KPMG

Auditoría Interna: Descubriendo el Valor de las Compañías de Tecnología

Las diez principales consideraciones de auditoría interna para las compañías de tecnología

www.kpmg.com/ve

En esta publicación sobre las diez consideraciones principales de auditoría interna para las compañías de tecnología, se esboza el papel crucial que tiene la auditoría interna como apoyo a dichas compañías para que puedan gestionar varias de las áreas de riesgo más importantes de una forma más efectiva y que durante este proceso, puedan descubrir el valor fundamental de la Compañía.

En estos diez sectores de interés se encuentran los riesgos principales que las compañías de tecnología deben encarar cuando diseñan sus estrategias y realizan inversiones.

La selección que KPMG realizó de las áreas de consideración se basó en varios aspectos, entre otros:

— Las conversaciones con los directores de departamentos de auditoría de compañías de tecnología.

— El foro de tecnología de auditoría interna de KPMG

— Las percepciones de los profesionales de KPMG que trabajan con compañías de tecnología.

— Los resultados de encuestas de KPMG, incluyendo el estudio reciente Añadiendo Valor gracias a la Auditoría interna, en el cual KPMG y Forbes encuestaron a más de 400 directores de Finanzas y directores de Comités de Auditoría para identificar cuáles son las percepciones que se tienen de lo que las funciones de auditoría interna están ofreciendo; así como también, cuáles son las oportunidades en las que los departamentos de auditoría interna de las empresas pueden mejorar.

Nota: Cada compañía de tecnología es única, por lo que es importante que al momento de desarrollar cuáles son las áreas de consideración para auditoría interna, dicho departamento trabaje con un análisis de riesgo específico para esa empresa en particular.

Las diez más importantes

01

Cybersecurity

Drivers:

— Evitar las costosas consecuencias originadas por la violación a la información tales como investigaciones, multas, compensación al cliente por pérdidas, esfuerzos para la remediación, pérdida de tiempo y esfuerzo de la Gerencia; así como también, la pérdida potencial de clientes y negocios.

— Evitar cualquier daño a la reputación de la organización, en especial los relacionados con la pérdida de información del cliente.

— Prevenir la pérdida de propiedad intelectual y de capital, así como cualquier otra información privilegiada de la Compañía.

CyberSecurity es un área de enfoque principal para muchas compañías de tecnología, la cual está dejando de ser un simple titular de noticiero y pasando a ser un ítem clave en las agendas de las juntas directivas. Diversos factores han impulsado la creciente atención que se le ha dado a los problemas sobre *cybersecurity*, incluyendo los rápidos cambios en la tecnología y el panorama de amenazas, así como la rigidez y diversidad en los medios regulatorios, los cambios sociales y los cambios en la cultura corporativa.

Las habilidades y técnicas empleadas por los hackers están en una evolución continua, en especial aquellas utilizadas para atacar información o a un individuo en específico. Nuevos métodos están siendo desarrollados constantemente por *hackers*, que son cada vez más sofisticados y que cuentan con mejores recursos (incluyendo el crimen organizado, estados, grupos de apoyo para *hackers*, infiltrados), quienes pueden atacar compañías no sólo de forma directa, sino también a través de un proceso de ingeniería social, estafas de robo de identidad *(phishing scams*) y mediante las relaciones con los proveedores principales y socios de negocios.

Las consecuencias de estas fallas en *cybersecurity* pueden ser desastrosas debido a que afectan el producto final y la reputación de la organización. Es de importancia crítica que las compañías de tecnología se mantengan vigilantes ante las amenazas emergentes y actualicen sus parámetros de protección.

La Auditoría Interna puede ejecutar evaluaciones técnicas y de procedimientos para identificar y evaluar cuáles son los riesgos de la empresa asociados a *cybersecurity*, para luego ofrecer estrategias y recomendaciones a fin de ayudar a mitigar los riesgos identificados.

Ejemplos de áreas de enfoque para auditoría interna:

— Realizar una evaluación de riesgo vertical de los procedimientos de *cybersecurity* de la Compañía, empleando los parámetros de la industria como guía y ofreciendo recomendaciones para mejoras a los procedimientos.

— Revisar los procedimientos y controles existentes para ayudar a garantizar que las amenazas en el entorno están siendo consideradas. Es importante destacar que dichas amenazas están presentes en un medio en constante evolución.

— Revisar la alineación entre las expectativas regulatorias y el marco de referencia de la organización para *cybersecurity*.

— Evaluar la implementación de los modelos de seguridad tecnológica, tales como las defensas en multinivel, los métodos de detección reforzados y la encriptación de la información que sale de la red.

