Supervisión de ciberseguridad y gobierno de datos

Consideraciones clave para los Directorios y los Comités de Auditoría

Los rápidos cambios que realizaron las empresas en 2020 y la primera mitad de 2021 para continuar con sus operaciones durante la crisis del COVID-19 —acuerdos de trabajo remoto, ajustes en la cadena de abastecimiento y mayor dependencia de las plataformas en línea— favorecieron el crecimiento del crimen organizado, los *hacktivistas* y ciberdelincuentes apoyados por gobiernos. Todos los tipos de ciberataques se proliferaron durante la pandemia. Titulares recientes sobre algunos ataques importantes, como el ataque de SolarWinds[1] y el ataque con un software malicioso (*ransomware*) a Colonial Pipeline[2], con consecuencias de gran alcance en las cadenas de abastecimiento y en la economía, ponen de manifiesto el continuo desafío que enfrentan las empresas en materia de ciberseguridad.

A medida que los Directorios evolucionan en sus debates sobre ciberseguridad, gobierno de datos y procesos de supervisión asociados, las siguientes consideraciones podrían ser útiles.

Revisar periódicamente la evaluación de riesgo de ciberseguridad realizada por la gerencia. Cada empresa debería llevar a cabo las evaluaciones de riesgos de ciberseguridad como parte de su operatoria habitual. ¿Cuáles son los activos digitales más valiosos de la empresa, y cuáles son las amenazas y los riesgos más grandes para dichos bienes? ¿Existen brechas de seguridad? ¿Con cuánta rapidez se puede detectar un incumplimiento (o una violación) de seguridad? Una evaluación del riesgo de ciberseguridad sólida debería incluir como áreas de atención clave el liderazgo en ciberseguridad y gobierno, los factores humanos o "riesgos de personas", el cumplimiento legal y regulatorio, la continuidad del negocio, la operativa y tecnología, y el riesgo de la información.

Desafíos e inquietudes generados por la ciberseguridad desde la mirada del Directorio

Nuestras encuestas recientes realizadas a los directores, incluidos los miembros del comité de auditoría, resaltan cada vez más la importancia continua y creciente de la ciberseguridad y el gobierno de datos en las agendas del Directorio y del Comité de Auditoría:

- Las lecciones aprendidas más importantes, y los cambios realizados más significativos, como resultado de la pandemia del COVID-19 en relación con la gestión de la crisis y la estrategia digital[3].
- Los dos asuntos de gobierno principales que los directores citan como los más importantes para la estrategia de su empresa en el año 2021 son las normas y prácticas de ciberseguridad y privacidad de datos[4].
- Muchos comités de auditoría aún tienen numerosas responsabilidades de supervisión de ciberseguridad (62 %) y privacidad de datos (42 %)[5].

[1] *SolarWinds Hack Victims: From Tech Companies to a Hospital* [Víctimas del ataque a SolarWinds: desde empresas de tecnología hasta hospitales], Wall Street Journal, 21 de diciembre de 2020.

[2] *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity* [El ataque a Pipeline enseña lecciones urgentes sobre ciberseguridad en los Estados Unidos], New York Times, 14 de mayo de 2021.

[3] *Views from the boardroom: 2021 pulse survey* [Las miradas del directorio: encuesta de opinión 2021], Board Leadership Center de KPMG, enero de 2021.

[4] Ibíd.

[5] *Challenges presented by COVID-19: 2020 audit committee pulse survey* [Los desafíos del COVID-19: encuesta de opinión al comité de auditoría 2020], Board Leadership Center de KPMG, octubre de 2020.

Si la empresa cuenta con recursos internos suficientes, la evaluación del riesgo de ciberseguridad se puede realizar internamente mediante el uso de marcos estandarizados, como el National Institute of Standards and Technology (NIST). Sin embargo, a medida que las amenazas de ciberseguridad se vuelven más sofisticadas, la empresa podría necesitar el apoyo de especialistas acreditados en seguridad. De hecho, las evaluaciones realizadas por terceros y los análisis sobre la administración de vulnerabilidad pueden ser herramientas útiles para evaluar la solidez de las protecciones asociadas a la seguridad de la información y si existen procesos que estén protegiendo los activos más valiosos.

