

A U D I T O R Í A I N T E R N A



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Guía para implantar con éxito un modelo de Auditoría Continua



Guía para implantar con éxito un modelo de Auditoría Continua

Octubre 2014

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN: Daniel Ponz Lillo, CIA, CRMA. Iberdrola.

Alejandro Barroso Bazán. Plus Ultra.

Cristina Bausá Rosa, CIA, CRMA. Mazars Auditores.

Juan Luis Escribano Soto, CIA, CRMA. EY.

Víctor Gómez López. Inversis.

Marta Grande Pérez. Mapfre.

Borja Guisasola Marrodán. Banco Santander.

Ismael Martín García, CIA. Cosentino.

Manuel Mendiola Antona, CIA, CRMA. KPMG.

Marcos Sánchez Sotes, CIA, CRMA. Ítaca Auditores.

Complejidad regulatoria, crisis financiera, presión sobre objetivos de negocio, exposición al fraude, cambio permanente y un largo etcétera son algunos de los crecientes desafíos y responsabilidades a los que se enfrentan los Consejos de Administración, los Comités de Auditoría y la Dirección de las compañías que demandan contar con un sistema de aseguramiento sobre la eficacia del control y la gestión de riesgos, fiable, sostenible y continuo.

Las Direcciones de Auditoría Interna tenemos el reto de dar respuesta a esta demanda de aseguramiento y hacerlo de una manera proactiva, proyectiva y continua.

Implantar un modelo de Auditoría Continua permite a la Dirección de Auditoría Interna determinar rápidamente dónde prestar mayor atención y recursos, incrementar el alcance y la capacidad de mitigar los riesgos, mejorar la comprensión de los procesos y, por tanto, mejorar la calidad del aseguramiento que proporciona a la Alta Dirección y al Consejo.

Esta guía hace un exhaustivo análisis de todas las cuestiones relevantes a considerar y no olvidar cuando se emprende la implantación de un modelo de Auditoría Continua, sus beneficios y desafíos.

La riqueza de este análisis radica en su flexibilidad, los autores presentan todas las opciones posibles con sus ventajas e inconvenientes para que cada Dirección de Auditoría Interna pueda valorar cuál de ellas se adapta mejor a la cultura, al marco de Gobierno, Riesgo y Cumplimiento y a la realidad de su organización.

El documento incluye además un caso práctico que afianza y aterriza el contenido teórico expuesto y despeja dudas para la implantación con éxito de este enfoque.

Felicito a los autores de esta guía por compartir generosamente su valiosa experiencia en la implantación de un modelo de Auditoría Continua que ayuda realmente a las Direcciones de Auditoría Interna a afrontar este proyecto estratégico con menor incertidumbre y mayor probabilidad de éxito.

Ernesto Martínez

Presidente del Instituto de Auditores Internos de España





Índice

RESUMEN EJECUTIVO	07
INTRODUCCIÓN	08
DECÁLOGO DE BUENAS PRÁCTICAS	11
CONSEJO 2320-4 SOBRE ASEGURAMIENTO CONTINUO	14
MODELO DE MADUREZ	14
CÓMO IMPLANTAR UN ENFOQUE DE AUDITORÍA CONTINUA EN NUESTRA ORGANIZACIÓN	16
Arranque del proyecto	16
Diseño de la plataforma	19
Desarrollo	24
Despliegue	27
Y luego... ¿qué?	29
CASO PRÁCTICO	33
Descripción de la empresa	33
Mapa de procesos	35
Modelo de Auditoría Continua implementado	36
Modelo de ejecución y mantenimiento continuo del modelo	39
ANEXOS	41
Glosario.....	41
Ejemplos de herramientas de mercado	42
Bibliografía	43





Resumen Ejecutivo

Los Comités y las Direcciones de Auditoría Interna se enfrentan actualmente a importantes retos: incremento de la complejidad regulatoria, crisis financiera, limitación de recursos, presión sobre objetivos de negocio, exposición al fraude, globalización, cambios tecnológicos y operativos, etc. Cuestiones que presuponen, más que nunca, la necesidad de contar con un “sistema de aseguramiento de la eficacia de los sistemas de control y gestión de riesgos” fiable, sostenible y continuo.

Habitualmente, son los auditores internos quienes analizan estos controles, pero lo hacen de forma retrospectiva y cíclica, en ocasiones, mucho después del momento en que se producen los hechos y con muestras limitadas de población. Un enfoque que restringe la cobertura del análisis y el tiempo de respuesta ante eventos relacionados con el cumplimiento regulatorio o incidencias operativas.

La Auditoría Continua, en cambio, permite evaluar los riesgos y sus controles, y realizar auditorías internas de carácter sustantivo, de manera automática y frecuente. Aunque la tecnología es un factor clave, la Auditoría Continua implica, además, un cambio de paradigma: las “revisiones periódicas de una muestra de transacciones” dan paso a “pruebas de auditoría permanentes sobre la totalidad”. Los resultados de estos análisis integran el proceso de auditoría interna en todos sus aspectos: desde el desarrollo y mantenimiento del plan anual, hasta la realización y el seguimiento de auditorías internas específicas.

Esta guía es eminentemente práctica y está orientada a comprender los elementos de un modelo de Auditoría Continua, sus beneficios y los desafíos que plantea.

La guía incluye:

- Definición del concepto de Auditoría Continua, cómo impacta en los procesos de Auditoría Interna y su relación con otras funciones de aseguramiento y del negocio en general.
- Los beneficios de la Auditoría Continua y una propuesta de modelos de madurez.
- Cómo implantar el enfoque de Auditoría Continua en su organización.
- Un caso práctico para afianzar el contenido teórico expuesto.
- Ejemplos de posibles herramientas que la Auditoría Continua incluye entre sus funcionalidades.

Los desafíos actuales a los que se enfrenta la actividad de Auditoría Interna acentúan la necesidad de contar con un sistema de aseguramiento de la eficacia de los sistemas de control y gestión de riesgos fiable, sostenible y continuo.

Para implantar en su organización un enfoque de Auditoría Continua, proponemos un Decálogo de Buenas Prácticas (*desarrollado en las páginas 11 a 13*).

