Deloitte.

Auditoría Interna:

Riesgos y Oportunidades para 2022

Tabla de Contenidos

Sobre riesgo, oportunidad y auditoría interna

Riesgo

A menudo se piensa que el riesgo es intrínsecamente negativo, pero una visión más matizada percibe una dualidad compleja. Se pueden encontrar paralelos en la literatura, como Jekyll y Hyde, riesgo y oportunidad en el mismo cuerpo, y en la ciencia, como la Tercera Ley de Newton; por cada riesgo hay una oportunidad.

Hay pocas dudas del porqué predomina el aspecto negativo del riesgo. En los últimos años, el mundo ha sido testigo de una confluencia sin precedentes de múltiples amenazas, muchas de las cuales han generado, entrelazado y / o exacerbado a las otras. Una lista muy fragmentada incluye la pandemia mundial, el cambio climático, la escasez de mano de obra, las interrupciones en la cadena de suministros, amenazas cibernéticas y manifestaciones políticas y sociales. Consideradas en conjunto, estas y otras amenazas han sacudido los cimientos mismos sobre lo que se ha construido, la sociedad y los negocios.

Oportunidad

Sin embargo, la oportunidad oculta el riesgo a cada paso. Considere, por ejemplo, el ámbito de los ESG: medioambiental, social y de gobernanza, donde las organizaciones enfrentan intensas presiones regulatorias y sociales para cumplir con altos estándares, y donde el fracaso puede provocar daños financieros, regulatorios y de reputación significativos. Sin embargo, si las empresas lo hacen bien en el ámbito ESG, pueden hacer grandes cosas, tanto en términos de hacer contribuciones positivas a problemas globales clave, como de igual importancia en la creación de una ventaja competitiva en el mercado.

Auditoría Interna

La auditoría interna (IA), al igual que el riesgo en sí, a menudo se malinterpreta. Históricamente, la profesión ha sufrido percepciones desfavorables, ya que a menudo se la ve como un cuerpo de vigilancia policial o como un área de amonestación que se precipitan para informar sobre lo que salió mal. Sin embargo, una definición más progresiva de auditoría interna también contiene una dualidad: proveedores esenciales de servicios tanto de aseguramiento como de asesoría. Auditoría interna es legítimamente cautelosa con la multitud de riesgos, y la función siempre se encargará de proteger a sus organizaciones a través del aseguramiento. Pero los grupos de auditoría interna verdaderamente evolucionados, también buscarán ayudar a la alta administración a embarcarse en futuros desafíos y tomar decisiones más informadas, aprovechando al máximo las oportunidades concurrentes que ofrece cada riesgo.

En esta publicación, presentamos una serie de riesgos y oportunidades claves que creemos que las organizaciones deberían tener en su radar, así como la auditoría interna en sus planes de auditoría...

La lista no es de ninguna manera exhaustiva; ni todos los temas se aplicarán a todas las organizaciones. Depende de cada entidad evaluar, clasificar y priorizar estos riesgos y oportunidades en relación con su propio perfil y circunstancias . (El concepto de clasificación de riesgos para centrarse en los riesgos que más importan se aborda con más detalle en nuestra publicación ¨Internal Audit 3.0: The future of internal audit is now.")

Si bien el entorno actual seguramente ha desencadenado muchos sentimientos de impotencia e incertidumbre, este artículo puede servir como contrapeso: una influencia motivadora y organizadora; un incentivo para poner su organización en orden, sus prioridades claras y su plan de acción. Los riesgos son abundantes, pero las oportunidades son aún mayores y la auditoría interna puede marcar la diferencia. Las dualidades ayudarán a sus organizaciones a emerger más fuertes de estos tiempos sin precedentes.

El rol de auditoria interna en

Gestión de Riesgos de Terceros (TPRM)

No luches contra los incendios. Instale puertas a prueba de fuego.

Nuestra Visión

Cuando todos los negocios se veían como silos, Auditoría Interna lo tenía fácil: la mayoría de los aspectos de la empresa se manejaban internamente y las preocupaciones de Auditoria interna terminaban en la puerta principal de la empresa.

Hoy, la puerta de entrada no se ha abierto de par en par, ha sido derribada, y las empresas a menudo subcontratan más funciones de las que retienen. Mientras tanto, los terceros (vendedores, distribuidores, proveedores y similares), también mantienen sus propias redes de relaciones (sí, incluso los terceros tienen terceros) creando un ecosistema masivo de cuartas y quintos partes y más allá, que requieren como mínimo de una conciencia total, pero por sobre todo de una supervisión activa.

El aseguramiento del TPRM, debe atravesar toda la empresa, y requiere algunos datos como línea de base. Comience solicitando a la gerencia el inventario de todas las relaciones con proveedores o terceros. (Alerta de spoiler: es probable que no haya una). ¿Con qué rapidez se puede producir un informe sobre todo el panorama de las relaciones y los riesgos asociados?

Sugerencia: si la respuesta es seis meses, usted tiene un problema. ¿Cuántas fallas de terceros ha experimentado la organización durante el último año? (Respuesta esperada: más de lo que cree). Cada relación con terceros (y más allá) conlleva su propio conjunto de riesgos, y la mayoría de las organizaciones invierten en tecnología lo cual clave para mitigarlos. Auditoría Interna debe estar preparada para asesorar a la administración y al comité de auditoría sobre cuales son las tecnologías apropiadas para monitorear el riesgo de terceros, como alertas en tiempo real y herramientas de análisis de tendencias.

Además, se debe brindar orientación a las partes interesadas sobre las ventajas de externalizar su TPRM. El desarrollo de capacidades en la empresa puede ser costoso y exigente, ya que TPRM es un campo de nicho que requiere conocimientos especializados. Las mismas motivaciones que impulsan a una empresa a entablar relaciones con terceros en primer lugar se aplican a la supervisión subcontratada de TPRM: la eficiencia, la competencia, el rigor, la auditabilidad y una perspectiva independiente se encuentran entre los beneficios para ser realizado.

News

En 2021, a un gran banco se le impuso una multa de 1 millón de dólares, además de pruebas adicionales y requisitos de capacitación debido a que no informó adecuadamente los datos financieros al regulador federal. Si bien el banco había contratado a un proveedor de servicios externo para manejar el proceso, el proveedor cometió errores persistentes que el banco no pudo supervisar adecuadamente y corregir de manera oportuna.

Datos Relevantes

Deloitte: Encuesta de gestión de riesgos de terceros

51%

De las organizaciones enfrentaron uno o más incidentes de riesgo de terceros desde el COVID-19.

13%

fueron incidentes de alto impacto que comprometieron gravemente el rendimiento financiero, perjudicando el servicio al cliente o infringió gravemente la regulación.

10%

De las organizaciones no estaban seguras si habían sufrido un incidente de terceros o no.

Gestión de Riesgos de Terceros (TPRM)

Para obtener más información:
Deloitte: Encuesta de gestión de riesgos de terceros 2021
Deloitte: El desafío de la gestión de riesgos de terceros
Wall Street Journal: Gestiona a terceros con tecnologías de vanguardia

Señales de advertencia

- **Subcontratación:** ¿Su tercero utiliza a terceros? Si, por ejemplo, su proveedor de nómina subcontrata algunos servicios, puede descubrir que ha perdido el control sobre los datos personales de sus empleados.
- **Proveedor malicioso:** Las quejas de los empleados sobre la confiabilidad o el desempeño de proveedores externos pueden ser un indicador de violaciones de contratos de terceros que deben investigarse más a fondo.
- **Concepto errado de la administración:** La administración a menudo piensa que puede hacer TPRM con muy poco dinero. Creen que pueden hacerlo rápidamente. Y creen que pueden hacerlo sin tecnología. No pueden. No pueden. Y no pueden.
- **Expansión de fronteras:** Existen muchas relaciones de terceros con empresas de otras jurisdicciones. Si sus proveedores operan en un entorno con estándares regulatorios laxos, prácticas comerciales potencialmente corruptas o una variedad de preocupaciones de ESG (ambientales, sociales y de gobierno), su exposición al riesgo puede exceder su apetito de riesgo.

