

EY Center for Board Matters

Temas de Directorio

Las prioridades y megatendencias que los directores deben abordar.

The EY logo consists of the letters 'EY' in a bold, white, sans-serif font. Above the 'Y' is a yellow chevron shape pointing to the right.

Building a better
working world



Temas de Directorio

Edición trimestral

03 Agenda del directorio

Como la agenda del directorio se está volviendo más compleja, los directores deben mantenerse al tanto de los principales temas que afectan a las empresas.

Conozca cuáles son las ocho prioridades para abordar la situación actual.

20 Cómo los directorios pueden usar las megatendencias para trazar un nuevo rumbo

De la supervisión a la previsión: los directorios deben adoptar una mentalidad orientada al futuro para reducir el riesgo de perderse el próximo gran acontecimiento.

Analizamos las cuatro megatendencias que más impactarán al quehacer de la junta directiva.

29 Revelaciones de las empresas sobre supervisión y riesgos de ciberseguridad en 2020

El riesgo de ciberseguridad se está intensificando, especialmente con el trabajo a distancia generalizado y el aumento de las interacciones en línea en medio de la pandemia.

Conozca las tendencias respecto de cómo las empresas de EE.UU. están informando a sus stakeholders los temas relacionados a ciberseguridad.



Agenda del Directorio

Ocho prioridades para los directorios a la hora de abordar el escenario actual.

Como la agenda del directorio se está volviendo más compleja, los directorios deben mantenerse al tanto de los principales temas que afectan a las empresas.

El Covid-19 es el mayor reto al que se ha enfrentado la mayoría de los directorios. La pandemia los está forzando a moverse en un ambiente de negocios extremadamente difícil y a cambiar de dirección rápidamente en respuesta a una serie de escenarios inesperados.

Sin embargo, éste no es el único desafío que los directorios enfrentan hoy en día. En su capacidad de supervisión, se espera que aborden una amplia gama de otros asuntos.

Estos abarcan desde las preocupaciones de siempre, como el establecimiento de estrategias, la participación de las partes interesadas y la aprobación de los objetivos y la remuneración de los ejecutivos, hasta los desafíos complejos y de gran escala que son oportunos por su naturaleza, como el cambio climático, la transformación digital y los delitos financieros.

Con tanto que considerar, puede ser difícil para los directorios identificar las áreas que más necesitan su atención. Por esta razón, el Centro EY para Temas de Directorio elaboró la Agenda del Directorio para los próximos meses. Además del Covid-19, la publicación identifica otros siete asuntos de gobierno corporativo que creemos deberían ser las prioridades estratégicas de los directorios y comités de auditoría en los próximos meses. Las prioridades sugeridas no están clasificadas por orden de importancia, ya que su significado variará según el país, la organización y el sector. No obstante, todas ellas requieren al menos cierta consideración por parte de los directorios.

Capítulo 1

Covid-19: enfrentarse a los desafíos de supervisión que plantea la pandemia

En un período de crisis, ¿cuál es la estrategia del directorio para ayudar a la organización a desenvolverse ahora, en el futuro y más allá?

La pandemia plantea riesgos significativos para casi todos los aspectos de las operaciones de una empresa. Inevitablemente, el Covid-19 exige que los directorios realicen una gran cantidad de intervenciones para resolver crisis a corto plazo.

Sin embargo, al mismo tiempo, la pandemia tiene repercusiones de largo alcance para las organizaciones en lo que respecta a sus modelos comerciales, las relaciones con las partes interesadas, las prácticas laborales y las estructuras de la fuerza de trabajo. Por esta razón, es crucial que los directorios tengan muy presente la perspectiva a mediano y largo plazo al tratar cualquier asunto urgente que surja.

Para sortear la incertidumbre permanente y la falta de visibilidad hacia el futuro, se beneficiarán de la evaluación continua de los planes de continuidad de negocio y de contingencia de su organización.

Los directorios deben tener presente que la forma en que su organización respondió a la crisis de Covid-19 será recordada por todas las partes interesadas en los años venideros.

Dependiendo del sector de la organización, los temas que los directorios podrían querer explorar, en conjunto con la gerencia, incluyen la recontractación de la fuerza de trabajo después de un período de permiso o de trabajo a distancia, volver a iniciar cualquier operación que se haya detenido por la crisis y la adaptación de las ofertas a los clientes para satisfacer las nuevas demandas. La solvencia de la organización será una preocupación primordial para varios directorios.

En vista de la grave recesión económica en la que nos encontramos, los directorios querrán saber qué están haciendo los equipos de gestión para restablecer las expectativas de las partes interesadas en áreas como los salarios, los presupuestos, las condiciones de pago y la gestión de la cadena de suministro. Ellos mismos tendrán que tomar decisiones delicadas sobre el pago de dividendos.

En cada decisión que tomen, los directorios deben tener presente que la forma en que su organización respondió a la crisis de Covid-19 será recordada por todas las partes interesadas en los años venideros.

Preguntas a considerar por el directorio

1. ¿Cómo apoya el directorio al equipo de gestión de la organización para afrontar la crisis de Covid-19? ¿Existen oportunidades de mejorar los canales de comunicación y de informar sobre parámetros adicionales para que el directorio pueda supervisar de mejor manera la exposición y la respuesta de la organización a las disrupciones relacionadas con las crisis?
2. ¿Qué medidas deben adoptarse ahora, a corto plazo y en adelante, para asegurar que la organización siga siendo viable en el futuro previsto? ¿Cómo pueden los miembros del directorio trabajar eficazmente con el equipo de gestión para reajustar y perfeccionar la estrategia durante un período de rápidos cambios?
3. ¿El equipo de gestión dispone de recursos suficientes y de las competencias adecuadas para sortear con éxito a las nuevas amenazas, o es necesario recurrir a expertos externos en ámbitos específicos como la ciberseguridad y la gestión de la cadena de suministro?
4. ¿Cómo puede el directorio garantizar que la organización evolucione durante la crisis actual de manera que esté bien situada para capitalizar la recuperación y las nuevas oportunidades de mercado a medida que vayan surgiendo?
5. ¿Cómo puede el directorio asignar el tiempo, de manera eficaz, para garantizar que tanto los problemas urgentes como los asuntos estratégicos futuros sean lo suficientemente atendidos y en consonancia con el sentido de propósito de la organización?



Capítulo 2

Propósito e integridad: nuevas formas de fortalecer y enfocar la toma de decisiones del directorio

¿Cómo puede el directorio apoyar a la organización para activar y articular su sentido de propósito?

Las empresas que cumplen con su propósito, mientras actúan con integridad, son más proclives a mejorar sus marcas y reputaciones y a construir relaciones sólidas con los clientes. También tienen más probabilidades de innovar con éxito, mitigar el riesgo, atraer y retener el talento, entre otros beneficios. En consecuencia, están bien situados para lograr un valor a largo plazo para una amplia gama de partes interesadas clave, lo que se traducirá en un sólido rendimiento financiero durante un período de tiempo sostenido.

El directorio tiene la responsabilidad, en su función de supervisión, de considerar cómo puede apoyar a la organización para activar y articular su sentido de propósito.

Un buen punto de partida es hacer preguntas importantes al equipo de gestión, como por ejemplo, ¿cuál es, según el equipo de gestión, el propósito principal de la empresa? ¿Cómo se utiliza el propósito de la empresa para informar la toma de decisiones e influir en las prácticas de trabajo en todas las áreas del negocio? ¿Cómo podría cambiar el propósito de la empresa en respuesta al Covid-19?

El directorio tiene la responsabilidad, en su función de supervisión, de considerar cómo puede apoyar a la organización a activar y articular su sentido de propósito

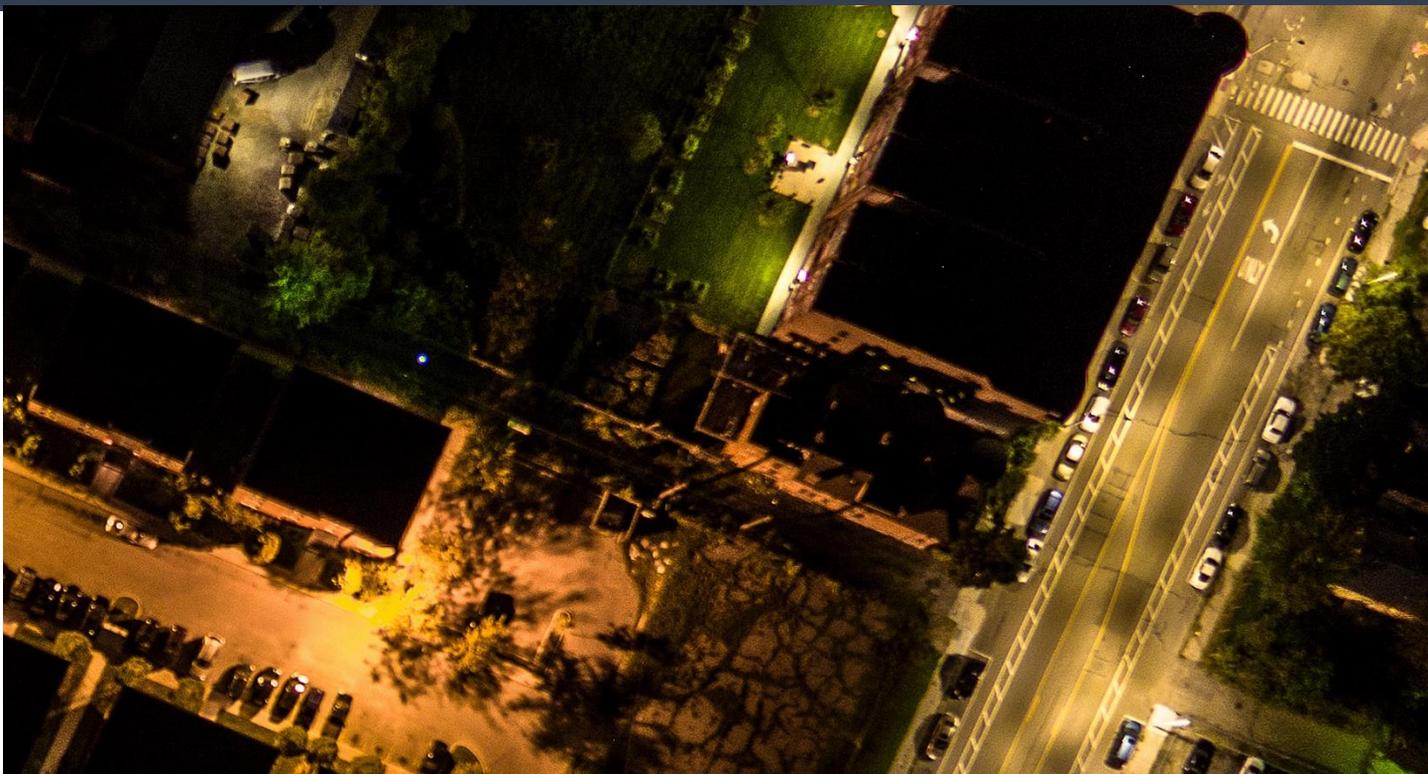
Cuando se cuestiona al directorio, vale la pena hacer consultas específicas sobre las políticas ambientales de la empresa, las prácticas de derechos humanos, las comunicaciones con los empleados y las relaciones con los proveedores. También son dignos de consideración los incentivos utilizados en los planes de remuneración.

Para que los directorios puedan supervisar eficazmente el propósito de su organización, deben estar compuestos por las personas adecuadas y contar con las estructuras de comité apropiadas. Puede ser necesario incorporar nuevos miembros al directorio que cuenten con competencias y habilidades especializadas.

Por otra parte, podría ser apropiado establecer un comité que se dedique a supervisar la forma en que el equipo de gestión adopta una ética empresarial responsable, que esté alineada con el propósito principal de la empresa.

