



# Actualizaciones trimestrales: abril 2024



## Una mirada hacia el futuro

La primera mitad del año representa una oportunidad para que el Consejo de Administración haga una pausa y reevalúe su agenda, con el objetivo de garantizar un enfoque adecuado en los temas críticos para las organizaciones.

Dada la creciente amplitud y complejidad de asuntos como la volatilidad e incertidumbre del entorno empresarial, así como sus posibles riesgos, vale la pena preguntarse si el Consejo asigna las responsabilidades correspondientes de supervisión de forma eficaz y si además se le dedica el tiempo necesario a esta labor, pues es importante prever escenarios futuros.

En este sentido, a medida que el Consejo y el Comité de Auditoría acotan estas prioridades dentro de sus agendas, destacamos los puntos críticos que deben considerarse en las discusiones durante el año, tales como:

- Actualización sobre informes financieros y de auditoría para conocer las principales conclusiones de la conferencia del Instituto Americano de Contadores Públicos Certificados (AICPA, por sus siglas en inglés) y el Instituto Colegiado de Contadores Gerenciales (CIMA, por sus siglas en inglés) sobre los más recientes acontecimientos de los reguladores en EE.UU. concernientes a los requisitos y obligaciones sobre la emisión de información climática y de sostenibilidad, entre otros indicadores ambientales, sociales y de gobierno corporativo (ASG)
- Impacto de las reglas fiscales del Pilar II dentro del marco inclusivo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)

Además, en esta edición también abordaremos los aspectos clave sobre la supervisión, la gestión de riesgos y el entorno de control, incluyendo la independencia entre el Comité y la firma de auditoría, así como las áreas de enfoque para el monitoreo del Consejo a fin de mantener programas efectivos de gestión de riesgos ante el cambiante panorama normativo y de cumplimiento regulatorio.

## Actualización sobre la emisión de informes financieros y de auditoría

### Conclusiones de la Conferencia AICPA y CIMA 2023

En diciembre, el AICPA y el CIMA organizaron una conferencia anual sobre los últimos acontecimientos de la Comisión de Bolsa y Valores de Estados Unidos (SEC, por sus siglas en inglés) y del Consejo de Supervisión Contable de Empresas Públicas (PCAOB, por sus siglas en inglés), con actores clave involucrados en la estructuración de informes financieros. Algunas de las principales conclusiones de este encuentro fueron:

#### 1. Relevancia de una cultura organizacional enfocada en generar y mantener la confianza

Los representantes de la SEC destacaron la importancia que esto tiene dentro de la firma de auditoría, mientras que el PCAOB señaló la responsabilidad compartida entre el Comité de Auditoría, la Alta Dirección y otras figuras en el ecosistema de información financiera para mantener la función de supervisión del auditor.

## 2. Generación eficiente de informes a través de la evaluación de riesgos

Es esencial que las empresas adopten un enfoque holístico en el tema, tomando en cuenta los riesgos de nivel entidad y los que afectan directamente a la información financiera. Los comités de auditoría deben ayudar a garantizar que los procesos de evaluación de riesgos y las revelaciones de la Administración sean sólidos y se comuniquen adecuadamente junto con los puntos de incertidumbre que enfrenta la compañía.

## 3. El papel crucial del Comité de Auditoría

Los representantes de la SEC alentaron a los comités de auditoría a comprometerse con el auditor independiente (formal e informalmente) de manera directa para promover el ejercicio del escepticismo profesional por parte del auditor, particularmente en las áreas de evaluación de riesgos y ciberseguridad.

## 4. Cuestionamientos ante la actualización de normas contables (ASU, por sus siglas en inglés)

Respecto a la nueva norma de información por segmentos del Consejo de Normas de Contabilidad Financiera (FASB, por sus siglas en inglés), el personal de la SEC señaló que las medidas adicionales de ganancias o pérdidas reveladas en los estados financieros pueden ser métricas Non-GAAP, a las cuales aplican sus normativas.