Obtener los fundamentos correctos

- **Involucre a los abogados**: La mayoría de las relaciones con terceros se rigen por contratos que especifican derechos y obligaciones. Su abogado responsable probablemente participó en la redacción de los acuerdos y puede ser un recurso valioso para interpretarlos.
- **Amplíe la visión:** ¿El programa actual de TPRM realmente abarca a todos los terceros o se limita a los proveedores? ¿Cubre todos los dominios de riesgo, como el antisoborno, la continuidad del negocio y los aspectos ESG?
- **Exponga el caso:** Examine el caso comercial para entablar relaciones con terceros y su alineación con la estrategia comercial general.
- **Comprender la cadena**: ¿Hasta dónde debe llegar en la cadena de suministro? Evalúe si se debe monitorear a los proveedores de terceros y con qué intensidad.
- **Evaluar todo tipo de proveedores**: El riesgo no disminuye en paralelo con el valor del contrato de sus relaciones con terceros. Su riesgo de reputación es el mismo con un proveedor de 10K que con un proveedor de 1M. Esa pequeña empresa en la que gasta unos pocos miles puede costarle millones.

Dando los siguientes pasos

- **Dé un salto:** Haga que su equipo participe en el proceso de selección de proveedores para examinar a los proveedores y evitar posibles problemas antes de que lleguen.
- **Implemente tecnología:** Exponga el caso al comité de auditoría para obtener recursos tecnológicos adicionales. Aquí hay una declaración de apertura: "En lugar de combatir incendios, la administración debería instalar puertas a prueba de fuego".
- **Mantenga el escepticismo:** Anticípese a las formas en que los gerentes pueden intentar eludir los controles internos que rigen las relaciones con terceros. Se debe asesorar a la dirección sobre los medios de fortalecimiento.
- **Mire el lado positivo:** No se limite a señalar las debilidades de terceros; como parte de su trabajo, esfuércese por identificar áreas para obtener un valor adicional de las relaciones.
- **Registre las sanciones:** Determine si existe un proceso definido para aumentar las preocupaciones, obtener mejoras y aplicar sanciones por incumplimiento del contrato, problemas de calidad u otros incumplimientos.

El papel de la auditoría interna en

Ambiental, Social y Gobernanza (ESG)

Aunque los informes ESG obligatorios aún no han llegado a muchas jurisdicciones, la adopción es inminente en varias importantes economías.

Nuestra Visión

Auditoría Interna siempre ha tenido un rol transversal, pero ahora la porción debe ser cultivada de manera sostenible, recolectada con mano de obra justa y transportada sin emisiones de carbono. Esto es suficiente para provocar un dolor de cabeza a cualquier área de auditoría.

Los grupos de auditoría interna de las grandes multinacionales pueden encontrar relativamente sencillo adecuar los temas ambientales, sociales y de gobernanza (ESG) en sus planes de auditoría. Pero para las organizaciones pequeñas y medianas, la sopa de letras de los estándares y marcos de ESG (GRI, SASB, TCFD, IIRC y más) puede resultar amedrentador. Para esos grupos, ofrecemos esa tranquilidad: Ustedes saben más de lo que piensan. Sí, hay nuevos requisitos, pero al igual que COSO, IFRS, FCPA y otros estándares, pueden manejar esto. Básicamente, la garantía de ESG sigue siendo contable, aunque utiliza otras métricas, como galones de agua, emisiones de carbono y diversidad de la fuerza laboral.

Aunque los informes ESG obligatorios aún no han llegado a muchas jurisdicciones, la adopción es inminente en varias economías importantes. La auditoría interna no debe demorarse en abordar el problema, ya que lo que está en juego es simplemente demasiado alto, con la presión ejercida por los reguladores, inversores, clientes, afiliados de terceros y la sociedad en general. Los beneficios de hacerlo bien pueden ser significativos, ya que "un alto rendimiento ESG puede traducirse en un mejor acceso al capital, el talento y las oportunidades comerciales".

Para las funciones de Auditoria Interna que recién comienzan en su viaje ESG, uno de los primeros desafíos será identificar a las partes responsables dentro de la organización. A menudo, encontramos al CFO apuntando a las relaciones con los inversores, quienes miran a RR.HH., que pasa la pelota a los legales, quienes redirigen a marketing. La coordinación eficaz entre estos grupos y un punto focal de responsabilidad será fundamental para el progreso.

News

Las conversaciones sobre el clima de la COP26 en Glasgow llevaron a acuerdos para eliminar gradualmente la energía del carbón, reducir las emisiones de metano, "ecologizar" el sector de servicios financieros y detener la deforestación. Sin embargo, no todos los países fueron signatarios, y algunos de los principales emisores de CO_2 se negaron a firmar. La adopción total, el cumplimiento y la responsabilidad siguen siendo obstáculos importantes.

Datos Relevantes

- La representación femenina en los consejos de administración de empresas varía drásticamente en todo el mundo: Australia, 34%; Canadá, 31%; Francia, 43%; Alemania, 25%; India, 17%; Japón, 11%; Holanda, 26%; Reino Unido, 34%; Estados Unidos, 28%.
- Los líderes mundiales en métricas de ESG incluyen a Dinamarca en desempeño ambiental, Finlandia en ausencia de discriminación y Singapur en calidad regulatoria. Estados Unidos no aparece actualmente en el top 10 en ninguna de estas categorías.

Ambienta, Social y Gobernanza (ESG)

Para obtener mas información :

- **Deloitte**: Finding the value in environmental, social, and governance performance
- **Wall Street Journal:** ESG and the role of internal audit
- **Wall Street Journal:** Five steps to building credible climate commitments

Señales de advertencia

- **Exageración de marketing:** Si su área de marketing hace afirmaciones que están en desacuerdo con los resultados de las auditorías de ESG, deberá tomar las riendas rápidamente.
- **Políticas obsoletas:** Las políticas organizativas sobre viajes de negocios, trabajo remoto, diversidad e inclusión, gobierno corporativo y más, deben revisarse y actualizarse para reflejar el entorno comercial actual y los objetivos ESG.
- **Enfoques en silos:** Las organizaciones pueden estar literal o figurativamente en todo el mapa, con estándares, prioridades y rigor que varían según la geografía o la unidad de negocio.
- **Separado de la estrategia:** Las consideraciones de ESG deben estar unidas a la estrategia empresarial. Un enfoque armonizado promoverá los objetivos de la empresa; un enfoque inconexo puede reducir el rendimiento.

Obtener los fundamentos correctos

- **Informe al equipo**: Familiarice a su equipo de Auditoría Interna con los estándares y marcos de informes ESG reconocidos, como la Iniciativa Global de elaboración de informes (GRI), Normas de contabilidad de sostenibilidad Board (SASB), protocolo de gases de efecto invernadero (GHG) y la Task Force on Climate-related Financial Disclosures (TFCD).
- **Verificar el estado:** Analizar el proceso actual de divulgación de ESG para los controles internos: ¿Se implementan los controles y son suficientes? ¿Se informan los hallazgos a la junta?
- **Ofrezca información:** Proporcione información sobre los indicadores de riesgo ESG. Ayude a evaluar cómo se han considerado los riesgos ESG dentro del proceso de gestión de riesgos corporativos de la organización. ¿ESG está integrado en la estrategia empresarial más amplia?
- **Revise los informes:** Determine cómo la administración ha identificado los problemas clave a revelar y si ha alineado esos temas con los estándares internacionales.
- **Evaluar de forma independiente:** Utilice evaluaciones independientes para comprender las políticas, el panorama de control y las responsabilidades adecuadas.