- 1 Considere la Auditoría Continua un proyecto estratégico.
- 2 Defina desde el primer momento cómo medir la rentabilidad.
- 3 Auditoría Continua no es sinónimo de “reducción de personal”: no lo convierta en su principal objetivo.
- 4 Un simple “conjunto de consultas” no es un buen modelo de Auditoría Continua.
- 5 Ponga los cimientos: defina el modelo antes de definir los indicadores.
- 6 Involucre al departamento de tecnología cuanto antes.
- 7 Las áreas de negocio son una fuente de ideas.
- 8 Cuanto más configurable sea, mucho mejor.
- 9 Tenga cuidado con el “umbral de tolerancia”.
- 10 Su negocio no deja de evolucionar, acompáñelo con su modelo.



Introducción

Los modelos de Auditoría Continua aportan múltiples beneficios: reducen costes, incrementan la productividad, facilitan la adaptación al cambio y mejoran el entorno de control de la organización .

Entre los principales beneficios que los modelos de Auditoría Continua aportan a las organizaciones que los implantan, destacamos los siguientes:

- **Reducción de costes** de desplazamientos, incremento de productividad y optimización de los equipos de Auditoría Interna, especialmente en el caso de organizaciones con centros de negocio y operativos dispersos geográficamente (por ejemplo, bancos, compañías de seguros, cadenas de super-

mercados o franquicias comerciales, cadenas hoteleras o de restauración, ...).

- **Mayor adaptación a cambios** en la organización (nuevos negocios, productos, actividades, ...) o del entorno (novedades regulatorias) que pueden implicar nuevos riesgos.
- **Mejora del entorno de control**, porque cubren ámbitos que no atendía Auditoría Interna, al operar con una sistemática, medios y herramientas de explotación intensiva de datos.

Además de estos motivos para implantar la Auditoría Continua; también son un buen incentivo los crecientes requerimientos de consolidación y supervisión de los sistemas de Control Interno de las organizaciones.

Existen varias definiciones de Auditoría Continua. La *Guía de Auditoría de Tecnología Global sobre Auditoría Continua* del Instituto Global de Auditores Internos (GTAG 3) la define como “todo método utilizado por los auditores internos para realizar actividades relacionadas con la auditoría en forma –más– continua. Es la secuencia de actividades que

abarcan desde la evaluación continua de control hasta la evaluación continua de riesgos (todas las actividades en la secuencia control-riesgo)”.

Las similitudes entre los conceptos de Auditoría Continua y Monitorización Continua pueden llevar a confusión, pero son conceptos diferentes: la Monitorización Continua es responsabilidad directa de la Dirección en materia de Buen Gobierno y la Auditoría Continua es responsabilidad de la Dirección de Auditoría Interna, en cuanto a supervisión. Sus diferencias son:

La Monitorización Continua es responsabilidad directa de la Dirección mientras que la Auditoría Continua es responsabilidad de la Dirección Auditoría Interna.

MONITORIZACIÓN CONTINUA

PROCESO AUTOMATIZADO Y CONTINUO QUE PERMITE A LA DIRECCIÓN:

- Evaluar la efectividad de los controles e identificar incidencias asociadas a los riesgos.
- Mejorar los procesos y actividades de negocio, a la vez que se adhiere a estándares éticos y de cumplimiento.
- Tomar a tiempo más decisiones basadas en riesgos cuantitativos y cualitativos.
- Incrementar el coste-eficiencia de los controles y la supervisión a través de soluciones de TI.

La Monitorización Continua permite a la Dirección determinar de forma más rápida y acertada dónde debe prestar atención y recursos, con el objetivo de mejorar los procesos, implementar correcciones, abordar riesgos o lanzar iniciativas para mejorar la capacidad de la organización de conseguir sus objetivos.

AUDITORÍA CONTINUA

PROCESO AUTOMATIZADO Y CONTINUO QUE PERMITE A AUDITORÍA INTERNA:

- Obtener información de los procesos, transacciones y cuentas, que soporten las actividades de Auditoría Interna.
- Conseguir un cumplimiento más rápido y menos costoso de las políticas, procedimientos y regulaciones.
- Avanzar desde un modelo de revisiones cíclicas o puntuales, con un alcance limitado, hacia un modelo de revisión más continuo, amplio y proactivo.
- Evolucionar desde un Plan de Anual de Auditoría Interna estático, a uno más dinámico basado en los resultados de los análisis de la Auditoría Continua.
- Optimizar los recursos de Auditoría Interna a la vez que se incrementa la eficiencia a través de soluciones de TI.

La Auditoría Continua permite a los auditores internos determinar de forma más rápida y acertada dónde deben prestar atención y recursos, con el objetivo de gestionar más eficientemente los recursos de auditoría interna y mejorar la calidad de sus trabajos y el soporte a la Dirección.



El enfoque y el grado de la Auditoría Continua que se aplique dependerá del nivel de implementación de la Monitorización Continua.

Según la GTAG 3, la relación entre la “idoneidad de la gestión de riesgos y de supervisión de la Dirección” (Monitorización Continua) y el “alcance de las pruebas detalladas de controles y evaluaciones de riesgos de los auditores” (Auditoría Continua) es proporcionalmente inversa.

El enfoque y el grado de aplicación de la Auditoría Continua depende del grado de implementación de la Monitorización Continua a cargo de la Dirección: una Monitorización Continua activa y adecuada permite limitar el trabajo de Auditoría Interna cuando evalúa su confiabilidad y efectividad.

Por ejemplo, si la Dirección monitoriza de forma activa y adecuada las transacciones y controles de ciertos sistemas y procesos de negocio, el auditor interno no deberá aplicar el mismo nivel de actividad de Auditoría Continua. En este caso, Auditoría Interna deberá evaluar la confiabilidad y efectividad de la Monitorización Continua por parte de la Dirección, reduciendo sus pruebas de auditoría

en estos procesos y dedicando sus recursos a otras áreas de alto riesgo o no cubiertas adecuadamente por la Monitorización Continua.

Por último, incluimos –tal y como indica el Instituto Global de Auditores Internos– la definición de Aseguramiento Continuo: combinación de la Auditoría Continua y la supervisión por parte de Auditoría Interna de la Monitorización Continua del entorno de control que realiza la Dirección.

Beneficios asociados a la Auditoría Continua

Con la ejecución de pruebas continuas y eficientes, la organización puede:

- Identificar y notificar tempranamente las debilidades, para seguirlas y corregirlas inmediatamente, priorizándolas y focalizándolas en nuevos indicadores.
- Incrementar el alcance de la Auditoría Interna, con un análisis más exhaustivo de los datos y el acceso a toda la población.