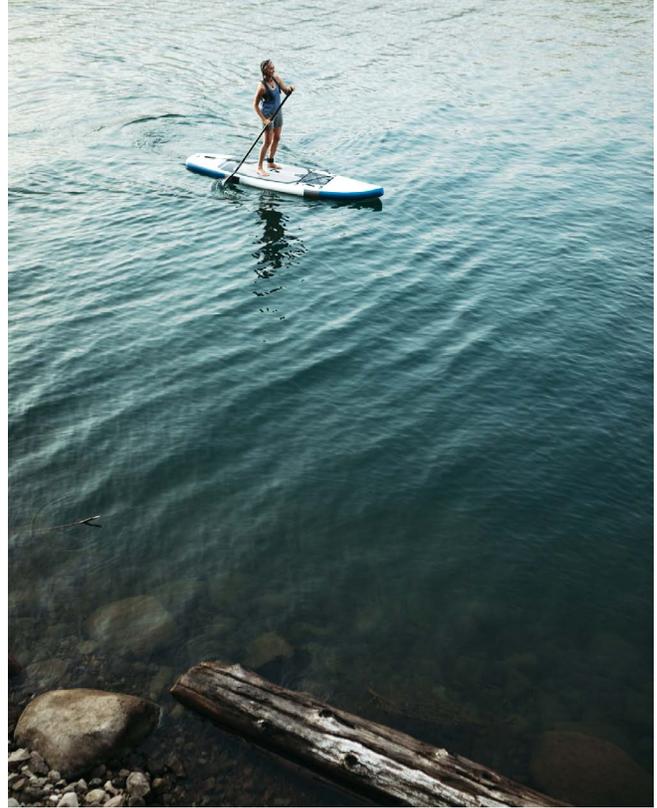
## 5. Inquietud sobre informes referentes al flujo de efectivo

Es importante considerar que no todas las empresas tienen procesos y controles rigurosos al mismo nivel que aquellos relacionados con otros estados financieros, por lo que los errores de clasificación deben evaluarse.

## 6. Inteligencia artificial generativa (IAGen)

Si bien se prometen mejoras en el uso de esta tecnología, como incrementar la velocidad y calidad en la elaboración de informes financieros, habrá nuevos requerimientos concernientes al gobierno corporativo, control interno y técnicas de auditoría para garantizar que estos elementos se utilicen de manera responsable.

Adicional a estos factores, se abordaron algunos puntos críticos sobre las nuevas reglas referentes a compensaciones y desempeño, así como métricas Non-GAAP, revelaciones sobre administración, discusión y análisis de datos.



## Actualización sobre informes ASG

En ausencia de una norma climática definitiva por parte de la SEC, surgen preguntas sobre los requerimientos dentro de los informes ASG, incluyendo si estarán relacionados con las nuevas leyes de revelación climática de California, en el caso de empresas con operaciones en EE.UU., y si tienen obligaciones legales de información en la Unión Europea (UE).

### Obligaciones legales de relevación fuera de EE.UU.

Algunos países están debatiendo si deben incorporar los lineamientos del Consejo de Normas Internacionales de Sostenibilidad (ISSB, por sus siglas en inglés) a los requisitos locales y cómo hacerlo, ya que estos exigen la revelación a los diferentes grupos de interés sobre riesgos y oportunidades. Entre los territorios que han mostrado interés en aplicarlos se encuentran: Brasil, Japón, Canadá y Reino Unido.

### Operaciones en la UE

Muchas empresas fuera de la región reportan bajo el enfoque de la Directiva sobre Informes de Sostenibilidad Corporativa (CSRD, por sus siglas en inglés) en virtud de los valores cotizados bajo las regulaciones de la UE o para mantener actividades sustanciales en ella.

El 1 de enero de 2024, los informes de sostenibilidad relacionados con las Normas Europeas de Información sobre Sostenibilidad (NEIS) entraron en vigor, y en ellas se establece la revelación de informes exhaustivos sobre riesgos y oportunidades a las partes interesadas sobre los aspectos materiales, es decir, la doble materialidad.



## Reglas fiscales del Pilar II

Las reglas globales anti-erosión (GloBE, por sus siglas en inglés) o del Pilar II entraron en vigor en enero de 2024 y se espera que tengan un impacto significativo en las empresas, particularmente en las funciones de Impuestos, Finanzas, Contraloría, Tecnologías de la Información (TI) y Auditoría Interna.

En este sentido, las organizaciones que cotizan en la bolsa de EE.UU. deberán informar sobre los efectos previstos del Pilar II en su provisión del impuesto sobre la renta (ISR) del primer trimestre de 2024 y considerar las obligaciones de revelación de la SEC del formulario 10-K de 2023, por lo que es prioritario que las multinacionales tengan una estrategia para cumplir con los siguientes requisitos:

1. Identificar qué entidades legales y jurisdicciones se verán afectadas
2. Evaluar si alguna calificará para hacer una transición segura país por país
3. Determinar si se adeudarán impuestos complementarios en función de los resultados previstos

Es muy probable que la implementación del Pilar II tenga un impacto en el proceso de auditoría externa, durante el cual se puede reevaluar la estrategia de implementación prevista (incluyendo los elementos mencionados), controles internos, datos y tecnología, abordando también si se ha utilizado o desarrollado algún modelo específico del Pilar II.