— Evaluar la respuesta ante incidentes de seguridad y los mecanismos de comunicación de la organización.

— Evaluar a los proveedores de seguridad externos para medir si el nivel en el que ellos están encarando, tanto los riesgos actuales como los riesgos emergentes, es completo y suficiente.

KPMG

Uso de Data & Analytics y monitoreo continuo en la auditoría interna

02

En los últimos años, Data & Analytics ha ayudado a revolucionar en la forma en que las compañías evalúan y monitorean, en especial en relación con la expansión eficiente del alcance de las auditorías y con las mejoras en los niveles de detalle en las que éstas son realizadas. El análisis de datos y monitoreo continuo pueden ayudar a los departamentos de auditoría interna a simplificar y mejorar sus procesos; esto resultaría en una mejor calidad de auditoría y un valor tangible para el negocio.

Tomemos en consideración el enfoque tradicional de auditoría, el cual está basado en un proceso cíclico que incluye la identificación manual de objetivos de control, la evaluación y prueba de controles, así como la realización de pruebas de auditoría, utilizando sólo una pequeña parte de la población como muestra para medir la efectividad de los controles o el desempeño operacional.

Ahora contrastemos esta visión con los métodos actuales, los cuales emplean análisis sostenibles y repetibles de información que ofrecen un enfoque más comprensivo y basado en riesgos. Con los análisis de datos, las compañías tienen la habilidad de revisar cada transacción (no sólo algunas muestras), lo que les permite un estudio más eficiente y a mayor escala. Esto también reduce la necesidad de auditorías costosas *in situ*.

Utilizando estos análisis de datos también está incluido un enfoque basado en los riesgos crecientes sobre la detección de fraudes y cumplimiento regulatorio.

Ejemplos de áreas de enfoque para auditoría interna:

— Apoyar en la creación de procesos de extracción automatizada, transformación y carga (ETL por sus siglas en inglés), así como de análisis y paneles de datos sostenibles y repetibles que le permitan a la auditoría interna o a la Gerencia monitorear de acuerdo con parámetros de riesgo específicos.

— Evaluar la alineación entre las metas y los objetivos estratégicos de las áreas de gestión de riesgo de las compañías de tecnología, ofreciendo al mismo tiempo un mecanismo para monitorear y priorizar continuamente los riesgos y objetivos estratégicos.

— Desarrollar programas de auditorías, con análisis de datos incorporados, que estén diseñados para verificar el análisis de datos subyacente y a su vez, puedan generar informes de riesgo a nivel de negocios.

— Realizar auditorías automatizadas enfocadas en el análisis de la causa central y la gestión de las respuestas de riesgo, incluyendo las anomalías de negocios y los eventos detonantes.

— Recomendar el uso consistente del análisis de datos, incluyendo los elementos descriptivos, así como los diagnósticos predictivos y prescriptivos.

Drivers:

— Aprovechar las grandes fuentes de información, tanto internas como externas, para ofrecer una visión organizacional holística.

— Facilitar una gestión de riesgo continua y en tiempo real.

— Permitir la detección temprana de casos potenciales de fraude, errores o abuso de funciones.

— Profundizar en las áreas de riesgo primordiales, mediante el análisis de información clave.

— Incrementar la eficiencia general de las auditorías que se están realizando (en cuanto a frecuencia, alcance, etc.).

— Reducir los costos de auditoría y monitoreo.

— Impulsar el uso de herramientas e infraestructura para el análisis de datos implementadas por la Gerencia.

03

Implementaciones y actualizaciones de sistema: proceso de transición a la nube

Drivers:

— Identificar las necesidades de soluciones en la nube para facilitar la transición e introducir los recientes avances en tecnología externa para mejorar la eficiencia operacional.

— Ofrecer una vista oportuna de los riesgos y problemas que le permita a la Gerencia corregir el curso o implementar estrategias de mitigación de riesgo antes de poner dichas estrategias en marcha.

— Permitir el monitoreo continuo de los riesgos de la información, así como de la nube luego de que ésta sea implementada. De ser posible, introducir la capacidad para la búsqueda de datos y análisis de seguridad para volúmenes considerables de información interna disponible.

— Incrementar la atención sobre la privacidad de la información, *cybersecurity* y resiliencia del negocio dentro del contexto de la nube.

— Implementar un proceso efectivo para identificar y gestionar los requerimientos regulatorios, legales y de cumplimiento en el mercado global, tanto antes como después de la implementación de la plataforma de la nube.