- Contar con una Auditoría Interna con mayor capacidad para mitigar los riesgos.
- Reforzar el elemento disuasorio, aumentando la sensación de control.
- Reducir errores financieros y la probabilidad de fraude.
- Lograr un enfoque sostenible y un coste eficiente para las actividades de cumplimiento y evaluación del entorno de control.
- Reducir la necesidad de viajes y costes de desplazamiento.
- Mejorar la fiabilidad de la información financiera.
- Aportar más valor por parte de la Dirección de Auditoría Interna y mejorar el entendimiento de los procesos, dar mayor cobertura a sus trabajos y más agilidad al identificar y escalar incidencias.



Decálogo de Buenas Prácticas

A continuación, proponemos 10 Buenas Prácticas de Auditoría Continua, fruto de la experiencia en la implantación de estos modelos:



1 Considere la Auditoría Continua un proyecto estratégico.

Los modelos y plataformas de Auditoría Continua mejoran notablemente el control de los procesos de negocio pero son proyectos complejos, que implican un cambio estratégico. No se deje engañar por “cantos de sirena” con la promesa de que logrará buenos resultados tan solo con implementar unas nuevas herramientas. La Dirección y el Comité de Auditoría deben involucrarse, sponsorizar el proyecto, y respaldarlo con las buenas prácticas de gobierno corporativo.

Es de vital importancia gestionar el cambio correctamente, tanto en el área de Auditoría Interna como en otras funciones afectadas.

- Gestionar el impacto en el análisis de datos, Auditoría Continua y Monitorización Continua en auditores y propietarios de los procesos de negocio.
- Adoptar y respaldar la monitorización continua por parte de la dirección.
- Integrar la Auditoría Continua en la planificación de un sistema de auditoría interna orientado a riesgos.



2 Defina desde el primer momento cómo medir la rentabilidad

Este proyecto debe contar desde el principio con los recursos económicos y de tiempo necesarios para su función; por eso es imprescindible el apoyo de la Dirección, y definir claramente cuál es el retorno de la inversión: establecer de forma clara y consensuada cuáles son los objetivos y criterios de implantación

La Auditoría Continua debe considerarse un proyecto estratégico y debe contar con el respaldo e implicación de la Dirección y del Comité de Auditoría.

La Dirección es la encargada de fijar los objetivos y criterios de implantación de un proyecto de Auditoría Continua, así como de establecer un sistema de medición de dicho proceso.

que definen el proyecto de Auditoría Continua. Debemos establecer sistemas de medición que demuestren las mejoras en eficiencia y demás beneficios que se producen, mayor cobertura y fiabilidad, incremento en la sensación de control, etc..

3 Auditoría Continua no es sinónimo de “reducción de personal”: no lo convierta en su principal objetivo.

Es habitual convertir la mayor “eficiencia” de la Auditoría Continua en un argumento para reducir los recursos utilizados. La Auditoría Continua permite una mayor cobertura del universo auditable sin incrementar los recursos, pero esto no implica necesariamente una reducción de personal. Todo depende de cuán ambiciosa sea la cobertura. El “umbral de tolerancia” que fijamos para cada “indicador” determina el volumen de “ocurrencias” que el sistema nos ofrece, e influye en el volumen de personal que necesitamos para analizarlas.

Además, para impulsar un proyecto de estas características, necesitamos mantener y desarrollar las competencias técnicas de nuestro personal, poner a su alcance la tecnología necesaria y los medios para que traten y analicen los datos de los sistemas de información.

4 Un simple “conjunto de consultas” no es un buen modelo de Auditoría Continua.

Existe Auditoría Continua desde el momento en que disponemos de una serie de consultas planificadas periódicamente. Sin embargo, un buen modelo realmente se plantea como un “sistema de información” específico que crea y gestiona diferentes indicadores, y centraliza, distribuye y analiza los resultados.

5 Ponga los cimientos: defina el modelo antes de definir los indicadores.

Aunque resulte paradójico, lo último que debe preocuparnos es la relación de indicadores de un sistema de Auditoría Continua. Antes tenemos que evaluar el ámbito de actuación del sistema, el diseño conceptual de la plataforma de gestión, cómo involucramos en el proceso a las áreas tecnológicas y de negocio, los cambios en la estructura de la Dirección de Auditoría Interna que permitirán analizar y seguir los nuevos indicadores, los cambios que realizaremos en la planificación anual (incluso nos preguntamos si el calificativo “anual” sigue teniendo sentido). En definitiva, cómo cambian nuestra estrategia y programas de auditoría interna.

6 Involucre al departamento de tecnología cuanto antes.

Es fundamental la cooperación del departamento de tecnología, especialmente en la obtención de la información. Da igual si la plataforma de la Auditoría Continua es una herramienta adquirida en el mercado o una solución a medida; si la desarrolla un proveedor externo o alguien del Departamento de Auditoría Interna. Para acceder a las fuentes de información que nutren esta herramienta, nos enfrentamos a diversos retos en los que necesitamos la colaboración del departamento de tecnología por diversas razones:

- Dificultad de acceso a los datos.
- Diversidad de sistemas de información, con diferentes formatos.
- Datos incompletos, con inconsistencias en la calidad.
- Problemas para acceder a los datos por cuestiones de privacidad o seguridad.
- Sistemas en constante evolución.

Si el departamento de tecnología no realiza el debido mantenimiento, el proceso de obtención de la información se verá afectado ante posibles cambios o modificaciones que pudieran tener lugar.

7 Las áreas de negocio son una fuente de ideas.

Consulte con las áreas de negocio para definir los indicadores de su sistema de Auditoría Continua: le permitirá ajustarlos a los riesgos de la actividad diaria, le facilitará también definir y ejecutar –de forma independiente, y como respaldo– determinadas pruebas sustantivas y controles que ya realiza la organización; o argumentar la necesidad de introducir la monitorización continua en algunas áreas de negocio donde hace falta mejorar el entorno de control.

8 Cuanto más configurable sea, mucho mejor.

Habitualmente, los indicadores de un sistema de Auditoría Continua son personalizables. Por ejemplo, “Clientes de más de X años de edad que hayan sacado del cajero más de Y Euros en el último mes”. Lo que no es tan habitual es que el usuario pueda configurar otros elementos más generales, como las tipologías de pesos, rankings o marcajes, departamentos existentes, situaciones especiales o incluso las cabeceras de los diferentes informes y pantallas de la herramienta. Y es menos habitual aún, que la plataforma permita elaborar, sin necesidad de modificar su programación, los “indicadores dinámicos”, es decir, incorporar indicadores nuevos al sistema, o modificarlos seleccionando sus atributos, definiendo cómo se relacionan entre sí, o qué resultados deben generar.

