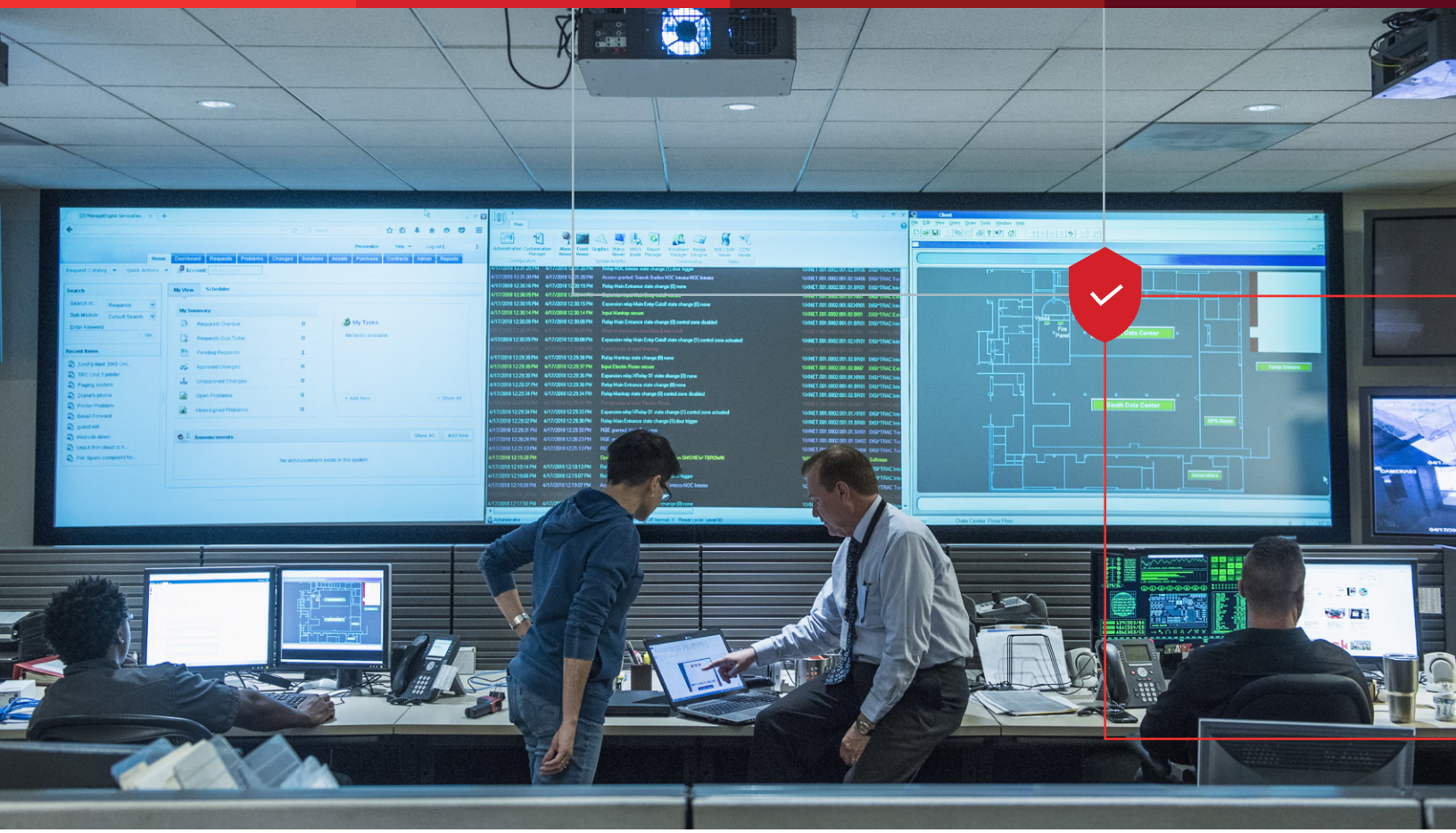
Diligent

Preparación de la auditoría interna para el futuro

Contenido



Nuevo juego de herramientas de auditoría interna

Los perfiles de riesgo de las organizaciones son cada vez más complejos y difíciles de administrar. Para mantenerse vigente, la auditoría interna debe responder a estos desafíos y proporcionar conocimientos estratégicos, no solo aseguramiento.