Cuando las compañías mueven sus infraestructuras de TI a la nube tienen que encarar ciertos riesgos y desafíos, esto se debe a que los servicios de la nube vienen en diferentes formas (por ejemplo: SaaS, PaaS y IaaS) y bajo diferentes modelos operacionales (por ejemplo público, privado o mixto). Esto incluye riesgos tales como que las implementaciones de sistemas de nube no puedan ofrecer el valor o los beneficios prometidos, que se sobrepasen del presupuesto o del cronograma, que se ignoren procesos o equipos de trabajo, también administrar a aquellas personas que estén renuentes al cambio. El diseño de la solución debe responder por la naturaleza de los riesgos en un ambiente bajo la nube, así como por su implementación, y debe determinar cómo el proveedor implementará los controles. La fase de diseño de la solución en la nube es la oportunidad principal para reducir o remediar los riesgos y esto se puede lograr si los equipos de TI se involucran de forma proactiva. Toda propuesta de servicios en la nube debe ser evaluada antes de que sea implementada para verificar que cumple con la normativa. Los ciclos de planificación de la nube también deben ser monitoreados continuamente durante todo el ciclo de vida de la solución en la nube (desde el diseño inicial, la selección del proveedor, implementación, uso y desmantelamiento/recopilación de datos).

Más allá de las implicaciones para TI, las operaciones cruciales del negocio, tales como impuestos, cumplimiento normativo, gestión de proveedores y una cantidad de otras áreas también están afectadas. Conforme las compañías navegan por el impacto generado por la continua globalización y recuperación económica, también ha emergido una creciente sensación de urgencia en torno a la seguridad y privacidad de la información. A medida que las compañías de tecnología incrementan su uso de plataformas en la nube, éstas tienen que garantizar que la información esté protegida.

Ejemplos de áreas de enfoque para auditoría interna:

— Revisar el proceso mediante el cual la administración propone la necesidad de la nube y que se realice la debida diligencia de los servicios ofrecidos, tales como la evaluación de los controles internos del proveedor y la cadencia de los roles y responsabilidades tanto del proveedor como de la compañía.

— Evaluar el enfoque de la organización en relación con la administración de cambios y la preparación de la empresa en torno a la implementación.

— Evaluar las políticas, prácticas y controles para la protección, segregación, ubicación y titularidad de la información para determinar si éstas están alineadas con los riesgos ya identificados, con el modelo de operaciones comerciales y con la solución de nube implementada.

— Valorar los programas relacionados con la gestión y comunicación de incidentes, en particular aquellos vinculados con las violaciones a la información y los accesos no autorizados.

— Analizar las disposiciones y responsabilidades ante la disponibilidad del sistema, recuperación después de un desastre y sobre la continuidad operacional, tanto dentro de la Compañía como por parte del proveedor (externa).

— Examinar el cumplimento legal y los requisitos normativos del proveedor, incluyendo una evaluación de las deficiencias conocidas, las responsabilidades de los controles de usuarios y los controles de la compañía sobre el uso de la nube para verificar que estos cumplan con los requerimientos regulatorios.

— Apoyar a la administración en el desarrollo de programas sólidos de seguridad y privacidad, incluyendo proveer entrenamientos.

— Supervisar las auditorías de seguridad de los servicios en la nube.

KPMG

04

Relaciones con terceros

Drivers:

— Reducir las pérdidas

— Prevenir los incrementos en los costos

— Cumplir con los requerimientos normativos

— Mitigar riesgos.

Las organizaciones están contratando a terceros para una variedad de servicios, tales como venta y distribución de productos, almacenamiento de información, administración de programas de control de fondos de mercado, atención al cliente y centros de atención telefónica. Contratar a terceros le permite a la organización disponer de recursos para enfocarse en sus competencias básicas y ayuda a reducir costos.

Si bien es cierto que contratar los servicios de terceros ayuda a facilitar las operaciones comerciales, también pueden exponer a la organización ante riesgos financieros, normativos y de reputación. Estos riesgos pueden ser extensos, incluyendo pérdidas de ganancias, exposición de las exportaciones/importaciones, violaciones a la privacidad de la información, problemas de seguridad cibernética y el riesgo de soborno o corrupción. Las empresas tienen la posibilidad de contratar externamente una variedad de funciones, sin embargo, siguen siendo responsables por estas actividades aun cuando sean realizadas por terceros.

Un programa de administración de relaciones con terceros efectivo, tal como el que incorpora una evaluación de riesgos de terceros, la debida diligencia y monitoreo continuo, puede ayudar a las compañías a gestionar su exposición a estos riesgos.

Ejemplos de áreas de enfoque para auditoría interna:

— Evaluar la metodología que la organización emplea para identificar a terceros, incluyendo la segmentación y clasificación, así como los riesgos asociados a estos.