Si la Dirección de Auditoría Interna es capaz de configurar todos estos aspectos a través de la auditoría continua, logra gran flexibilidad y autosuficiencia, porque no depende sistemáticamente del área de tecnología para realizar cambios.

9 Tenga cuidado con el umbral de tolerancia.

El volumen de ocurrencias de cada indicador depende del “umbral de tolerancia. Si éste es muy bajo, el departamento se colapsa ante el aluvión de resultados, si es muy alto, apenas hay ocurrencias para revisar. Defina el proceso de gestión de ocurrencias en función del número que puede gestionar por cada indicador, cambie la configuración del sistema hasta alcanzar ese volumen prefijado de forma constante, analice el umbral de tolerancia, y evalúe si es el adecuado para su organización. Si no es así, tendrá que aumentar o reducir los recursos de personal para el seguimiento de las ocurrencias.

El Director de Auditoría Interna debe garantizar que los hallazgos de la auditoría son transmitidos, recibidos y tenidos en consideración por la Dirección cuando evalúa actividades como supervisión de controles, medición de desempeño y gestión de riesgo empresarial.

10 Su negocio no deja de evolucionar, acompañelo con su modelo.

La configuración inicial del modelo de Auditoría Continua puede quedar obsoleta rápidamente ante la evolución del negocio, por eso es necesario un mantenimiento constante (nuevos indicadores, cambios en los parámetros, etcétera).

El modelo inicial de Auditoría Continua puede quedar obsoleto rápidamente ante la evolución del negocio, es necesario un mantenimiento constante.



Consejo 2320-4 sobre Aseguramiento Continuo

El Consejo 2320-4 sobre “Aseguramiento Continuo” del Marco Internacional para la Práctica Profesional de Auditoría Interna constituye una referencia clave para la Auditoría Continua.

¿Qué dice el *Marco Internacional para la Práctica Profesional de Auditoría Interna* (MIPP) sobre el Aseguramiento Continuo?

Una referencia clave para la Auditoría Continua es el *Marco Internacional*. En su Consejo 2320-4 sobre “Aseguramiento Continuo” considera que, en aquellos casos en los que el perfil de riesgo requiera de información frecuente sobre la efectividad de los sistemas de control interno, la forma más efectiva es la combinación de la “monitorización continua” de la dirección y la “auditoría continua” de Auditoría Interna. El *Marco* enfatiza el papel relevante de la tecnología y establece como clave el que se involucren otras áreas y funciones de la organización, además del apoyo de la alta dirección, aspectos que trata en el apartado “Cómo implantar un enfoque...”.

De esta forma, el *Marco* considera que:

- El Plan de Auditoría debe identificar las áreas susceptibles de un enfoque de Auditoría Continua, de acuerdo con el marco de gestión de riesgos de la organización y del proceso de evaluación de riesgos de Auditoría Interna.
- La frecuencia y el alcance de la Auditoría Continua depende del perfil de riesgo de la organización, y del nivel y naturaleza de las responsabilidades de Monitorización continua de la Dirección.
- La efectividad y la eficiencia de un modelo de Auditoría Continua deben ser evaluadas periódicamente por el auditor interno, con los cambios y ajustes que sean necesarios.



Modelo de madurez

El “modelo de madurez” es una herramienta que facilita la identificación de la situación actual y la definición de planes de acción de forma gráfica e intuitiva. Conocer el grado de madurez del modelo de Auditoría Continua es

imprescindible para establecer los posteriores objetivos, diferentes en función del punto de partida: ¿tenemos ya algún tipo de herramienta que haga las funciones que buscamos?, ¿cuál es su grado de evolución? Otro

punto importante es la madurez de la función de Auditoría Interna, los requerimientos regulatorios, las necesidades de la organización (estratégicas, operativas, etcétera) y, finalmente debemos tener en cuenta el nivel mínimo que buscamos con la Auditoría Continua.

A su vez, y con visión de largo plazo, definimos las preguntas que queremos responder con el nuevo modelo. Por ejemplo, podemos plantearnos los siguientes tipos de análisis:

- **Descriptivo:** responde a “¿qué ha pasado o qué pasa ahora mismo, y compara con tendencias/patrones históricos?”
- **Diagnóstico:** responde a “¿por qué ha pasado esto?”
- **Predictivo:** responde a ¿qué pasará?, ¿qué es lo más probable?
- **Prescriptivo:** responde a ¿cuál es la acción recomendada?

En estos momentos, las organizaciones con sistema de Auditoría Continua se centran en los dos primeros tipos de análisis. El siguiente cuadro es una guía para determinar en qué nivel de madurez se encuentra nuestro modelo de Auditoría Continua.

BÁSICO	<ul style="list-style-type: none"> - El uso de herramientas: se lleva a cabo ocasionalmente en el mejor de los casos. - No existe un enfoque analítico, procedimientos o metodología. - Auditoría Interna no dispone de herramientas específicas. - Se depende de un número pequeño de personas con habilidades en el uso de herramientas informáticas, que se usan en menos de un 10% de los proyectos de Auditoría Interna.
EVOLUTIVO	<ul style="list-style-type: none"> - Utilizadas para, al menos, el 25% de los proyectos de Auditoría Interna. - Reconocido como generador de valor para los proyectos de Auditoría Interna para la elección de muestras y pruebas. - No institucionalizado. - Recae en grupo central o en un individuo. - Hay herramientas, pero se emplean de manera no consistente o de manera errónea.
ESTABLECIDO	<ul style="list-style-type: none"> - Utilizadas en, al menos, el 50% del ciclo de vida de auditorías. - Existencia de políticas y metodología de uso de herramientas. - Uso de herramientas promovido por la Dirección. - Se analizan los resultados ofrecidos por las herramientas. - Comprensión del negocio a partir de los procedimientos y resultados de los análisis.
AVANZADO	<ul style="list-style-type: none"> - La metodología está institucionalizada y es usada en, al menos, el 75% de los proyectos de Auditoría Interna incluyendo el impacto derivado de las incidencias detectadas. - La Dirección se involucra en los esfuerzos de la auditoría continua y estimula su uso. - La Dirección utiliza la información derivada del uso de herramientas. - Rediseño de los procedimientos de análisis. - Las herramientas son usadas para la optimización de recursos de Auditoría Interna.
LIDERAZGO	<ul style="list-style-type: none"> - Las prácticas desarrolladas en niveles básicos que han evolucionado hasta los avanzados se utilizan para mejorar continuamente los procesos, procedimientos y resultados de los análisis. - Los sistemas de monitorización continua son utilizados activamente por la Dirección y los propietarios de los procesos, y la Auditoría Continua permite evaluar la eficacia de dichos sistemas de forma continua. - Auditoría Interna es capaz de ofrecer aseguramiento continuo sobre la gestión de riesgos de la organización. - Innovación en nuevas técnicas de Auditoría Continua (ej. minería de datos, big data, modelos predictivos, etc.)