Tradicionalmente, las funciones de la auditoría interna se centraban en los sistemas de cumplimiento y control interno. Pero para colaborar con la alta gerencia y la junta directiva, la auditoría interna debe comprender los riesgos claves de la organización e identificar de forma proactiva los riesgos emergentes.

Para cumplir con estas exigencias, los auditores internos deben comenzar a utilizar nuevas herramientas y tecnologías como inteligencia artificial, aprendizaje automático y automatización robótica de procesos, y aprovechar mejor los estudios analíticos de datos para la toma de decisiones.

Diligent

La tecnología es clave

¿Cuenta con las herramientas para ayudar a su organización a identificar y administrar los mayores riesgos que conlleva la nueva economía digital?

La adopción de la tecnología es esencial para impulsar la preparación de las funciones de auditoría interna para el futuro. Las personas y los procesos forman la base, y la tecnología es el acelerador que necesita la auditoría interna para ser más innovadora y eficaz.

Un estudio de Protiviti[1] reveló que la adopción de capacidades de última generación para la auditoría interna aún está en sus primeras etapas. Sin embargo, el 71 % de los directores de auditoría (CAE, por sus siglas en inglés) creen que sus funciones de auditoría tienen alto impacto e influencia y piensan aumentar su inversión en innovación en los próximos años.[2] En adelante, los CAE deberán tomar la iniciativa para colocar esta transformación tecnológica fundamental en la agenda del comité de auditoría.

Este libro electrónico analiza las tecnologías que los CAE y los equipos de auditoría interna deben adoptar a efectos de preparar sus funciones de auditoría para el futuro y aumentar la eficiencia.

[1] **Protiviti,** 2019 Embracing the next generation of internal auditing (Adopción de la próxima generación de auditoría interna)
[2] **Deloitte,** 2018, The innovation imperative: Forging internal audit's path to greater impact and influence (El imperativo de la innovación: forjar el camino para que la auditoría interna tenga mayor impacto e incidencia)

Digitalización y transformación digital

La digitalización no es una palabra empresarial de moda: se trata del uso de la tecnología para mejorar el rendimiento y crear nuevas oportunidades de negocios.

Con tantos avances y cambios en la tecnología para empresas y consumidores, la digitalización ahora implica la integración de diferentes tipos de tecnologías. Entre otras, computación en la nube, movilidad, estudios analíticos de "big data", aprendizaje automático, inteligencia artificial (IA) e Internet de las cosas.

Este impulso hacia la digitalización, la automatización y las inversiones en robótica, aprendizaje automático, IA y estudios analíticos avanzados es una nueva forma de transformación empresarial comúnmente llamada Industria 4.0.[3]

Y casi todos los equipos de auditoría están aprovechando estas tecnologías en alguna medida. Un informe reciente de Protiviti reveló que el 76 % de los grupos de auditoría interna están en proceso de transformación digital.[4]

En el caso de las grandes organizaciones actuales, la pregunta no es si la digitalización va a revolucionar sus negocios, sino cuándo.

Aunque los ejecutivos estén al tanto de las tecnologías emergentes con potencial innovador, suele ser difícil determinar qué impacto tendrá esta innovación en la organización.

Pero no es novedad; la transformación digital se está procesando desde hace muchos años. Entre los grandes cambios de las décadas pasadas se encuentra la introducción de los flujos de trabajo automatizados, los papeles de trabajo electrónicos y los sistemas dedicados de gestión de auditoría. Estas tecnologías se consideraron revolucionarias cuando aparecieron por primera vez, pero ahora son la norma. El objetivo de los CAE y los comités de auditoría que marcan el paso del cambio es lograr que las tecnologías digitales actuales lleguen al mismo estado de adopción estándar.