Preguntas a considerar por el directorio

1. ¿Qué tan bien comprenden el directorio y el equipo de gestión el propósito principal de la organización, y qué tan bien la organización expresa ese propósito claramente a sus interesados?
2. ¿Cómo se refleja el propósito principal de la organización, tal como se ha comunicado, en la forma en que ejecuta su estrategia?
3. ¿Cómo repercute el propósito de la organización, tanto positiva como negativamente, en la sociedad, la economía y el medio ambiente? ¿Y cuáles son las posibles consecuencias de este impacto para la organización?
3. ¿Cómo hace el equipo de gestión para activar el propósito principal de la organización en el contexto de sus actividades cotidianas?
4. ¿Qué tan bien está constituido el directorio para evaluar el desempeño de la organización en relación con su propósito principal? ¿Hasta qué punto las actividades y el enfoque del propio directorio son coherentes con ese propósito?



Capítulo 3

Cambio climático y sostenibilidad: de lo ambiental, social y de gobierno corporativo (ESG¹) a una sólida estrategia de negocios

¿Su directorio considera el cambio climático y otros asuntos relacionados con la sostenibilidad en su toma de decisiones?

Los directorios tienen la responsabilidad de interés público de hacer que sus empresas sean más sostenibles. Las partes interesadas, incluidos los encargados de la formulación de políticas a nivel mundial, los reguladores, los inversionistas y el público en general, esperan que aborden los desafíos mundiales.

Además, el Covid-19 ha puesto de relieve cómo las principales amenazas al bienestar humano pueden alterar gravemente las operaciones comerciales.

La prioridad de los directorios es comprender cómo los riesgos y oportunidades asociados al cambio climático y los asuntos sociales podrían afectar a su compañía.

También deberían alentar a los equipos de gestión a considerar cómo pueden ajustarse las operaciones y el modelo de negocios de la

La sostenibilidad puede ser una oportunidad para que la empresa se vuelva más competitiva, eficiente y resiliente que sus pares.

empresa para capitalizar desarrollos como la energía renovable, las técnicas avanzadas de reciclaje y el auge de la economía circular.

La sostenibilidad puede ser una oportunidad para que la empresa se vuelva más competitiva, eficiente y resiliente que sus pares.

Por supuesto, la forma en que una empresa integre el cambio climático y los asuntos sociales en su estrategia variará en función de su modelo de negocio, sus objetivos y su sector, así como de los riesgos específicos a los que se enfrente.

Teniendo esto en cuenta, los directorios tendrán que asegurarse de que disponen de suficiente información y conocimientos especializados, así como de las estructuras y procesos adecuados, para proporcionar una orientación eficaz a los equipos de gestión.

Asimismo, deben prestar atención a la creciente tendencia a la inversión responsable. Ésta se debe a que los inversionistas creen que las empresas sostenibles tienen más probabilidades de crear valor a largo plazo. Los directorios deben asegurarse de que los inversionistas reciban información fidedigna sobre la forma en que sus empresas se ven afectadas por el cambio climático y otros asuntos sociales y ambientales importantes, y sobre cómo están respondiendo a ellos.

1. Siglas en inglés para ambiental, social y gobierno corporativo.

Preguntas a considerar por el directorio

1. ¿Qué tan buena es la comprensión del directorio y del equipo de gestión de los riesgos y oportunidades significativos que el cambio climático y otros asuntos relacionados con la sostenibilidad presentan a la organización?
2. ¿Qué tan bien integrados están el cambio climático y otros riesgos y oportunidades relacionados con la sostenibilidad en la estrategia comercial general?
3. ¿Cómo se presentan los asuntos relacionados con el clima y la sostenibilidad en el proceso de toma de decisiones de la organización, tanto a nivel estratégico como operacional?
4. ¿Cómo hace el directorio para que el equipo de gestión sea responsable de establecer, cumplir y medir los objetivos como parte de la gestión de los riesgos y oportunidades de la organización relacionados con el cambio climático y la sostenibilidad?
5. ¿Qué tan bien se relacionan el directorio y el equipo de gestión con los inversionistas en cuanto a la sostenibilidad de la organización a largo plazo, incluida la forma en que se integra el riesgo relacionado con el clima en su modelo de negocios?



Capítulo 4

La lucha contra el fraude y el lavado de dinero: consideraciones clave para los directorios

¿Comprende cuán expuesto está su negocio al riesgo de lavado de dinero?

El crimen financiero es un problema en espiral y los legisladores esperan que las empresas ayuden a combatirlo. En los últimos años, la legislación contra el lavado de dinero se ha vuelto cada vez más estricta.

Mientras tanto, los reguladores a nivel mundial están prestando mucha atención a las monedas virtuales como el bitcoin, porque son un método de liquidación predilecto para los que lavan dinero y los terroristas.

La exposición a este tipo de delitos es un riesgo especialmente grave para las empresas que operan en el sector de los servicios financieros. No obstante, los directorios de las empresas de todos los sectores deben observar la evolución del entorno regulatorio como parte de su supervisión de gobierno corporativo.

Deberán pedir a sus equipos de gestión que proporcionen una evaluación de hasta qué punto la empresa está expuesta a riesgos de cumplimiento de las normas contra el lavado de dinero, como las criptomonedas o las personas políticamente expuestas y cómo piensan mitigar esos riesgos.

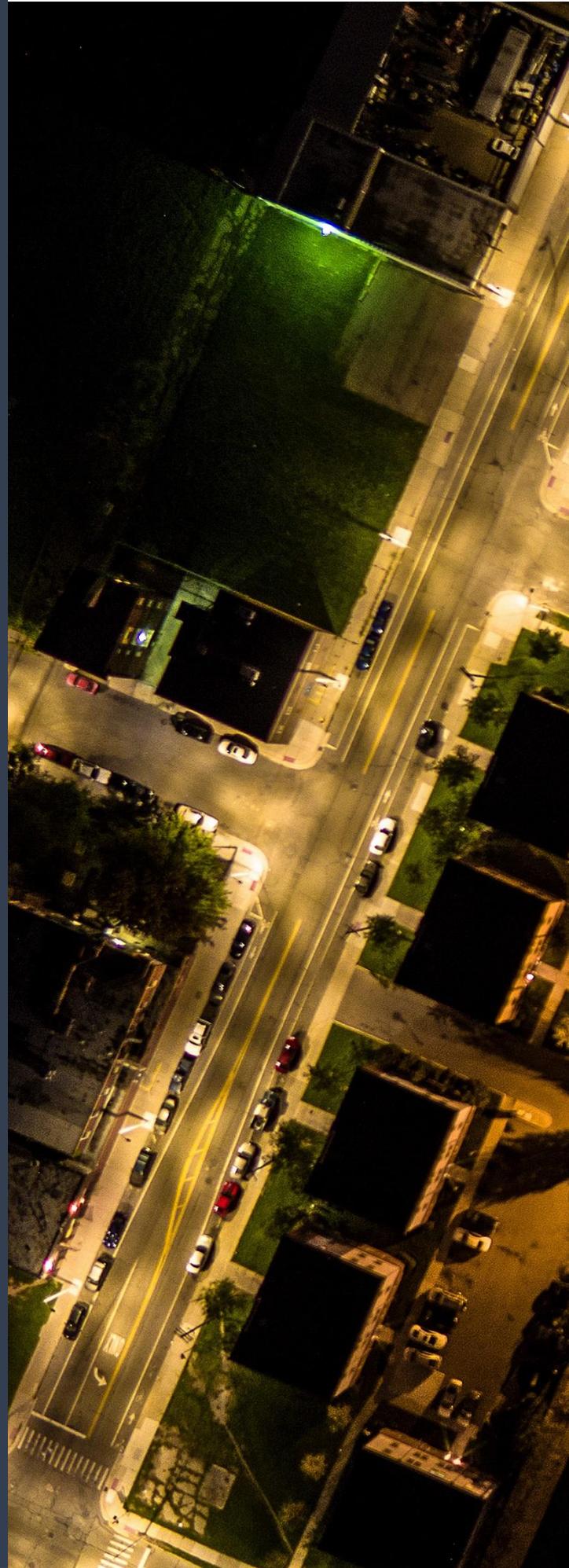
Además, ¿qué se está haciendo para mejorar la detección y prevención de los delitos económicos dentro de la empresa? ¿Está la empresa haciendo un uso efectivo de las herramientas tecnológicas o colaborando con socios y pares para compartir las mejores prácticas?

Los directorios deben pedir a sus bancos que expliquen lo que están haciendo para cumplir con las leyes contra el lavado de dinero y qué prácticas están realizando para inculcar conductas éticas y responsables dentro de sus organizaciones.

Otra forma en que los directorios pueden reforzar las defensas de su empresa contra los delitos financieros es garantizar que se establezcan los procesos adecuados para incentivar la denuncia de las actividades ilegales. Por ejemplo, una línea de ayuda anónima para la denuncia de irregularidades podría poner de relieve algunas prácticas deficientes y proporcionar información valiosa sobre las esferas de la organización en que los delitos financieros plantean un riesgo particular.

Preguntas a considerar por el directorio

1. ¿Qué tan buena es la comprensión del directorio acerca de los métodos y procesos que la organización utiliza para mover el dinero de manera segura en todo el mundo? ¿Qué grado de visibilidad tiene la gerencia sobre las principales contrapartes financieras de la organización, en particular los bancos, y cómo aplica la due diligence de terceros para evaluar esas contrapartes?
2. ¿Cómo supervisa el directorio las conexiones que la organización tiene con personas políticamente expuestas?
3. ¿De qué manera la organización está invirtiendo en nuevas tecnologías para ser más eficaz en el cumplimiento de la legislación contra el lavado de dinero?
4. ¿Cuánta confianza tiene el directorio en que la gerencia dispone de un marco para vigilar y mitigar los riesgos de lavado de dinero y en que este marco funciona eficazmente?



Capítulo 5

Transformación del negocio digital: gestión del riesgo y aprovechamiento del lado positivo de la disrupción

¿El directorio está al tanto de la forma en que la organización puede utilizar las nuevas tecnologías para crear más valor para sus stakeholders a largo plazo?

La transformación del negocio digital presenta a los directorios algunas materias clave que deben considerar en su función de supervisión. El punto de partida es comprender la oportunidad estratégica: ¿Cómo la digitalización puede hacer que la empresa mejore sus operaciones y cree una mejor experiencia para sus clientes y proveedores?

Una vez que entiendan esto, los directorios pueden ver cómo la empresa podría utilizar las nuevas tecnologías como plataforma para aumentar la eficiencia, acelerar el crecimiento, desarrollar nuevas alianzas y revisar y ajustar sus modelos de negocios para lograr una ventaja competitiva.

También pueden explorar lo que la empresa está haciendo para atraer y retener al personal con habilidades digitales y cómo está utilizando los programas de gestión del cambio para incorporar nuevos enfoques y procesos.

Mediante el uso de herramientas como el análisis de datos, los directorios podrán identificar las megatendencias emergentes y brindar orientación a la gerencia para abordar los desafíos que éstas presentan

Un punto relevante para los directorios es la aparición de algunos riesgos importantes relacionados con la tecnología. Estos incluyen, por ejemplo, incidentes de ciberseguridad, robo de datos de clientes, riesgos éticos o un sistema de inteligencia artificial que toma decisiones sesgadas porque ha sido instruido utilizando un conjunto de datos inexactos o incompletos.