Dando los siguientes pasos

- **Ir por el verde esmeralda, no el crudo:** Esté atento a los "blanqueamientos verdes". Un mayor escrutinio ha frenado la tendencia, pero muchas organizaciones aún hacen afirmaciones endebles sobre su perfil ecológico en lugar de reflejar su verdadero color.
- **Fomentar el conocimiento:** Inicie la capacitación según sea necesario para llenar las lagunas de conocimiento, tanto dentro de Auditoría Interna como en toda la organización en general. Genere concientización, sesiones de inmersión profunda y puntos de vista holísticos.
- **Genere credibilidad:** Actualice las calificaciones de auditoría interna con certificaciones y acreditaciones relacionadas con ESG obtenidas a través de organizaciones profesionales.
- **Financiar al equipo**: Invierta en recursos con la experiencia y las habilidades adecuadas para comprender, reconocer y evaluar los riesgos de ESG. Considere la posibilidad de crear puestos dedicados a ESG dentro de la auditoría interna para permitir la experiencia especializada y un mayor enfoque.
- **Integre ESG:** Incluya los riesgos de ESG dentro de cada programa de auditoría para indagar sobre los aspectos de ESG dentro de cada función. Se debe informar sobre ESG a lo largo de cada informe de auditoría.

El papel de la auditoría interna

Contra el Fraude

Una frase de la medicina también suena válida para las empresas: es mejor prevenir que curar.

Nuestra Visión

Cada país tiene su medio de noticias sensacionalistas. Y todos los ejecutivos y Directorio Ejecutivo de Auditoría (DEA), esperan no ver nunca a su empresa en esa portada.

De hecho, no hay forma más segura de atraer publicidad no deseada que sufrir un caso de fraude interno. Pero el daño se extiende mucho más allá de los titulares. El fraude daña no solo la reputación de la empresa, sino también las carreras de aquellos bajo cuya vigilancia ocurrió el engaño. Las consecuencias financieras, las sanciones regulatorias, la pérdida de clientes y las ganancias de la competencia son resultados comunes. Y, en casos extremos, el fraude puede presentar una crisis existencial para la propia organización.

El problema atraviesa las líneas de la industria. Si bien los servicios financieros y el sector público generalmente están más enfocados en este riesgo, debido en gran parte a los estrictos entornos regulatorios en los que operan, la mayoría de las otras industrias se quedan atrás. Las empresas emergentes, en particular, pueden luchar contra el fraude y sus consecuencias.

Curiosamente, a pesar de la importancia del tema, muchas organizaciones operan en un estado de negación. Pero esta postura de "fuera de la vista / fuera de la mente" oculta un factor clave: el fraude, por su naturaleza, implica engaño. No hay luces intermitentes que digan "mira aquí". Los estafadores cubren sus huellas y harán todo lo posible para dirigir su atención a otra parte. Entonces, cuando las organizaciones dicen: "No tenemos un problema de fraude", la respuesta estándar tal vez debería ser: "Sí, lo tienes. Simplemente no lo has encontrado todavía".

Lo que es cierto en la medicina también suena cierto en los negocios: es mejor prevenir que curar. La mejor manera de minimizar las pérdidas por fraude es evitar que ocurra el fraude en primer lugar.

News

Cuando la empresa alemana de tecnología financiera Wirecard reveló que más de 2.000 millones de dólares en efectivo habían desaparecido de sus libros, las consecuencias fueron graves: el precio de las acciones se desplomó en más del 90%; el CEO renunció; la empresa se declaró en insolvencia; y varios ejecutivos fueron arrestados por cargos de fraude contable.

Datos Relevantes

De acuerdo con la **Asociación de Examinadores de Fraude Certificados**:

5%

Las organizaciones pierden en media el 5% de sus ingresos anuales debido al fraude.

$4.5B

Más de US $ 4,5 billones se pierden debido a las actividades fraudulentas cada año.

14 meses.

El típico caso de fraude dura 14 meses antes de que se detecte.

Contra el Fraude

Para obtener más información:

- **Deloitte:** The nature of fraud is changing
- **Deloitte:** Building confidence in your fraud risk framework
- **Wall Street Journal:** Five actions to fortify whistleblower plans

Señales de advertencia

- **Estilo de vida extravagante:** Si el asistente contable júnior de una organización conduce hacia al trabajo en un Mercedes-Benz, es posible que deba volver a comprobar sus registros financieros. Un empleado que vive más allá de sus medios es el signo más común de actividad fraudulenta. (Puede parecer obvio, pero aún ocurre).
- **Problemas personales:** Ciertos problemas personales también pueden ser una señal de advertencia temprana de un posible fraude, incluidas las dificultades financieras, el divorcio y la adicción. Según la Asociación de Examinadores de Fraude Certificados, "En el 63% de los casos, el defraudador mostró una alerta roja en su comportamiento que esta asociado con su vida personal".
- **Problemas laborales:** Algunos comportamientos en el lugar de trabajo también pueden ser un indicador de fraude subyacente. Entre las primeras preocupaciones: relaciones inusualmente cercanas con proveedores o clientes; interacciones tensas entre colegas y evaluaciones de desempeño deficientes.

Obtener los fundamentos correctos

- **Estudie el panorama:** Para obtener un control real de los riesgos que enfrenta su organización, realice una evaluación de riesgo de fraude exhaustiva y completa. Los resultados deben impulsar las actividades posteriores: dónde concentrarse, dedicar su tiempo e invertir. Este no es un ejercicio único de cinco minutos: hable con las partes interesadas, realice encuestas anónimas, organice talleres, actualice y cuestione los resultados con regularidad.
- **Implemente Línea Base de Control**: Es sorprendente cuántas organizaciones tienen lagunas o debilidades fundamentales en los controles internos básicos. Para disuadir el fraude, adhiérase a los conceptos básicos: segregar funciones, accesos limitados, establecer autorizaciones máximas, conducta por antecedentes de cheques, rotar responsabilidades laborales y hacer cumplir
- **Fortalezca la infraestructura**: Establezca mecanismos sólidos de denuncia de fraude para que los utilicen los colaboradores y contratistas, lo que permite referencias anónimas. A menudo, estos implican el uso de líneas directas de terceros; sin embargo, es vital que los informes recibidos se clasifiquen y se tomen las medidas de seguimiento adecuadas.

Dando los siguientes pasos

- **Tenga cuidado con las brechas:** Una vez que comprenda sus riesgos clave, correlacione con los controles existentes para identificar brechas, debilidades y ganancias rápidas. Empiece a cerrar esas brechas. Algunos requerirán arreglos a más largo plazo; otros serán sencillos sin requerir una gran inversión.
- **Capacitar a la organización:** Una vez identificados los riesgos y establecidos los mecanismos de denuncia, puede comenzar la capacitación antifraude. Asegúrese de resaltar el verdadero costo del fraude, las señales de advertencia y los mecanismos de denuncia. Comunicar una política de tolerancia cero.
- **Delegue a las partes interesadas**: La mejor defensa son las partes interesadas: colaboradores, mandos intermedios y terceros. Edúquelos sobre las amenazas y los riesgos claves. Ayúdelos a comprender cómo detectar y señalar problemas emergentes. No abra completamente la puerta. Mantenga en secreto la información confidencial sobre sus mejores técnicas de detección de fraudes.

Rol de la auditoría interna en

Fusiones & Adquisiciones

La negociación aumentará en la economía post-pandémica.
La auditoría interna puede ayudar a que las transacciones tengan éxito.

Nuestra Visión

Los ejecutivos de fusiones y adquisiciones están enviando señales claras y contundentes de que la negociación será una palanca importante a medida que las empresas se recuperen y prosperen en la economía posterior al COVID-19. Así como los consumidores están reabriendo sus billeteras después del cierre de la pandemia, las empresas y los inversores privados han acumulado mucho capital que están dispuestos a gastar. Pero para que el acuerdo sea un ganador a largo plazo, con un enfoque en el valor y el riesgo desde el principio, la auditoría interna debe ser un actor clave: antes, después y hacia todo lo demás.

Entre los temas más delicados estará la integración del sistema de TI. No es raro encontrar docenas de sistemas de TI entre las empresas que se fusionan, todos los cuales deberán evaluarse en cuanto a compatibilidad y redundancia. El anuncio inicial de fusiones y adquisiciones probablemente incluirá una evaluación optimista de las posibles sinergias, pero a medida que se acerca la fecha de cierre, esos modelos de sinergia pueden reducirse repentinamente. Habrá una presión intensa para que las proyecciones iniciales funcionen, y los sistemas de TI es donde a menudo dejan caer la pelota.

