Deloitte.

Audit Committee *Brief*

Seleccione un tema

Tecnologías emergentes

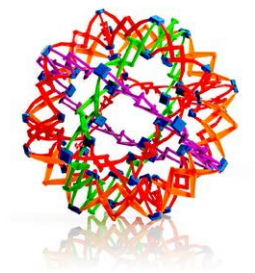
Seguridad cibernética

Tecnología a la vanguardia

La creciente adopción de las tecnologías emergentes a través de todos los tipos de negocios refleja la expansión rápida de los dispositivos y aplicaciones de alta tecnología que han transformado las vidas diarias de las personas en todo el mundo. Dada su importancia global, las implementaciones de la tecnología y las actividades relacionadas con la seguridad ya no pueden considerarse solo en el ámbito de la función de TI. Tales esfuerzos se están volviendo vinculados de manera inextricable con las actividades más amplias de negocios, gobierno y riesgo, tanto para el comité de auditoría, como para los otros miembros de la junta, y para la administración.

Las oportunidades que ofrece el acceso a un conjunto amplio de fuentes de datos y de información tienen que ser balanceadas con el reconocimiento de los desafíos y riesgos – tanto conocidos como desconocidos – que presentan. De acuerdo con ello, los comités de auditoría se pueden beneficiar del entendimiento del panorama general, los planes y las prioridades de la tecnología de la compañía. Para hacerlo, puede ser útil que el comité de auditoría se reúna con el CIO y otros líderes de tecnología al menos anualmente.

Esta edición de *Audit Committee Brief* encuesta las tendencias y los desarrollos recientes en varias áreas relacionadas con la tecnología, incluyendo grandes datos, medios de comunicación social, computación en la nube, implementaciones de TI, y seguridad cibernética. También incluye algunas preguntas que los miembros del comité de auditoría pueden hacerle a la administración y a los especialistas en TI para confirmar que los riesgos y las oportunidades son supervisados de la manera adecuada.



Tecnologías emergentes

Grandes datos

El mundo de los grandes datos se está expandiendo exponencialmente tanto en volumen como en complejidad, y el crecimiento continuado hace que cada año aparezca un panorama virtualmente nuevo para la administración de los datos. Tal y como se observa en *The Dual Roles of the CIO in the Digital Age*, de Deloitte:

- El número de dispositivos móviles y conexiones inalámbricas creció a siete billones globalmente en el año 2013, un incremento de 500 millones en un año.[1]
- Las empresas gastaron más de $30 billones globalmente en hardware, software, y servicios para grandes datos en el año 2013, un 25 por ciento más que en 2011.[2]
- La publicidad en medios de comunicación social se incrementó en un 60 por ciento entre 2011 y 2013 hasta $6 billones.[3]

Claramente ha habido un incremento importante en el volumen de los datos disponibles, pero el término “grandes datos” comprende no solo datos que son grandes en cantidad, sino también información que no está estructurada, es obtenida de formas no tradicionales, o está disponible en tiempo real, incluyendo mediante dispositivos móviles. Las compañías algunas veces enfrentan la perspectiva desalentadora de almacenar y analizar de manera eficiente estos datos diversamente provenientes.

Aunque administrar tales datos puede ser desafiante, hay beneficios importantes e incluso transformadores derivados del aprovechamiento de las nuevas tecnologías de análisis de datos. Pueden ser usadas para mejorar la capacidad de respuesta y la productividad de la compañía, para desarrollar nuevos modelos para dirigir los negocios, y para proporcionarles luces innovadoras a los clientes. Por lo tanto, la organización de TI puede hacer aportes importantes en relación con estrategia e innovación. El CIO será consciente de muchos aspectos del valor y de los riesgos que tales tecnologías pueden proporcionar, y otros miembros de la administración y del comité de auditoría pueden aportar su conocimiento de los riesgos de toda la empresa y de las necesidades del negocio.