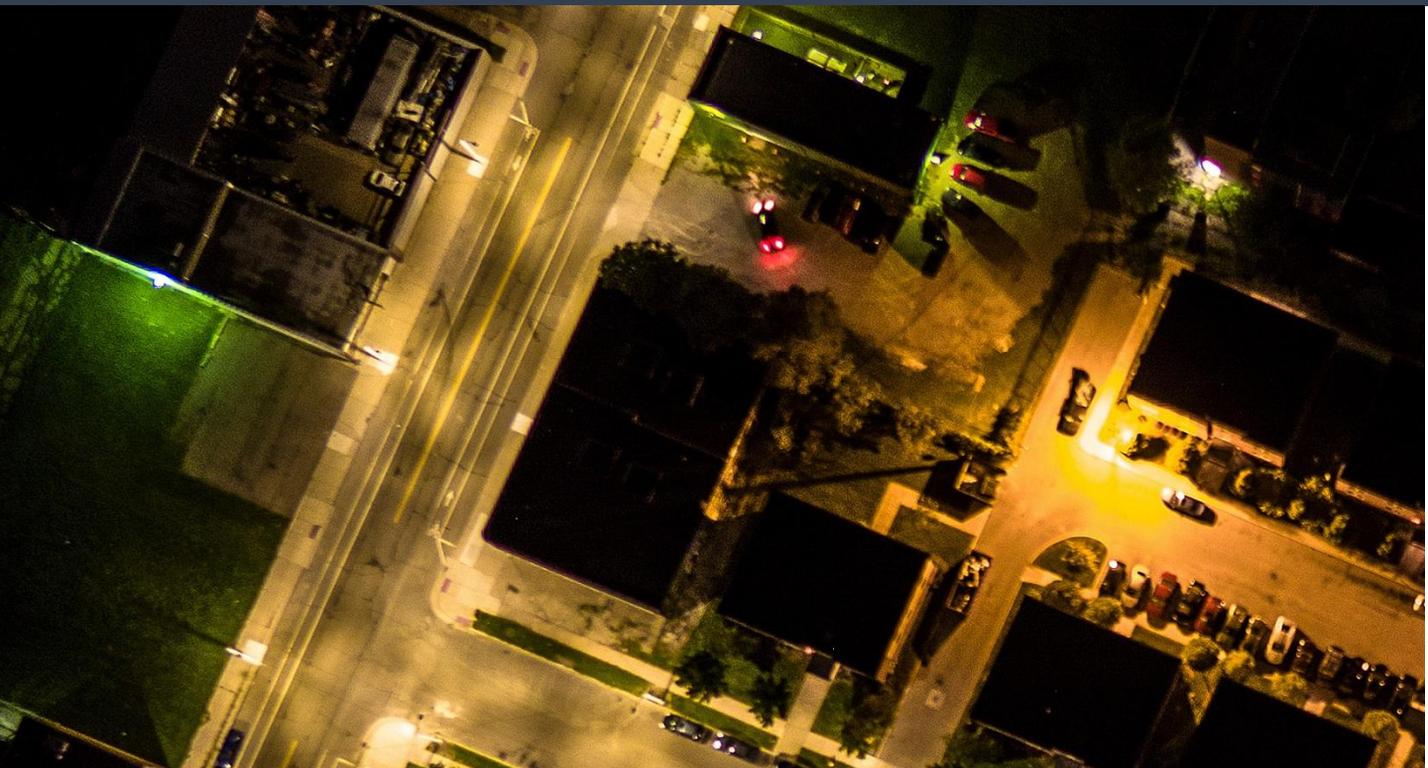
Otro riesgo, sobre todo si se tiene en cuenta el Covid-19, es la aparición de un competidor disruptivo que debilite el modelo comercial de la empresa o se apodere de la cuota de mercado por haber desarrollado una oferta de servicios digitalizados que los clientes prefieran.

Para tener éxito en el futuro, las empresas necesitarán que sus directorios utilicen la inteligencia de datos exponencialmente mayor que puede aprovecharse mediante el poder de la tecnología.

Mediante el uso de herramientas como el análisis de datos, los directorios podrán identificar las megatendencias emergentes y brindar orientación a la gerencia para abordar los desafíos que éstas presentan. Los conocimientos que obtengan de los datos también les permitirán apoyar a la gerencia para desarrollar modelos de negocio más innovadores, colaborar con nuevos socios e incubar nuevas ideas para lograr una ventaja competitiva.

Preguntas a considerar por el directorio

1. ¿Qué tan bien entiende el directorio las oportunidades estratégicas que la digitalización crea para la organización?
2. ¿Cómo puede el directorio mejorar su conocimiento colectivo, su composición y su experiencia para poder participar plenamente en una estrategia de transformación empresarial a gran escala?
3. ¿Cómo se asegura el directorio de tener una buena visibilidad sobre el talento y las estrategias de preparación cultural de la organización, así como de sus capacidades de gestión de cambio?
4. ¿De qué manera la organización, el directorio y el equipo de gestión están utilizando en forma eficaz y legítima las importantes capacidades de inteligencia de datos que pueden proporcionar las nuevas tecnologías?
5. ¿Qué tan sostenible es la organización a largo plazo? ¿Cómo el directorio y el equipo de gestión están trabajando juntos de manera efectiva para orientar la dirección estratégica de la organización hacia un modelo de negocio digitalizado y adaptado al futuro?



Capítulo 6

Gestión de riesgos: mejora de la supervisión de las amenazas y oportunidades estratégicas

¿Tiene el directorio suficiente visibilidad de los distintos riesgos emergentes que podrían afectar a la organización?

La rápida evolución del panorama empresarial exige que los directorios consideren un sinnúmero de riesgos emergentes.

Aparte de los riesgos relacionados con la tecnología, deben tener en cuenta los riesgos reglamentarios y los relacionados con la sostenibilidad, tales como los que plantean el cambio climático, los brotes de enfermedades, la falta de habilidades y las deficiencias de la cultura organizacional.

El Covid-19 también ha puesto de relieve la posibilidad de que riesgos inesperados amenacen el bienestar y la productividad del personal, interrumpan las cadenas de suministro y reduzcan los ingresos y las ganancias.

Para supervisar eficazmente una gama tan amplia de riesgos, los directorios deben trabajar con sus ejecutivos de primer nivel para elaborar un esquema de todo el panorama de riesgos a los que se enfrentan sus organizaciones, incluidos los riesgos tradicionales y los atípicos.

Con el objetivo de obtener nuevas perspectivas, podrían revisar sus marcos de información y adoptar informes que reflejen el cambiante panorama de los riesgos.

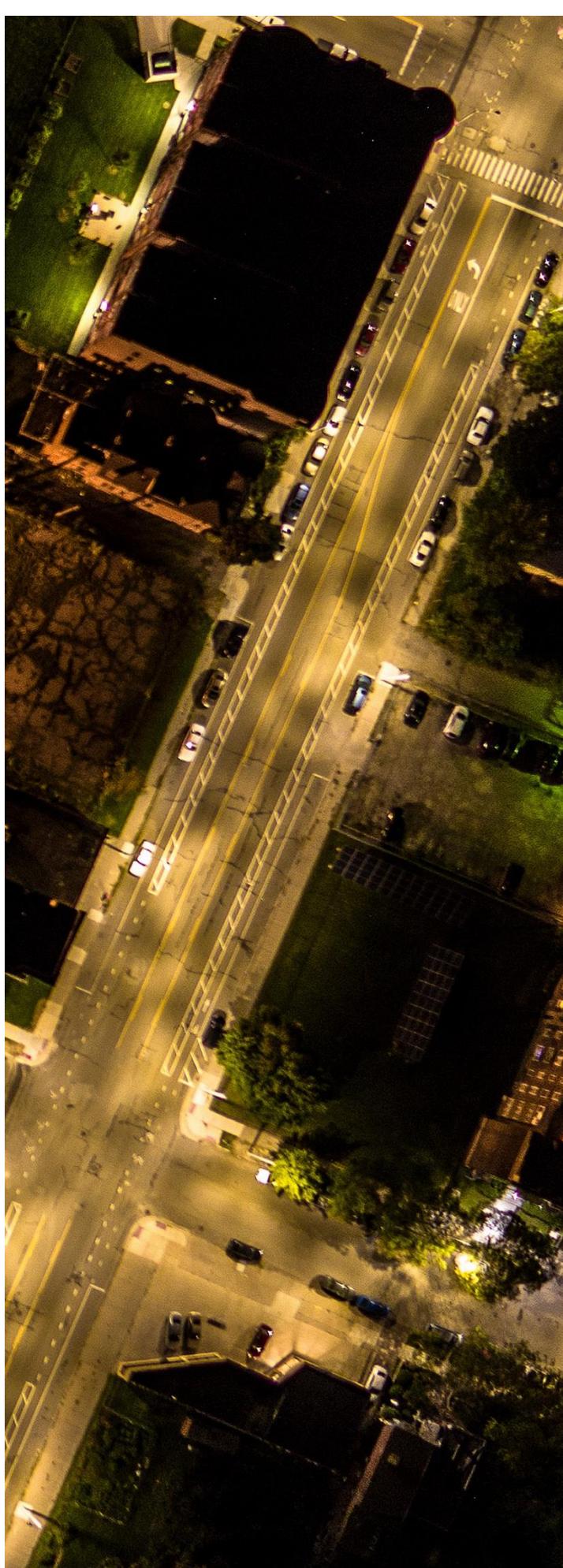
De cara al futuro, por ejemplo, es probable que exijan información relacionada con activos intangibles como la cultura, la reputación y el talento.

También necesitarán información sobre los competidores nuevos y emergentes y otras innovaciones del mercado que podrían poner en peligro la estrategia de la organización y dar lugar a riesgos relacionados con la cultura y la conducta.

Puede ser necesario que el directorio dedique más tiempo a debatir los riesgos emergentes y las oportunidades estratégicas. En este caso, podrían disponer de tiempo reorganizando las estructuras y los horarios de los comités. También deben examinar la forma en que utilizan los datos internos y externos correspondientes a la organización en su proceso de toma de decisiones.

Una prioridad válida para el directorio podría ser evaluar si los directivos de la empresa y los altos ejecutivos tienen las habilidades y competencias necesarias para afrontar los mayores riesgos estratégicos de hoy en día. En los casos en que se carezca de esas habilidades y competencias, podrían sugerir que la organización los contrate o que se reúna con expertos externos que tengan conocimientos especializados.

La función de gestión de riesgos de la empresa debería resultar ser un recurso valioso para el directorio, especialmente si es capaz de desplegar herramientas tecnológicas potentes para identificar, evaluar, vigilar y predecir el riesgo.



Preguntas a considerar por el directorio

1. ¿Cuáles son los mayores riesgos estratégicos y oportunidades, tanto tradicionales como atípicos, a los que se enfrenta su organización hoy en día?
2. ¿Qué papel desempeña el directorio en la supervisión del proceso de identificación de riesgos? ¿El directorio y los ejecutivos están en consonancia con los mayores riesgos y oportunidades estratégicas?
3. ¿Cómo se asegura el directorio de que la gestión de riesgos y la presentación de informes de la organización son lo bastante exhaustivos en todo el panorama, para facilitar la adopción de decisiones firmes con la debida consideración de estos riesgos?
4. ¿Qué puede hacer el directorio para asegurarse de que su composición actual es la adecuada? ¿Están presentes en el directorio las personas y las competencias correctas para garantizar una supervisión eficaz del riesgo y aprovechar las nuevas oportunidades para mejorar aún más el modelo de negocio? ¿Pueden sus habilidades y conocimientos ser complementados con experiencia externa?
5. ¿Cómo utiliza la organización la tecnología para identificar, comprender y mitigar de mejor manera los riesgos emergentes? ¿Está la organización entrenando a sus empleados para que puedan diseñar y utilizar nuevas herramientas tecnológicas y comprender plenamente los resultados de los datos generados?

Capítulo 7

Perspectiva del comité de auditoría: comprender las crecientes responsabilidades del CFO

¿Cómo puede el comité de auditoría fortalecer el gobierno corporativo de la organización capitalizando la experiencia del gerente de finanzas como socio estratégico?

En este entorno de extrema incertidumbre, los gerentes de finanzas o CFO están proporcionando perspectivas de futuro a los directorios y los equipos de gestión. Para ello, se basan en tecnologías emergentes, como el análisis predictivo.

Al mismo tiempo, siguen realizando las actividades que habrían sido el pilar de la función del director financiero en el pasado, tales como la gestión del efectivo y la liquidez de la empresa, la supervisión de los procesos de presentación de informes financieros y el establecimiento y la vigilancia de los controles internos.

Es importante que haya una estrecha relación entre el director de finanzas y el comité de auditoría, con la confianza como base.

En este contexto, la fuerza de la relación entre el gerente de finanzas y el directorio, y en especial el comité de auditoría, es un asunto de gran importancia estratégica.

El Covid-19 presenta algunos inconvenientes importantes para la presentación de informes financieros en áreas como el deterioro de los activos, la contabilidad de los contratos y las empresas en funcionamiento. Por lo tanto, es importante que los comités de auditoría se mantengan bien informados, con una fuerte relación con el CFO, con la confianza como base.