— Compartir experiencias o conocimientos y retroalimentación sobre el programa de gestión de terceros de la empresa, incluyendo el proceso de investigación de antecedentes, debida diligencia y monitoreo.

— Realizar revisiones a terceros basadas en riesgo, que incluyan procedimientos personalizados para solucionar los riesgos específicos que estos terceros puedan presentar.

— Investigar las anomalías identificadas como resultado del proceso de investigación de antecedentes de terceros de la Compañía.

KPMG

Seguridad de producto

El mercado actual se encuentra centrado en los servicios en la nube; en éste los productos son la vida e imagen de las compañías de tecnología. Por lo tanto, la seguridad del producto se ha convertido en un punto de enfoque primordial en el área de seguridad cibernética para las empresas. Cada producto tiene sus propios requerimientos normativos, políticas de privacidad y vulnerabilidad que le añaden un nivel adicional a la complejidad para los equipos de seguridad comercial. Desafortunadamente, el concepto de seguridad del producto juega un segundo lugar ante la seguridad corporativa, esto ha generado una proliferación de problemas incluyendo pérdidas financieras, juicios largos y reputaciones destruidas.

Cuando se implementa de forma adecuada, la seguridad del producto puede generar el desarrollo de un ciclo de vida seguro y, junto con un monitoreo continuo y un registro forense de la información efectivo, puede minimizar las vulnerabilidades del día cero (*Day Zero* en inglés), reducir los costos de mantenimiento y eliminar potencialmente las próximas amenazas. Es vital que las compañías de tecnología comprendan la importancia de la seguridad del producto y que la empleen para complementar y optimizar sus políticas de seguridad cibernética.

Ejemplos de áreas de enfoque para auditoría interna:

— Evaluar los procesos de encriptación de información para los contenidos en reposo (*at-rest)* y en movimiento (*in-motion)*, para implementar los parámetros de la industria como guía para ofrecer recomendaciones.

— Analizar las políticas de acceso al producto en función de los cargos para garantizar el cumplimiento con las regulaciones en cuanto a la confidencialidad y el *need-to-know*.

— Realizar una evaluación total de riesgo en los puertos de acceso de sistemas operativos, bases de datos y aplicaciones que sean vulnerables, para ayudar a asegurar que se mantenga la integridad de la información.

— Evaluar el cumplimiento normativo de cada producto.

— Evaluar los procesos existentes efectivos de monitoreo continuo y de registro de la información, así como ofreciendo recomendaciones para mejorar dichos procesos.

05

Drivers:

— Reducir los riesgos de mercado, reputacionales y regulatorios asociados con las vulnerabilidades del producto.

— Mitigar las fallas en la seguridad del producto que puedan exponer información del cliente o de la Compañía.

— Apoyar a los diseñadores de producto para que puedan alcanzar un balance entre lo que es conveniente para el cliente y la seguridad del producto.

— Ayudar para que la organización pueda responder adecuadamente ante las vulnerabilidades encontradas o reportadas.

06

Erosión de la base imponible y traslado de beneficios (beps por sus siglas en inglés) y reformas fiscales globales

Drivers:

— Reducir el riesgo de gastos por impuestos a escala global y controlar la volatilidad de los aranceles de impuestos gracias a los cambios rápidos y significativos en la normativa fiscal internacional y las reformas diseñadas para eliminar las estructuras comunes de impuestos empleadas por muchas empresas transnacionales (MNE por sus siglas en inglés).

— Evitar el daño reputacional a la empresa a causa de los nuevos requerimientos regulatorios para una mejor transparencia fiscal y la presentación de informes país por país.

— Disminuir los riesgos por incumplimiento fiscal relacionados con la proliferación de requisitos normativos antiBEPS a lo largo de muchos países.

Las bases para la reforma fiscal mundial ya están completas con la emisión de las recomendaciones para la lucha contra erosión de la base imponible y traslado de beneficios (BEPS) emanadas de la Organización para la Cooperación y el Desarrollo Económico (OECD por sus siglas en inglés) el 5 de octubre de 2015. Durante el 2016 y en lo sucesivo, se espera que las administraciones fiscales del mundo adopten las recomendaciones BEPS dentro de la legislación local. Incluso, algunos países ya las han adoptado. Las recomendaciones de octubre 2015 representan un pilar principal en los esfuerzos del G-20 en la lucha contra la planificación fiscal agresiva de las MNE.