Otro aspecto a considerar de las tecnologías de análisis de datos es el impacto que las nuevas implementaciones y los nuevos enfoques tienen en los sistemas heredados. Muchas infraestructuras y aplicaciones viejas son inflexibles y pueden ser alteradas con codificación extra que no cumplió plenamente los requerimientos o que era innecesariamente compleja, lo cual menoscaba la capacidad para ser ágil en la implementación de los nuevos enfoques. En consecuencia, puede haber desafíos relacionados con ganar la aceptación de los ejecutivos organizacionales principales o de los líderes de TI debido a las preocupaciones acerca de la madurez y estabilidad de las nuevas tecnologías que apalancan los grandes datos. Esas consideraciones resaltan adicionalmente la importancia de la comunicación regular con la función de TI para sopesar de manera exacta los riesgos y los beneficios de la adopción de las nuevas tecnologías.

---

[1] http://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networking-index-vni/white_paper_c11-520862.html.
[1] IT Hardware Report," UBS (September 17, 2013).
[1] IA/Kelsey U.S. Local Media Forecast, http://www.marketingtechblog.com/social-ad-spending-forecast/; http://www.clickz.com/clickz/news/2174656/social-media-spendingreach-usd98-billion.

Medios de comunicación social
Las analíticas obtenidas de los medios de comunicación social ya no son el ámbito exclusivo del departamento de mercadeo; también pueden iluminar varios puntos de datos internos casi en tiempo real que pueden mejorar el desempeño de la compañía, haciendo por lo tanto que el uso de los medios de comunicación social sean más prospectivos que muchas medidas tradicionales de datos. Además, el uso estratégico de los lugares de encuentro que ofrecen los medios de comunicación social puede ofrecer una manera importante para que los empleados innoven y colaboren unos con otros. Las compañías deben considerar si más allá de mercadeo hay medios efectivos para usar los medios de comunicación social para los propósitos de negocio, y qué métricas serían más útiles para mejorar la eficiencia y el desempeño operacionales.

Computación en la nube
Recientemente, ha habido un cambio importante en muchas compañías en relación con cómo almacenan los datos. De manera creciente las organizaciones se están moviendo desde las configuraciones tradicionales de TI que incluyen el almacenamiento en-casa para volúmenes relativamente bajos de datos estructurados usando arquitecturas tradicionales de tecnología, hacia un entorno más flexible y adaptable que use arquitecturas híbridas y de nube públicas.

La computación en la nube proporciona acceso diseminado a los datos, desde datos compartidos a los cuales pueden tener los accesos desde cualquier localización. Tal entorno les permite a las organizaciones trabajar con múltiples tipos de datos y volúmenes de información que de lejos exceden los permitidos por los enfoques tradicionales. Con el incremento en la portabilidad y cantidad de los datos viene un incremento acompañante en la complejidad de los datos que pueden ser analizados.

El propósito y el valor de negocios de la computación en la nube deben ser discutidos al comienzo de cualquier implementación asociada. La estructura de control debe ser planeada antes de y monitoreada de manera cuidadosa para evitar los costos asociados con el re-equipamiento. Las compañías también deben confirmar que los proveedores externos protegerán sus datos adecuadamente, y que las actividades de cumplimiento regulatorio y de gobierno de la seguridad de los proveedores satisfacen los estándares de la compañía.

Implementaciones de TI
Las implementaciones de TI afectan toda la organización, dado que a menudo enmarcan el enfoque mediante el cual el negocio es dirigido y la información es difundida. Percibir tal implementación como una tarea solamente relacionada con TI puede incrementar el riesgo del fracaso del proyecto y puede afectar de manera negativa la línea de resultados de la organización, dado que puede no llevarse a cabo todo el valor de la solución. Los prospectos para el éxito son mejorados por la participación activa de la administración principal y de los líderes de todas las funciones afectadas por la organización.

También pueden surgir problemas si el proveedor externo que implementa el sistema no tiene en cuenta plenamente el entorno de control de TI de la organización. El conocimiento técnico del proveedor debe ser complementado por el input específico de la compañía proveniente del equipo interno de TI, con la vigilancia activa de la administración y de la junta. Adicionalmente, pueden surgir interrupciones del negocio si hay provisión insuficiente para las demoras potenciales en el proyecto. El rigor de las actividades de prueba y de valoración del riesgo también puede ser afectado si hay atajos suficientes para estar al ritmo con una programación inflexible.