Las reuniones periódicas entre este gerente y el comité de auditoría son esenciales. Fomentan una comunicación abierta y regular y permiten que los temas pertinentes, como la gestión de riesgos, se analicen oportunamente.

Adicionalmente a abarcar importantes asuntos relacionados con la presentación de informes y la contabilidad de las empresas, en las reuniones se deberían explorar temas estratégicos más amplios que podrían tener un impacto a corto o largo plazo en el desempeño y el valor de la empresa.

También pueden ser una oportunidad para que el comité de auditoría comprenda mejor la calidad de las relaciones que tiene el gerente de finanzas, no sólo con el directorio y el director ejecutivo, sino también con los demás miembros del equipo de gestión y los ejecutivos de alto nivel.

Además, el comité de auditoría puede reconocer las responsabilidades cada vez mayores y el área de autoridad estratégica del CFO, asegurándose de que la función de finanzas tenga el talento adecuado para apoyar los objetivos de la empresa en el futuro.

Preguntas a considerar por el directorio

1. ¿Qué tan estrecha es la relación entre el comité de auditoría y el CFO? ¿Hasta qué punto existen la apertura y la confianza?
2. ¿Cómo el comité de auditoría cuestiona efectivamente al CFO, le pide que rinda cuentas y establece si éste se está desempeñando de manera eficaz?
3. ¿Cómo se le encomienda al CFO que garantice el diseño y la aplicación de un marco de riesgos apropiado para apoyar la presentación de informes periódicos y sólidos sobre los principales riesgos? ¿Qué tan eficiente es para compartir informes y análisis de riesgos sólidos con el comité de auditoría?
4. ¿Cuánta confianza tiene el directorio en que la función de finanzas de la organización tiene la combinación adecuada de habilidades y conocimientos especializados? ¿Necesita cambiar la composición del personal mediante la contratación de talento adicional?
5. ¿Con qué regularidad se reúne el comité de auditoría con el CFO, y hasta qué punto estas reuniones cubren los asuntos financieros y los más estratégicos?



Capítulo 8

Eficiencia del directorio: la cambiante dinámica del gobierno corporativo

¿Cómo el directorio puede operar de manera más eficiente para cumplir mejor con las expectativas de las partes interesadas?

Un directorio eficiente, a los ojos de sus partes interesadas, garantizará que su empresa actúe con propósito y sirva a una amplia gama de stakeholders, desde los inversionistas hasta los clientes, empleados, proveedores y la comunidad.

También tendrá miembros del directorio con las habilidades, competencias y experiencia adecuadas para realizar las funciones de gobierno corporativo del directorio según la estrategia de la empresa.

Sin lugar a dudas, el presidente desempeña un papel crucial en la mejora de la eficiencia del directorio. Puede hacerlo supervisando un programa regular de autoevaluaciones del directorio y estableciendo una atmósfera de inclusión y confianza dentro de la sala de juntas.

A un nivel más práctico, puede asegurarse de que en las reuniones del directorio se traten los temas correctos y se asigne el tiempo suficiente para discutir los temas prioritarios.

Si un solo miembro del directorio no cumple con sus obligaciones, puede perjudicar significativamente la eficiencia general del directorio.

Sin embargo, la eficiencia no es, y nunca debe ser, de exclusiva responsabilidad del presidente. Los buenos directorios se definen por su capacidad de trabajar bien en equipo. Los miembros del directorio deben ser capaces de colaborar ofreciendo un desafío constructivo y expresando opiniones contrarias.

Es importante señalar que si un solo miembro del directorio no cumple con sus obligaciones, puede perjudicar significativamente la eficiencia general de éste.

La diversidad es un criterio clave de la eficiencia general del directorio. Las investigaciones sugieren que los directorios que aportan una amplia gama de perspectivas suelen estar mejor situados que sus homólogos menos diversos para ayudar a las empresas a aprovechar las oportunidades del mercado y gestionar los riesgos.

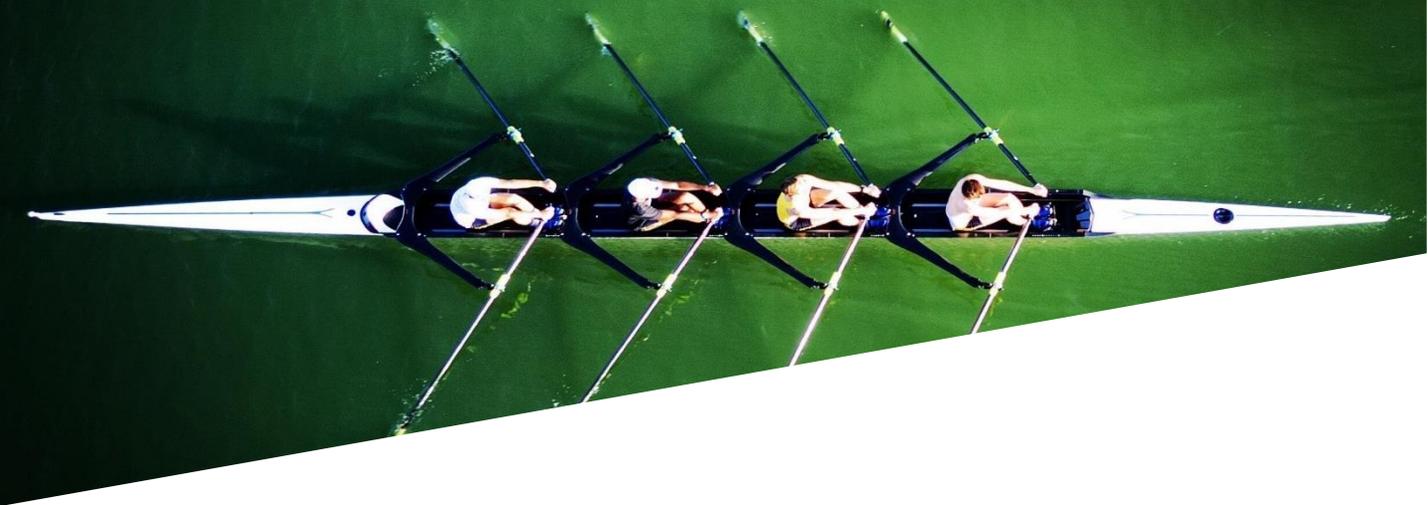
La eficiencia también se ve potenciada por los límites de duración de los cargos de los directores. Estos permiten que la composición del directorio evolucione de acuerdo con la estrategia de la empresa.

Para ser eficientes, los miembros del directorio deben ser capaces de buscar el conocimiento de la gerencia para mejorar aún más su propia comprensión, sin invadir el papel del equipo de gestión. También necesitan recibir un flujo fluido de información desde la gerencia, que sea de alta calidad y oportuno.

Preguntas a considerar por el directorio

1. ¿Cuánta confianza tiene en que el directorio está compuesto por un grupo diverso de directores calificados y experimentados que ofrecen una variedad de experiencias, perspectivas y habilidades que apoyan a la organización para lograr su estrategia?
2. ¿Qué puede hacer el directorio para incorporar a más mujeres en funciones ejecutivas y no ejecutivas?
3. ¿Las reuniones del directorio se llevan a cabo de una manera inclusiva, que permita a sus miembros hacer una contribución completa y ofrecer un desafío constructivo?
4. ¿Cómo puede el directorio dedicar más tiempo a las reuniones para analizar los temas que son de mayor importancia para la organización?
5. ¿Con qué frecuencia el directorio evalúa formalmente el desempeño de los miembros por separado y el desempeño del directorio como equipo? Además, ¿cómo se asegura de que estas evaluaciones sean objetivas? ¿Utiliza a terceros independientes para llevarlas a cabo?





Cómo los directorios pueden usar las megatendencias para trazar un nuevo rumbo

De la supervisión a la previsión: los directorios deben adoptar una mentalidad orientada al futuro para reducir el riesgo de perderse el próximo gran acontecimiento.

En resumen

- ▶ Cuatro megatendencias: descarbonización, economía conductual, futuro del pensamiento y trabajo y vida sin límites, tendrán el mayor impacto en los directorios.
- ▶ Los directorios deben analizar cuidadosamente estas tendencias y considerar la posibilidad de incorporarlas en la planificación de escenarios para ayudar a dar forma a su respuesta.
- ▶ ¿Cómo saldremos de esta pandemia actual de una manera de la que podamos sentirnos orgullosos? ¿Cómo ayudaremos a proteger nuestras organizaciones al mismo tiempo que apoyamos un cambio estratégico para crear valor a largo plazo? ¿Miraremos hacia atrás y estaremos seguros de que nos hemos tomado el tiempo necesario para mirar realmente hacia delante y replantear el futuro?
- ▶ Estas son algunas de las preguntas que, sin duda, están ocupando las mentes de los miembros de los directorios en este momento. Mientras que la gerencia se enfrenta a la resiliencia durante este período crítico, los directorios deben adoptar una mentalidad "futurista" para garantizar la sostenibilidad de la organización a largo plazo. En otras palabras, necesitan reconocer y responder a la forma en que la sociedad está cambiando en un mundo postpandémico.
- ▶ Algunos de estos cambios ya estaban ocurriendo pero ahora se han acelerado. Por ejemplo, tecnologías como la inteligencia artificial (IA) y el internet de las cosas ya estaban transformando todo, desde el comportamiento de los consumidores hasta la naturaleza del trabajo antes de que llegara el Covid-19.

Mientras que la gerencia se enfrenta a la resiliencia durante este período crítico, los directorios deben adoptar una mentalidad "futurista" para garantizar la sostenibilidad de la organización a largo plazo.

- ▶ Entonces, ¿qué hay en el horizonte y se aproxima rápidamente, qué necesitan los directorios tener a la vista?
- ▶ Los supuestos de larga data sobre las estructuras de la industria, los mercados y la naturaleza de la competencia debida a la convergencia estarán en tela de juicio. Y el sistema mundial será remodelado por todo, desde la dinámica del cambio de poder hasta la asistencia de los robots.
- ▶ El Informe EY Megatendencias, publicado cada dos años por EYQ, el grupo de expertos de EY, ofrece a los presidentes de los directorios y a otros directores un marco de organización para ajustar y adaptar su estrategia para estar a la vanguardia de estos y otros cambios disruptivos significativos.

El informe se centra en ocho megatendencias creadas por cuatro fuerzas primarias: la innovación tecnológica, la globalización, los cambios demográficos y el cambio ambiental.

De las ocho (descarbonización, guerra fría tecnológica, economía conductual, medios sintéticos, futuro del pensamiento, trabajo y vida sin límites, microbiomas y biología sintética), el Centro global EY para temas de directorio (del inglés [EY Global Center for Board Matters](#)) ha identificado cuatro que tienen el mayor impacto y aplicabilidad en los directorios de todas las industrias, geografías o modelos de gobernanza.

Las megatendencias que más impacto tendrán para los directorios son:

1. Descarbonización
2. Economía conductual
3. Futuro del pensamiento
4. Trabajo y vida sin límites

Establecemos las repercusiones de cada una de ellas para los directorios y luego ofrecemos recomendaciones sobre lo que pueden hacer para responder.

Descarbonización

El descontento con el progreso de los gobiernos en cuanto a la acción climática ha ido en aumento desde hace algún tiempo y la sociedad está cada vez más pendiente de las empresas para cerrar la brecha.

El informe de 2019, CEO Imperative Study, revela que tanto los inversionistas como los directorios esperan que los directores ejecutivos respondan a los mayores desafíos de la humanidad, incluyendo el cambio climático, con muchos inversionistas que ahora aumentan las apuestas en relación con la búsqueda proactiva de inversiones éticas.

Esto significa que los directorios deben seguir impulsando las consideraciones relacionadas con el clima con sus equipos de gestión para asegurarse de que se tengan en cuenta en sus continuos procesos de toma de decisiones. Hacerlo, si es verdaderamente auténtico, no sólo posicionará a la organización como una propuesta de inversión favorable, sino que también asegurará que atraigan el talento que necesitan para el crecimiento a largo plazo.