[3] **KPMG,** 2019, Top 20 risks in internal audit before 2020 (Veinte principales riesgos de la auditoría interna antes de 2020)
[4] Protiviti,2019, Embracing the next generation of internal auditing (Adopción de la próxima generación de auditoría interna)


Diligent

Creciente rol de ciberseguridad de la auditoría interna...

El riesgo de ciberseguridad está creciendo y evolucionando en todo el mundo, al igual que el rol de la auditoría interna para mitigarlo.

Según la encuesta de 2019 sobre capacidades de auditoría, el riesgo de ciberseguridad es la segunda prioridad de los CAE.[5] Y dada la frecuencia con la que aparecen importantes incumplimientos cibernéticos en los titulares de las noticias, la ciberseguridad está en la mira de la auditoría interna, más que nunca.

La auditoría interna trabaja para gestionar las ciberamenazas proporcionando evaluaciones independientes de los riesgos existentes y ayudando al comité de auditoría y a la junta directiva a comprender y enfrentar esos riesgos. Deloitte[6] reporta que muchas organizaciones reconocen la necesidad de una tercera línea de defensa cibernética: una revisión independiente de las medidas de seguridad y su desempeño llevada a cabo por la auditoría interna. Los equipos de seguridad o de informática no son los únicos responsables de la ciberseguridad, ya que afecta e involucra a todas las áreas de negocios. En un enfoque tradicional compartimentado, cada departamento trata los riesgos independientemente. No existe un lenguaje común ni un marco para examinar los ciberriesgos de forma holística. Centrarse en los riesgos elimina las barreras y posibilita que los propietarios de los procesos de negocios prioricen y actúen en función de los hallazgos.

Mediante el uso de un lenguaje común para los riesgos en todos los departamentos y con personas en las tres líneas de defensa, un auditor puede evaluar realmente la eficacia del programa de ciberseguridad y tener una imagen precisa de la situación de la organización.

Un enfoque basado en riesgos también permite que la auditoría interna colme las expectativas de la junta directiva e identifique los principales vacíos tácticos y estratégicos de gobernanza de la ciberseguridad.

ACTIVIDADES COMUNES DE LA AUDITORÍA INTERNA FRENTE A LOS CIBERRIESGOS

01 Evaluar independientemente las medidas de prevención y detección relacionadas con la ciberseguridad.

02 Evaluar los aspectos estándar (como configuraciones de seguridad, software maligno y filtración de datos) de los activos informáticos de los usuarios con acceso privilegiado.

03 Hacer el seguimiento de la diligencia de las acciones correctivas.

04 Evaluar los ciberriesgos de organizaciones de servicios, terceros y proveedores.

[5] **Protiviti,**2019, Embracing the next generation of internal auditing (Adopción de la próxima generación de auditoría interna)
[6] **Deloitte,** 2017, Cybersecurity and the role of internal audit (Ciberseguridad y el rol de la auditoría interna)

Diligent

Realización de evaluaciones de ciberriesgos

Solo la mitad de los jefes de auditoría interna indicaron que sus grupos han realizado evaluaciones de ciberriesgos.

Entre aquellos que realizaron evaluaciones de ciberriesgos, las tres cuartas partes desarrollaron un plan de auditoría basado en la evaluación.[7]

La realización de una evaluación integral de los ciberriesgos permite a la auditoría interna presentar evaluaciones objetivas y hallazgos a los miembros del comité de auditoría y de la junta directiva y utilizar esos hallazgos para desarrollar un amplio plan de auditoría interna que incluya los ciberriesgos.

Una evaluación de ciberriesgos también puede estructurarse para generar una lista de vacíos de ciberseguridad y proporcionar a la organización una hoja de ruta para las acciones correctivas de corto y largo plazo.