Si bien es importante reconocer los riesgos inherentes en las implementaciones de TI, se debe entender que las actualizaciones del sistema también pueden mitigar un rango amplio de riesgos e ineficiencias.

Por ejemplo, muchas compañías tienen sistemas ampliamente diseminados en localizaciones dispares en todo el mundo debido a los esfuerzos de trabajar en el extranjero y otros esfuerzos para incrementar la costo-efectividad y la eficiencia. Si bien ciertamente hay situaciones en las cuales tales enfoques pueden ser útiles, se debe considerar si la computación en la nube u otros esfuerzos centralizarían y consolidarían el valor proporcionado por tales sistemas dispares, y si se podrían reducir las redundancias en los datos. Examinar qué arquitectura y qué enfoques tecnológicos tienen más sentido en una base global puede mejorar la seguridad, agregar valor, y resultar en ahorros de costos en el largo plazo.

Preguntas a hacer al CIO y a otros especialistas en TI acerca de las tecnologías emergentes

- ¿Cuáles tecnologías u otras oportunidades tienen el potencial para proporcionar beneficios importantes o transformadores para la compañía?
- ¿Nuestra estructura de datos está apropiada y completamente organizada, y mitiga el riesgo de que información crítica abandone la compañía?
- ¿Cómo aseguramos nuestros dispositivos móviles y cómo difundimos la política que gobierna su uso apropiado?
- ¿Nuestra organización está usando computación basada en la nube, y si es así, los beneficios financieros han sido sopesados contra los riesgos consiguientes? ¿Tenemos un plan para monitorear los riesgos de la computación en la nube?
- ¿Cómo pueden ser integrados la computación en la nube y los sistemas tradicionales para crear soluciones centralizadas que proporcionen desempeño seguro y predecible y que reduzcan las redundancias?
- ¿Cuáles sistemas se deben basar en la nube, y cuáles deben ser operados en el sitio?
- ¿Tenemos una política completa en relación con el uso de los medios de comunicación social por parte de los empleados que sea entendida en toda la organización?
- ¿En qué extensión la compañía apalanca los medios de comunicación social y cómo?
- ¿Cuáles son los riesgos más importantes de los medios de comunicación social que la organización enfrenta?
- ¿Cómo monitoreamos el uso interno de los medios de comunicación social, así como las menciones externas de la organización en los medios de comunicación social?

Seguridad cibernética

Numerosos eventos de interés periodístico han tenido a los problemas relacionados con la seguridad cibernética en la vanguardia de las agendas de la junta y del comité de auditoría en los últimos meses. Incluyen varias infracciones al por menor de alto perfil y, más recientemente, el descubrimiento de la vulnerabilidad de la seguridad Heartbleed, que ofrece un desafío sistémico principal para el almacenamiento y la transmisión seguros de información vía Internet.

Además, el gobierno y los reguladores han incrementado de manera importante su atención puesta en las amenazas cibernéticas. El National Institute of Standards and Technology (NIST) publicó en febrero de 2014 la Cybersecurity Framework [Estructura para la seguridad cibernética] en respuesta a la orden ejecutiva del Presidente Obama dada en el 2013 para mejorar la infraestructura crítica para la seguridad cibernética. Además, la SEC's Office of Compliance Inspections and Examinations (OCIE) publicó en abril 15, 2014 un documento que resalta preguntas muestra y áreas potenciales de solicitudes informativas que la OCIE puede usar al realizar los exámenes, de las entidades registradas, en relación con la seguridad cibernética. Si bien la orientación contenida en el documento no tiene la intención de ser comprensiva, ofrece preguntas útiles para considerar en relación con las vulnerabilidades y adicionalmente demuestra la atención que los funcionarios principales del gobierno le están dedicando a las amenazas cibernéticas.

La estructura de NIST y otros problemas relacionados con la seguridad cibernética fueron discutidos en la mesa redonda que sobre la seguridad cibernética realizó la SEC en marzo 26, 2014. Más información se puede encontrar en el *Heads Up* de Abril 8, 2014, de Deloitte.