La expectativa de la generación Z (ver [Generation Z's expectation](#)) es que las organizaciones y las marcas irán más allá del *marketing* a diferencias verdaderamente cuantificables. Y a medida que la Generación Z madure, se espera que las organizaciones no solo sean climáticamente neutrales sino que también hagan una contribución positiva neta.

Como tal, los directorios desempeñan un papel fundamental en la exigencia de indicadores de información más frecuentes y exhaustivos sobre el desempeño social y ambiental. No cabe duda de que los inversionistas analizan y comparan cada vez más las organizaciones para las compensaciones de asignación de capital a medida que las partes interesadas les piden que rindan cuentas.

Al estar en revisión los paquetes de remuneración e incentivos de los ejecutivos y del directorio, es probable que veamos un mayor interés en esta área desde un punto de vista estratégico y respaldado por decisiones políticas en evolución.



Acciones para el directorio

- ▶ Abordar el corto plazo de frente, no sólo centrándose en los beneficios, sino también en las personas y el planeta.
- ▶ Asumir la responsabilidad personal de encontrar los mecanismos apropiados (incluyendo la remuneración y el liderazgo personal) en la formulación de planes a corto y largo plazo, que contribuyan a resolver los desafíos más amplios en el futuro entorno operacional de la empresa.
- ▶ Dirigir la gerencia para desarrollar parámetros de desempeño que promuevan oportunidades sostenibles y expresen las iniciativas de valor a largo plazo de la organización; ser transparente con las partes interesadas en torno a cuáles son los parámetros y revisar y compartir regularmente los progresos realizados en relación con ellos.

Preguntas a considerar por el directorio

1. ¿La gerencia incentiva la innovación que contribuye a un modelo de negocios descarbonizado? Si es así, ¿cómo estamos midiendo nuestro progreso? Si no, ¿cuáles son los costos de oportunidad de no hacerlo?
2. ¿Qué información está disponible para el directorio sobre el impacto de los asuntos de riesgos relacionados con el clima? ¿Cuál es la fuente de la información? ¿Con qué frecuencia se revisa? ¿Nos comparamos con los compañeros de la industria? ¿Y somos capaces de medir relativamente el impacto tangible y no tangible, tanto en nuestra marca como en los resultados financieros?

Economía conductual

El comportamiento humano se está convirtiendo en un bien de consumo, cuantificado, estandarizado, empaquetado y comercializado, tanto como los datos de los consumidores lo son hoy en día.

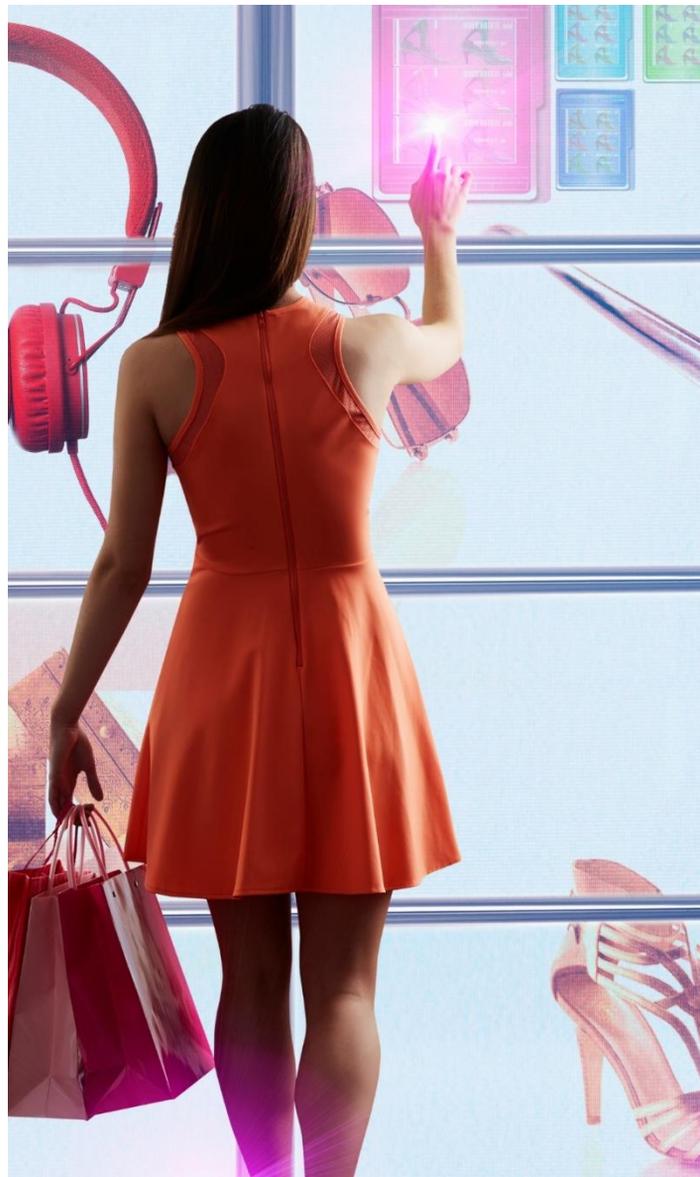
Esta comercialización, combinada con la maduración de disciplinas como la economía conductual y la computación afectiva, puede permitir a las organizaciones influir y moldear el comportamiento del consumidor como nunca antes.

Mientras que la economía conductual aplica los conocimientos de la psicología en la toma de decisiones de las personas, la computación afectiva, también conocida como IA de las emociones, lleva a las máquinas al reino de las emociones humanas.

Por consiguiente, las organizaciones deben utilizar la economía conductual y la computación afectiva para medir, comprender y moldear el comportamiento y, al mismo tiempo, ser transparentes con sus consumidores.

Simultáneamente con la comprensión de las preferencias de los clientes, las organizaciones también deben considerar qué tipo de consumidor está surgiendo y qué nuevos segmentos de clientes se están creando. El índice EY Future Consumer Index, publicado en abril de 2020, mostró que el 62% de los encuestados es más probable que compre a empresas que hacen un bien a la sociedad. Esto significa que las organizaciones deben dar todo de sí, en todo momento. Una mayor transparencia, no el secreto o la defensa, es la clave. Y aquellos que lo hagan bien tendrán una considerable ventaja competitiva.

62% de los consumidores del Índice de Consumidores a Futuro (del inglés Future Consumer Index) afirma que es más probable que realicen compras a empresas que están haciendo un bien a la sociedad.



Acciones para el directorio

- ▶ Dirigir a la gerencia para que revise sus estrategias, a fin de llevar la voz del cliente a la sala de juntas.
- ▶ Llevar expertos en materia de comportamiento a las salas de juntas para entender mejor las cambiantes necesidades del consumidor.
- ▶ Adoptar técnicas sofisticadas centradas en el cliente, tales como la economía conductual o la computación afectiva.
- ▶ Continuar impulsando una conversación sólida acerca de la marca y la promesa de marca sobre cómo seguiremos siendo relevantes para los clientes del mañana y sus expectativas en torno al papel de la organización en la sociedad.

Preguntas a considerar por el directorio

1. ¿Qué datos están disponibles sobre los impactos en la industria derivados de los cambios en el comportamiento de los consumidores?
2. ¿Qué nuevos riesgos plantea la economía conductual (regulatorios, de reputación y de mercado) y cómo podríamos entenderlos y ayudar a mitigarlos?
3. ¿Cómo podemos abordar fundamentalmente la tensión entre la creación de valor a largo plazo y la presión de los ingresos a corto plazo?

Futuro del pensamiento

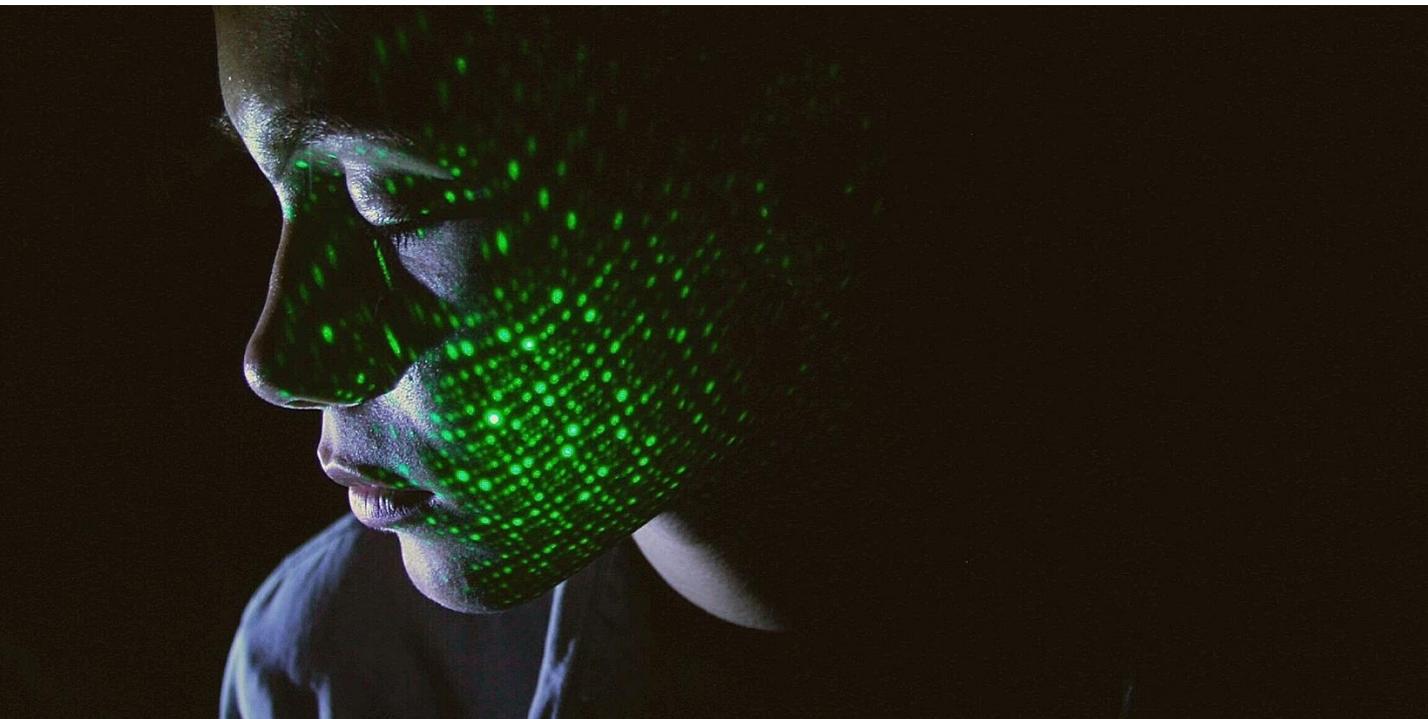
No hay duda de que la tecnología está cambiando profundamente la forma en que pensamos y actuamos: desde las redes sociales y los teléfonos inteligentes hasta las "tecnologías inteligentes" como la automatización de procesos robóticos y la IA. Y en el trabajo, está presente en casi todo lo que hacemos.

Como tal, es fundamental que las organizaciones alcancen el equilibrio adecuado para adoptar y utilizar tecnologías digitales que liberen al personal para que realicen actividades de mayor valor y, al mismo tiempo, preserven la esencia humana.

La tecnología también está creando nuevos desafíos con respecto a la confianza. En una era de tecnologías de medios de comunicación sintéticos como los videos falsificados o "deepfakes", ¿cómo se asegurarán las organizaciones de que la información y las tecnologías que despliegan sean fiables? ¿Y cómo pueden asegurarse de que están protegiendo y mitigando los riesgos cibernéticos, incluyendo la desinformación, el phishing y el malware?

El no hacerlo tiene un alto costo, tanto financiero como de reputación, y pocas organizaciones hoy en día pueden permitirse dar pasos en falso evitables.

Por eso no puede ser responsabilidad exclusiva de la oficina de tecnología, sino que debe integrarse en los procesos de gestión de riesgos en consonancia con la cultura de la empresa.