PASOS DE EVALUACIÓN DE CIBERRIESGOS

1

Caracterizar el sistema (proceso, función o aplicación)

Responda a las preguntas: ¿Qué es? ¿Qué datos usa? ¿Cuáles son los proveedores involucrados? ¿Cuál es el flujo de datos? ¿A dónde va la información?

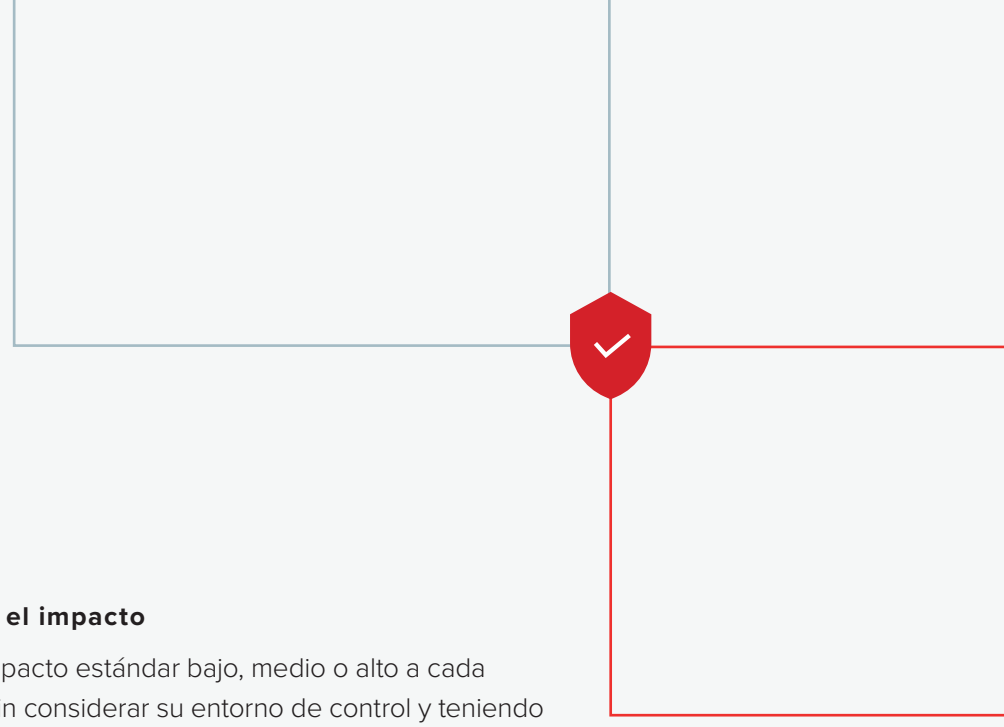
2

Identificar amenazas

Las amenazas varían según la organización, pero las comunes son:

- Acceso no autorizado
- Mal uso de la información por un usuario privilegiado
- Pérdida de datos
- Interrupción del servicio

[7] **Deloitte,** 2018, The innovation imperative: Forging internal audit's path to greater impact and influence (El imperativo de la innovación: forjar el camino para que la auditoría interna tenga mayor impacto e incidencia)



3 **Determinar el riesgo inherente y el impacto**

Aplique una calificación de riesgo/impacto estándar bajo, medio o alto a cada una de las amenazas identificadas (sin considerar su entorno de control y teniendo en cuenta qué pasaría si el riesgo se concretara).

4 **Analizar el entorno de control**

Identifique los controles de prevención, mitigación y detección de amenazas (p. ej.: controles para el aprovisionamiento de usuarios, administración, seguridad del centro de datos, continuidad del negocio) y sus relaciones con las amenazas identificadas.

5 **Determinar una calificación de probabilidad**

Evalúe la probabilidad, dentro de su entorno de control, de que cualquier vulnerabilidad o riesgo dado se concrete dentro de su organización (nuevamente, use la calificación: baja, media, alta).