Cómo implantar un enfoque de Auditoría Continua en nuestra organización

En el comienzo de un proyecto de Auditoría Continua se deben fijar los objetivos del mismo y la estrategia de desarrollo de indicadores para optimizar tiempos y costes.

ARRANQUE DEL PROYECTO

La definición de los objetivos influye en el desarrollo del proyecto. Así, puede ocurrir que el proyecto:

- **Persiga únicamente alcanzar un estadio “básico” o, como mucho, “evolutivo”.** Es decir, generar o acceder directamente a información y datos para su explotación por parte del área de Auditoría Interna con los medios y herramientas disponibles.
- **Pretenda dar un paso adicional** que mejore su nivel de madurez con la utilización de sistemas y herramientas de tratamiento automatizado de esa información y genere alertas y ocurrencias para Auditoría Interna.
- **Acometa las dos fases anteriores de forma escalonada en el tiempo.**

En el estudio inicial, debemos fijar la estrategia de desarrollo de los indicadores de Auditoría Continua según el nivel de cobertura que hayamos definido, con el objetivo de generar un modelo completo. Acertar en esta elección será relevante en tiempo y costes.

Los indicadores pueden ser:

- **Fijos:** El área de Auditoría Interna define los indicadores y, normalmente, el departamento de Tecnología (o un proveedor exter-

no) los programa en la plataforma. Su inconveniente es que cuando se requieren nuevos indicadores, este sistema resta operatividad y ralentiza la adaptación a nuevos riesgos.

- **Dinámicos:** No es necesario modificar la programación de la plataforma para incorporar un indicador nuevo, sino que éste se incluye mediante la selección y combinación de campos de información a través de menús u otras funcionalidades similares. Esta alternativa permite indicadores ilimitados, da autonomía e independencia a la función de Auditoría Interna, a la gestión de los indicadores y permite una rápida respuesta ante los nuevos riesgos; pero, como contrapartida, obliga a invertir más en el diseño y desarrollo inicial de la plataforma.

En ocasiones, se elige un enfoque mixto: con indicadores fijos y un contenido mínimo, a los que se incorpora un módulo con el que el área de Auditoría Interna puede añadir indicadores dinámicos cuando el negocio o los riesgos lo requieran.

Impactos en la Organización

Un modelo de Auditoría Continua impacta directamente en el Entorno de Control de la Or-





ganización, y afecta a las tres líneas de defensa que configuran su Sistema de Control Interno.

En relación al **MODELO DE LAS TRES LÍNEAS DE DEFENSA**, recomendamos la lectura de la Guía del Instituto de Auditores Internos de España *Marco de relaciones de auditoría interna con otras funciones de aseguramiento: guía práctica*, publicada en 2013 dentro del marco de LA FÁBRICA DE PENSAMIENTO.

Primera línea de defensa:

- El principal objetivo de un modelo de Auditoría Continua es recorrer los procesos que la organización considera claves y establecer criterios de seguimiento sobre los riesgos previamente definidos.
- Los departamentos responsables de los procesos cubiertos por Auditoría Continua participan en el seguimiento de las excepciones y en la identificación de sus causas.

Segunda línea de defensa:

- Un modelo de Auditoría Continua proporciona indicadores de contraste frente a los implementados por esta segunda línea, o

nuevos indicadores para la misma. Por ejemplo, a las funciones de Cumplimiento y Defensa Penal puede aportarles indicadores que permitan validar el grado de desempeño de una normativa o establezcan alertas sobre posibles incumplimientos.

- Conviene convertir la segunda línea de defensa en parte del alcance del modelo de Auditoría Continua.
- La segunda línea da soporte a los gestores de Auditoría Continua en el análisis de las causas de las excepciones.

Tercera línea de defensa:

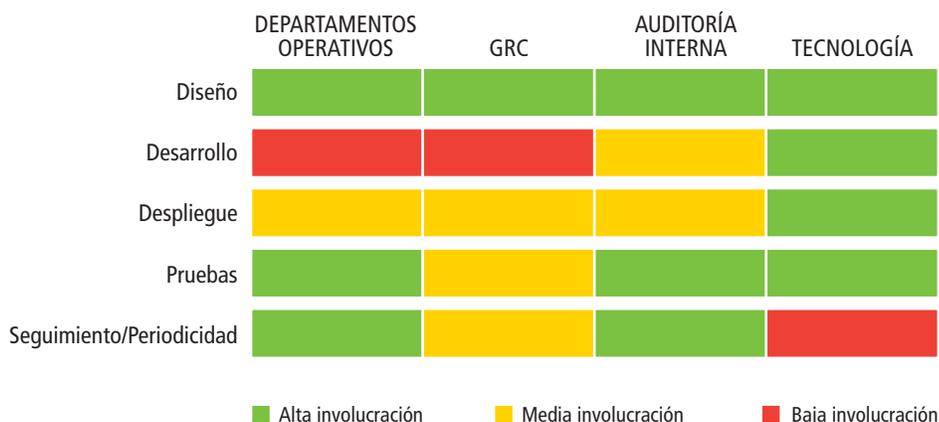
- El sistema de Auditoría Continua permite realizar al área de Auditoría Interna una reevaluación continua de los principales riesgos, gestionar de forma dinámica el Plan Anual de Auditoría Interna y planificar y ejecutar determinados trabajos.

ALINEAMIENTO CON EL ENFOQUE GRC (GOBIERNO, RIESGO Y CUMPLIMIENTO) DE LA ORGANIZACIÓN

Los requerimientos formales referidos a la Gestión de Riesgos Corporativos (ERM) o Sis-

Un modelo de Auditoría Continua afecta directamente al Entorno de Control de la Organización e impacta en las tres líneas de defensa que constituyen su Sistema de Control Interno.