Acciones para el directorio

- ▶ Marcar la pauta correcta desde el directorio y trabajar con la gerencia para incentivar una cultura de inclusión.
- ▶ Trabajar con la gerencia para reimaginar la forma de captar talentos en el nuevo entorno operativo descentralizado y alentar a la gerencia a realizar encuestas de percepción frecuentes y corregir el rumbo cuando sea necesario.
- ▶ Pensar cuidadosamente en la promesa de marca existente a los empleados y segmentos dentro de la fuerza de trabajo, para asegurarse de que es novedosa, relevante, viable y auténtica.
- ▶ Darle prioridad a la agenda de las personas, en especial en lo que respecta al bienestar de los empleados, y contar con expertos en la materia, tales como profesionales de la salud mental cuando sea necesario.

Preguntas a considerar por el directorio

1. ¿Estarán los empleados más comprometidos con un futuro de trabajo a distancia? Y de ser así, ¿se está preparando la gerencia para hacer cambios a largo plazo en las prácticas laborales?
2. ¿Cómo podemos hacer que la gerencia establezca prioridades y construya su "cultura de la gente"? ¿De qué manera la gerencia sigue impulsando una cultura de inclusión? ¿Existen foros apropiados de medición o de rendición de cuentas que midan verdaderamente su eficacia de manera oportuna? ¿Existen mecanismos de retroalimentación para los empleados que ofrezcan comentarios honestos y constructivos?

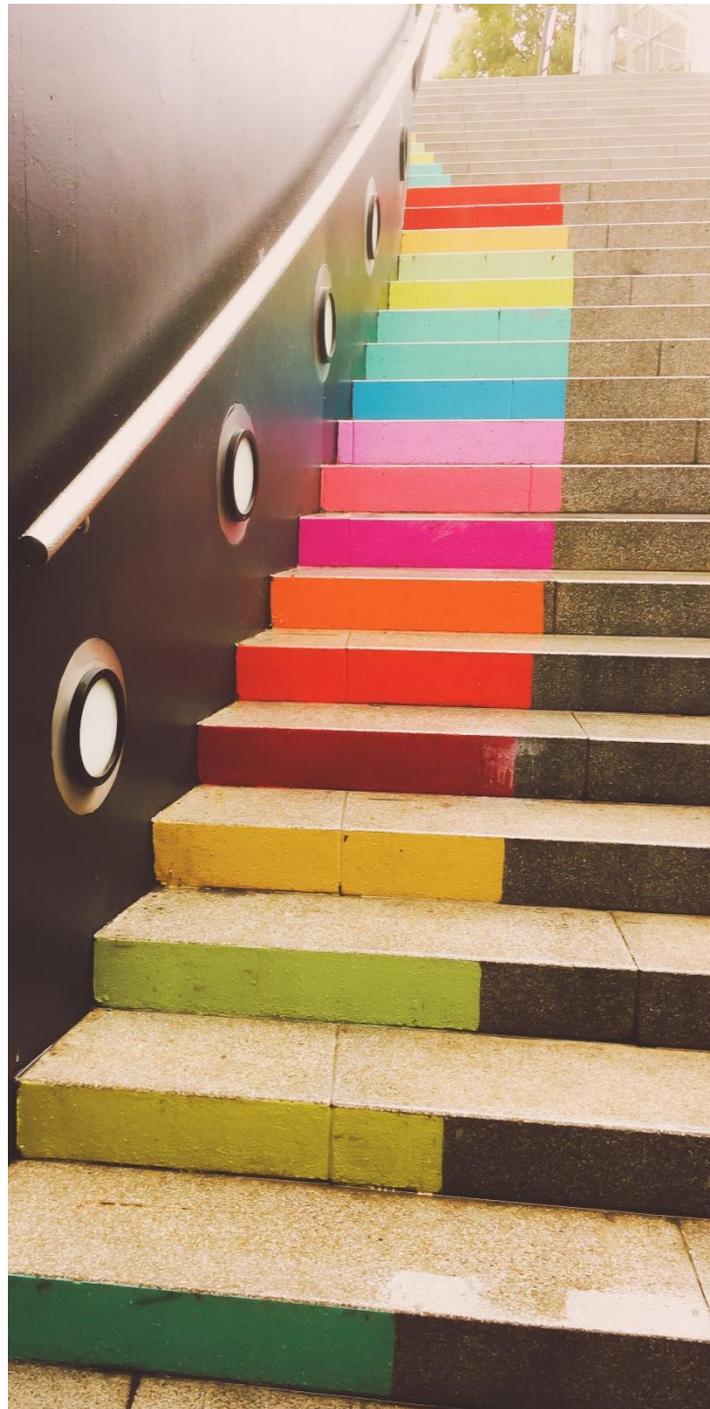
¿Cuáles son los siguientes pasos para los directorios

Al adoptar una mentalidad futurista y ver sus organizaciones a través de la óptica de estas megatendencias, los directorios estarán mejor equipados para trabajar con sus equipos de gestión, con el fin tomar medidas informadas y decisivas para el éxito a largo plazo.

Sugerimos a los miembros del directorio que analicen cuidadosamente cada megatendencia y que consideren los posibles impactos y repercusiones, no sólo como asuntos individuales sino como fuerzas interdependientes que deben incorporarse a los marcos estratégicos de la organización. Más importante aún, recomendamos que los directorios y los equipos de gestión desarrollen escenarios que contengan estas tendencias e identifiquen las áreas de riesgo y los espacios de posibilidad asociados.

El desarrollo de escenarios es una herramienta a menudo discutida pero rara vez utilizada por los equipos directivos y ejecutivos para poner a prueba su pensamiento; cuando se hace correctamente, proporciona una base para aprovechar las ventajas y anticipar mejor las desventajas.

Finalmente, los directorios con visión de futuro ya están explorando nuevos impulsores de valor. Sin embargo, muchos de los impactos sociales que la pandemia ha desencadenado aún no se han producido. Por lo tanto, es fundamental que todo el directorio, conducido por su presidente, continúe liderando y "escuchando y aprendiendo, no simplemente enseñando y explicando".





Revelaciones de las empresas sobre supervisión y riesgos de ciberseguridad en 2020

El riesgo de ciberseguridad se está intensificando, especialmente con el trabajo a distancia generalizado y el aumento de las interacciones en línea en medio de la pandemia. La rápida adaptación de numerosos procesos y protocolos de negocio para hacer posible este entorno virtual ha aumentado exponencialmente la superficie de ataque de las compañías e introducido nuevos riesgos para la confidencialidad, la integridad y la disponibilidad de información crítica de las empresas y los sistemas de respaldo.

El regreso de algunos trabajadores a un lugar de trabajo físico también está generando nuevos riesgos para la seguridad de los datos y cuestionamientos acerca de la privacidad, con empresas que recaban datos relacionados con la salud de los empleados, contratistas y clientes, como las pruebas de Covid-19, los controles de temperatura y el seguimiento de los contactos. A su vez, el aprovechamiento de tecnologías nuevas y disruptivas, y el hecho de que se permita la confianza de las partes interesadas y del mercado para hacerlo, es clave para ayudar a las organizaciones a liderar, innovar y diferenciarse.

En este entorno, mantener la ciber resiliencia y fomentar la confianza de las partes interesadas en las prácticas de seguridad y privacidad de datos de la empresa es un imperativo estratégico. Las revelaciones públicas de información pueden ayudar a crear confianza al proporcionar transparencia y seguridad sobre la forma en que los directorios cumplen sus responsabilidades de supervisión de los riesgos de ciberseguridad.

Por tercer año consecutivo, los investigadores de EY han analizado las revelaciones de información relacionadas con ciberseguridad en las declaraciones de representación (proxy statements, información que acompaña a la citación para la junta de accionistas) y en los formularios 10-K de las empresas de la lista Fortune 100, para identificar las tendencias y los desarrollos emergentes y ayudarlas a identificar las oportunidades para mejorar la comunicación.

Examinamos 76 compañías de la lista Fortune 100 que presentaron esos documentos desde 2018 hasta el 31 de mayo de 2020. Nos centramos en los ámbitos de la supervisión de ciberseguridad en el directorio (incluida la supervisión de los comités del directorio y las certificaciones de los directores), las declaraciones sobre los riesgos en materia de ciberseguridad y privacidad de los datos y la gestión de riesgos (incluida la mitigación de los riesgos de ciberseguridad y las medidas de respuesta y la colaboración con consultores de seguridad externos). También examinamos el panorama actual de la reglamentación y las políticas públicas de los EE. UU. en lo que se refiere a la ciberseguridad, así como las perspectivas de los inversionistas, directores y profesionales de ciberseguridad de EY.

Lo que descubrimos

Muchas empresas están mejorando sus revelaciones de información sobre ciberseguridad, con ligeros aumentos en la mayoría de las rastreadas. Los cambios más significativos de este año se relacionaron con el área de supervisión del directorio, incluyendo la de los comités del directorio y la identificación de las habilidades y la experiencia de sus miembros. Otros hallazgos importantes son la permanente escasez de revelaciones de información relacionadas con las simulaciones de disposición cibernética y el uso de asesores externos independientes, prácticas que prevalecen en el mercado y que son vitales para mejorar la ciber resiliencia desde la perspectiva de EY (ver "Nuestras observaciones sobre el mercado").

Revelaciones de ciberseguridad de las empresas de la lista Fortune 100

Tema	Revelación	2020	2019	2018
Supervisión del directorio				
Enfoque de supervisión de riesgos	Se reveló un enfoque sobre ciberseguridad en la sección de supervisión de riesgos de la declaración de representación.	89%	88%	79%
Supervisión del comité del directorio *	Se reveló que al menos un comité del directorio se encargaba de la supervisión de los asuntos de ciberseguridad.	87%	82%	74%
	▶ Se reveló que el comité de auditoría supervisa la ciberseguridad.	67%	62%	59%
	▶ Se reveló la supervisión por parte de un comité no relacionado con la auditoría (por ejemplo el comité de riesgo o de tecnología).	26%	28%	20%
Habilidades y conocimientos especializados de los directores	La ciberseguridad se incluyó entre las áreas de especialización requeridas por el directorio o citadas en la biografía de, al menos, uno de los directores.	58%	51%	39%
	▶ La ciberseguridad se incluyó entre las áreas de especialización requeridas en el directorio.	37%	29%	22%
	▶ La ciberseguridad fue citada en la biografía de, al menos, uno de los directores.	46%	41%	30%
Estructura de presentación de informes de gerencia	Se entregaron perspectivas sobre la presentación de informes de gerencia al directorio o a los comités que supervisan los asuntos de ciberseguridad.	61%	58%	54%
	▶ Se identificó, al menos, a una "persona encargada" (por ejemplo, el Director de Seguridad de la Información o el Director de Informática).	33%	34%	25%
Frecuencia de presentación de informes de gerencia	Se incluyó lenguaje sobre la frecuencia en que la gerencia informa al directorio o a los comités, pero la mayor parte de este lenguaje fue vago.	47%	45%	38%
	▶ Se reveló una frecuencia de presentación de informes de, al menos, una vez al año o trimestralmente. Las empresas restantes utilizaron términos como "regularmente" o "periódicamente".	17%	17%	14%
Declaraciones sobre el riesgo de ciberseguridad				
Declaración de factores de riesgo	Se incluyó la ciberseguridad como factor de riesgo.	100%	100%	100%
	Se incluyó la privacidad de los datos como factor de riesgo.	99%	99%	93%
Gestión de riesgos				
Medidas de gestión de riesgos de ciberseguridad	Se hizo referencia a los esfuerzos para mitigar el riesgo de ciberseguridad, como el establecimiento de procesos, procedimientos y sistemas.	92%	91%	83%
	Se hizo referencia a la capacidad de respuesta, como la planificación, la recuperación de desastres o las consideraciones de continuidad del negocio.	62%	57%	50%
	Se declaró que la preparación incluye simulaciones, ejercicios de simulación teórica o pruebas de capacidad de respuesta.	7%	3%	3%
	La ciberseguridad se incluyó en las consideraciones sobre la remuneración de ejecutivos.	5%	1%	1%
Educación y capacitación	Se revelaron las medidas educacionales y de capacitación para mitigar el riesgo de ciberseguridad.	29%	26%	18%
Compromiso con la comunidad de seguridad externa	Se reveló la colaboración con pares, grupos industriales o legisladores.	12%	12%	7%
Uso de un asesor externo	Se reveló el uso de un asesor externo independiente.	16%	13%	16%
	Se reveló la colaboración del directorio con un asesor externo independiente.	5%	4%	3%

Los porcentajes se basaron en el total de las revelaciones de información de las empresas. Los datos se basaron en las 76 empresas de la lista Fortune 100 de 2020 que presentaron el Formulario 10-K y las declaraciones de representación en 2018, 2019 y hasta el 31 de mayo de 2020.