Otra preocupación involucrará los procesos contables. Durante el período del acuerdo de servicio de transición (TSA), los procesos de contabilidad y control interno pueden fracasar, lo que da como resultado problemas de informes financieros potencialmente dañinos. Muchas empresas subestiman el esfuerzo necesario para separar o integrar sus sistemas. Es esencial involucrar los conjuntos de habilidades correctos, en lugar de simplemente dedicar recursos al problema.

Y finalmente, los DEA no solo deben preocuparse por el esfuerzo de integración general, sino que también tendrán que lidiar con la fusión de dos grupos distintos de auditoría interna. Las funciones de Auditoría Interna deberán conciliar las diferencias en la visión y el rol, los modelos operativos, la documentación del papel de trabajo, las herramientas, tecnología, y más. Esta integración de AI no puede ser un tema secundario: dado que auditoría interna asesorará sobre la integración general, es esencial para la credibilidad de la organización que tenga su propia casa en orden. Empezar temprano y moverse rápidamente son las claves del éxito.

News

En 2001, el favorito de las puntocom América Online se fusionó con uno de los líderes del cable y contenido Time Warner para crear un potencial gigante de los medios. Pero las sinergias no realizadas, las culturas en conflicto y la explosión de la burbuja de las puntocom llevaron a AOL / Time Warner a sufrir una perdida de 99.000 millones de dólares en 2002, lo que le valió a este acuerdo de fusiones y adquisiciones el sobrenombre de "la peor fusión de todos los tiempos". Si bien el trato es de hace más de veinte años, los aprendizajes de esta fusión aún se aplican.

Datos Relevantes

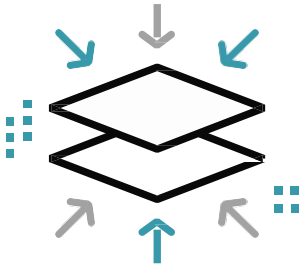
De acuerdo con la investigación de Deloitte "Future of M&A Trends":

61%

de los negociadores de EE. UU. esperan que la actividad de fusiones y adquisiciones vuelva a los niveles anteriores a COVID-19 en los próximos 12 meses.

51%

Las amenazas de ciberseguridad son lo más importante para el 51% de los encuestados, ya que las empresas gestionan los acuerdos de forma virtual.



Fusiones & Adquisiciones

Para obtener más información:

Deloitte: M&A trends survey: The future of M&A

Deloitte: M&A: The intersection of due diligence and governance

Deloitte: Regulatory realities amid the M&A market's momentum

Señales de advertencia

- **Desajustes fundamentales:** Organigramas planos frente a organigramas jerárquicos. Toma de decisiones metódica versus no estructurada. Liderazgo conservador versus extravagante. Algunos obstáculos culturales pueden ser difíciles de superar.
- **Justificación insuficiente:** El logro de economías de escala a menudo se cita como un factor impulsor de los acuerdos de fusiones y adquisiciones, pero si fusiona dos empresas con estrategias defectuosas, liderazgo deficiente o competencia despiadada, lo único que aumentará es la probabilidad de fracaso.
- **Problemas de ESG:** ¿Tiene la empresa adquirida un historial irregular de ESG (medioambiental, social y de gobernanza)? ¿El acuerdo va a retrasar varios años su propio programa de ESG?

Obtener los fundamentos correctos

- **Realice la debida diligencia:** a medida que se evalúan los posibles acuerdos, la auditoría interna debe garantizar que se cubran todas las áreas del proceso; evaluar el entorno de control interno existente; y revisar asuntos materiales de auditorías recientes. Analice las sinergias: los negociadores a veces presentan una imagen demasiado optimista de las posibles sinergias. Tome una mirada independiente e informe los hallazgos a la junta. Haga un seguimiento durante un año o más después de la transacción para ver dónde está y dónde no se está logrando la sinergia.
- **Incorporar a Auditoría Interna:** Auditoría interna debe unirse a las sesiones de diseño, enfocando su mirada de riesgo y control y haciendo preguntas difíciles. (En algunos acuerdos, la auditoría interna puede quedar excluida del plan, pero una vez que se anuncia el acuerdo, la función debe presionar para participar).
- **Deberes del día 1**: Auditoría Interna tiene una visión única y amplia de la organización: quién es quién, cómo está conectada la empresa, dónde encaja la nueva empresa. Ese conocimiento debe utilizarse como parte de la planificación y el apoyo de la preparación del primer día.

Dando los siguientes pasos

- **Compare y asesore:** Controle los procesos, los controles y la tecnología en la empresa de destino. Identificar estados actuales; crear sinergias y determinar despidos; identificar lo que cubre la TSA.
- **Encuentra la salida:** Examina la TSA y recomienda cambios según sea necesario. Realice un seguimiento de las fechas de finalización de la TSA y evalúe cómo la empresa se está preparando para una salida oportuna sin extender la TSA para cubrir los déficits.
- **Mire hacia atrás:** Realice evaluaciones posteriores a la transacción para determinar las lecciones aprendidas que se pueden aplicar a los acuerdos en el futuro.
- **Considerar el cumplimiento**: Si el acuerdo empuja a la empresa adquirente a nuevos mercados, entrarán en juego requisitos regulatorios y de informes adicionales. Evalúe temprano para evitar el incumplimiento y los plazos incumplidos evitando los dolores de cabeza que traen consigo.

Rol de la auditoría interna en:

Seguridad Psicológica

El viejo dicho, "La seguridad es lo primero", adquiere un nuevo significado para la auditoría interna.

Nuestra Visión

Se ha convertido en una especie de estereotipo empresarial para quienes afirman que los entornos de trabajo deben abarcar la apertura, la colaboración y el aprendizaje, pero de hecho existen datos concretos que respaldan la afirmación. En un estudio de dos años realizado por Google sobre el desempeño del equipo, todos los equipos con mejor desempeño adoptaron el concepto de "seguridad psicológica", la noción de que los errores son un precursor del éxito y que quienes los cometen deben ser apoyados, no castigados. Google concluyó que cuando los equipos tienen la libertad de participar en la toma de riesgos estratégicos en un entorno de apoyo, su confianza colectiva, creatividad, y la productividad aumentará.

El estudio de Google es convincente, pero antes de que la auditoría interna comience a defender la seguridad psicológica para los organización en general, tal vez se justifique una mirada hacia adentro. ¿El grupo de AI está contribuyendo de manera positiva o negativa a los niveles de seguridad psicológica de la organización? Para determinar la respuesta, comience con una encuesta de una sola pregunta a las partes interesadas internas: "¿Cómo se siente ser auditado por nosotros?"

Las respuestas pueden resultar impactantes: para la mayoría de los auditados, someterse a una auditoría interna es similar a un examen médico invasivo, necesario e importante quizás, pero detestado y temido de todos modos.

Entonces, para la auditoría interna, la seguridad psicológica comienza en casa. Tome medidas para que su función sea menos un adversario, más un asesor. No solo resaltes lo malo, también celebra lo bueno. No solo rebusque el pasado, sino que visualice el futuro.

Para promover la seguridad psicológica, los equipos de AI pueden adoptar la declaración conocida como "La Directiva Principal": "Independientemente de lo que descubramos, entendamos y creamos verdaderamente que todos hicieron el mejor trabajo que pudieron con la informacion disponible, lo que sabían en ese momento, sus habilidades, los recursos disponibles y la situación en cuestión ". (Norm Kerth, Project Retrospectives:
Un manual para revisión en equipo)

News

Al principio de su carrera, Western Union despidió al inventor estadounidense Thomas Edison después de que un experimento fallido dañara la propiedad de la empresa. La cancelación de su contrato fue poco visionaria por parte de su empleador, ya que Edison pasó a presentar más de 1.000 patentes, inventando la ampolleta, el fonógrafo, la cámara cinematográfica y muchos otros dispositivos. Años más tarde, Western Union, después de descuidar la creación de un entorno de trabajo seguro, terminó comprando los derechos de uno de los inventos de Edison.