Prestar atención a la cadena de abastecimiento y otras vulnerabilidades de terceros. Un informe sólido sobre los riesgos de terceros, y su estrecha relación con el proceso de administración de los riesgos de la empresa, debería constituir un tema central para el Directorio. La pandemia del COVID-19 resaltó y, en muchos casos, aceleró la fuerte dependencia de las relaciones con terceros. ¿Cómo ha cambiado el perfil del riesgo de terceros de la empresa como consecuencia del COVID-19? ¿Cómo ha cambiado la evaluación del riesgo de la gerencia para no quedar desactualizada? Los debates del directorio deberían enfocarse, particularmente, en si el inventario de la empresa asociado a riesgos de terceros está actualizado y si los controles de ciberseguridad de terceros se han adaptado al ambiente de riesgo cambiante. Lo más importante es: ¿se ajustan los terceros a las normas de la empresa?

Establecer la importancia de la ética y la limpieza de datos en el debate. Independientemente del cumplimiento técnico de las leyes y regulaciones de privacidad, incluidas las normas estatales o internacionales[6], las empresas necesitan lidiar con la tensión existente entre cómo utilizan legalmente la información del cliente y las expectativas que tienen los propios clientes sobre cómo se utiliza dicha información. A medida que los clientes, empleados, reguladores y otros grupos de interés prestan mayor atención a los asuntos relacionados con la privacidad de datos, esta tensión genera riesgos de confianza y de reputación significativos para las empresas. Para ello, la limpieza de datos debería ser un tema habitual en los debates de gobierno de datos: ¿estamos compilando y guardando información que, en realidad, no necesitamos? ¿Quiénes tienen acceso a nuestra información, además de los vendedores y terceros? Un criterio útil para que el directorio tenga en cuenta durante los debates sobre la limpieza de datos es el siguiente: solo porque podemos, no significa que debemos.

Insistir en el tablero de control de ciberseguridad. Muchos comités de auditoría y Directorios analizan con la gerencia un tablero de control de ciberseguridad (para el período más reciente) que incluye el volumen de los incidentes de ciberseguridad identificados, la importancia y la naturaleza de dichos incidentes, cómo se abordaron, las tendencias claves, y los desarrollos en el ámbito externo (por ejemplo, en el sector público y privado, y a nivel legislativo). Un tablero de control de ciberseguridad puede ayudar a mejorar la calidad de la información y el diálogo del directorio sobre este asunto.

Entender el plan de respuesta de la empresa ante un incidente de ciberseguridad. Como un director de sistemas de información líder nos contó recientemente, es desafiante definir un proceso exacto o un conjunto de pasos específicos para abordar un incidente de ciberseguridad, ya que no todos los incidentes poseen los mismos atributos o generan las mismas consecuencias para la empresa y sus clientes. Dicho esto, la administración de incidentes es un componente muy importante del programa de riesgo de ciberseguridad, y la efectividad del plan de respuesta ante el incidente depende de varios factores. En primer lugar, planificar el escenario es fundamental, y los participantes clave, incluidos los equipos de comunicaciones, legales y políticas, necesitan estar involucrados. Luego, establecer una responsabilidad clara. Si existe un incumplimiento (o una violación), ¿quién es responsable? Finalmente, tomar decisiones, especialmente si el incidente tiene consecuencias externas (como sucede muchas veces). Cuando sea necesario notificar a terceros o clientes, es importante tener un marco para la toma de decisiones, a menudo, de forma muy rápida.

Realizar una designación clara y directa de las responsabilidades de supervisión de ciberseguridad y gobierno de datos.
La ciberseguridad ha evolucionado: pasó de ser un asunto bastante limitado a TI/cumplimiento normativo, típico del comité de auditoría, a ser un asunto del Directorio que, en conjunto con el comité de auditoría o algún otro comité del Directorio, realiza un análisis más profundo. De hecho, dada la nutrida agenda del Comité de Auditoría podría ser útil contar con otro comité del directorio que supervise los asuntos de ciberseguridad y gobierno de datos, y que realice el trabajo pesado. Si bien varios directorios han creado comités de riesgo o tecnología con responsabilidades específicas sobre la seguridad de la información, muy pocos tienen comités permanentes que aborden exclusivamente asuntos de ciberseguridad o tecnología[7].