*Algunas empresas designan la supervisión de la ciberseguridad a más de un comité del directorio.

Supervisión del comité del directorio

Más directorios están asignando responsabilidades de supervisión de ciberseguridad a un comité. Este año, el 87% de las empresas han encomendado, al menos, a un comité del directorio la supervisión de ciberseguridad, en comparación con el 82% del año pasado y el 74% en 2018. Los comités de auditoría siguen siendo la principal opción para esas responsabilidades. Este año, el 67% de los directorios asignaron la supervisión de ciberseguridad al comité de auditoría, en comparación con un 62% en 2019 y un 59% en 2018.

El año pasado observamos un aumento significativo de directorios que asignaban la supervisión de la ciberseguridad a comités que no están relacionados con la auditoría, la mayoría de las veces comités de riesgo o de tecnología (28% en 2019 en comparación con el 20% en 2018), pero ese porcentaje ha disminuido este año (26% en 2020). Una menor cantidad de directorios, el 7% en total, asignó responsabilidades cibernéticas tanto al comité de auditoría como a otro diferente.

Entre los directorios que confieren responsabilidades de supervisión de ciberseguridad al comité de auditoría, casi dos tercios (el 65%) formalizan esas responsabilidades en los estatutos. Entre los directorios que asignan esas responsabilidades a los comités que no son de auditoría, la mayoría (el 85%) incluyen esas responsabilidades en los estatutos.

Identificación de las habilidades y conocimientos especializados de los directores

En los últimos años, el porcentaje de empresas que abordan la ciberseguridad en el contexto de las cualificaciones de los directores ha aumentado considerablemente. En 2020, el 58% de las empresas incluyó la ciberseguridad como un área de especialización requerida por el directorio o citada en la biografía de uno de sus miembros, en comparación con el 51% del año pasado y el 39% en 2018.

Sin embargo, algunas empresas citaron explícitamente la experiencia en ciberseguridad en ciertas biografías de directores un año pero no el otro. Las revelaciones indican que las compañías están prestando más atención a señalar la experiencia o los conocimientos especializados de los directores en materia de ciberseguridad.

Privacidad de los datos

Casi todas las empresas (el 99%) que revisamos abordaron la privacidad de los datos en las revelaciones de factores de riesgo incluidas en sus formularios 10-K de 2020 y 2019, en comparación con el 93% en 2018. El grado de atención explícita a la privacidad de los datos, como riesgo significativo, varió ampliamente. Alrededor de una cuarta parte (un 24%) se centró en la privacidad de los datos como factor de riesgo independiente, observando a menudo reglamentos de privacidad de datos cada vez más complejos y cambiantes que crean una alta exposición financiera y jurídica, además de los riesgos de reputación y operacional que conllevan. El 30% agrupó la privacidad de los datos con la ciberseguridad como factor de riesgo, abordando los riesgos superpuestos en forma conjunta. Poco menos de la mitad (el 45%) de las empresas abordó la privacidad de los datos en el contexto de factores de riesgo más amplios, por lo general aquellos relacionados con los riesgos informáticos o reglamentarios.

Las tendencias de la industria no fueron pronunciadas. Las empresas de los sectores en que los riesgos de privacidad de los datos son menos prominentes (por ejemplo, el sector energético y el industrial), figuraban entre las que trataban la privacidad de los datos como un factor de riesgo único, y las empresas de los sectores con importantes riesgos para la privacidad de los datos (por ejemplo, atención de salud, servicios financieros y el retail), figuraban entre las que abordaban la privacidad de los datos sólo en el contexto de riesgos más amplios.

Incentivos de compensación

El 5% de las empresas incluyeron la ciberseguridad en las consideraciones relativas a la remuneración de los ejecutivos, generalmente como un factor cualitativo considerado en relación con el pago de incentivos anuales.

Especialmente, en los últimos tres años unas pocas empresas han recibido propuestas de los accionistas que buscan integrar los parámetros de ciberseguridad en los incentivos de remuneración para los altos ejecutivos. Sin embargo, ninguna de esas compañías está dentro de las pocas que identificamos en nuestra revisión.

Las propuestas que se sometieron a votación obtuvieron un promedio del 17% de apoyo, y las empresas seleccionadas explicaron que, por lo general, no existe necesariamente una correlación entre las acciones de un alto ejecutivo y la prevención de incidentes de ciberseguridad, o que la contraprestación ya existe como parte del desempeño general de un ejecutivo en particular, si procede.

Simulaciones de capacidad de respuesta y ejercicios de simulación teórica

Si bien el porcentaje de empresas que revelaron haber realizado simulaciones de ciberincidentes o ejercicios de simulación técnica se duplicó con creces (pasando de un 3% el año pasado a un 7% en 2020), el número de compañías que hacen esta revelación sigue siendo bajo. Del reducido número que comunicaron que se habían realizado simulaciones, simulacros o ejercicios de simulación teórica en la gerencia, ninguna informó si el directorio participó en éstos.

Las simulaciones son una práctica de preparación de riesgos fundamental que los líderes de EY y otros creen que las empresas deben priorizar. Ni siquiera el programa de ciberseguridad más robusto puede eliminar todos los riesgos. Si no se practican los planes y se produce una violación, la reacción es, en gran parte, improvisada.

Las simulaciones de incidentes bien diseñadas y los ejercicios de simulación teórica pueden someter a la organización a una prueba de estrés y mejorar la preparación al proporcionar claridad en las funciones, los protocolos y los procesos de escalamiento.

La gerencia debe realizar estas prácticas para probar las vulnerabilidades significativas de la empresa y dónde está en juego el mayor impacto financiero. Los directorios deben considerar la posibilidad de participar en, al menos, una de estas iniciativas al año.

Es más, estos ejercicios ayudan a las empresas a desarrollar y poner en práctica planes de acción relacionados con asuntos de privacidad de datos. Las violaciones de ciberseguridad pueden (y a menudo lo hacen) causar la pérdida de datos personales.

En EE.UU. estos eventos requieren el cumplimiento de una serie de leyes estatales y federales (todas las cuales exigen una pronta notificación a los estados, los legisladores y las personas afectadas), y pueden requerir el cumplimiento de las leyes de jurisdicciones no estadounidenses. La práctica es clave para mantener la preparación y responder eficazmente.

Uso de un asesor externo independiente

El número de empresas que revelaron el uso de un asesor externo independiente para apoyar a la gerencia se mantuvo bastante estable. Este año, 12 empresas revelaron esta información, frente a 10 en 2019 y 12 en 2018. Entre las empresas que revelaron información en 2020, sólo 4 dejaron claro que el directorio se reunió directamente con un tercero independiente. La Asociación Nacional de Directores Corporativos (NACD por sus siglas en inglés) y el [Manual de Supervisión de Riesgos Cibernéticos para Juntas](#) (del inglés *Director's Handbook on Cyber-Risk Oversight*) de la Alianza por la Seguridad en

Internet -recientemente actualizado-, alienta a los directorios a considerar la posibilidad de celebrar reuniones informativas en profundidad con expertos independientes externos, para validar si el programa de ciberseguridad de la empresa está cumpliendo sus objetivos.

Nuestra investigación no identificó ningún debate sobre si se obtuvo una opinión utilizando el marco "Controles del sistema y de la organización para la ciberseguridad" del Instituto Estadounidense de Contadores Públicos Certificados, que contempla una evaluación independiente en toda la entidad del programa de gestión de riesgos de ciberseguridad de la empresa.

Muestra de revelaciones de Fortune 100 en 2020

Estructura y frecuencia de los informes de gerencia

Como parte de su programa de supervisión periódica, el Comité de Riesgos es responsable de supervisar el riesgo de ciberseguridad, la seguridad de la información y el riesgo tecnológico, así como las medidas de la gerencia para identificar, evaluar, mitigar y remediar problemas materiales. El Comité de Riesgos recibe informes trimestrales periódicos del Director de Seguridad de la Información y del Director de Riesgos de Ciberseguridad sobre el perfil de riesgo de ciberseguridad de la Empresa y el programa de ciberseguridad empresarial y se reúne con el Director de Seguridad de la Información al menos una vez por trimestre. Anualmente, el Comité de Riesgos revisa y recomienda la política de seguridad de la información y el programa de seguridad de la información de la Empresa al Directorio para su aprobación. Por lo menos una vez al año, el Comité de Riesgos revisa y recomienda la política de seguridad de la información y el programa de seguridad de la información de la empresa al Directorio para su aprobación. Al menos una vez al año, el Directorio revisa y analiza la estrategia tecnológica de la Empresa con el Director de Informática y aprueba el plan estratégico tecnológico de la Empresa.

Capacidad de respuesta y ejercicios de simulación técnica

Tenemos un sólido Plan de Respuesta a las Crisis Cibernéticas que proporciona un marco documentado para el manejo de incidentes de seguridad de alta gravedad y facilita la coordinación entre las distintas partes de la empresa. Colaboramos con nuestros pares en las áreas de inteligencia de amenazas, gestión de la vulnerabilidad y respuesta y simulacros. Realizamos simulaciones de rutina y simulacros tanto a nivel técnico como de gestión. Incorporamos revisiones y conocimientos especializados externos en todos los aspectos de nuestro programa. Todos los colegas reciben una capacitación anual de sensibilización sobre ciberseguridad.

Uso de un asesor externo independiente y participación del directorio

Continuamos una práctica líder en la industria de contratar un asesor independiente de ciberseguridad por cuarto año consecutivo y revisamos un ejercicio de simulación de crisis cibernética que fue utilizado por nuestros altos mandos para prepararse para una posible crisis cibernética. El comité de auditoría recibe regularmente informes de su asesor independiente sobre nuestro programa de ciberseguridad.

Muestra de lenguaje del estatuto sobre las principales responsabilidades de supervisión de ciberseguridad

- ▶ Supervisar el plan de ciberseguridad de la Corporación, el programa de continuidad de negocios, la estrategia de gestión de la protección de la información y los riesgos relacionados con todas estas áreas.
- ▶ Revisar las pólizas de seguro cibernético de la Corporación para asegurar una cobertura apropiada.
- ▶ Revisar el plan de desarrollo y capacitación de la Corporación para el personal clave de TI, así como la planificación de su sucesión

Observaciones del mercado

En los dos últimos años, los líderes de EY se han comprometido regularmente con los directorios y han celebrado reuniones de directores y expertos en ciberseguridad para analizar los desafíos y las prácticas principales en este ámbito. Esto incluye una serie de diálogos de directores a finales de 2019 y a lo largo de 2020 en las que participan más de 500 ejecutivos. A principios de 2020, publicamos las [preguntas recomendadas](#) que los directorios, y en especial los comités de auditoría, deberían considerar para estar más atentos en la supervisión de riesgos de ciberseguridad en el actual entorno de trabajo virtual post Covid-19.