Las reformas BEPS fueron impulsadas en buena parte por la presión política que ha surgido gracias a los informes sobre la evasión fiscal que han aparecido en los principales medios de comunicación, las investigaciones gubernamentales y los crecientes niveles de la deuda pública. Este impulso continuará motivando hacia una adopción global de las recomendaciones BEPS de octubre 2015. Las recomendaciones BEPS tratan sobre varios aspectos de fiscalización corporativa, haciendo énfasis en las mejoras a la transparencia fiscal, normas para fijar los precios de transferencia forzando el pago de impuestos a las ganancias en las jurisdicciones donde las MNE hagan negocios (no en los paraísos fiscales) y ampliando las reglas sobre el vínculo fiscal (Tax Nexus en inglés) para extender el alcance fiscal de los entes regulatorios en los países en los que residen los clientes de las MNE.

Las reformas BEPS tendrán el respaldo de requerimientos de documentación extensos y en algunos países incluirán multas por incumplimiento. Los nuevos requisitos para la presentación de informes serán extensos en muchos casos y muchas de las medidas anti-BEPS son altamente complejas, lo cual generará retos de cumplimiento para las MNE.

Ejemplos de áreas de enfoque para auditoría interna:

— Apoyar a la empresa y al departamento de impuesto para elaborar una evaluación de preparación BEPS y desarrollar un plan de acción para encarar los riesgos que surjan directamente de las reformas por BEPS; así como también, de la implementación de estrategias remediales de BEPS.

— Asesorar en las mejoras o en el desarrollo de un código de conducta para impuestos comerciales y los controles fiscales de apoyo que conforman el nuevo medio normativo.

— Evaluar la preparación de la empresa para el cumplimiento de las diferentes medidas de transparencia a las cuales las MNE serán sometidas, incluyendo la identificación de los interesados y las fuentes de la información necesarias, para poder informar adecuadamente las ganancias y los impuestos pagados por país.

— Ayudar a la Compañía en la evaluación de la efectividad de los programas automatizados de cumplimiento para la generación de informes de transparencia fiscal y para la documentación sobre los precios de transferencia.

KPMG

Fusiones, adquisiciones y desinversiones

07

La necesidad de gestionar los riesgos de forma efectiva está impulsando a muchas compañías de tecnología para que añadan más rigor en sus programas de fusiones, adquisiciones y desinversiones para de esta forma ayudar a garantizar que el proceso de diligencia, valoración, planificación e implementación sea uno, bien controlado y basado en la información.

La tendencia actual en las desinversiones en la industria de tecnología ha motivado a emplear mayores niveles de esfuerzo para gestionar proyectos cada vez más complejos y que requieren de más tiempo.

Ejemplos de áreas de enfoque para auditoría interna:

— Realizar revisiones *post mortem* en acuerdos previos o en desinversiones para evaluar la efectividad de los procedimientos y manuales.

— Evaluar el cumplimiento de las listas de verificación a la debida diligencia de los controles internos y de contabilidad, las cuales trabajan sobre las áreas clave de operación (por ejemplo, la calidad de las ganancias, de los bienes, flujo de caja y las obligaciones no registradas) e identificar las fallas de los controles internos tanto en la compañía adquirida como en la unión de ambas.

— Comprender cómo funcionan los procesos de comunicación entre Finanzas, Auditoría Interna y los equipos de trabajo, para así poder evaluar las implicaciones de control a los cambios al ejecutar procesos comerciales durante procesos activos de integración o escisión.

— Realizar una revisión al proyecto de evaluación de riesgo de la integración comercial o del proceso de escisión, haciendo un énfasis especial en los riesgos potenciales, los análisis de datos del éxito de la integración y los sistemas de información.

Drivers:

— Incrementar el volumen de actividad para el sector de tecnología en el área de M&A y desinversiones.

— Énfasis en los riesgos estratégicos para M&A y para las desinversiones, incluyendo el impacto en otras áreas del negocio, por ejemplo, costos irrecuperables y complicaciones operativas luego de concluida la fusión, adquisición o desinversión.

— Mejorar los procesos de integración (o de disociación) a lo largo de todas las áreas principales.

— Garantizar que la entidad adquirida o escindida cumpla con la ley SOX-404 (Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista), normalmente dentro de los 12-24 meses después de que la transacción haya sido completada.

08

Drivers:

— La aplicación contínua de normativas anticorrupción por parte de los entes reguladores tanto locales como internacionales.

— Enfatizar las iniciativas del Departamento de Justicia de los EE.UU. (DOJ por sus siglas en inglés) para que la legislación contemple que los individuos sean responsables por las infracciones corporativas que cometan.

— La reavivación del enfoque sobre la efectividad de los programas de cumplimiento.

— El incremento en los recursos distribuidos para el DOJ y el FBI para hacer que se cumpla la FCPA.

Cumplimiento con la Ley de prácticas corruptas en el extranjero de EE.UU. (FCPA por sus siglas en inglés) y la normativa anti-soborno y corrupción (ABC por sus siglas en inglés)

El 9 de septiembre de 2015 el DOJ publicó el Memo de Yates, en el cual se anunció el enfoque del DOJ para que los individuos sean responsables por los actos ilegales corporativos cometidos y resalta estos seis puntos de interés para los fiscales del DOJ:

— Las empresas deben presentar al DOJ todos los hechos relevantes sobre los individuos involucrados, en el acto ilícito, para que puedan ser considerados para cualquiera de los créditos por cooperación.

— Las investigaciones corporativas deben enfocarse en los individuos desde el momento de inicio de la investigación.

— Los abogados civiles y penales que se encarguen de la investigación corporativa deben estar en contacto constante entre sí.

— Salvo en el caso de circunstancias extraordinarias, ninguna resolución corporativa ofrecerá protección a la responsabilidad civil o penal para individuo alguno.

— Los casos corporativos no deben ser resueltos si no se tiene un plan claro para la resolución de los casos individuales y los casos de declinaciones, en los cuales se debe dejar registro de dicho evento.

— Los fiscales deben enfocarse consistentemente en los individuos así como en las compañías para evaluar si se debe proceder a un reclamo judicial contra el individuo sin consideración a su capacidad de pago.

Recientemente, el DOJ ha añadido recursos que son los responsables de ofrecer guía a los fiscales del DOJ en relación con la existencia y efectividad de cualquier programa de cumplimiento que la Compañía tenga implementado al momento de que el comportamiento origine cargos penales, así como para evaluar el cumplimiento de la empresa y las medidas remediales.

Ejemplos de áreas de enfoque para auditoría interna:

— Apoyar a la administración para el diseño de una estrategia de cumplimiento antisoborno global que esté basada en el conocimiento y experiencia de campo del departamento de auditoría interna.

— Actualizar los programas de auditoría interna para garantizar que contengan procedimientos antisoborno y anticorrupción que sean aceptables.

— Facilitar la gestión de las actividades de evaluación de riesgo de soborno y corrupción, para ayudar a garantizar que los riesgos emergentes específicos al sector y a las líneas de negocio de la compañía sean identificados y priorizados efectivamente.

— Colaborar con el equipo de negocios y otros equipos de cumplimiento para crear conciencia y realizando campañas educativas, en particular a escala mundial.

— Trabajar con la empresa para mejorar los programas antisoborno y anticorrupción existentes, incluyendo la gestión de riesgo de terceros, la debida diligencia y el análisis avanzado de información

— Ayudar a la compañía para que garantice que se cumpla con los requerimientos/directrices por parte del DOJ en relación con los elementos para un programa de cumplimiento antisoborno y anticorrupción efectivo.

KPMG

Administración de la información

09

Hay una explosión de información que está siendo recolectada y almacenada en plataformas para grandes cantidades de información. Las organizaciones líderes en todas las industrias están impulsando el poder que tiene la tecnología para grandes cantidades de información para recolectar, fusionar y analizar datos internos y externos, de transacciones o hechos históricos, estructurados o no, y con esto la posibilidad de cambiar la forma en la que se realizan negocios y en algunos casos conseguir nuevos negocios. Las empresas que emplean el poder de esta información están viviendo los beneficios.

Sin embargo, el riesgo también está creciendo con la formación de cementerios de información (*data lakes* en inglés). Las regulaciones requieren que las empresas aseguren su información, protejan la información personal del cliente (*Personal Identifiable Information*, PII en inglés), obtengan la autorización del cliente para utilizar su información o le notifiquen a los clientes cómo será utilizada o compartida su información. La auditoría interna juega un papel principal en garantizar que las grandes cantidades de información no generen mayores problemas.

