensaje de que la seguridad de la compañía es responsabilidad de cada empleado. La capacitación del talento, la incorporación de las mejores prácticas de gobernanza de datos en la cultura de la compañía y la creación de puntos de contacto regulares entre el Consejo y la función de Tecnología son elementos integrales para el éxito. No existe un enfoque único para todos. En su lugar, los líderes afirman que "es tarea de todos", incluyendo a profesionales calificados que evalúen e identifiquen continuamente las amenazas emergentes y desarrollen programas integrales para hacerles frente.[17]

Dado el ritmo vertiginoso de la innovación en el sector tecnológico, es una tarea compleja. No obstante, si las empresas de tecnología establecen hoy una sólida estrategia de gestión de los riesgos informáticos, podrán disfrutar de una considerable ventaja competitiva en el futuro, que consolide o incremente su reputación y brinde certeza sobre los riesgos operativos, financieros y la generación de informes oportunos.

[17] *Technology companies lean on cyber to go faster and gain trust,* KPMG LLP, 2022.

Acerca de KPMG Board Leadership Center en México

Es un programa global con presencia local exclusivo para miembros del Consejo de Administración en México, que tiene como objetivo promover un gobierno corporativo efectivo para impulsar el valor de la empresa a corto, mediano y largo plazo, generando confianza en los *stakeholders* de las organizaciones.

kpmg.com.mx
800 292 5764 (KPMG)
blc@kpmg.com.mx

KPMG MÉXICO · KPMG MÉXICO · @KPMGMEXICO · KPMGMX