También, se espera que la persona responsable de la auditoría ejecute procedimientos independientes para verificar la información y montos utilizados, y determinar el impacto en los estados financieros.

## Responsabilidades de supervisión del Consejo en la gestión de riesgos sobre terceros

El aumento del daño reputacional en las empresas por incumplimiento de expectativas de vendedores, proveedores, servicios en la nube, consultores, canales de distribución, entre otros, ha fomentado que la Dirección General se enfoque en los programas de gestión de riesgos de terceros (TPRM, por sus siglas en inglés), ya que plantean la misma gama compleja y cambiante de riesgos a los que se enfrentan las organizaciones. Además, las compañías han desarrollado programas sólidos de TPRM, logrando alinearlos al entorno desafiante, incluyendo las regulaciones y el cumplimiento.

A medida que el Consejo supervisa los esfuerzos de la Administración para mantener la efectividad de estas medidas, las áreas clave de enfoque deberán puntualizar lo siguiente:

### 1. Riesgos de ciberseguridad y privacidad de datos

De acuerdo con un estudio realizado por KPMG,<sup>1</sup> actualmente, los riesgos de ciberseguridad y privacidad de datos de terceros se encuentran entre los principales retos en aumento, derivado de la creciente sofisticación de los ataques de *ransomware* que incorporan el uso de IAGen.

En este sentido, un reciente informe del Foro Económico Mundial (WEF, por sus siglas en inglés) señala que realizar un monitoreo continuo y tener visibilidad para identificar posibles riesgos y problemas de ciberseguridad de terceros es clave, lo que requiere aprovechar la automatización, alinear las evaluaciones de control interno, externo y de terceros, así como comprender cómo la Alta Dirección está mejorando la gestión de amenazas en tiempo real.<sup>2</sup>

<sup>1</sup> *Third-Party Risk Management Outlook 2022*, KPMG International, 2022.

<sup>2</sup> *Global Cybersecurity Outlook 2023*, World Economic Forum, 2023.

Por lo anterior, las recientes normas de seguridad cibernética de la SEC exigen una mayor revelación en la materia, incluyendo si la empresa cuenta con los procesos necesarios de supervisión e identificación de amenazas correspondientes al uso de cualquier proveedor de servicios externo.

Aunque las reglas finales no eximen a las organizaciones de proporcionar información sobre incidentes en los sistemas de terceros, estas no están obligadas a realizar consultas adicionales fuera de sus canales habituales de comunicación con proveedores externos, de acuerdo con sus controles y procedimientos de revelación;<sup>3</sup> no obstante, el Consejo debe confirmar que la Dirección General cuenta con planes de comunicación eficaces con los proveedores de servicios externos que promuevan la evaluación y revelación oportuna de los incidentes materiales de ciberseguridad.

Sin duda, este tema plantea riesgos de cumplimiento, por lo que las empresas deben monitorear los acontecimientos de privacidad de los datos legales y normativos a nivel global, y en caso de que los terceros tengan acceso a datos personales, deben asegurarse de contar con los controles necesarios para gestionarlos de acuerdo con las leyes, reglamentos y políticas de privacidad de datos.

## 2. Riesgos sobre el uso de herramientas de IA

Hoy en día, las empresas reconocen la necesidad de abordar los crecientes riesgos asociados con el uso o integración de herramientas de IA de terceros.

Como resultado, las empresas deben reevaluar su estructura y procesos de gobierno corporativo sobre el uso de esta tecnología, así como su desarrollo, protección de sistemas y modelos, incluyendo el de herramientas de IAGen de terceros.

También es necesario identificar qué riesgos de cumplimiento normativo y reputación plantean el uso de herramientas de IAGen y cómo puede mitigarlos la Alta Dirección.

## 3. Riesgos relacionados con factores ASG

Las demandas de grupos de interés sobre contar con revelaciones de mayor calidad en materia ASG impulsan a los consejos a centrar su atención en esfuerzos para poder gestionar adecuadamente los posibles riesgos en la cadena de suministro.

Para lograrlo, se deben monitorear los acontecimientos normativos de los reguladores, así como cumplir con nuevos mandatos de revelación, lo que incluye obligatoriamente dar a conocer el impacto del cambio climático en la cadena de suministro, datos sobre emisión de gases de efecto invernadero (GEI) de alcance 3 y una serie de riesgos de sostenibilidad y temas de índole social como los derechos humanos y el trabajo forzado.

Además, mientras se esperan las reglas finales de la SEC sobre la revelación de información asociada al clima, las empresas de diversas jurisdicciones deben monitorear y mantener el cumplimiento de otras regulaciones, como las del ISSB y las NEIS.