El rol del comité de auditoría en la seguridad cibernética

La extensión de la participación del comité de auditoría en los problemas relacionados con la seguridad cibernética varía de manera importante por compañía e industria. En algunas organizaciones, el riesgo de seguridad cibernética es tarea directa del comité de auditoría, mientras que en otras, hay un comité de riesgos independiente. Las compañías para las cuales la tecnología constituye la columna vertebral de su negocio a menudo tendrán un comité dedicado al riesgo cibernético que se centre de manera exclusiva en la seguridad cibernética.

Independiente de la estructura formal adoptada, el ritmo rápido de la tecnología y el crecimiento de los datos, así como los riesgos asociados resaltados por las brechas en la seguridad demuestran la creciente importancia de entender la seguridad cibernética como un riesgo de negocios de toda la empresa, sustantivo, y no como un problema aislado de TI. Tal y como se discute en el *Audit Committee Brief de Agosto 2013*, los comités de auditoría deben ser conscientes de las tendencias de la seguridad cibernética, de los desarrollos regulatorios, y de las principales amenazas para la compañía, dado que los riesgos asociados con las intrusiones pueden ser severos y tener consecuencias económicas y de negocios de carácter sistémico que puedan afectar de manera importante a los accionistas.

Comprometerse en diálogo regular con el CIO y otros líderes organizacionales centrados en la tecnología puede

ayudarle al comité a entender de mejor manera dónde se debe dedicar la atención. Hay dos líneas fundacionales de cuestionamiento que los comités de auditoría pueden querer tener en mente en la vigilancia de los riesgos relacionados con la seguridad cibernética:

- ¿Cómo sabemos cuáles datos están abandonando la compañía, y qué actividades asociadas de monitoreo están en funcionamiento?
- ¿Tenemos un plan de respuesta ante los incidentes cibernéticos? ¿Está actualizado y lo hemos practicado?

Esas consideraciones iniciales pueden servir como plataforma de lanzamiento para indagaciones más detalladas.

Desarrollo y monitoreo del plan de seguridad cibernética
Los planes de seguridad cibernética deben tener en cuenta el pasado, el presente, y el futuro en relación con los riesgos de la seguridad cibernética. Se debe considerar qué porcentaje del presupuesto disponible debe ser dedicado a los esfuerzos de prevención, a la respuesta inmediata a los ataques, y a los esfuerzos relacionados con la capacidad de recuperación. Los atributos importantes de un plan efectivo de seguridad cibernética incluyen los siguientes:

- Asegura: ¿Están en funcionamiento controles para guardarse contra las amenazas conocidas y emergentes?
- Vigilante: ¿Podemos detectar las actividades maliciosas o no autorizadas?
- Capaz de recuperación: ¿Podemos actuar y recuperar rápidamente para minimizar el impacto?

Es riesgoso ver los problemas relacionados con la seguridad cibernética como solo materias relacionadas con el cumplimiento; el solo cumplimiento por sí mismo no implica un nivel aceptable de seguridad.

Mary Calligan
Former FBI Special Agent in Charge, Cyber and Special Operations, New York Office
Director, Deloitte & Touche LLP

La cybersecurity disclosure guidance de la SEC [orientación de la SEC sobre la revelación de la seguridad cibernética] aborda los riesgos de la seguridad cibernética que las compañías pueden necesitar revelar en sus registros corporativos, y tales revelaciones deben ser tenidas en consideración al desarrollar y mantener el programa de seguridad cibernética. La orientación puede ser el catalizador para modernizar los programas de seguridad de la información y respaldar el crecimiento del negocio. Las compañías pueden obtener ventaja competitiva mediante el seguimiento de la orientación de la SEC, dado que las amenazas y vulnerabilidades pueden ser priorizadas desde la perspectiva del crecimiento y el riesgo del negocio.