6 **Calcular su calificación de riesgo**

La ecuación de la calificación del riesgo es muy simple: impacto (si se concreta) X probabilidad (de que se concrete dentro del entorno de control). Con un sistema de calificación de bajo, elevado y grave, se determinan los niveles de las calificaciones de los riesgos individuales, que es el siguiente paso.

7 **Priorizar los riesgos**

Use el sistema de calificación de riesgos que prefiera para priorizar los riesgos por orden de magnitud.

8 **Documentar los resultados en un reporte de evaluación de riesgos**

Genere un reporte de evaluación de riesgos para ayudar a la gerencia en la toma de decisiones sobre presupuesto, políticas y procedimientos.


Diligent

Cómo puede contribuir la auditoría interna a mitigar ciberriesgos

Como tercera línea de defensa, la auditoría interna juega un papel importante en el abordaje de los ciberriesgos.

¿QUÉ PASOS PUEDE DAR LA AUDITORÍA INTERNA?

- Trabajar con la gerencia y la junta directiva para desarrollar una estrategia de ciberseguridad
- Mejorar la capacidad de la organización para identificar, evaluar y mitigar los riesgos de ciberseguridad
- Aumentar la consciencia y el conocimiento sobre las ciberamenazas y asegurarse de que la junta directiva permanezca muy comprometida con las cuestiones de ciberseguridad
- Integrar el riesgo de ciberseguridad en el plan de auditoría
- Evaluar el programa de ciberseguridad en relación con los marcos de referencia establecidos (p. ej.: PCI DSS, NIST)
- Expresar a los interesados que la mejor prevención es una combinación de consciencia, capacitación, vigilancia y tecnología
- Enfatizar que el monitoreo de la ciberseguridad y la respuesta a los incidentes cibernéticos debe ser una alta prioridad de la gerencia
- Atender cualquier escasez de personal y recursos de auditoría o de TI, así como de las herramientas o tecnologías de apoyo que sean necesarias

Diligent

Aprendizaje automático y automatización robótica de procesos

En años recientes, la auditoría interna ha sentido el impacto de las tecnologías emergentes como IA, aprendizaje automático y automatización robótica de procesos (RPA).

El aprendizaje automático y la RPA pueden transformar el funcionamiento de la auditoría. RPA utiliza la tecnología para automatizar procesos como la recopilación de datos, mientras que el aprendizaje automático utiliza algoritmos para analizar los datos, establecer relaciones y hacer predicciones.

Analicemos algunas de las aplicaciones actuales y futuras del aprendizaje automático y la RPA en la auditoría interna.

Aprendizaje automático

El aprendizaje automático es una categoría de la IA que se basa en la idea de que las máquinas pueden aprender de forma similar a los humanos.

El aprendizaje automático puede usar modelos para analizar datos, comprender patrones y hacer predicciones. Aún es una tecnología emergente en la auditoría interna y está primordialmente en la fase de investigación y desarrollo.

Varias de las más grandes empresas de contadores públicos están creando sistemas de aprendizaje automático y las empresas más pequeñas podrán aprovechar esta tecnología a medida que mejore.

A pesar de que su aplicación aún está en una fase relativamente inicial, los potenciales beneficios de esta tecnología para los equipos de auditoría interna de vanguardia son muy interesantes. Estos son algunos ejemplos de la vida real.[8]

EY

EY está utilizando el aprendizaje automático para detectar anomalías y facturas fraudulentas. La compañía reveló que la tecnología tiene un 97 % de precisión al identificar facturas erróneas. La tecnología ha ayudado a EY a minimizar significativamente su exposición a riesgos relacionados con sanciones por infracciones, normas antisoborno y otros aspectos de la ley de prácticas corruptas en el extranjero.