La recopilación y el cálculo de los datos de emisiones de GEI de alcance 3, supondrán un reto importante por el número de terceros involucrados en la cadena de suministro, ya que dichos datos están fuera del control de la empresa, por lo que se deberá planificar una recolección de cálculos de calidad.

## 4. Proyectos de la Alta Dirección sobre la vulnerabilidad del negocio: mejorar la resiliencia y sostenibilidad

En los últimos años, las organizaciones han enfrentado retos operativos y comerciales sin precedentes. Por ello, se llevan a cabo iniciativas para reducir los riesgos en la cadena de suministro mediante la adopción de un enfoque que comprenda la función que desempeñan los terceros en la entrega de bienes y servicios e identificando las vulnerabilidades de estas dependencias para mejorar su resiliencia y sostenibilidad.



<sup>3</sup> Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, SEC, 2023.

Los proyectos varían según la empresa y pueden incluir la actualización de los planes de continuidad y recuperación ante desastres, la diversificación de la base de proveedores, la reevaluación de la estructura de la cadena de suministro, así como el desarrollo de más cadenas locales y regionales. También debe considerarse el despliegue de tecnología para mejorar la visibilidad de las operaciones comerciales y la gestión de riesgos, sin olvidar la mejora de programas de ciberseguridad y el desarrollo de planes para hacer frente a futuras interrupciones.

A corto plazo, el Consejo debe ayudar a garantizar que los proyectos para repensar, reelaborar o restaurar las operaciones por parte de la Dirección General se lleven a cabo de manera efectiva. Es importante destacar que, dada la complejidad de este proceso, es fundamental que la empresa mantenga una visión y estrategia general para gestionar la cadena de suministro en el contexto de riesgo amplio, por lo que es esencial contar con un liderazgo enfocado en conectar puntos críticos y en una rendición de cuentas precisa.

#### 5. Preguntas clave para el Consejo de Administración

La creciente complejidad y variedad de riesgos de terceros plantea un importante desafío de supervisión, por lo que inversionistas, reguladores, empresas evaluadoras de temas ASG y otras partes interesadas, exigen revelaciones de mayor calidad sobre estos desafíos y sobre cómo los consejos y sus comités supervisan la gestión relacionada, por lo que deben plantearse las siguientes preguntas:

- ¿Las personas responsables de gestionar riesgos específicos comprenden el alcance y magnitud del riesgo gestionado por terceros? ¿Esto se gestiona y controla de acuerdo con las políticas de la empresa?
- ¿La Alta Dirección cuenta con un inventario de riesgos clasificados por nivel sobre los servicios críticos que proveen terceros, incluyendo los subcontratistas?
- ¿Con qué frecuencia el Consejo solicita actualizaciones sobre el riesgo de terceros? ¿Cómo se gestiona la información? ¿Los datos están disponibles en tiempo real?
- Dentro del Consejo, ¿dónde debe ubicarse la supervisión del riesgo de terceros? ¿Es responsabilidad de todo el Consejo, el comité de riesgos u otro comité? ¿El Comité de Auditoría es responsable de los riesgos de la cadena de suministro desde el diseño o por defecto?
- ¿Se aborda el programa TPRM de manera holística, como una actividad de toda la empresa? ¿Se integra de manera efectiva con las funciones de gestión de riesgos y cumplimiento?
- ¿El equipo del TPRM y otras funciones tienen el talento, financiamiento y tecnología necesarios?
- ¿Cuándo debe participar el Consejo en la supervisión y aprobación de servicios grandes o complejos que involucran a terceros?



#### 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



Las declaraciones realizadas en este informe y los estudios de casos relacionados se basan en los resultados de nuestra encuesta y no deben interpretarse como una aprobación de KPMG a los bienes o servicios de las empresas.

Es posible que algunos o todos los servicios descritos en este documento no estén permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.

La información aquí contenida es de naturaleza general y no tiene el propósito de abordar las circunstancias de ningún individuo o entidad en particular. Aunque procuramos proveer información correcta y oportuna, no puede haber garantía de que dicha información sea correcta en la fecha en que se reciba o que continuará siendo correcta en el futuro. Nadie debe tomar medidas con base en dicha información sin la debida asesoría profesional después de un estudio detallado de la situación en particular.

© 2024 KPMG Cárdenas Dosal, S.C., sociedad civil mexicana y firma miembro de la organización mundial de KPMG de firmas miembros independientes afiliadas a KPMG International Limited, una compañía privada inglesa limitada por garantía. Todos los derechos reservados. Prohibida la reproducción parcial o total sin la autorización expresa y por escrito de KPMG.