Datos Relevantes

- La encuesta del Comité de Auditoría Global 2020 de Deloitte encontró que el 86% de los presidentes de los comités de auditoría dijeron que se alienta a la administración a presentar problemas y hallazgos al comité de auditoría, pero las barreras institucionales a menudo impiden que esto suceda.
- La encuesta de investigación del Director Ejecutivo de Auditoría Global de 2018 de Deloitte reveló que solo el 33% de los DEA cree que su función de auditoría interna se ve de manera muy positiva.
- El sitio de recursos Internal Audit 360 encontró que los informes de AI "no suelen comunicar los aspectos positivos del entorno de gobierno y control interno".

Seguridad Psicológica

Para obtener más información:

- **Deloitte:** Optimizing internal audit: Developing top-flight teams
- **Deloitte:** Creating resilience through psychological safety
- **New York Times:** What Google learned from its quest to build the perfect team

Señales de advertencia

- **Ejecutivos sensibles:** Si sus informes de auditoría provocan erupciones en la alta dirección y genera habitualmente resistencia en los equipos, puede ser seguro suponer que la seguridad psicológica aún no se ha logrado en toda la organización.
- **Objetivos desalineados**: La falta de camaradería o simpatía entre auditoría interna y otras unidades de negocio puede ser una señal de que las relaciones son tensas, lo que dificulta un entorno de seguridad psicológica estable.
- **Misión mal interpretada:** Si el propósito percibido de la auditoría interna (dentro y fuera de la función) es "brindar servicios de aseguramiento y asesoría", en lugar de "ayudar a la organización a tener éxito", entonces la base sobre la que se construye la seguridad psicológica debe reforzarse.

Obtener los fundamentos correctos

- **Hágase una auditoría a sí mismo:** Pregunte a sus partes interesadas qué se siente al ser auditado. Si los auditados encuentran sus auditorías desagradables o incómodas, o si lo perciben más como policía y menos como asesor, es posible que sea necesario realizar una recalibración.
- **Cuide su lenguaje**: Analice el tono que usa al informar a la gerencia y al comité de auditoría. ¿Qué tan útil es en términos de facilitar buenos resultados y crear un ambiente positivo? Considere la posibilidad de reformularlos para evitar el lenguaje emotivo y acusatorio.
- **Influir en las personas influyentes:** Identifique a las partes interesadas influyentes y hable con ellas sobre los posibles pasos para crear un entorno en el que las personas tengan una respuesta positiva a las auditorías. ¿Cómo se pueden suavizar las zonas rugosas?

Dando los siguientes pasos

- **Renueve los informes:** Esfuércese por contar mejor la historia. Considere separar los problemas del entorno de control del resto del informe, reconociendo que un entorno de control deficiente puede ser una anomalía temporal debido a factores como la implementación de nuevos procesos o la expansión a un nuevo mercado o país.
- **Acentúe lo positivo:** Celebre los comportamientos positivos tanto en sus informes como a través de medios separados, como boletines internos, premios u otros reconocimientos. Tales acciones no solo benefician al destinatario, sino que también arrojan luz sobre la propia auditoría interna.
- **Ayude a cambiar la visión del comité de auditoría:** Como consumidor principal de los informes de auditoría interna, el comité de auditoría desempeña un papel clave para permitir la seguridad psicológica: liderar con el ejemplo, establecer el tono y responder a los hallazgos de la auditoría como una oportunidad de aprendizaje y mejora, en lugar de como ocasión de críticas y amonestaciones.

El papel de la auditoría interna en

Ciberseguridad

La tecnología emergente es igual a las amenazas emergentes.

Nuestra Visión

P: ¿Cuál es el mayor temor en ciberseguridad de un director ejecutivo de auditoría?

R: Todo lo que la gerencia piensa que está bajo control.

La ansiedad del DEA está bien justificada. Aquí hay una lista abreviada de cosas que la administración generalmente subestima:

- ¿Cuántos ex-empleados todavía tienen derechos de inicio de sesión?
- Cual es el número de proveedores externos con acceso a sistemas de TI corporativos
- Cantidad de cuentas en la nube que usa la empresa
- Total de infracciones de ciberseguridad que ha experimentado la empresa

Al corregir estos conceptos erróneos, los DEA deben prestar especial atención a los siguientes problemas:

Nube: la complejidad aumenta a medida que las empresas subcontratan servicios a la nube, lo que introduce múltiples dependencias de terceros (riesgo de la cadena de suministro), lo que da como resultado una superficie de ataque más amplia. Auditoría Interna necesita aprovechar las habilidades de la nube cibernética para abordar el riesgo en este entorno de TI complejo y moderno. Si bien la nube mejora la capacidad de aprovechar rápidamente nuevas capacidades como inteligencia artificial, aprendizaje automático, blockchain, entre otros, estos servicios también conllevan un conjunto concurrente de riesgos.

Considere enfoques como una estrategia de migración a la nube de “garantía por diseño” basada en riesgos; aprovechar los servicios nativos en la nube; también incorporar seguridad y participar en una estrategia de múltiples nubes. Para Auditoría interna TI, el aseguramiento de la nube será un viaje de varios años, no solo con una auditoría.

Privacidad: Con los reguladores y los inversores aumentando la presión, la privacidad debe ser una prioridad para los DEA. La auditoría interna primero debe comprender todos los lugares donde residen los datos personales, y luego debe plantear algunos desafíos a la administración: ¿Necesitamos y usamos toda la información de identificación personal (PII) que recopilamos? ¿Todos los que tienen acceso a los datos realmente lo necesitan? ¿Tenemos suficientes garantías para proteger la PII? ¿Tenemos procesos de des-credencialización para ex-empleados? ¿El trabajo remoto ha afectado la privacidad de los datos?

Talento: Atraer y retener a especialistas en la nube y la ciberseguridad representa un desafío importante para la auditoría interna, pero ganar la guerra del talento es obligatorio. Al hablar con el equipo de tecnología sobre sus sistemas y controles, los auditores internos de TI que carecen de "credibilidad pública" serán cancelados por estar impulsados por listas de verificación y no agregar valor. Algunas soluciones para la escasez de talento se pueden encontrar en bonos de antigüedad, oportunidades de capacitación, mejoras en la trayectoria profesional o subcontratar la Auditoría Interna de TI a un tercero de buena reputación.

News

A pesar de las violaciones de datos frecuentes y muy publicitadas, los medios, publican solo una fracción de todos los ciberataques diarios que sufren las organizaciones. Según la revista Security, "más de la mitad de los propietarios de empresas admiten haber ocultado una filtración de datos".

Datos Relevantes

43%	de los ciberataques se dirigen a las pequeñas empresas.
64%	de las empresas han experimentado ataques basados en la web.
9.7M	Registros de atención médica se vieron comprometidos solo en septiembre de 2020.
75B	Para 2025, 75 mil millones de dispositivos de Internet de las cosas (IoT) estarán en línea.

Ciberseguridad

Para obtener más información:

- **Deloitte:** Cybersecurity and the Role of Internal Audit
- **Deloitte:** Assurance in the Cloud
- **ISACA:** Cloud Computing for Auditors

Señales de advertencia

- **Silencio cibernético**: Si su grupo de TI no ha informado de intentos de ciberataques, el problema puede ser una falta de capacidad de detección en lugar de la ausencia de ataques.
- **Control de la nube:** Si en su migración a la nube, la estrategia no ha desarrollado estándares o un catálogo de riesgos basado en la nube para los servicios que se van a consumir, es posible que esté dejando riesgos sobre la mesa donde su organización tiene la responsabilidad de implementar controles para restringir el acceso de los usuarios, personalizar interfaces o cifrar datos, lo que lleva a una problema de control de la nube.
- **Responsabilidades indefinidas:** Debe existir una delimitación clara de responsabilidades entre el proveedor de la nube y el cliente. Si no se define, la falta de claridad en esta área puede dar una falsa sensación de seguridad a todas las partes.