Basándonos en los conocimientos compartidos a través de estos encuentros con los directores, así como en lo que los profesionales de la ciberseguridad de EY están haciendo en todo el mundo y en todas las industrias y empresas de diferentes tamaños, hemos identificado las siguientes prácticas principales de los directorios:

- ▶ **Marcar la pauta.** Demostrar que la ciberseguridad y el riesgo de privacidad son asuntos críticos del negocio, aumentando el tiempo y el esfuerzo del directorio o el comité para discutir el tema.
Mantenerse al día. Aumentar la frecuencia de las actualizaciones del directorio o los comités sobre acciones específicas para abordar los nuevos problemas y amenazas de ciberseguridad y privacidad como resultado del abrupto cambio al trabajo a distancia. Esto incluye tener debates regulares, no filtrados, del directorio con el Director de Seguridad de la Información en sesiones ejecutivas.
- ▶ **Determinar el valor en riesgo.** Comprender el valor en riesgo de la empresa en dólares, más allá del seguro, y cuadrarlo con la tolerancia al riesgo del directorio.
- ▶ **Incorporar la seguridad desde el comienzo.** Adoptar la filosofía "Trust by Design" (Confianza por diseño), diseñando nueva tecnología, productos y acuerdos comerciales, teniendo en cuenta la seguridad.
- ▶ **Evaluar de forma independiente el Programa de Gestión de Riesgos de Ciberseguridad (CRMP, por sus siglas en inglés).** Confirmar que el CRMP es evaluado de forma independiente y apropiada por un tercero con una retroalimentación directa al directorio.
- ▶ **Comprender los protocolos.** Obtener un conocimiento profundo del incidente de ciberseguridad y del proceso y protocolos de escalamiento de la violación, incluyendo un plan de comunicación definido para cuando el directorio deba ser notificado.
- ▶ **Gestionar el riesgo de terceros.** Comprender los procesos de la gerencia para identificar, evaluar y gestionar el riesgo asociado a los proveedores de servicios y a la cadena de suministro. Además, considerar la necesidad de una evaluación para cubrir los riesgos de terceros a lo largo de la cadena de suministro de la empresa.
- ▶ **Someter a prueba la respuesta y la recuperación.** Mejorar la resiliencia de la empresa, sometiéndola a prueba de la capacidad de respuesta y recuperación de ésta mediante simulaciones y acordando protocolos con profesionales externos antes de una crisis.
- ▶ **Monitorear la evolución de las prácticas.** Estar pendiente de la evolución de las prácticas de supervisión de ciberseguridad y revelación de información del directorio y los comités, incluyendo un análisis comparativo con las revelaciones de los pares de los últimos dos o tres años.

Revelación de incidentes cibernéticos

La revelación de incidentes significativos de ciberseguridad aumenta constantemente, pero sigue siendo baja, un 13%, frente al 12% en 2019 y el 7% en 2018. En 2020, 10 empresas revelaron incidentes cibernéticos y cada una de ellas informó un solo evento. Sólo uno de esos acontecimientos se produjo el año pasado y el resto se remontaba a 2006. Alrededor de un tercio de las violaciones de datos se relaciona con ataques cibernéticos de proveedores de servicios externos.

La profundidad de las revelaciones varió, a menudo basándose en qué tan reciente fue el evento. Éstas iban desde la declaración de la ocurrencia de un incidente y sus amplias repercusiones correspondientes hasta la presentación de un informe más detallado, incluyendo el número de titulares de cuentas afectados, la naturaleza de los datos y las medidas correctivas adoptadas para corregir la vulnerabilidad de la seguridad.

En un informe reciente de Audit Analytics, *Trends in Cybersecurity Breach Disclosures*, en el que se examinan las violaciones a la ciberseguridad que afectaron a las empresas públicas de 2011 a 2019, se determinó que el número de incidentes informados alcanzó un máximo de 140 en 2019, lo que representa un aumento del 400% desde 2011. En el informe también se constató que, en promedio, las empresas tardaron más de 100 días en descubrir que se había producido una violación.

Perspectivas de los inversionistas

La ciberseguridad sigue siendo una prioridad para la participación de los inversionistas. Como parte de nuestro programa anual de contacto con inversionistas del Centro EY para Temas de Directorio, en el otoño de 2019 preguntamos a más de 60 inversionistas institucionales, que representaban más de 35 billones de dólares americanos en activos administrados, lo que ellos consideran como las mayores amenazas para el éxito estratégico de las empresas de la cartera en los próximos tres a cinco años.

La ciberseguridad y la privacidad de los datos ocupaban el tercer lugar entre los riesgos más mencionados. Estas conversaciones tuvieron lugar mucho antes del Covid-19 y la consiguiente aceleración del trabajo a distancia.

Los inversionistas, en general, comentaron que todas las empresas de todos los sectores están expuestas a esos riesgos y que, a medida que las preferencias de los consumidores y las exigencias de eficiencia empresarial conduzcan a un mundo cada vez más digitalizado y conectado electrónicamente, los riesgos seguirán multiplicándose. Tras la aparición del Covid-19, esos riesgos se han multiplicado, incluso desde que se celebraron esos debates de acercamiento entre los inversionistas.

Dado que no se puede eliminar la amenaza de una trasgresión, algunos inversionistas recalcaron que están especialmente interesados en la resiliencia, incluida la forma (y la velocidad) en que las empresas detectan y mitigan los incidentes de ciberseguridad.

Algunos preguntan a las empresas de su cartera acerca de prácticas concretas de ciberseguridad, como, por ejemplo, si la empresa ha realizado una evaluación independiente, mientras que otros se centran cada vez más en la privacidad de los datos y en si las compañías están identificando y abordando adecuadamente las preocupaciones pertinentes de los consumidores y los crecientes requisitos reglamentarios.

Orientaciones de la SEC

La Comisión de Valores y Bolsa de Estados Unidos (SEC por sus siglas en inglés) continúa con su énfasis en la ciberseguridad.¹ En un informe de enero de 2020, la Oficina de Cumplimiento e Inspecciones de la SEC señaló que "la gravedad de las amenazas y las posibles consecuencias para los inversionistas, los emisores y otros participantes en el mercado de valores, así como para los mercados financieros y la economía en general, son considerables y van en aumento".²

Con el cambio acelerado impulsado por el Covid-19 hacia los negocios digitales y los cambios masivos, probablemente permanentes, hacia el trabajo a distancia, incluyendo reuniones virtuales de directorio y de gestión ejecutiva, los riesgos de la ciberseguridad son exponencialmente mayores.

La División de Finanzas Corporativas de la SEC también publicó en diciembre de 2019 orientaciones relativas a la revelación de la propiedad intelectual y los riesgos tecnológicos asociados a las operaciones internacionales, debido a la creciente dependencia de la tecnología digital para realizar y gestionar negocios.³

¹ Ver *Spotlight on Cybersecurity, the SEC and You*, Comisión de Valores y Bolsa de Estados Unidos.

² *Cybersecurity and Resiliency Observations*, Oficina de Exámenes e Inspecciones de Cumplimiento, Comisión de Valores y Bolsa de Estados Unidos, enero de 2020.

³ *Intellectual Property and Technology Risks Associated with International Business Operations*, División de Finanzas Corporativas, Comisión de Valores y Bolsa de Estados Unidos, diciembre de 2019.

Las orientaciones de la División establecen, en parte, que:

Alentamos a las empresas a que evalúen los riesgos relacionados con el posible robo o la puesta en peligro de su tecnología, sus datos o su propiedad intelectual en relación con sus operaciones internacionales, así como la forma en que la materialización de esos riesgos puede repercutir en sus negocios, incluida su situación financiera y los resultados de las operaciones, y los efectos en su reputación, el precio de sus acciones y su valor a largo plazo. Cuando estos riesgos son importantes para las decisiones de inversión y votación, deben ser revelados, y alentamos a las empresas a que proporcionen información que permita a los inversionistas evaluar estos riesgos a través de los ojos de la gerencia. Es importante que la revelación de estos riesgos se adapte específicamente a los hechos y circunstancias singulares de la empresa. De la misma manera, cuando la tecnología, los datos o la propiedad intelectual de una empresa están siendo o han sido comprometidos significativamente, robados o se ha accedido a ellos ilícitamente de alguna otra forma, la revelación hipotética de los posibles riesgos no es suficiente para satisfacer las obligaciones de presentación de informes de una empresa. Creemos que las empresas deben seguir considerando esta área de riesgo en constante evolución y evaluar su importancia relativa de manera continua.

Las orientaciones de la División también reiteran lo indicado por la SEC en 2018, que aclararon las obligaciones de las empresas de revelar los riesgos de ciberseguridad, las violaciones significativas y el posible impacto de las violaciones en los negocios, las finanzas y las operaciones, con el objetivo de permitir que los inversionistas tomen decisiones de inversión más informadas sobre los riesgos.⁴

Tanto las orientaciones de la División como las de la Comisión recuerdan a las empresas que una serie de requisitos de revelación de información vigentes de la SEC podrían exigir la revelación de asuntos de ciberseguridad, incluso en la sección de negocios, los procedimientos jurídicos, discusión y análisis de gestión (MD&A por sus siglas en inglés), la sección financiera, controles y procedimientos de revelación de información, el papel del directorio en la gestión de riesgos y los factores de riesgo.

“ Desde el punto de vista de la revelación del emisor, es importante que los inversionistas reciban suficiente información sobre los riesgos e incidentes significativos de ciberseguridad que afectan a las empresas en las que invierten.

Jay Clayton, Presidente de la SEC

La SEC también ha hecho hincapié en la importancia de establecer fuertes controles y procedimientos de revelación para permitir la revelación oportuna y precisa de los riesgos e incidentes de ciberseguridad, así como claras prohibiciones del uso de información privilegiada en relación con los incidentes de ciberseguridad.⁵

El personal de la SEC examina y comenta las revelaciones relacionadas con la ciberseguridad como parte de sus revisiones periódicas de las declaraciones de las empresas públicas. El personal también supervisa los informes noticiosos sobre violaciones cibernéticas para ayudar en este proceso.⁶

El personal de la SEC ha dicho que “no critica los ejercicios de juicios de buena fe sobre las revelaciones de incidentes cibernéticos. Pero también hemos advertido que la respuesta de una empresa a un evento de este tipo podría ser tan deficiente que podría justificarse una medida de aplicación de la ley”.⁷ Ya se ha presentado un caso de este tipo.⁸ Además, la SEC ha presentado una demanda contra una empresa por engañar a los inversionistas acerca de los riesgos que enfrentaba por el mal uso de los datos de los usuarios.⁹

⁴ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Declaración de la Comisión de Valores y Bolsa de Estados Unidos, 2018. Ver también “SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks,” discurso del Presidente de la SEC, Jay Clayton, 6 de diciembre de 2018; publicación de EY 2018 AICPA Conference on Current SEC and PCAOB Developments.

⁵ Ver también How the SEC views cybersecurity disclosures and board’s oversight role de EY.

⁶ “SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks,” discurso del Presidente de la SEC, Jay Clayton, 6 de diciembre de 2018; publicación de EY 2018 AICPA Conference on Current SEC and PCAOB Developments.

⁷ Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay \$35 Million, comunicado de prensa de la SEC, 24 de abril de 2018.

⁸ Ibidem.

⁹ Facebook to Pay \$100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, comunicado de prensa de la SEC, 24 de julio de 2019.

Contacto

Cristián Lefevre

Presidente EY Chile

cristian.lefevre@cl.ey.com

Teléfono: +56 (2) 2676 1165

Departamento de Estudios

estudios@cl.ey.com

EY Chile

Assurance | Impuestos | Consultoría | Estrategia y transacciones | Legal | BPO
www.eychile.cl

| Santiago

EY Chile

Avda. Presidente Riesco 5435

piso 4, Las Condes, Santiago

Teléfono: +56 (2) 2676 1000

| Viña del Mar

| Concepción

| Puerto Montt

Acerca de EY

EY es líder mundial en auditoría, impuestos, transacciones, consultoría y asesoría legal y tributaria. Los puntos de vista y servicios de calidad que ofrecemos ayudan a construir confianza, en los principales mercados y economías donde estamos presentes. Desarrollamos líderes excepcionales que trabajan en equipo para lograr cumplir nuestros compromisos con nuestros distintos grupos de interés. Al hacerlo, jugamos un papel fundamental en la construcción de un mejor mundo laboral; para nuestros colaboradores, clientes y comunidades.

EY se refiere a la organización global y/o uno o más de las empresas de Ernst & Young Global Limitada, cada una de las cuales es una entidad legal individual. Ernst & Young Limited, una compañía del Reino Unido limitada por garantía, no proporciona servicios a clientes. Para obtener más información acerca de nuestra organización, por favor visita www.eychile.cl.

© 2020 Ernst & Young

Todos los derechos reservados.

¿Quiere saber más?

Acceda a información adicional y pensamiento líder en el Centro EY de Temas de Directorio:

ey.com/boardmatters