Es esencial integrar el modelo de Auditoría Continua dentro del marco de Gobierno, Riesgo y Cumplimiento de la organización.



temas de Control Interno de Elaboración de Información Financiera (SCIIF) varían significativamente dependiendo del sector de actividad y de aspectos como la cotización del capital o la deuda. Estos aspectos pueden requerir indicadores específicos en un proyecto de Auditoría Continua. Son indicadores que miden el ratio de eficacia o cumplimiento de aspectos como SCIIF, prevención de blanqueo de capitales, cumplimiento específico de normativa, refuerzo de los sistemas de defensa penal, etc.

También pueden incluirse determinados indicadores en los Sistemas de ERM que detectan el grado de cumplimiento de controles mitigantes o la posible alerta sobre riesgos.

Es fundamental integrar el modelo de Auditoría Continua dentro del marco GRC de la organización.

POSIBLE GRADO DE INVOLUCRACIÓN

En un proyecto de este tipo, las diferentes áreas involucradas participan en mayor o menor medida en cada una de las fases. En la matriz destacamos, para cada una de las fa-

ses de implantación, un ejemplo teórico del posible grado de implicación.

Costes y presupuesto

El coste de un proyecto de este tipo depende de varios factores:

- Los objetivos y la cobertura del proyecto.
- El modelo de desarrollo de los indicadores (fijos o dinámicos).
- La posible contratación de recursos externos.
- Las herramientas externas o internas, etcétera.

Es recomendable plantear la posibilidad de establecer fases dentro del proyecto, y definir claramente los recursos destinados a cada una, para medir los hitos en base a las necesidades del área Auditoría Interna. Al considerar los costes de un proyecto de Auditoría Continua, se debe tener en cuenta, más allá de su implementación inicial, el coste de la operación, mantenimiento y expansión del sistema.



Presentación del proyecto a la Dirección

La Auditoría Continua es un nuevo paso frente a las técnicas de control tradicionales. Las organizaciones evolucionan, los riesgos varían y la Dirección de Auditoría Interna quiere dar respuestas rápidas y fiables. Estas medidas aseguran que los “riesgos posibles” están controlados. El modelo de Auditoría Continua compromete a todas las áreas, tanto a Sistemas de la Información como a las áreas implicadas en el seguimiento. Es un proyecto transversal que afecta a todas las áreas auditadas, con las que se fijan los riesgos de cada actividad.

Para lograr el apoyo de la Dirección, se puede plantear un proyecto piloto, con un número reducido de indicadores –en caso de que se opte por dinámicos, es mejor limitar el número de campos disponibles– pero con una arquitectura que posteriormente sea compatible y escalable al modelo completo.

DISEÑO DE LA PLATAFORMA

Arquitectura o planificación inicial

Se deben considerar los siguientes pasos:

1. IDENTIFICAR REQUERIMIENTOS.

La Dirección de Auditoría Interna elabora una solicitud en la que explica el objetivo del sistema, de acuerdo con los afectados o “usuarios” del proyecto. Conviene estimar de forma preliminar aspectos como el volumen de datos o las áreas a las que se dirigen las ocurrencias.

2. DETERMINAR LAS CARACTERÍSTICAS BÁSICAS DE LA PLATAFORMA.

Los modelos de Auditoría Continua pueden orientar a la Dirección de Auditoría Interna en la configuración de los Planes de Auditoría ya que, entre otras cosas, impactan significativamente en sus programas de trabajo, permiten identificar información suficiente, fiable, relevante y útil, para evaluar los riesgos relevantes, localizan las probabilidades de que se produzcan errores, fraude o incumplimientos y facilitan a los auditores internos la evaluación del gobierno, la gestión de riesgos y los controles en la unidad auditada.

Para alcanzar estos objetivos, tenga en cuenta los siguientes criterios:

1. Es una **herramienta transversal** que abarca todas las Áreas de la organización susceptibles de formar parte de los Planes de Auditoría Interna.
2. Se implanta con **propósito de permanencia** y con capacidad de adaptarse a los nuevos procesos y factores de riesgo que surjan.
3. Su arquitectura es suficientemente versátil mediante el uso de **tecnologías escalables**, ágiles y flexibles, que no obliguen a acudir a nuevos desarrollos informáticos. En caso contrario, existe el riesgo de hacer el proyecto inviable a medio y largo plazo.
4. Debe **involucrar a todas las áreas** implicadas en las funciones de monitorización continua como complemento a Auditoría Interna. Así se pueden justificar o solucionar las ocurrencias que se pongan de manifiesto.

La creación de un proyecto piloto de Auditoría Continua puede constituir un instrumento eficaz a la hora de lograr el apoyo de la Dirección.

Algunos de los requisitos de una plataforma de Auditoría Continua son la transversalidad, la versatilidad, su estabilidad, su naturaleza colaborativa o su posible parametrización.

5. Se recomienda el uso de **sistemas colaborativos** que aumentan la conexión entre los usuarios afectados por los indicadores y permiten conocer las deficiencias y establecer mejoras. Esta interconexión configura un sistema de seguimiento continuo en los procesos de la organización.
6. Esto significa que se permite el acceso a cualquier usuario que determinen las Unidades de Auditoría Interna, mediante un **sistema de permisos** que los discrimina en función de los procedimientos de protección de datos y seguridad.
7. La complejidad y cantidad de variables que gestionan los Sistemas de Auditoría Continua, obligan a simplificar el sistema de configuración e inclusión de nuevos indicadores. En caso contrario, la complejidad del seguimiento afecta a su gestión. Hay que generar criterios que discriminen entre **indicadores** para otorgarles pesos relativos y permitan el recálculo automático.
8. El sistema es más potente y flexible cuanto más **parametrizable** es su diseño. Por ello, además de los pesos, hay que establecer parámetros para todos los aspectos relacionados con un indicador (valores que generan ocurrencia, periodicidad de ejecución, importancia...).
9. Cuanto mayores son las áreas afectadas, más elevado es el número de indicadores gestionados y, por tanto, más complicado su seguimiento. Se facilita la gestión con la creación de un **cuadro de mando**: una visión rápida e intuitiva de las principales áreas y conceptos de riesgo, una panorámica con las principales variables, un esquema de las áreas revisadas y las conclusiones y sugerencias. El cuadro de mando puede basarse en valores de alerta u objetivos, y el peso relativo de cada indicador. También puede incluir herramientas de seguimiento, como gráficos, y la **posibilidad de bajar al máximo nivel posible** hasta el dato concreto en aquellas variables que se consideren.
10. Los **datos** deben estar **actualizados**, a ser posible diariamente. Sirve un sistema que acumule 11 meses e incorpore la información del día en el mes en curso. No obstante, las escasas variaciones intradía y el esfuerzo tecnológico que requiere, aconseja actualizaciones con plazos superiores, que no deben exceder el mes. También debe considerarse la generación de información en periodos de doce meses, en lugar de las referidas al ejercicio vigente, para evitar la estacionalidad de determinados meses junto con la posibilidad de falsos positivos cuando el número de meses es reducido.
11. Establecer un proceso que garantiza la **calidad de los datos**, mediante el acceso a las bases de datos principales de la Organización o a una réplica de las mismas. Es positivo revisar periódicamente los datos para evitar desajustes ante cambios organizativos o de producto.
12. Los sistemas de Auditoría Continua sirven a otras áreas en el seguimiento de indicadores que les atañen. Por tanto, se necesitan **sistemas de reporting** que identifiquen el trabajo realizado y permitan seguir las conclusiones y sugerencias.