Obtener los fundamentos correctos

- **Evalué sus capacidades:** Evalúe el conjunto de habilidades cibernéticas y de nube existente de su equipo. Aborde las brechas mediante la contratación, la capacitación y/o la subcontratación según sea necesario. Considere enfoques creativos para atraer y retener personal clave para su equipo.
- **Siga un marco:** Establezca un programa integral basado en riesgos que se construya en un marco cyber y de nube probado. Utilizando el marco como guía, brinde servicios de garantía y asesoría para medir las ciber-capacidades y la madurez del programa a implementar.
- **Evaluación de servicio:** Antes de decidirse por un proveedor en la nube, solicite pruebas de la resistencia de la infraestructura, el tiempo de inactividad del servicio, el rendimiento y otras métricas. Revise el informe de controles de organización y sistema (SOC) correspondiente, si está disponible. Infórmese sobre el cumplimiento normativo y las evaluaciones de controles independientes. Observe las señales de alerta y busque soluciones o alternativas si es necesario.

Dando los siguientes pasos

- **Adopte el futuro:** Amplíe su plan de auditoría para abarcar los riesgos emergentes, incluida la gobernanza de datos y TI; cuestiones de ritmo de cambio; infraestructura de TI ilimitada; y nuevas tecnologías como AI, RPA, blockchain, realidad virtual y aumentada y también IoT.
- **Prepárese para las preguntas:** Dados los recientes ciberataques de alto perfil y las pérdidas de datos, se han generado crecientes expectativas de los reguladores, en este sentido la auditoría interna debe comprender los ciber-riesgos y prepararse para las preguntas e inquietudes expresadas por el comité de auditoría y la junta directiva.
- **Cruce la frontera**: Los requisitos reglamentarios sobre la privacidad de los datos varían según la jurisdicción. Lleve a cabo una revisión integral proactiva que mapee las áreas de operación, tanto físicas como virtuales, de acuerdo con las leyes y regulaciones locales.

El papel de la auditoría interna en

Diversidad, Igualdad e Inclusión

La auditoría interna tiene la oportunidad y la obligación de fomentar una cultura diversa e inclusiva.

Nuestra Visión

Históricamente, la auditoría interna ha sido principalmente una operación cuantitativa, centrándose en datos concretos y resultados medibles y evitando los problemas cualitativos que carecen de KPI distintos. Esos días ya pasaron.

Los acontecimientos y las tendencias actuales, incluidos los cálculos sobre el racismo, la injusticia y la desigualdad, han llevado a la auditoría interna a un nuevo ámbito: la diversidad, la igualdad y la inclusión (DEI). Si bien esto representa un área no tradicional para la función y tiene numerosos factores, la relevancia debe ser elevada y las medidas pragmáticas: obligar a la auditoría interna a tomar el stock de iniciativas del DEI a través de toda la organización y adelantarse a desempeñar un rol.

- Las prácticas discriminatorias son inherentemente objetables. La auditoría interna tiene la oportunidad y la obligación de ayudar a una organización a fomentar una cultura diversa e inclusiva.
- Una fuerza laboral diversa y una cultura inclusiva son componentes esenciales de organizaciones exitosas, correlacionadas con un mejor desempeño laboral, menor rotación y menor ausentismo.
- La diversidad, la igualdad y la inclusión son atributos críticos para quienes buscan trabajo, y las organizaciones que adoptan DEI tendrán una ventaja en la contratación y retención de los mejores talentos.

La auditoría interna, con su amplia perspectiva sobre el riesgo y sus extensas relaciones en toda la organización, es especialmente adecuada para ayudar a las organizaciones en la evaluación de su estado actual de DEI y asesorar sobre los caminos adecuados a seguir. Esto incluye actuar como catalizadores al asesorar sobre indicadores de riesgo y KPI; evaluar si los programas DEI están cumpliendo sus objetivos previstos; e informar los resultados a la junta, los comités y los altos ejecutivos.

La auditoría interna debe estar alerta y desaconsejar cualquier solución rápida o superficial propuesta o promulgada por la gerencia. Si la iniciativa DEI parece un enfoque de parche, los colaboradores y el mercado lo notarán rápidamente.

News

En 2018, un tribunal del Reino Unido dictaminó que una firma de marcas de lujo tenía un "punto ciego étnico". En un caso de discriminación presentado por un empleado, el Tribunal Laboral del Centro de Londres citó múltiples delitos por parte de la empresa, incluido un proceso de contratación sesgada; formación inadecuada en igualdad y diversidad; y vigilancia encubierta injustificada del trabajador .

Datos Relevantes

En una encuesta de Deloitte de 2019, el 64% de los encuestados dijeron que habían experimentado o presenciado prejuicios en el lugar de trabajo durante los 12 meses anteriores, lo que sugiere una debilidad significativa en la cultura de muchas organizaciones. Sin embargo, alrededor del 70% de los grupos de auditoría interna no evalúan la cultura organizacional como parte de su plan de auditoría.

Diversidad, Igualdad e Inclusión

Para obtener más información:

- **Deloitte:** The inclusion imperative for boards
- **Wall Street Journal:** Internal audit's role in driving diversity, inclusion
- **Wall Street Journal:** Board diversity improves but key goals decades away

Señales de advertencia

- **Renuncias constantes:** Las renuncias y las razones detrás de ellas pueden ofrecer pistas sobre si existen problemas de diversidad o inclusión. Si las causas fundamentales de las renuncias revelan un patrón, evalúe los problemas culturales subyacentes.

- **Daños de Imagen:** Publicaciones negativas en bolsas de trabajo o redes sociales pueden ser un presagio de problemas de DEI. Inicie un escaneo regular de sitios para mantenerse al tanto de las tendencias; las herramientas automatizadas o un contrato de terceros pueden hacer que este proceso sea más rápido y no tan desgastante.

- **Prejuicios demográficos:** Los datos demográficos de su organización pueden arrojar luz sobre los prejuicios o las prácticas discriminatorias. Examinar la composición de la junta, la alta dirección y el gerente general; las prácticas de contratación, promoción y despido; los premios de salario, bonificación y beneficios; y otras métricas.

Obtener los fundamentos correctos

- **Comience con algo pequeño:** Desarrolle una evaluación de la cultura para determinar la existencia y el alcance de las iniciativas DEI. Documente lo que su organización está haciendo actualmente para comprender, comunicar y dar forma a su cultura corporativa.
- **Incorpore riesgos**: Incluya los riesgos de DEI en su plan de auditoría. Evalúe las iniciativas actuales de DEI para determinar si están cumpliendo sus objetivos. Informar a las partes interesadas sobre las oportunidades de mejora de DEI y el progreso en cada informe de auditoría.
- **Ayudar y empujar:** Ayude al liderazgo a comprender las implicaciones de una cultura organizacional poco saludable vista a través de una mirada de riesgo. Proporcionar información sobre capacitación, comunicaciones y políticas.
- **Haga preguntas:** Para comprender las percepciones y experiencias de los empleados e identificar los riesgos potenciales, desarrolle como parte del plan de auditoría un cuestionario estándar para guiar las entrevistas con las partes interesadas. Realice entrevistas con una muestra diversa de colaboradores.

Dando los siguientes pasos

- **Facilitar la mejora:** Evalúe los métodos utilizados para monitorear, medir e informar sobre el programa y evaluar si se pueden realizar mejoras.
- **Validar estadísticas:** Si su organización publica estadísticas DEI en el mercado, proporcione seguridad sobre la precisión de la información y los controles realizados.
- **Aproveche las herramientas y la tecnología:** Aproveche las herramientas y tecnologías innovadoras, como la detección de riesgos, para evaluar los problemas de DEI e identificar riesgos potenciales.
- **Reconciliar realidades:** Desarrolle recomendaciones para cerrar la brecha entre las percepciones del liderazgo y las realidades de los empleados en la cultura corporativa.

El papel de la auditoría interna en

Aseguramiento desde el Diseño

Para las transformaciones o implementaciones, los controles deben ser una previsión, no una ocurrencia tardía.

Nuestra Visión

Si gastas medio millón en un Lamborghini, seguramente aprovecharías al máximo su enorme motor de 12 válvulas, su aceleración de fuerza G y su multiplicidad de aplicaciones y ruidos.