DELOITTE

Deloitte está usando el aprendizaje automático para revisar cientos de miles de documentos legales con el fin de identificar disposiciones de control de cambios como parte de la venta de una unidad de negocios de un cliente. Este proceso antes ocupaba a docenas de empleados durante medio año, pero ahora completarlo lleva menos de un mes con un equipo de ocho personas, lo que libera al personal para que dedique su tiempo y su energía a otros trabajos.

DEPARTAMENTOS DE ASEGURAMIENTO

La IA se utiliza para aumentar la eficiencia y reducir las tareas manuales. En lugar de realizar pruebas aleatorias basadas en muestreos, puede usarse la IA para analizar el libro mayor completo e identificar las transacciones de alto riesgo.

Sin duda, la IA puede aumentar drásticamente la eficiencia, reducir las tareas manuales y permitir que el personal de auditoría disponga de tiempo para el pensamiento crítico. Con un proceso de aprendizaje a partir de las excepciones y las conclusiones o juicios de los auditores, el aprendizaje automático aumenta su precisión a medida que aprende a identificar mejor las excepciones en los datos.[9]

Para profundizar en las aplicaciones del aprendizaje automático en GRC, lea nuestro libro electrónico *Machine learning essentials* (Conceptos esenciales sobre aprendizaje automático).

[8] **The CPA Journal,** 2019, Machine learning in auditing: Current and future applications (Aprendizaje automático en la auditoría: aplicaciones actuales y futuras)
[9] **International Federation of Accountants,** 2018, Why accountants must embrace machine learning (Por qué los contadores deben adoptar el aprendizaje automático)

Diligent

Automatización robótica de procesos

Dado que las tecnologías de automatización avanzan con rapidez y quienes las adoptaron tempranamente demuestran su eficacia, la RPA comienza a ganar terreno en las funciones de auditoría interna.[10]

RPA es una forma mucho más accesible de IA. Utiliza robots de software para automatizar procesos repetibles con sistemas basados en reglas. Estos robots son fáciles de configurar, no requieren grandes conocimientos de TI ni de ciencia de datos y en poco tiempo se pueden entrenar e implementar para automatizar tareas manuales.

RPA Y AUDITORÍA INTERNA

Mediante la automatización, los auditores internos pueden hacer más con los mismos recursos, por ejemplo:

- Mejorar la calidad y la coherencia de los procesos de auditoría interna
- Mejorar la eficiencia de las actividades de planificación, pruebas y reportes
- Aumentar la cobertura y la frecuencia de las pruebas
- Ampliar el alcance de las auditorías individuales
- Pasar de las pruebas de muestras limitadas a probar la población completa
- Administrar las limitaciones geográficas y de mano de obra

USOS DE RPA EN AUDITORÍA INTERNA

- Evaluaciones de riesgos. Los robots pueden ayudar a clasificar riesgos mediante reglas predefinidas, puntos de datos y tendencias para evaluar los riesgos. Esto permite mayor rapidez en la identificación de áreas y transacciones de alto riesgo.
- Asistencia en las pruebas de controles. Los robots pueden probar poblaciones enteras de datos (no solo muestras), lo que aumenta la confianza en los controles y deja tiempo libre a los auditores internos.
- Recopilación de datos y procesamiento de grandes volúmenes de transacciones. Los robots pueden procesar grandes volúmenes de datos con mayor rapidez, eficiencia y precisión que los métodos manuales o basados en hojas de cálculo.
- Recolección y depuración de datos. Los robots ejecutan estudios analíticos personalizados, como la extracción de datos para uso de los auditores internos, incluida la validación de integridad de los campos, comparaciones y duplicados.

[10] Deloitte,2018, Adopting automation in internal audit (Adopción de la automatización en la auditoría interna)

PwC estima que el 45 % de las actividades de trabajo pueden automatizarse y que esta automatización podría ahorrar a las organizaciones hasta USD 2 billones en costos globales de mano de obra.[11]

[11] **PwC,** 2017, Robotic process automation: A primer for internal audit professionals (Automatización robótica de procesos: manual básico para profesionales de la auditoría interna)

Diligent

Estudios analíticos de datos

La tecnología de los estudios analíticos de datos es una de las que lidera la conformación del futuro de la auditoría interna.