3. DEFINIR POSIBLES MÓDULOS QUE DEBEN INCORPORARSE

La Auditoría Continua es un sistema de múltiples consultas en el que participan muchas áreas de la Organización, por eso dicho sistema necesita un elevado nivel de seguimiento para gestionar y centralizar los diferentes indicadores y distribuir y analizar adecuadamente los resultados. Es una herramienta compleja que debe disponer de una serie de módulos que faciliten su manejo para:

- **Extracción.** Proporciona a la plataforma la información necesaria.
 - **Cálculo.** Ejecuta los diferentes indicadores definidos en la plataforma.
 - **Gestión de Usuarios.** Define los usuarios con acceso a la aplicación, administración de perfiles (administrador, usuario,...), indicador de las transacciones y operaciones a las que tienen acceso. También establece equipos de trabajo y demás operativas que afectan al área de Auditoría Interna.
 - **Parámetros Generales.** Cuantos más parámetros se establezcan, mayor independencia y flexibilidad tiene el área de Auditoría Interna para diseñar su modelo de Auditoría Continua.
- Entre los posibles aspectos parametrizables se encuentran:
- Marcas sobre cada indicador analizado, con algún tipo de clasificación sobre los resultados de su revisión (por ejemplo, incidencia a seguir, falso positivo, etcétera).
 - Pesos asignados a cada indicador en función de su relevancia en el proceso.
 - Periodicidad: frecuencia de ejecución establecida para cada indicador (diaria, semanal, quincenal, una fecha concreta...).
 - Mensajes tipo: definición de textos utilizados como plantilla en los mensajes y comunicaciones enviados a las unidades auditadas.
 - Modelos de reporting: plantillas de diferentes tipos de informes y resultados proporcionados por la plataforma y la revisión.
- **Creación de Indicadores.** Este módulo permite diseñar los indicadores de la plataforma. La versatilidad del modelo depende de si los indicadores son *fijos* (programados "a medida" directamente en la plataforma) o *dinámicos* (configurables sin necesidad de cambios en la programación de la plataforma). Sean fijos o dinámicos, debe ser posible definir, como mínimo, los parámetros –importes, porcentajes, fechas, etcétera– utilizados en el indicador, e incluso su peso específico, seleccionado a partir de la tipología de pesos configurada anteriormente al determinar las características básicas de la plataforma.
 - **Consultas.** Permite analizar los resultados a través de los indicadores.
 - **Agenda.** Módulo donde se asignan las tareas a los integrantes del área de Auditoría Interna. Por ejemplo, cada auditor o equipo tendrá asignadas automáticamente y por defecto una determinada tipología de ocurrencias. También debe ser posible la asignación específica o puntual de las mismas.
 - **Simulación.** Pruebas con diferentes parámetros asociados a los indicadores para

Un sistema de Auditoría Continua es una herramienta compleja que debe disponer de módulos que faciliten su utilización.

Establecer si los datos que analizan los indicadores se consultan directamente de las bases de datos de las aplicaciones ya existentes o si se crea un repositorio específico, es un aspecto clave a la hora de diseñar una plataforma de Auditoría Continua.

analizar su impacto, sin necesidad de modificar la configuración existente o afectar a los históricos anteriores.

- **Comunicación.** Módulo de comunicación con una unidad auditada mediante el envío de mensajes automáticos. Pueden definirse determinados mensajes para ser enviados de forma automática cuando se materializa un determinado tipo de ocurrencia. Conviene que el módulo controle aspectos como qué mensajes reciben respuesta y cuáles no, su repetición automática si no se recibe contestación, etc.
- **Ratings y Rankings.** Definir ratings alineando la puntuación de un área en función de ciertas puntuaciones establecidas por el administrador de la herramienta, y rankings entre varias unidades análogas incluidas en el proceso de Auditoría Continua.
- **Otros posibles módulos.** Por ejemplo, el de análisis histórico de ocurrencias, el de creación y gestión de diferentes versiones de parametrización de la plataforma, o un gráfico para medir la evolución de uno o varios indicadores, etc.

4. OBTENER LA INFORMACIÓN: ¿ACCESO DIRECTO A APLICACIONES O A REPOSITARIOS?

Es necesario determinar si los datos que analizan los indicadores se consultan directamente de las bases de datos de las aplicaciones ya existentes o si se debe crear un repositorio específico. De ambas decisiones se derivan beneficios:

Del acceso directo a las bases de datos existentes.

- Se reduce el riesgo de fallos de integridad de la información y el uso de información no actualizada.

- No se duplica la información y se genera un ahorro en almacenamiento.
- El tiempo de ejecución es más rápido al no ser necesaria la extracción y consolidación de la información.

De un repositorio específico.

- Facilita la generación de información histórica.
- Minimiza el impacto en el rendimiento de las aplicaciones de negocio (especialmente para datos con actualización instantánea).
- El modelo de datos es más sencillo de diseñar y adaptar a las necesidades del área de Auditoría Interna.
- Independiza el diseño de la plataforma del diseño de las aplicaciones.
- Es más fácil de mantener en caso de que la estructura de la información de las aplicaciones varíe.
- Es más sencillo implantar una plataforma de indicadores dinámicos.