Sin embargo, no se puede decir lo mismo de las organizaciones que invierten sumas similares en sistemas de planificación de recursos empresariales (ERP). En nuestra experiencia, una amplia gama de funciones de control interno de ERP no están suficientemente validadas e implementadas, o no se utilizan por completo. Es el equivalente a comprar un costoso automóvil deportivo italiano y nunca sacarlo de la segunda marcha.

Aprovechar el valor de su inversión en ERP comienza mucho antes de la puesta en funcionamiento. Comienza con la adopción de una mentalidad consciente de los controles para gestionar eficazmente los riesgos operativos y estratégicos en toda la organización.

Es decir, en lugar de considerar su sistema ERP simplemente como un medio para administrar de manera eficiente los recursos humanos, el inventario, finanzas, clientes o cadena de suministro, debe considerarlo como una herramienta para gestionar los numerosos riesgos asociados con estas actividades.

Una mentalidad de controles relacionada con las implementaciones/transformaciones significativas de la empresa comienza con la alineación entre la naturaleza y el alcance de las actividades realizadas en las tres líneas de defensa para navegar de manera eficiente en los riesgos y también garantizar que no haya brechas: las unidades de negocios de primera línea, la segunda línea con profesionales de riesgo y cumplimiento, y los auditores internos en tercera línea. Este ejercicio de coordinación/colaboración no debe tomarse a la ligera, ya que es la base sobre la que se construye una implementación o actualización exitosa de ERP.

News

En una auditoría de 2018 de una agencia del gobierno de EE. UU., casi la mitad de las deficiencias citadas estaban relacionadas con sus sistemas de TI. Entre sus hallazgos, los auditores señalaron que la agencia no implementó controles de seguridad destinados a detectar cambios accidentales o no autorizados en los datos financieros.

Datos Relevantes

En una encuesta reciente de Deloitte, casi la mitad de todos los ejecutivos dijeron que las implementaciones de tecnología, incluidos ERP, automatización, migración a la nube y controles relacionados con el trabajo remoto y los riesgos asociados, impulsarán a sus organizaciones a remediar los procesos financieros en el próximo año.

Aseguramiento desde el Diseño

Para obtener más información:

- **Deloitte:** Assurance by design: Drawing up the control playbook for transformations
- **Deloitte:** Modernizing the three lines of defense model
- **Wall Street Journal:** Assurance by design – consider control needs up front

Señales de Alerta

- **Sub-utilización Tecnológica:** Un número sorprendente de organizaciones no logra aprovechar los controles sólidos integrados en el software de planificación de recursos empresariales (ERP), como SAP y PeopleSoft. Los entornos de control que dependen en gran medida de los controles manuales pueden ser más susceptibles a retrasos, errores y fraudes.
- **Aumento de Costos:** Sus costos posteriores a la implementación podrían ser significativamente mayores si los controles y el aseguramiento asociado no se considera adecuadamente desde el principio.
- **Duplicidad de controles**: La confusión y las ineficiencias pueden reinar si los equipos de cumplimiento no tiene claro quién está haciendo qué en el ámbito de control interno.

Obtener los fundamentos correctos

- **Alcance:** Conéctese con amplios grupos de las partes interesadas de toda la empresa para ayudar a identificar las capacidades de control y procesos comerciales necesarios.
- **Comparta el conocimiento:** Aconseje a los líderes empresariales que consideren no solo el riesgo financiero, sino también el riesgo operativo y estratégico, que por necesidad implicará un conjunto más amplio de controles y capacidades necesarias para lograr los objetivos comerciales.
- **Visión futura**: Identifique oportunidades para automatizar o modernizar los controles para aumentar la eficiencia, reducir los errores y automatizar la provisión de garantía.

Dando los siguientes pasos

- **Aproveche la experiencia:** Si su organización está considerando un proyecto transformador o la implementación de un sistema, asegúrese de que los responsables del control se comprometan con el riesgo, el cumplimiento y la auditoría interna desde el principio.
- **Alinee con la estrategia:** Tómese el tiempo para alinear sus tres líneas de defensa. Aclare roles y responsabilidades. Disminuya las tensiones y evite las guerras territoriales. Piense de forma detallada en torno a los pasos y las actividades.
- **Y los auditores:** Desarrolle una metodología y una estrategia detallada sobre cómo se consideran y validan los controles durante la implementación, y alinéese completamente con los auditores de la empresa para evitar sorpresas después de la puesta en funcionamiento**.**
- **Considere a los responsables de controlar, no solo los controles:** Observe la disposición del propietario del control, no solo el control mismo. Esto implica capacitar a los propietarios del control sobre lo que deben hacer después de la puesta en funcionamiento para cumplir con los requisitos de cumplimiento.

El papel de la auditoría interna en

Bullying y Acoso

El mal clima organizacional ha surgido como una causa fundamental de muchas empresas en quiebra. La auditoría interna puede ayudar a aclarar las cosas.

Nuestra Visión

Dada la preponderancia de historias de acoso e intimidación en el lugar de trabajo en las noticias, teníamos curiosidad: ¿por qué no hay más empresas que se enfrenten a este problema?

Las excusas eran tan variadas como equivocadas:

1. "Si le da mucha importancia, recibirá un montón de quejas e informes".
2. "Hemos tenido algunos casos, pero no están relacionados y no es indicativo de nuestra cultura corporativa en general ".
3. "Tenemos un código de conducta de larga data que nos protege".

La auditoría interna tiene un papel importante que desempeñar para ayudar a una empresa a tomar en serio el riesgo cultural y minimizar la dependencia de estos conceptos erróneos.

El propósito de la auditoría interna no es ser un moralizador, árbitro o fiscalizador, sino más bien como facilitador, observador y asesor.

El riesgo cultural se puede evaluar triangulando puntos de datos de diversas fuentes, incluidas encuestas, entrevistas, grupos focales, herramientas de detección de riesgos, análisis y programas de cumplimiento/conducta.

El análisis de una combinación de fuentes cualitativas y cuantitativas, permite construir una imagen completa para anticipar y mitigar áreas problemáticas potenciales.

Los beneficios de abordar de manera proactiva los problemas culturales pueden ser múltiples. Por ejemplo, en un entorno donde la competencia por los mejores talentos es feroz, las organizaciones que construyen un entorno positivo, de apoyo y de confianza que permite que los empleados prosperen atraerán y retendrán a los trabajadores mejor preparados.

En última instancia, una cultura laboral positiva permite el logro de los objetivos de la organización. Por el contrario, las organizaciones que no cultiven dicha cultura pueden sufrir importantes repercusiones financieras, legales, reglamentarias y de reputación.

News

En 2021, el gobernador de Nueva York, Andrew Cuomo, renunció a su cargo en medio de una investigación por acoso sexual tras las acusaciones presentadas por casi una docena de mujeres. Una investigación describió el trabajo ambiente en la oficina del gobernador como "extremadamente tóxico y abusivo"

Datos Relevantes

86%

de los ejecutivos encuestados en todo el mundo califican la cultura como "muy importante" o "importante".

12%

de las empresas creen que sus organizaciones están impulsando una "cultura adecuada".

Bullying y Acoso

Para obtener más información:

- Deloitte: Cultura y conducta en el lugar de trabajo: desafíos y oportunidades
- Deloitte: Diseñar el trabajo para el bienestar
- Wall Street Journal: el bienestar puede ofrecer beneficios saludables

Señales de advertencia

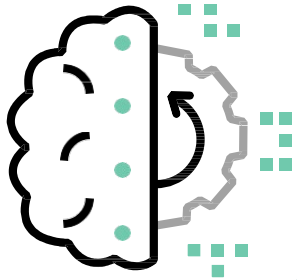
- **Baja reportabilidad**: Una señal de advertencia puede ser que no existan denuncias para un periodo de tiempo definido. Es posible que los empleados se hayan quedado en silencio porque las quejas anteriores han caído en oídos sordos. Otros silenciadores de la comunicación: miedo a represalias; procesos de informes complicados, entre otros.
- **Sequía de talentos**: Si ha notado un desgaste acelerado o una contratación más lenta, los problemas culturales pueden ser un factor.
- **Daños de Imagen:** Los comentarios negativos en las redes sociales y los sitios de búsqueda de empleo pueden ser precursores de crisis de la imagen de una organización.
- **Presión excesiva**: Las organizaciones que ejercen una presión implacable en torno a las ganancias trimestrales y los objetivos de ventas pueden estar creando un entorno en el que surgen el acoso y la intimidación. El comportamiento abusivo a menudo se correlaciona con demandas de desempeño irreales o inalcanzables.