Esto lo confirman los CAE que identificaron el uso limitado de los datos como uno de los diez principales riesgos de 2018.[12] Y de acuerdo con un artículo de Internal Auditor,[13] todavía no se ha generalizado el uso de los estudios analíticos de datos y otras herramientas tecnológicas valiosas en los departamentos de auditoría interna.

El problema es que muchos departamentos de auditoría interna, en especial los que tienen problemas de recursos, no saben por dónde comenzar. Protiviti entrevistó a más de 1500 CAE y descubrió que los departamentos de auditoría interna aún están intentando desarrollar una metodología formal para integrar los estudios analíticos de datos.[14] Y muchas funciones de auditoría solo usan herramientas de estudios analíticos como "soluciones puntuales" en casos individuales y no como parte de una iniciativa estratégica más amplia que abarque todo el proceso de auditoría.

La encuesta indica que el 66 % de las funciones de auditoría que no utilizan actualmente estudios analíticos de datos planea hacerlo como parte del proceso de auditoría en los próximos dos años, mientras que el 34 % todavía no tiene planes al respecto.

La adopción de estudios analíticos de datos será un elemento central para los departamentos de auditoría interna de cara al futuro. En la figura 1, se muestra un diagrama de flujo (adaptado de PwC) que detalla cómo un departamento de auditoría interna podría implementar un programa de estudios analíticos de datos.

La auditoría interna no solo debe considerar los estudios analíticos de datos como elementos estándares de sus funciones de negocios, también debe asumir un rol más relevante en la gobernanza de datos, impulsar las normas y políticas relacionadas con la recopilación y la calidad de los datos y la gestión formal de los activos de datos en toda la organización.

[12] **PwC,** 2017, Robotic process automation: A primer for internal audit professionals (Automatización robótica de procesos: manual básico para profesionales de la auditoría interna)
[13] **Internal Auditor,** 2018, Out of step with analytics (Desfase con los estudios analíticos)
[14] **Protiviti,** 2018, Internal audit capabilities and needs survey (Encuesta de capacidades y necesidades de la auditoría interna)

FIGURA 1: FLUJO DE IMPLEMENTACIÓN DEL PROGRAMA DE ESTUDIO ANALÍTICO DE DATOS

Gestión de la información

01 Identificar los orígenes de los datos

Revisar e identificar los orígenes de los datos entre los sistemas de origen, los datos de reportes y los datos a nivel de aplicaciones

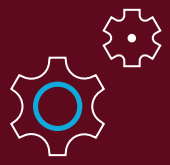
02 Definir la frecuencia

Definir el origen de datos necesario de forma regular (necesidad diaria, mensual, trimestral o por única vez)

03 Repetitividad

Desarrollar procesos manuales y automatizados para reducir la carga de la recopilación de datos

Capacidades y herramientas de los estudios analíticos



04 Definir recursos

Definir círculos concéntricos del equipo principal, experto de los estudios analíticos e inspirador de las capacidades de todo el departamento

05 Elegir tecnologías

Identificar capacidades y necesidades en términos de soluciones de estudios analíticos, visualización, gestión de datos y monitoreo

06 Crear capacitación

Crear programas e incentivos para desarrollar mentalidad y competencias analíticas

Cultura orientada a los datos

07 Desarrollar metodología

Desarrollar normas de ejecución y de calidad para los estudios analíticos en el plan de auditoría y las pruebas de controles.