Las actividades relacionadas con la seguridad cibernética deben extenderse más allá de los esfuerzos de cumplimiento; la auditoría general de TI no reemplaza la auditoría cibernética completa. Confinar los problemas cibernéticos a la esfera del mantenimiento y la seguridad de TI puede no tener en cuenta plenamente la extensión y generalidad del riesgo asociado.

Además, cuando se consideran los planes cibernéticos sobre una base global, los comités de auditoría y la administración deben tener en cuenta las leyes relacionadas con la privacidad, las cuales varían de país a país, y tales consideraciones deben informar el desarrollo de la infraestructura de la tecnología para el monitoreo. Se debe prestar consideración cuidadosa a dónde se construyen y ubican las plataformas, dónde se almacena la información, y quién tiene acceso a esa información.

Por encima de todo, es crítico que haya una comunicación fuerte dentro de la organización en la planeación de cómo comprometer las partes afectadas.

Estructura de NIST

La Cybersecurity Framework [Estructura de la seguridad cibernética] de NIST puede ayudar a focalizar la conversación entre el comité de auditoría, otros miembros de la junta, y la administración principal en relación con cuáles planes relacionados con la seguridad cibernética están en funcionamiento y dónde pueden existir brechas. La estructura ha sido desarrollada mediante la colaboración continua entre el gobierno y la industria privada. Ofrece orientación para ayudarles a las organizaciones a alinear de manera voluntaria las prácticas específicas relacionadas con la seguridad cibernética y las estrategias organizacional de nivel más alto.

Un objetivo clave de la estructura es fomentar que las organizaciones consideren el riesgo de seguridad cibernética como una prioridad similar al riesgo financiero y operacional cuando examinen los riesgos sistémicos más grandes para la organización. Esto puede ayudar a eliminar la brecha entre el mundo aparentemente técnico de la seguridad cibernética y cómo se traslada en las decisiones de gobierno que toman las juntas y los ejecutivos principales. También fomenta el diálogo entre las compañías en industrias similares que tienen interés compartido en identificar y abordar las vulnerabilidades.

El núcleo de la estructura consta de cinco funciones – identifique, proteja, detecte, responda, y recupere – y las actividades relacionadas que proporcionan un punto de vista estratégico, de alto nivel, sobre la administración de la organización en relación con el riesgo de seguridad cibernética y examina las prácticas, las guías y los estándares existentes sobre la seguridad cibernética.

La estructura ofrece un lenguaje común mediante el cual se pueden comparar los enfoques entre las compañías y se pueden compartir las prácticas líderes. Incluso si la estructura de NIST no es adoptada por la organización, puede ser benéfico que el comité de auditoría indague acerca de qué procesos están en funcionamiento o están siendo implementados.

Trabajando con el cumplimiento forzoso de la ley

Las interacciones gubernamentales y otras de carácter externo en relación con la seguridad cibernética son más frecuentes y surgen más temprano a que muchos comités de auditoría se den cuenta. Tan frecuentemente como el 40 por ciento de las veces, las compañías primero escuchan acerca de los incumplimientos de organizaciones externas tales como el FBI, un proveedor de servicios financieros, o una compañía de telecomunicaciones, más que mediante sus propios sistemas de monitoreo. Cuando los problemas son planteados a través de esos medios, cambia el enfoque para enfrentar los incumplimientos, dado que puede haber solicitudes de información, exposición pública incrementada, y la necesidad de orientación legal. Tener en funcionamiento un plan efectivo y demostrable es lo más importante cuando se trabaja con las agencias del gobierno.

Las organizaciones pueden enfrentar solicitudes de cumplimiento forzoso de la ley para tener acceso a sus redes, y esas solicitudes frecuentemente implican procesos legales e indagaciones de reguladores y clientes. Mientras abordan esos problemas, las organizaciones tienen que cumplir con las diversas leyes estatales sobre incumplimiento con los datos y considerar cómo comunicarse de mejor manera con los accionistas y con el público.