Obtener los fundamentos correctos

- **Haga un balance:** Haga un inventario y revise los códigos de ética, los programas antifraude, las políticas y procedimientos de mala conducta, y las líneas directas o los mecanismos alternativos de denuncia con miras a la puntualidad, la claridad, la relevancia y la aplicabilidad.
- **Taller de charlas:** Anime a la junta y al comité de auditoría a agregar la cultura laboral como un tema recurrente en sus agendas.
- **Aporta una visión global:** Considere quién está a cargo de los asuntos culturales. A menudo, la responsabilidad está fragmentada entre las unidades de RR.HH., legal, de cumplimiento y de negocio. A veces, un equipo plantea inquietudes, otro investiga y el resto de la organización se queda en la oscuridad. Conviértete en el intermediario que une a las partes.

Dando los siguientes pasos

- **Consultar:** Asesorar a la gerencia sobre el establecimiento de un marco de evaluación de riesgos de la cultura que brinde información sobre la cultura organizacional, el compromiso y los comportamientos de los empleados, así como evalúe las señales del mercado**.**
- **Medida:** Agregue seguridad cultural a su plan de auditoría. Establezca, monitoree e informe sobre métricas relacionadas con la conducta de los colaboradores y las violaciones éticas. Asegúrese de que la junta revise estos puntos mencionados permanentemente.
- **Incentivar:** Recomendar la realineación del pago por desempeño y reconsiderar cómo los incentivos de pago impulsan el comportamiento.
- **Difundir:** Instar a la comunicación frecuente y la formación integral sobre cuestiones culturales.



El papel de la auditoría interna en

Automatización

Entre muchas preguntas difíciles: "¿Cómo aprovecha la Auditoría Interna la automatización para mantenerse al día?"

Nuestra Visión

Los gourmets de algunos restaurantes italianos, han debatido durante mucho tiempo una pregunta irritante: "¿Qué vino primero, el pollo a la parmesana o los huevos a la florentina?“

La gerencia enfrenta un dilema similar cuando se trata de auditoría interna: "¿Qué viene primero: poner nuestra casa en orden y luego traer auditoría interna? ¿O traer auditoría interna para ayudarnos a poner nuestra casa en orden?"

El problema es particularmente agudo cuando se trata de soluciones automatizadas como la Inteligencia Artificial (incluida la automatización y la inteligencia cognitiva). La implementación puede ser complicada; los controles de gobernanza pueden ser descuidados; la seguridad puede ser permeable, todo lo cual puede afectar significativamente el ROI esperado de la administración para su viaje de automatización y, lo que es peor, crear riesgos estratégicos internos y externos.

Si la gerencia duda en involucrarse con su grupo de auditoría interna por temor a hallazgos negativos, aquí está su respuesta: "La automatización llegó para quedarse, pero la tecnología evolucionará continuamente. El software, el hardware, las oportunidades y las vulnerabilidades representan un objetivo en movimiento. Como por tanto, es posible que el valor comercial de la automatización nunca será percibido si no se involucra la auditoría interna ".

Una vez que su equipo de Auditoría Interna está comprometido, ¿cuáles son las prioridades? Empiece por ayudar a la dirección a encontrar un equilibrio entre la absorción de riesgos y el apetito por el riesgo. Conéctese al principio del proceso, cuando se toman por primera vez las decisiones estratégicas sobre la automatización. Idealmente, la relación incluirá tanto elementos de asesoría como de aseguramiento, ayudando a la organización a obtener el ROI y luego brindando servicios de aseguramiento para su implementación de automatización.

Simultáneamente, adapte su plan de auditoría al nuevo entorno. Evalúe el riesgo de nuevas capacidades (procesos de negocio impactados, formas de trabajo y nuevas tecnologías habilitadoras) en los dominios de riesgo clave, como financiero, operativo, regulatorio, tecnológico y estratégico, y luego priorice en función de los criterios de impacto y vulnerabilidad.

A continuación, evalúa tus propias capacidades dentro del team de auditoría interna. Determine las habilidades necesarias para auditar soluciones automatizadas. ¿Puedes entrenar para llenar los vacíos? ¿O tendrá que contratar personal nuevo con las credenciales necesarias?

Finalmente, tendrás que lidiar con tu propio enigma:

"¿Cómo aprovechamos la automatización para mantenernos al día?"

News

El pronóstico parecía sombrío para una gran empresa de tecnología con un ambicioso plan para revolucionar la atención médica a través de la inteligencia artificial (IA), después de que su supercomputadora lanzará “múltiples ejemplos de inseguridad e incorrectas recomendaciones de tratamiento” para pacientes con cáncer.

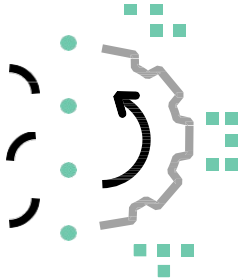
Datos Relevantes

En una encuesta reciente de Deloitte:

83% de los ejecutivos dijo que la inteligencia artificial será importante para el éxito de su negocio en los próximos dos años.

23% dijo que su equipo actualmente audita las capacidades digitales avanzadas.

59% dijo que no participaron en el desarrollo del programa de automatización de su organización.



Automatización

Para obtener más información:

- **Deloitte: Auditando los riesgos de las tecnologías disruptivas | Mantén el tiempo**
- **Deloitte: Profundizar la auditoría interna en la era digital: Parte I**
- **Deloitte: Profundizar la auditoría interna en la era digital: Parte II**

Señales de advertencia

- **Enfoques ad hoc:** Si RR.HH. está implementando Inteligencia Artificial mientras AP está implementando RPA y la I+D está jugando con la PNL, entonces se tiene un enfoque gradual en la implementación de la automatización que probablemente esté plagado de vulnerabilidades.
- **Posicionamiento de auditoria interna**: Si auditoría interna no tiene un lugar en la mesa cuando se discuten por primera vez las soluciones automatizadas, las posibilidades de una implementación exitosa se reducen.
- **Falta de acceso:** Un obstáculo importante para auditar soluciones automatizadas es la incapacidad de revisar el código de software y la documentación de diseño.

Obtener los fundamentos correctos

- **Haga un balance:** Comprenda la estrategia comercial, la visión, y desarrollo relacionado con el despliegue de soluciones automatizadas. ¿Cómo se consideran los asuntos relacionados con el riesgo como parte de ese viaje?
- **Haga preguntas:** ¿Qué nuevos riesgos conllevan estas nuevas tecnologías? ¿Cómo nos aseguramos de que nuestras métricas y modelos sean precisos? ¿Cómo nos protegemos contra el sesgo en nuestros algoritmos?
- **Tomar controles:** Determinar los objetivos comerciales para asesorar sobre el diseño de actividades de control y / o realizar revisiones previas a la implementación.

Dando los siguientes pasos

- **Estructura de construcción:** Cree una estrategia de gestión de riesgos de tecnología de automatización y una estructura de gobierno para gestionar los riesgos y permitir el cumplimiento.
- **Proyecte una amplia red**: Al auditar soluciones de automatización, incluya áreas como controles, gobernanza, ciclo de vida de desarrollo, estrategia y revisiones de código.
- **Renovar los informes:** Modernice sus informes para la nueva era. Identificar el nivel y la estructura de los informes que se realizarán, incluido el nivel de tecnología frente al nivel de función empresarial y el de aseguramiento consultivo. Reconsidere la frecuencia y rapidez de sus auditorías.

Deloitte.

Manuel Gálvez
Socio Líder Accounting & Internal Controls Deloitte
mangalvez@deloitte.com

Fernando Pino
Director Líder Auditoría Interna Deloitte
fepino@deloitte.com