08 Crear consciencia

Garantizar que las herramientas tecnológicas dentro del departamento estén alineadas con la metodología y tengan la capacidad de hacer un seguimiento de la adhesión a la metodología

09 Compartir triunfos

Definir “medidas de éxito” y comunicar y compartir los triunfos en todo el departamento para cambiar la cultura

Adaptado de: PwC, 2018, Transforming internal audit through data analytics (Transformación de la auditoría interna a través de estudios analíticos de datos)

Diligent

El rol de la auditoría interna en la gobernanza de datos

A medida que crece la importancia de los datos en nuestra vida diaria personal y laboral, se vuelve esencial la gobernanza digital y de datos.

La gobernanza de datos ayuda a las organizaciones a cumplir con las políticas y normas de seguridad de datos e información personal, además de asegurar la precisión, la integridad y la adecuada administración de los datos. El departamento de auditoría interna de cada organización debería participar en este proceso.
Las organizaciones necesitan datos confiables, depurados, precisos y accesibles para mantener la competitividad. Por ejemplo, RPA depende de buenos datos para procesar la información de forma precisa y eficiente. Sin embargo, si no existe una gobernanza general de datos para guiar este proceso, la probabilidad de que los datos no sean fiables es mucho mayor. Además, aumenta el riesgo de que las nuevas tecnologías no sean eficaces.

Los auditores internos con visión de futuro deben preguntar:

- ¿La gobernanza de datos es un área de interés dentro de sus auditorías de tecnología este nuevo año?
- ¿Tiene confianza en los controles de datos (incluidos los de seguridad, privacidad, acceso y precisión) para el uso que hace la organización de las nuevas tecnologías?

La auditoría interna no puede participar en todos los proyectos, tampoco lo pueden hacer otras áreas de gobernanza, riesgo y cumplimiento (GRC), como gestión de riesgos o cumplimiento. No obstante, si se vincula estrechamente con la estrategia digital o de innovación de la organización y participa desde el inicio en las iniciativas importantes, la auditoría interna puede ampliar su cobertura de riesgos ayudando a conformar la gobernanza de datos.
Un marco de gobernanza de datos puede guiar muchos proyectos que integran la misma tecnología emergente para diferentes casos de uso y aumentar las posibilidades de que también se integren las consideraciones de controles.
La auditoría interna puede centrarse luego en las pruebas para verificar que las directrices se sigan y se ratifiquen. En un estudio reciente de PwC, el 40 % de los equipos de auditoría interna de alto rendimiento ayudaron a establecer estándares de gobernanza para las organizaciones.[15] ¿Está listo para unirse a ese 40 %?

[15] **PwC,** 2019, State of the internal audit survey (Encuesta del estado de la auditoría interna)

Diligent

Conclusión

A pesar de que los conocimientos de los auditores internos y el uso de los procesos adecuados son esenciales, la tecnología emergente es la mejor manera de preparar la auditoría interna para el futuro.

No se trata de sustituir a las personas con aprendizaje automático o robótica, y los auditores internos no deben temer a esta transformación digital.
En realidad, dominar estas tecnologías en pleno avance es beneficioso para los auditores internos. El trabajo se vuelve más eficiente, preciso y automatizado. Además, los auditores tienen más tiempo para dedicarse a iniciativas estratégicas y al desarrollo de su carrera.

¿Está listo para descubrir de qué forma puede ayudarle la Gestión de auditoría a agregar valor, gestionar mejor su flujo de trabajo de auditoría y aportar conocimientos estratégicos?

Acerca de Diligent Corporation

Diligent™ es el principal proveedor de servicios de software (SaaS) de gobernanza, riesgo y cumplimiento (GRC) y atiende a más de un millón de usuarios de más de 25.000 organizaciones alrededor del mundo. Nuestra moderna plataforma de GRC asegura que las juntas directivas, los ejecutivos y otros líderes tengan una visión holística e integrada de auditoría, riesgo, seguridad de la información, ética y cumplimiento en toda la organización. Diligent brinda tecnología, información y confianza a los líderes para que puedan crear organizaciones más eficaces, equitativas y exitosas.

Para obtener más información o solicitar una demostración:

Correo electrónico: info@diligent.com | Visite: diligent.com