La elección de qué área del comité se ocupará de la ciberseguridad depende de varios factores. Algunos de ellos incluyen la importancia relativa de los asuntos de ciberseguridad (o de tecnología) dentro de la empresa (¿es central para el negocio o la empresa ha experimentado fallas significativas relacionadas con la ciberseguridad?), la cantidad de información que tienen los comités existentes,

[6] Por ejemplo, la Ley de Privacidad del Consumidor de California, la Reglamentación General de la Protección de Datos, y otras leyes y reglamentaciones relevantes.

[7] Según el análisis de KPMG en base a la información de BoardEx al mes de mayo de 2021, solo el 12 % de las empresas S&P 500 cuentan con un comité de directorio con "ciber" o "tecnología" en su nombre.

y la formación necesaria de los directores en esta materia. En resumen, se debe reconocer la ciberseguridad como una responsabilidad específica del Directorio, y asignar claramente las responsabilidades sobre la seguridad de la información a los comités correspondientes, con el objetivo de enfocar y supervisar este asunto correctamente.

Reforzar los protocolos de ciberseguridad propios del directorio. Además de una mayor vigilancia en relación con la seguridad de las reuniones y comunicaciones del Directorio, el uso de correos electrónicos personales, dispositivos personales o software no autorizado por parte de los directores para realizar sus actividades puede presentar riesgos informáticos graves. ¿El asesor legal o el funcionario a cargo de la seguridad de la información le ha explicado al Directorio los protocolos de ciberseguridad de la empresa que aplican a directores y empleados en el contexto del nuevo entorno operativo? Es probable que a las empresas que cuenten con modelos digitales sólidos, que impulsan las cadenas de abastecimiento y de clientes, la conectividad del empleado y las operaciones basadas en datos e información les vaya mejor. Sin embargo, en el futuro, esa ventaja dependerá de la seguridad subyacente y la mentalidad digital general de la empresa.

Recordar que la ciberseguridad es fundamentalmente un asunto relacionado con el negocio. Si bien resulta útil mantener un diálogo estándar o uniforme en torno al riesgo de ciberseguridad y las actividades para mitigarlo, es frecuente que los debates sobre ciberseguridad recaigan en un lenguaje técnico. El Directorio debería insistir en que la gerencia (asesor de seguridad de la información, asesor de tecnología y asesor de información) aborde estos temas con el Directorio (es decir, las implicancias para la estrategia, el riesgo y la reputación), en un lenguaje claro y en el contexto del negocio.

Autores

Kyle Kappel
Líder de la práctica de Servicios de Ciberseguridad en KPMG LLP

John Rodi
Líder del Board Leadership Center de KPMG

Acerca del Board Leadership Center de KPMG

El KPMG Board Leadership Center (BLC por sus siglas en inglés) promueve un gobierno corporativo de excelencia con el fin de generar valor a largo plazo y fortalecer la confianza de los grupos de interés. A través de una serie de datos, perspectivas y programas, el BLC, que incluye al Instituto de Comités de Auditoría de KPMG y trabaja en estrecha colaboración con otras organizaciones líderes de dirección, promueve la educación continua y la mejora del gobierno corporativo. El BLC trabaja junto con directores y líderes empresariales en los temas críticos que impulsan las agendas de los directorios, desde la estrategia, el riesgo, el talento y los aspectos ESG hasta la administración de los datos, la calidad de la auditoría, las tendencias de representación y muchos otros temas.

Para más información:

kpmg.com/us/blc
T: 1-800-808-5764
E: us-kpmgmktblc@kpmg.com

ICA
INSTITUTO DE COMITÉS DE AUDITORÍA

Contactos

Para más información, por favor visítenos online en www.home.kpmg/ar/ICA o envíenos un email a ica@kpmg.com.ar:

Ariel Eisenstein
Socio Líder de Auditoría
+54 11 4316 5812
aeisenstein@kpmg.com.ar

Viviana Picco
Socia de Auditoría
+54 11 4316 5828
vpicco@kpmg.com.ar

Romina Bracco
Socia Líder de ESG y Sostenibilidad
+54 11 4316 5910
rbracco@kpmg.com.ar

En el Instituto de Comités de Auditoría patrocinado por KPMG brindamos una variedad de recursos diseñados para asistir a Directores y miembros de Comités de Auditoría a mantenerse actualizados y a compartir experiencias que son esenciales para cumplir apropiadamente con su rol. Ofrecemos un programa integral que contempla el patrocinio de eventos y sesiones de capacitación, y la publicación de artículos de especialistas que abordan temas de actualidad.

kpmg.com.ar