Dadas esas sensibilidades, las compañías a menudo son renuentes a compartir con el gobierno la información que no es requerida, pero las entidades que hacen forzoso el cumplimiento de la ley a menudo tienen información que las compañías no, y esto puede ser efectivo para desarrollar una relación con las agencias del gobierno local y nacional de manera que las líneas de comunicación estén abiertas en el evento de un problema. A menudo, ni el gobierno ni la compañía tienen la descripción plena de lo que ha ocurrido, de manera que puede ser benéfico trabajar conjuntamente para llenar las brechas.

Preguntas que el comité de auditoría puede considerar hacerle a la administración para valorar la preparación de la compañía para prevenir y responder ante los ataques cibernéticos

- ¿Cómo sabemos quién está teniendo acceso a nuestra red, y desde dónde?
- ¿Cómo rastreamos qué información digital está saliendo de nuestra organización y a dónde está yendo? ¿Tenemos un programa efectivo de prevención de la pérdida de datos?
- ¿Cuáles amenazas y vulnerabilidades cibernéticas poseen el mayor riesgo para el negocio y la reputación de la organización? ¿Cuáles son los activos clave a ser protegidos? ¿Cuál es nuestra estrategia para abordar las debilidades identificadas?
- ¿Qué sistemas están en funcionamiento para proteger la información transferida mediante tecnologías móviles? ¿Hay una cultura de responsabilidad en relación con las responsabilidades de cada empleado en el uso de dispositivos móviles?
- ¿La administración está focalizada en hacer que el riesgo cibernético sea parte del trabajo de cada uno, y no solo de TI?
- ¿Tenemos los medidores correctos para medir el éxito de nuestro programa de administración de la amenaza cibernética?
- ¿Estamos planeando mapear nuestras políticas de acuerdo con la estructura de NIST? ¿Si ya estamos siguiendo un estándar reconocido en la industria, qué tanto esfuerzo llevaría mapear frente a la estructura los pasos que hemos dado?
- ¿Cuáles son nuestros programas de entrenamiento para educar a nuestro personal acerca de los riesgos y responsabilidades cibernéticos?

Visite el Center for Corporate Governance en www.corpgov.deloitte.com para la última información para las juntas de directores y sus comités.

Para suscribirse a *Audit Committee Brief* y a otras publicaciones de Deloitte, vaya a https://deloitte.zettaneer.com/subscriptions.

Conclusión

Para casi la mayoría de los líderes sabios en tecnología en las organizaciones es altamente desafiante mantenerse al día con el alcance y el ritmo de los desarrollos relacionados con grandes datos, medios de comunicación social, computación en la nube, implementaciones de TI, seguridad cibernética, y otros problemas de tecnología. Tales desarrollos conllevan un conjunto complejo de riesgos, la mayoría de ellos serios que pueden comprometer información sensible e interrumpir de manera importante los procesos de negocio. Pero cuando se implementan exitosamente esas tecnologías también ofrecen tremendo potencial para analíticas de datos, innovación, eficiencias de negocio mejoradas, y compromiso del cliente y del inversionista.

Cuando los comités de auditoría saben cómo centrarse de mejor manera en la vigilancia del riesgo puesta en los problemas de tecnología más críticos para la compañía y para su industria, pueden de manera eficiente confirmar que esté en funcionamiento la estructura apropiada y que el monitoreo continuo y las iniciativas de mejoramiento son adoptados y sostenidos.

Recursos adicionales

The Dual Roles of the CIO in the Information Age

August 2013 Audit Committee Brief: Cybersecurity and the Audit Committee

April 8, 2014, Heads Up: Highlights of the SEC's Cybersecurity Roundtable

iPad app disponible para descarga

Ahora usted puede tener acceso al *Audit Committee Brief* mediante una aplicación gratis, fácil de usar. Las nuevas ediciones del resumen están disponibles para descarga cada mes y se caracterizan por contenido multimedia útil que no está disponible en la edición impresa.
La aplicación también incluye una edición interactiva de la popular *Audit Committee Resource Guide*.

Haga clic aquí o visite la App Store y busque "Deloitte Audit Committee Resources" para descargar la aplicación.

Esta es una traducción al español de la versión oficial en inglés de **Audit Committee Brief, May/June 2014 – Technology at the forefront,** publicado por Deloitte Development LLC 2014 **–** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia