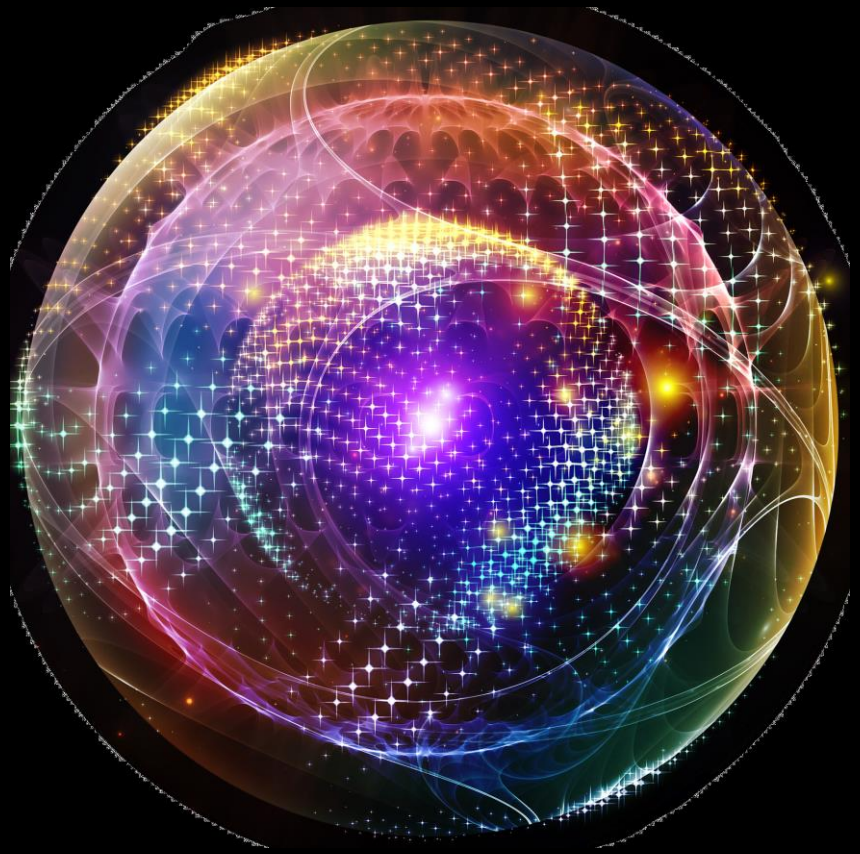
Deloitte.



Internal Audit Insights 2018

Las áreas foco de alto impacto

Marzo 2018

Risk Advisory

Las áreas foco de alto impacto

Nuestras investigaciones y experiencia nos indican que los accionistas esperan que la Auditoría Interna se enfoque más en los riesgos y los problemas del futuro que en los del pasado. Esto significa pasar de auditar el pasado a asesorar sobre el futuro, centrándose en actividades que presentan nuevos y desconocidos riesgos. Algunos requerirán nuevos marcos de trabajo e interacciones con nuevos grupos de interés. Sin embargo, quedarse atrás en el paso de la evolución de la organización y en los requerimientos ambientales, pone en riesgo el papel de la Auditoría Interna como un actor relevante, comprometido y estratégico dentro de la organización.

Para ayudar a las áreas de Auditoría Interna a avanzar con los tiempos, Deloitte realiza anualmente este reporte, que en esta ocasión destaca **13 áreas de alto impacto para el año 2018**, identificando actividades y riesgos que presentan oportunidades para que la Auditoría Interna tenga un impacto positivo, ya sea mediante la adopción de nuevos métodos, como un monitoreo continuo automatizado o la adopción de un enfoque ágil.

Áreas foco de alto impacto

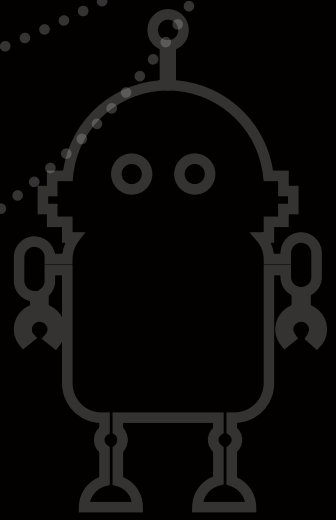
- Automatización Robótica de Procesos y la Inteligencia Cognitiva
- Auditoría del Riesgo Digital
- Cyber Security
- Privacidad de Datos
- Auditoría Interna Analítica
- Monitoreo Continuo Automatizado
- Migrando a la Nube Digital
- Riesgo de Terceros
- Cultura del Riesgo
- Monitoreo del Riesgo Operacional
- Gestión de Crisis
- Auditando Ágil
- Auditoría Interna Ágil

Automatización Robótica de Procesos y la Inteligencia Cognitiva

Automatización de procesos robóticos (*RPA*) es el uso de software para realizar las tareas basadas en reglas en un entorno virtual mediante la imitación de las acciones del usuario para obtener los mismos o mejores resultados. RPA a menudo se nutre de múltiples sistemas y en general, hace que las actividades manuales repetitivas sean más eficientes y eficaces.

Inteligencia cognitiva (*CI*) – un paso más allá *RPA*- incluye el procesamiento y generación del lenguaje natural, la inteligencia artificial y aprendizaje automático. CI puede extraer conceptos y las relaciones de los datos, "comprender" su significado, y aprender de los patrones de datos y experiencia previa.

Tanto *RPA* y *CI* están siendo adoptados en negocio y en funciones de segunda línea, especialmente en los servicios financieros y otras industrias de uso intensivo de datos. Además de muchos beneficios, el *RPA* y *CI* presentan riesgo operacional, financiero, normativo, de organización y tecnología



Importante

- **Como se adoptan funciones RPA, CI, y tecnologías similares,**
  la Auditoría Interna debe apoyar en la identificación, evaluación y seguimiento de los riesgos que vienen junto con estas tecnologías. Esto requiere la comprensión de los nuevos riesgos y demanda controles bien diseñados e implementados adecuadamente, controlando el uso de estas tecnológías en áreas como la integridad, acceso a datos, protocolos de cambio y de seguridad.

- **Los planes de Auditoría Interna deberían abordar los efectos de RPA y CI en los procesos, administración y la organización.**
  Para proporcionar una seguridad razonable, Auditoría Interna debería involucrarse desde el inicio. Revisar la documentación de procedimientos de prueba, documentando resultados generados, y problemas registrados. Asegurando de que exista un marco y un proceso para monitorear los "*bots*" en entornos de pruebas y producción y evaluar los problemas. Las oportunidades incluyen el asesoramiento en la mitigación de riesgos, prácticas líderes y estrategias de automatización.

- **La Auditoría Interna debería considerar el uso de *RPA***
  para automatizar las pruebas de los controles repetitivos y las tareas de informes internos.

Auditoría del Riesgo Digital

Muchas organizaciones han establecido estrategias de transformación digital; creando equipos para desarrollar aplicaciones, sitios web y otros canales digitales.

La Auditoría Interna generalmente tiene un retraso en la comprensión y adopción de las tecnologías, los métodos y las herramientas de las iniciativas digitales. Estos incluyen métodos de desarrollo de aplicaciones, equipos de desarrollo de operaciones (que combinan profesionales de desarrollo y operativos) y herramientas que automatizan los controles.

Las aplicaciones y los sitios web utilizados en la adquisición e interacción de clientes pueden generar una variedad de riesgos de identidad, privacidad y seguridad. Lo anterior, sumado a que muchas organizaciones carecen de marcos de riesgo y de la capacidad para gestionar las complejidades y desafíos de esos riesgos y los que plantean los socios externos que proporcionan estas nuevas tecnologías, canales y servicios.

Importante

- En la planificación de la auditoría, use los temas claves de riesgo de los programas digitales, procesos y productos.
- Revise la estrategia digital y la hoja de ruta y decida dónde enfocarse, dados los temas de riesgo.
- La Digitalización plantea los riesgos cibernéticos habituales, además de nuevos riesgos estratégicos, reputacionales y de terceros, en un entorno acelerado.
- La Auditoría Interna debe tener como objetivo comprender las herramientas utilizadas para automatizar procesos y controles, y luego evaluar la integridad de las herramientas.
- Realice un seguimiento de los proyectos digitales y participe en las primeras etapas y en las iteraciones seleccionadas.
- Céntrese en cómo están involucradas las funciones de riesgo relacionadas, ya que están más cerca de los equipos de entrega. Promueva marcos de riesgo digital adecuados para el propósito, métodos y supervisión en la primera y segunda línea. Esto incluye proporcionar el nivel adecuado de seguridad sobre los marcos para la gestión de partes externas en iniciativas digitales.
- La integración de las plataformas desdibuja los límites entre las organizaciones y los terceros, por lo que debe aclarar los procesos, los flujos de datos y las implicaciones normativas.
- Los grupos de Auditoría Interna utilizan cada vez más *CoSourcing, upskilling* y equipos dedicados para desarrollar el enfoque y los recursos necesarios en esta área.

Cyber Security

En los últimos años, las auditorías de seguridad cibernética a menudo se han centrado en el cumplimiento regulatorio, como la privacidad de los datos, la seguridad de TI y la continuidad del negocio. Estas auditorías generalmente han determinado el cumplimiento de las normas y estándares (como ISO 27000). El cumplimiento seguirá siendo alto en el radar de la mayoría de las organizaciones, especialmente para las organizaciones que cotizan en los Estados Unidos con la Comisión de Bolsa y Valores, haciendo que la seguridad cibernética sea una prioridad en su Programa Nacional de Exámenes. Además, diariamente se desarrollan nuevas regulaciones, en paralelo con el nuevo examen de gestión de riesgos de ciberseguridad *AICPA* (American Institute of Certified Public Accountants). Las compañías deben seguir centrándose en la seguridad, al tiempo que comprenden que el cumplimiento de las normas existentes difícilmente garantiza una gestión de riesgos cibernéticos alta, o incluso adecuada. Cabe destacar que aunque la mayoría de las actividades de seguridad cibernética se centran en el área de TI, correo electrónico corporativo y similares, los riesgos más altos provienen de equipos de negocios que utilizan sistemas basados en la nube, trabajan con desarrolladores externos y usan aplicaciones fuera de TI. Gran parte de esta actividad escapa a la atención del CIO, el CISO y la Auditoría Interna, y presenta serios riesgos.

El desafío ahora es identificar una gama más amplia de riesgos cibernéticos antes de que ocurran.

Importante

- Los auditores internos necesitan nuevos modos de pensar y métodos, para seguir proporcionando seguridad relacionada con el cumplimiento. Comience por pensar ampliamente. Por ejemplo, en una compañía farmacéutica, Auditoría Interna puede auditar los riesgos cibernéticos relacionados con las regulaciones de privacidad y los ensayos con medicamentos, pero pasar por alto los relacionados con un pequeño reactor nuclear utilizado en radioisótopos (una situación real).
- En la planificación de Auditoría Interna, sea proactivo y establezca una amplia red. Mire más allá de los planes de auditoría rotacional para buscar nuevas iniciativas, productos, mercados, contratos y partes externas. Luego desafíe a la gerencia en la identificación de riesgos, el monitoreo y la gestión en esas áreas.
- La alta gerencia debe inculcar una cultura en torno al riesgo, inculcando cómo las decisiones y comportamientos aumentan o minimizan el riesgo cibernético.
- Fomente el uso de "*war gaming*" para evaluar el impacto de los incidentes cibernéticos en las operaciones, la infraestructura, los datos, las finanzas, la reputación y la recuperación, y para medir las respuestas y la capacidad de recuperación, que deben evaluarse periódicamente.

Privacidad de Datos

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea (UE), vigente a partir del 25 de mayo de 2018, afecta a todas las organizaciones de la UE que recopilan o procesan datos sobre individuos y organizaciones no pertenecientes a la UE con operaciones de la UE.
El GDPR amplía enormemente la capacidad de los individuos para determinar qué datos personales se recopilan sobre ellos y cómo se tratan. Por ejemplo, las personas tendrán que optar por permitir ciertos usos de sus datos. El GDPR establece fuertes sanciones por incumplimiento y exige el nombramiento de un Oficial de Protección de Datos (*DPO*) y documentación detallada de funciones, responsabilidades y procesos relacionados con la recopilación, el uso y la retención de datos sobre personas, incluidos empleados y contratistas independientes.

En Chile, la Ley de Protección de Datos, que se encuentra en el Congreso, se vislumbra en la misma línea.

En este sentido La Auditoría Interna puede ayudar a la organización a gestionar el mayor riesgo que plantean las nuevas reglamentaciones y a darse cuenta del potencial de una mejor comprensión de los datos que este trabajo puede crear.

Importante

- Las organizaciones deben establecer responsabilidades claras en torno a los datos. Además de designar un DPO, esto significa aclarar quién es responsable de abordar los requisitos específicos, como las solicitudes de datos, la respuesta de incumplimiento y la retención de datos. Las responsabilidades y los procesos relacionados deben documentarse en un marco que explique la ejecución de las solicitudes de información, la retención de datos y otros procedimientos.
- Las compañías deben enfocarse en el ciclo de vida de los datos y en las políticas de retención y eliminación.
- Las empresas deben documentar qué datos se recopilan por qué sistemas, dónde se transfieren y almacenan los datos y con qué fines.
- Se debe realizar un mapeo de los datos, identificando repositorios y flujo de datos, quién los usa y quién puede modificarlos. Con esto la organización podría responder a consultas de información y gestionar el consentimiento individual.
- Adopte un enfoque basado en riesgo en la planificación de la Auditoría Interna, para abordar las solicitudes y los requisitos. Enfatice los sistemas clave, según lo definido por el volumen de datos, la importancia y la sensibilidad.
- Asegúrese de que se realice una evaluación de Impacto de la Privacidad de los Datos (DPIA) para cualquier nueva iniciativa que implique datos individuales y preste especial atención a la entrega de datos a terceros.

Analytics para Auditoría Interna

El *analytics* es un área perenne de alto impacto por varias razones. Primero, más allá de lo básico, el análisis es el estímulo más poderoso de la eficacia y eficiencia de la Auditoría Interna. Segundo, la digitalización continua de los negocios genera enormes cantidades de datos, que *analytics* puede transformar en información valiosa y conocimientos del negocio. Tercero, las herramientas para analizar y visualizar datos ahora son más simples, baratas, disponibles y fáciles de usar que nunca. Finalmente, las necesidades de los stakeholders de garantías de alto nivel, conocimientos y anticipación del riesgo, nunca han sido mayores.

Sin embargo, la adopción de *analytics* por parte de la Auditoría Interna, ha sido relativamente desigual y lenta. La Auditoría Interna es, sin dudas, una función que puede encontrar difícil cambiar el status quo y adaptarse a una nueva forma de vida. Una barrera para el progreso a menudo no diagnosticada puede ser la metodología: los enfoques de auditoría tradicionales pueden ahogar la innovación, restringir la recopilación de datos y tratar el análisis como una capacidad de conexión en lugar de un imperativo.

Importante

- El *analytic* debe ser considerado parte integrante de toda la planificación, ejecución y generación de informes de Auditoría Interna, y deben reflejarse en los métodos y las habilidades correspondientes.
- Utilice los datos en la etapa de determinación del alcance de la auditoría para resaltar patrones inusuales, relaciones inesperadas y cambios en las condiciones del negocio.
- Inicie proyectos pilotos para demostrar el valor de los análisis, donde los datos estén fácilmente disponibles, el éxito es bastante cierto y los resultados generarán valor (como la reducción de fraudes, desperdicios u otras infracciones de políticas).
- Comience con una hipótesis y recopile datos relevantes; por ejemplo, esperamos un cierto comportamiento o resultado aquí; ¿Es eso apoyado por los datos? A continuación, repita los datos para generar un muestreo y generar información relevante (en lugar de listas de excepciones) y comuníquese con las herramientas de visualización de datos.
- Además, considere usar RPA y CI (como se indicó anteriormente) para automatizar las tareas repetitivas y acelerar los informes. Fije sus miras en "IA digital", un conjunto integrado de capacidades analíticas orientadas al uso de tecnologías avanzadas de auditoria.

Monitoreo Continuo Automatizado

Los líderes se dan cuenta de que los riesgos asociados con las actividades normales deben gestionarse incluso mientras persiguen nuevas iniciativas, y esperan una continua garantía de estas actividades básicas. Los grupos de Auditoría Interna deberían moverse para proporcionar esta comodidad continua -seguridad continua- en esos procesos centrales, controles y actividades a la gerencia y la junta.

El monitoreo automatizado implica informes en tiempo real que marcan los elementos accionables. Estos permiten una remediación rápida, con la opción de un monitoreo continuo a la espera de nuevas notificaciones. En este punto, utilizar un enfoque de muestreo cuando toda la población podría ser monitoreada e informar detalles irrelevantes, se está convirtiendo en un sello distintivo de una función de Auditoría Interna que no puede mantenerse al día con los desarrollos o proporcionar seguridad de manera eficiente.

Las tecnologías para facilitar el aseguramiento automático y la generación de informes en tiempo real incluyen herramientas listas para usar, que ofrecen algunos beneficios, y soluciones personalizadas que pueden brindar seguridad automática sobre la mayoría de los procesos y controles más críticos.

Importante

- Evalúe los procesos centrales en la primera línea, su criticidad y los riesgos, y luego priorice en consecuencia respecto a los impulsores de valor.
- Promulgue el uso de las herramientas **tecnológicas** y las capacidades de estas para automatizar la garantía del núcleo y la integración de ellas en procesos y sistemas. Las funciones de primera y segunda línea a suelen desconocer estas capacidades, y los proveedores rara vez las enfatizan.
- No todo lo conversado con los accionistas debe ser automatizado, ya sea la identificación de riesgos claves o los controles para monitorearlos .Esto trae distintos problemas de alcance, ya sea, por ejemplo, los riesgos y controles financieros u operacionales
- Familiarícese con las posibilidades de las herramientas de automatización y encuentre ganancias fáciles y rápidas, que suelen estar en torno a reconciliaciones y controles financieros claves.
- La automatización ofrece ahorro de costos y una mayor seguridad al mismo tiempo. La automatización del monitoreo continuo también permite a la Auditoría Interna asignar recursos a áreas y actividades de mayor valor.

Migrando a la Nube Digital

El uso de servicios en la nube puede alterar significativamente el perfil de riesgo de una organización, junto a el servicio en la nube y el tipo de modelo. El término nube incluye Software como un Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS). SaaS y PaaS proporcionan software y plataformas basados en la nube, mientras que IaaS proporciona servicios de infraestructura.

Los modelos de servicios en la nube incluyen modelos privados, públicos o híbridos (una combinación de servicios en las instalaciones).

Los riesgos para estos tipos de servicios dependen principalmente del acceso y la criticidad de los datos. Dado los diferentes niveles de control del usuario, los requisitos de seguridad diferirán para cada servicio y tipo de modelo. Los controles de seguridad también dependerán de los datos y procesos involucrados.

Independientemente del tipo de servicio, en una nube pública, le está confiando datos a un tercero, y puede auditar el diseño y la ejecución de los controles solo hasta un punto, después del cual usted confía en la seguridad de esa parte. Independiente de la protección que se obtenga del proveedor de la nube o de la adquisición, la visión del proveedor es limitada..

Importante

- Las auditorías tradicionales de áreas siguen siendo relevantes para la nube, como por ejemplo en la configuración de red, la protección de activos, el control de acceso, el registro y el monitoreo, y la evaluación de vulnerabilidad, pero estas pueden diferir.
  Los estándares y directrices de nube de SANS Institute, NIST, ISO y Cloud Security Alliance son útiles, pero cada uno tiene su propio enfoque, por lo que debe adaptar un enfoque que se adapte a la estrategia de su organización, perfil de riesgo, caso (s) de uso de la nube y servicio en la nube

- Evalúe tanto el entorno de la nube de manera integral como los elementos de gobierno y las responsabilidades compartidas.

- Considere obtener certificación en la nube y aprovechar la experiencia externa.

- Garantice el valor óptimo eligiendo cuidadosamente los servicios, monitoreando y administrando los recursos de manera rigurosa, y desactivar los componentes innecesarios con prontitud, todos los elementos para revisar

- Asegúrese de que la gerencia comprenda cuáles responsabilidades contractuales son las del proveedor de servicios en la nube, las de la organización o las compartidas.

Riesgo de Terceros

Desde hace tiempo, los líderes organizacionales esperan garantías sobre los distintos procesos en los que están incluidos los proveedores. También esperaban auditorías orientadas a identificar posibles ahorros de costos y recuperación.

Los desarrollos en tecnología y automatización han introducido capacidades analíticas más avanzadas y garantía en tiempo real. Más allá de esto, sin embargo, los líderes quieren -y necesitan- una imagen más integral de los riesgos de terceros y su gestión.

Esto requiere que la Auditoría Interna comprenda el enfoque completo de la organización a las relaciones con terceros. Como se señaló en una encuesta de Deloitte Global del 2016, el universo de riesgo de terceros incluye el ecosistema de terceros, la gestión de riesgos y la gobernanza de estos.

Si bien el ahorro de costos y la recuperación siguen siendo claves, la excelencia en la gestión extendida de riesgos empresariales (EERM) también es
imprescindible. Esto se debe a que los terceros se han vuelto críticos para la mayoría de las organizaciones a la vez que presentan innumerables riesgos.

Importante

- Comience con una evaluación de los contratos de terceros sobre la base del gasto y el riesgo, cuando planifique sus auditorías internas.
- Promueva la adopción de herramientas automatizadas para analizar el gasto y el rendimiento del proveedor, si no están en su lugar; si están en su lugar, asegure su integridad y eficacia.
- Estas herramientas también liberan recursos para trabajar en otros riesgos de terceros o empresas extendidas.
- Utilice un marco general de EERM para exponer áreas clave de riesgo específicamente integradas dentro del ecosistema de terceros.
- Reduzca el riesgo sobre el abastecimiento de bienes y servicios más críticos para la estrategia y las operaciones comerciales mediante programas efectivos de auditoría que evalúan la salud del ecosistema y sus componentes.

Cultura del Riesgo

La cultura de una organización juega un papel importante en el rendimiento del negocio y la reputación del mercado. La misma también puede crear riesgos para la organización cuando hay una desalineación entre los valores de una organización.

El centro de atención suele estar en cuestiones de riesgo cultural solo después de una crisis o incidente organizacional, pero un número creciente de líderes están cambiando el enfoque que lo convierte en un habilitador de valor y en un impulsor del desempeño organizacional. Este se sustenta en información sobre la cultura de la organización y el comportamiento de los empleados.

Como tercera línea de defensa, la Auditoría Interna desempeña un papel vital en la gestión del riesgo de la cultura: brinda seguridad y asesoramiento sobre la cultura según corresponda y valida las actividades de mitigación. La cultura de auditoría se trata de desarrollar una comprensión del enfoque de las personas para gestionar el riesgo.

En una cultura fuerte, existe una clara conciencia y alineación de valores, procesos organizacionales, normas de comportamiento, declaraciones internas y externas y sistemas de recompensa para promover las decisiones correctas, los comportamientos correctos de gestión de riesgos, la conducta correcta y, por lo tanto, el derecho cultura.

Importante

- Considere aspectos de la cultura a lo largo del ciclo de vida de una Auditoría Interna; coordine con las partes interesadas culturales para comprender las posibles áreas de riesgo para optimizar la cobertura de auditoría
- Vincule las evaluaciones culturales y de participación de los empleados con las evaluaciones de riesgos de Auditoría Interna e incorpore la cultura aspectos de métricas y control en los programas de auditoría, incluidos los aspectos de riesgo cultural en los informes de auditoría.
- Proporcione recomendaciones a gestión y realice procedimientos adicionales para evaluar la efectividad de los programas de gestión del riesgo cultural. Una evaluación del riesgo de la cultura puede proporcionar información sobre los factores intangibles de riesgo, la efectividad de los controles, las fallas en el cumplimiento y la posible mala conducta.
- Dicha evaluación puede incluir una variedad de actividades, como entrevistas confidenciales, grupos focales y análisis de datos orientados a descubrir dónde los controles funcionan bien, causar frustración o no entregar los resultados esperados.
- Evalúe cómo la cultura difiere entre las ubicaciones y determine si el marco de gestión de riesgos puede identificar y abordar el comportamiento atípico.
- Trabajar para garantizar que la segunda línea de defensa tenga visibilidad de la cultura en la primera línea, y garantizar que la gerencia y la Junta entiendan que la cultura siempre seguirá siendo un trabajo en progreso.

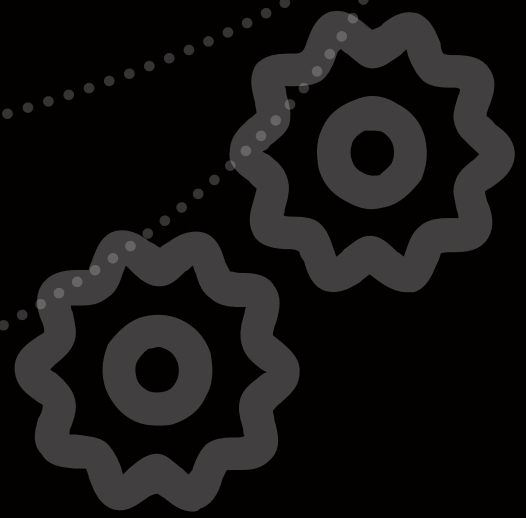
Monitoreo del Riesgo Operacional

Si bien funciones como la seguridad cibernética y la salud y seguridad de los empleados ya brindan protección en torno a las operaciones, la Auditoría Interna debe realizar evaluaciones más profundas de la eficiencia operativa, la efectividad y la gestión de riesgos.

Las auditorías operacionales se enfocan principalmente en activos y procesos no financieros. Su objetivo es determinar cómo el rendimiento se alinea con las expectativas de la administración, identificar las áreas que se investigarán y proponer mejoras

Incluso en industrias de capital intensivo como la manufactura, el petróleo y el gas, las auditorías tradicionales pueden pasar por alto las operaciones básicas.

Los grupos de Auditoría Interna en tales industrias suelen realizar auditorías útiles a nivel de compañía en torno a la cadena de suministro, ciberseguridad, cumplimiento de contratos, proyectos de capital, capital humano y sostenibilidad. Sin embargo, las auditorías a nivel de campo (productividad, gestión del rendimiento de los activos, actividades de mantenimiento) pueden presentar más oportunidades para agregar valor.



Importante

- Un enfoque claro en las operaciones centrales exige una comprensión de las operaciones a nivel de campo, así como de los riesgos operacionales a nivel de la compañía.
- Asegúrese de que las actividades de segunda línea brinden la seguridad adecuada y, de lo contrario, ayúdeles a hacerlo o proporcione la garantía adicional necesaria
- Vincule las actividades operativas de auditoría a los objetivos y estrategias de la organización y a los riesgos operacionales clave que se les plantean cuando desarrolle el plan de Auditoría Interna.
- Identifique los próximos proyectos de capital, mantenimiento significativo e iniciativas similares, utilizando un lente de riesgo operacional.
- **Observe la evaluación de riesgos de la organización** y el sistema de monitoreo del riesgo operacional, pero también mantenga conversaciones sólidas con los principales ejecutivos operativos.
- Aplique análisis para procesar datos para aislar tendencias, patrones, anomalías y causas raíz, y mejore los informes a través de herramientas de visualización, información adicional y anticipación al riesgo.
- Considere si se pueden necesitar recursos externos especializados en la materia o si se puede acceder al conocimiento internamente a través del auditor invitado o los programas de rotación.

Gestión de Crisis

La gestión de crisis proporciona la estructura, el liderazgo, la toma de decisiones y las comunicaciones para ayudar a la organización a gestionar una situación de crisis. Abarca la continuidad del negocio, la recuperación de desastres, la respuesta al incidente cibernético y la planificación y ejecución de la respuesta a la crisis del mercado financiero.

La mayoría de las organizaciones principales cuentan con planes básicos de continuidad comercial y planes de recuperación ante desastres, en particular para TI, cadenas de suministro e instalaciones.

Por lo general, la Auditoría Interna revisará los planes de manera rotatoria, brindará garantías sobre el cumplimiento relacionado y realizará revisiones posteriores al evento.
Sin embargo, el enfoque en la gestión de la continuidad se ha ampliado para incluir cualquier evento que pueda dañar irreparablemente las finanzas, las operaciones, las capacidades cibernéticas, la reputación u otros activos esenciales.

Un plan de gestión de crisis proporciona un marco y planes de contingencia para los altos ejecutivos si surge la necesidad. La responsabilidad de la gestión de crisis recae en los altos directivos, lo que significa que Auditoría Interna es la fuente lógica y quizás única de garantía y asesoramiento.

Importante

Una organización necesita un programa de gestión de crisis que abarque la gobernabilidad, los procesos y los riesgos.

A) La gobernabilidad organiza la propiedad del programa y los roles y responsabilidades de seguridad, legal, informática, Auditoría Interna y otras funciones.

B) Los procesos son necesarios para abordar la respuesta a crisis, la toma de decisiones, la recuperación, las comunicaciones y los planes de contingencia.

C) Deben identificarse los riesgos para permitir la planificación de escenarios y el desarrollo de la capacidad de respuesta mediante capacitación y simulaciones.

Considere si los líderes pueden responder las preguntas: ¿Para qué están preparados? ¿Qué tan preparado están?

- Asegúrese de que las simulaciones se realicen regularmente y se usen para desarrollar y probar planes generales, así como libros de jugadas para eventos específicos.
- Vaya más allá de la guía regulatoria y las listas de verificación y audite no solo la existencia de los planes, sino también su posible efectividad.
- Además, considere los temas específicos de la industria y las regulaciones en evolución, como los requisitos de informes GDPR de la UE para las infracciones

Auditando Ágil

Las organizaciones están adoptando cada vez más Métodos Ágiles (*Agile*) de administración de proyectos y procesos. Las empresas y las funciones en tecnología y servicios financieros lideran el camino, pero otros que buscan mayor velocidad, eficiencia e innovación también se suman. (Incluyen las funciones de Auditoría Interna, ver a continuación.) Los resultados deseados incluyen resultados más rápidos, un mayor enfoque en las necesidades del usuario, una toma de decisiones más ágil y una documentación reducida.

Agile permite que las personas tomen decisiones y tomen riesgos calculados basados en objetivos más específicos entregados en plazos más cortos, pero estos atributos pueden enfatizar algunos entornos de control. Un ritmo acelerado puede introducir impactos o errores más frecuentes.

Un enfoque intenso en las necesidades de los usuarios puede pasar por alto otras consideraciones, como las preocupaciones de seguridad o reglamentarias, que pueden mitigarse asegurando que los estándares sean conocidos y aplicados en los equipos de *Agile*.
La reducción de la documentación puede dificultar saber qué se hizo, por quién, cuándo y por qué.

La Auditoría Interna debe conocer los procesos y proyectos ágiles en la organización y sus posibles problemas e impactos.

Importante

- Los auditores internos deben comprender los métodos ágiles y aclarar las responsabilidades, los cronogramas, los recursos, los entregables, y los riesgos y controles, en una conversación con los líderes del equipo ágil.
- Una estructura más plana puede significar una mayor variabilidad en la forma en que se logran los resultados, mientras que una menor cantidad de documentación puede reducir la visibilidad de los riesgos.
- **La Auditoría Interna debe evaluar los riesgos y controles durante todas las fases**, desde la ideación hasta la pre-implementación.
- Auditoría Interna puede acercarse mejor a *Agile* entendiendo qué se debe entregar, qué objetivos del proyecto o proceso de *Agile* se logran, riesgos de entrega y controles propuestos, y entendiendo cómo se está entregando, incluida la administración de riesgos y el uso de controles.
- El compromiso proactivo de Auditoría Interna **es clave** para establecer cómo se puede gestionar *Agile* y mantener niveles de control equilibrados y sostenibles.

Auditoría Interna Ágil

Los grupos de Auditoría Interna con visión de futuro están aplicando principios y prácticas de desarrollo ágil a auditorías y proyectos. Los Métodos Ágiles (*Agile*) fomentan una respuesta rápida a problemas emergentes, una colaboración más estrecha con las partes interesadas, ciclos de entrega más rápidos y generación de informes simplificada.

Agile también cambia el enfoque que los auditores internos llevan a su trabajo. Por ejemplo, en lugar de auditar a un cronograma periódico, se realizan auditorías internas cuando es necesario, particularmente cuando la necesidad es urgente. En lugar de esperar hasta que se complete una Auditoría Interna, los auditores entregan actualizaciones semanales o incluso diarias a medida que surgen hallazgos o problemas. En lugar de presentar detalles innecesarios, los informes ofrecen información sobre qué
lo que mas importa.

Agile tiene el poder de revolucionar la Auditoría Interna haciendo que las auditorías y revisiones sean más relevantes, basadas en el riesgo y en tiempo real.

Importante

- Primero, tenga en claro qué es *Agile* y qué no es. Si bien es una metodología flexible, simplemente llamar a un proceso ***Agile*** (o usar términos como *Sprint, Scrum y Backlog*) no lo hace. La Auditoría Interna ágil adapta las necesidades de *Agile* a Auditoría Interna.

- Depende de usted decidir si *Agile* podría funcionar y en qué función. Los buenos candidatos son áreas con la necesidad de informes más receptivos y relevantes, proyectos de gran importancia como instalaciones de TI o integraciones de fusión, y donde los grupos de Auditoría Interna necesitan hacer más con menos.

  Aprenda sobre *Agile* de practicantes internos en el desarrollo de software o sistemas, o solicite nuestra ayuda.

- Comprenda que la adopción de *Agile* exige un cambio de mentalidad así como de métodos, y no todos los auditores internos pueden adaptarse. Sin embargo, aquellos que lo hacen generalmente encuentran que saborean el ritmo del trabajo, el compromiso con las partes interesadas y la mayor efectividad que resulta de la Auditoría Interna *Agile*.

El año que tenemos por delante...

Claramente, este año requiere un fuerte enfoque en todo lo digital. De nuestros 13 temas, más de la mitad están alineados directa o estrechamente con la tecnología y las capacidades de la información. La mayoría de los grupos de Auditoría Interna deben priorizar la garantía y el trabajo de asesoramiento sobre los usos de estas tecnologías en la organización y las formas de utilizarlas para mejorar su propio trabajo. Del mismo modo que los clientes tienden a superar a las organizaciones en sus usos de las tecnologías digitales, ahora muchas partes interesadas superan a la Auditoría Interna de manera similar.

Las funciones de Auditoría Interna con visión de futuro no solo buscan proporcionar seguridad y asesoramiento, y aplicar tecnologías digitales a su propio trabajo, sino también anticiparse a los problemas y riesgos asociados con esas tecnologías. Anticipan los posibles movimientos de las partes interesadas hacia nuevas tecnologías, estrategias y modelos comerciales para que puedan prepararse a sí mismos y a la organización para esos movimientos.

De esta forma, ayudan a los accionistas en algunas de las áreas más desafiantes a las que se enfrentan: nuevas áreas donde surgen riesgos y donde se puede crear un nuevo valor, aumentando así su impacto e influencia en formas visibles y valiosas.

Deloitte.

www.deloitte.cl

Deloitte presta servicios profesionales de auditoría, impuestos, consultoría y asesoría financiera, a organizaciones públicas y privadas de diversas industrias. Con una red global de firmas miembro en cerca de 164 países, Deloitte brinda su experiencia y profesionalismo de clase mundial para ayudar a que sus clientes alcancen el éxito desde cualquier lugar del mundo en donde operen. Los aproximadamente 200.000 profesionales de la firma están comprometidos con la visión de ser el modelo de excelencia.

Oficina central

Rosario Norte 407
Las Condes, Santiago
Chile
Fono: +56 227 297 000
Fax: +56 223 749 177
deloittechile@deloitte.com

Regiones

Simón Bolívar 202
Oficina 203
Iquique
Chile
Fono: +56 572 546 591
Fax: +56 572 546 595
iquique@deloitte.com

Av. Grecia 860
Piso 3
Antofagasta
Chile
Fono: +56 552 449 660
Fax: +56 552 449 662
antofagasta@deloitte.com

Los Carrera 831
Oficina 501
Copiapó
Chile
Fono: +56 522 524 991
Fax: +56 522 524 995
copiapo@deloitte.com

Alvares 646
Oficina 906
Viña del Mar
Chile
Fono: +56 322 882 026
Fax: +56 322 975 625
vregionchile@deloitte.com

Chacabuco 485
Piso 7
Concepción
Chile
Fono: +56 412 914 055
Fax: +56 412 914 066
concepcionchile@deloitte.com

Quillota 175
Oficina 1107
Puerto Montt
Chile
Fono: +56 652 268 600
Fax: +56 652 288 600
puertomontt@deloitte.com