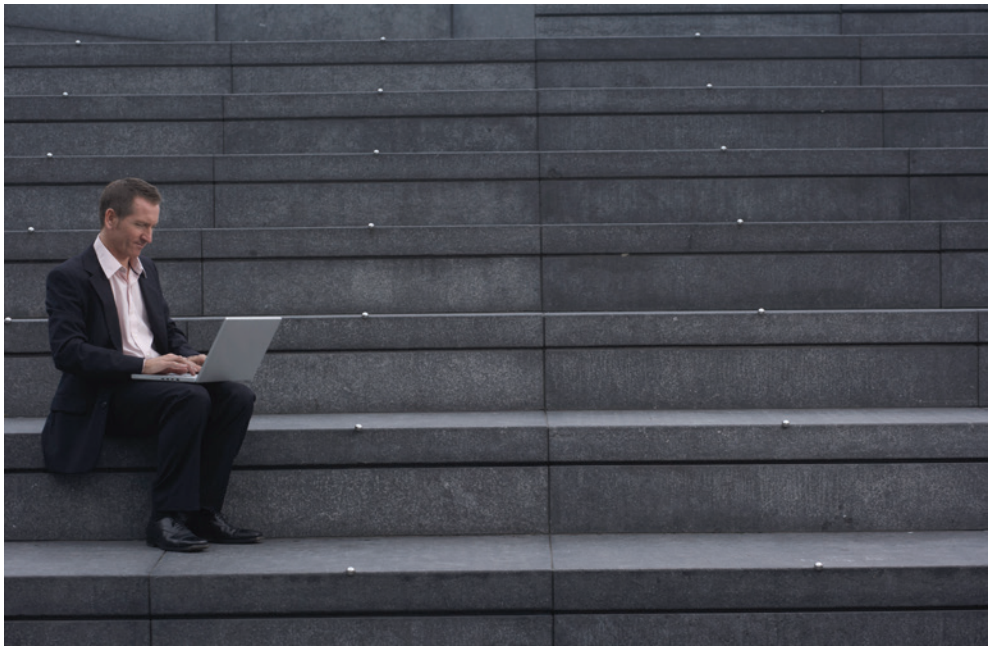
Ejemplos de áreas de enfoque para auditoría interna:

— Apoyar en la creación o en la revisión de las políticas y procesos de administración de la información, para incrementar la exactitud e integridad de los metadatos de la empresa.

— Documentarlos modelos de datos y los puntos de control para poder así identificar las fallas de seguridad. ¿Qué información es recolectada? ¿Dónde es almacenada? ¿Cómo es utilizada? ¿Quién tiene acceso a los sistemas de almacenamiento?

— Ayudar en la creación, o en la revisión, de las políticas de administración de la información que incluyan: diseño, organización, obtención y distribución de la información en la forma que sea más eficiente.

— Revisar la efectividad en la capacidad de respuesta de la empresa ante nuevas políticas y legislaciones emergentes (ordenanzas y normativas), con información apropiada.



Drivers:

— Validar y mantener la exactitud, integridad y el control de las versiones de grandes cantidades de información de la Compañía.

— Garantizar la implementación y cumplimiento de las políticas adecuadas para la seguridad de la información.

— Incrementar la utilización y la comprensión de los metadatos (metadata en inglés se refiere a los datos sobre datos) por parte de los dueños de las empresas.

— Convertir, de forma operativa, los metadatos para que estos puedan ser ejecutables.

10

Drivers:

— Ayudar a garantizar que la información privilegiada específica de la empresa sea almacenada de forma segura y reducir los riesgos de filtración de la información.

— Reconocer cuándo la estrategia de propiedad intelectual (IP por sus siglas en inglés) no está alineada con la estrategia de producto o del negocio y ajustarla hasta alcanzar dicha alineación.

— Garantizar que los procesos de gestión de IP están alineados con los requerimientos para el cumplimiento.

— Reducir los gastos relacionados con errores y litigios.

— Confirmar la protección de las ideas presentadas por sus mejores investigadores, ingenieros y científicos.

— Determinar si debe comprar o crear la PI.

— Identificar y conseguir las mejores ideas para así saber cuáles se deben proteger.

— Identificar qué IP se debe abandonar o vender.

— Decidir si se debe comercializar la IP.

Protección a la propiedad intelectual

La propiedad intelectual es una de las competencias primordiales que se encuentra en el corazón de las compañías de tecnología y en sus relaciones comerciales. Identificar y proteger los bienes de IP es un desafío crítico para las compañías que buscan maximizar el valor de su propiedad intelectual.

Cuando se trata de la identificación de IP, la Gerencia debe tener en juego un proceso que garantice que las mejores ideas están siendo presentadas e identificadas para su protección. En la era actual de la contratación de terceros, servicios en la nube y opciones de acceso remoto (tales como VPN), surgen nuevos retos en torno a la protección de la información que es enviada a terceros, tanto desde una perspectiva tecnológica (por ejemplo, la encriptación de información) como desde una perspectiva empresarial (políticas consistentes en cuanto al intercambio de información).

Los procesos y controles de la compañía en torno a cómo esta transferencia de información es gestionada y asegurada se ha convertido en un punto central para hacer que sus empleados estén conscientes de las políticas existentes y de cuál información es considerada como privilegiada.

Ejemplos de áreas de enfoque para auditoría interna:

— Realizar una auditoría de los accesos de TI y de la seguridad en torno a la tecnología de IP de la compañía, para determinar si existen áreas potenciales de riesgo, en especial, en relación con los cambios en la compañía tales como nuevos sistemas, fusiones/adquisiciones, etc.

— Apoyar en la implementación de controles para ayudar a mejorar la integridad y seguridad de la información crítica de la empresa.

— Ayudar en el desarrollo de parámetros de cumplimiento consistentes y, cuando sean aprobados, informar sobre estos a las personas relevantes mediante un programa de entrenamiento y creando consciencia.

— Realizar una evaluación del proceso, el riesgo y las deficiencias de los procesos internos de IP conforme trabajan con el ciclo de vida de IP.

— Guiar la evaluación de riesgo de terceros y sus medidas de cumplimiento que estén específicamente relacionadas con los acuerdos entre IP y terceros.

Cómo KPMG puede ayudar:

Un equipo con experiencia. Una red global.

Los profesionales de KPMG en las áreas de Auditoría Interna, Riesgo y Cumplimiento combinan el conocimiento de la industria junto con la experiencia técnica necesaria para ofrecer percepciones que ayudarán a los líderes de tecnología para que empleen la ventaja de las oportunidades tecnológicas existentes y las emergentes, y de esta forma puedan gestionar proactivamente los desafíos empresariales.

Los profesionales del área de Advisory de KPMG combinan habilidades técnicas, de mercado y comerciales, las cuales les permiten ofrecer asesoramiento y guía para ayudar a que los clientes de la Firma hagan crecer sus negocios, mejoren su desempeño y gestionen riesgo de forma más efectiva.

Nuestros profesionales tienen una vasta experiencia trabajando con compañías globales de tecnología o empresas nuevas.

Vamos más allá de los retos de hoy y anticipamos las posibles consecuencias a corto o largo plazo de los cambios empresariales en el área de tecnología.

De una presencia mundial, KPMG continúa trabajando en el éxito de nuestras firmas miembro gracias a nuestra clara visión, al mantenimiento de nuestros valores y a nuestra gente en 155 países.

Tenemos el conocimiento y la experiencia para navegar el panorama global.

KPMG

Contáctenos

José O. Rodrigues
Socio de servicios de Auditoría Interna
y Cumplimiento Regulatorio
T: +58 (212) 277 79 79
E: jrodrigues@kpmg.com

Ivan A. Briceño
Socio de servicios de Auditoría Interna,
Cumplimiento Regulatorio y Servicios Forenses
T: +58 (212) 277 79 79
E: ibriceno@kpmg.com

kpmgvenezuela@kpmg.com

kpmg.com/ve

@KPMG_VE

KPMG en Venezuela

KPMGVenezuela

KPMG Venezuela

Caracas
Avenida Francisco de Miranda, Torre KPMG, Chacao, Caracas, estado Miranda, Venezuela.
Telfs.: 58 (212) 277.78.11
Fax: 58 (212) 263.63.50

Puerto La Cruz
Centro Comercial Plaza Mayor, Edificio 6, nivel 2, Ofic. 6C-254
Complejo Turístico El Morro, Municipio Urbaneja, Puerto La Cruz, estado Anzoátegui, Venezuela.
Telfs.: 58 (281) 282.08.33 / 01.33

Barquisimeto
Multicentro Empresarial Crystal Plaza, entre Av. Terepaima y prolongación Av. Los Leones vía Urbanización El Pedregal, PH-A,
Barquisimeto, estado Lara, Venezuela.
Telfs.: 58 (251) 267.65.66
Fax: 58 (251) 267.55.74

Puerto Ordaz
Centro Comercial Orinokia Mall, nivel Titanio. piso 1, Ofic. 1,
Av. Guayana, Alta Vista, Puerto Ordaz, estado Bolívar, Venezuela.
Telfs: 58 (286) 962.42.87 /7460
Fax: 58 (286) 962.67.94

Maracaibo
Torre Financiera BOD, piso 5,
calle 77 / Av. 5 de Julio,
entre Av. 3C y 3D, Maracaibo,
estado Zulia, Venezuela.
Telfs.: 58 (261) 793.47.80 / 49.33
Fax: 58 (261) 793.45.75

Valencia
Torre B.O.D., piso 5, Urbanización San José de Tarbes, Parroquia San José, Valencia,
estado Carabobo, Venezuela.
Telfs.: 58 (241) 823.50.25 / 74.60
Fax: 58 (241) 823.95.35