5. DETERMINAR LA PERIODICIDAD DE ACTUALIZACIÓN DE LOS RESULTADOS

Es necesario decidir si se quieren los resultados de forma instantánea, *on line*, o con determinada periodicidad: diaria, semanal, mensual, etc. Existen argumentos a favor de ambos:

De la actualización instantánea, *on line*.

- La información necesaria para evaluar los indicadores está permanentemente actualizada. Este enfoque no permite el uso de repositorios, salvo que se actualicen en tiempo real.

- Esta frecuencia permite identificar un incidente nada más producirse, lo que es muy útil en indicadores críticos.

De la actualización periódica.

- Los procesos de ejecución de indicadores pueden retrasarse a los momentos en que los sistemas tienen menos trabajo y así impactar menos en su rendimiento.
- Podemos graduar la antigüedad de la información analizada y el momento en que se ejecuta cada indicador según su importancia. Por ejemplo, puede establecerse que los indicadores críticos se ejecuten una vez al día con información que se actualiza cada noche.
- La implementación y gestión del sistema es más sencilla.
- Normalmente, el coste de actualización instantánea es superior y puede no justificar la necesidad que pueda tener el área de Auditoría Interna de disponer *on line* de información sobre una determinada ocurrencia.

6. DEFINIR EL DISEÑO TÉCNICO

Una vez determinadas las características del desarrollo informático, se prepara la información para desarrollar una guía detallada, *Diseño Técnico*, del sistema. El documento lo elaboran las áreas de desarrollo del Departamento de Tecnología e incluye aspectos tales como:

- Entorno físico del sistema: hardware, comunicaciones, instalaciones, etc.
- Diseño técnico: componentes o subsistemas, interfaces con otros módulos o con otros sistemas, requerimientos de seguridad, concurrencia de usuarios y procesamiento en tiempo real.

- Diseño detallado de componentes del sistema: lógica de proceso, pantallas e informes.
- Diseño de bases de datos o ficheros: tablas, vistas, etc.

Definición de indicadores iniciales, sus parámetros y pesos

Durante el proceso del diseño del modelo hay que decidir si los indicadores son dinámicos o fijos, así como su periodicidad de actualización de los resultados. Estas decisiones condicionan el tipo de herramienta, las interconexiones con otros sistemas, el coste y el plazo de entrega.

Durante el diseño y el programa piloto de implantación del modelo de Auditoría Continua, es conveniente que el área de Auditoría Interna realice un estudio basado en los siguientes pasos:

1. Identificar los procesos objeto de análisis.
 2. Si la organización tiene identificados y mapeados esos procesos, obtener el detalle de subprocesos.
 3. Revisar las áreas que afectan a dichos procesos y mapear las fases de los mismos si la organización no los tenía identificados.
- Realizar una primera aproximación a los indicadores que identifican los riesgos o permiten evaluar los controles que afectan a dichas áreas.
 - Comentar los resultados con los responsables y pedir información sobre las causas que provocan falsos positivos.
 - Preguntar por nuevos indicadores.

En la fase de diseño del sistema debe decidirse si los indicadores son dinámicos o fijos, así como su periodicidad de actualización de resultados.

La selección e implantación de las herramientas tecnológicas adecuadas así como su utilización efectiva es elemento clave en el éxito de un modelo de Auditoría Continua.

- Agrupar los indicadores en un cuadro de mando ordenado por procesos.
- Comprobar que la información obtenida es consistente con la información gestionada por los distintos departamentos.

¿Herramienta de mercado o desarrollo interno?

El éxito de un modelo de Auditoría Continua depende, en gran medida, de la selección e implantación (o desarrollo) de las herramientas tecnológicas adecuadas y de su utilización efectiva. Las organizaciones deben evaluar, por tanto, las características y funcionalidades de las herramientas que se adecúen a sus necesidades: coste de implantación, explotación y mantenimiento, agilidad y flexibilidad para adecuarse a cambios organizativos, a distintos los procesos o a los riesgos e indicadores que se monitoricen.

Existe un abanico de soluciones –basadas en herramientas para tratamiento masivo de la información– que sirven de soporte a la Auditoría Continua y que facilitan la interconexión de sistemas:

- Herramientas ofimáticas. Hojas de cálculo o bases de datos, por ejemplo.
- Herramientas estándar de auditoría, herramientas CAATT, *Computer Assisted Audit Tools and Techniques*.
- Procedimientos convencionales de presentación de información. Por ejemplo, de un sistema ERP.
- *Business intelligence*: cuadros de mando, informes, etc.
- Herramientas con módulos específicos de Auditoría o Monitorización Continua –herramientas de tipo GRC.

Tanto si se decide por el desarrollo interno como si se adquiere una solución pre-parametrizada, hay que adaptar esas herramientas a los requisitos definidos en el modelo de trabajo de Auditoría Continua. En el proceso de selección, debe estudiarse la existencia de herramientas similares en la propia organización, que exploten el almacén de datos o que ya utilicen otras áreas para su trabajo. Adaptarlas mejorará el retorno de la inversión.

Ventajas de una herramienta comercial versus una herramienta de desarrollo interno

- Menor riesgo de incidencias durante el desarrollo –desviaciones en tiempo o coste, funcionalidades no implementadas de forma completa, etc.
- Productos probados.
- Puesta en marcha en menor tiempo.

Inconvenientes

- Puede no facilitar todas las funcionalidades que proporciona un desarrollo a medida o no adaptarse a las necesidades específicas de la organización y sus procesos.
- Dependencia externa.

De cualquier forma, en cualquier desarrollo interno o adaptación hay que considerar su posterior administración –desde el área de Auditoría Interna, en la medida de lo posible– y los futuros cambios, bien en el alcance del proyecto o por cambios en la organización.

DESARROLLO

Identificar los atributos de la información que se recopila

Para desarrollar los indicadores, es necesario analizar la fuente de los datos y sus atributos, así se podrá calificar adecuadamente la información y facilitar su gestión.





En dicho proceso se debe considerar:

- Las distintas fuentes de obtención de datos con los que calculamos los indicadores.
- El uso de información externa a la organización, sobre todo al comparar datos y valorar posibles alertas.
- La validación de los datos obtenidos.
- La posible existencia de falsos positivos como consecuencia de comparaciones no homogéneas entre datos obtenidos de fuentes diversas.
- Que los indicadores incluyan información suficiente para su correcto estudio.

Además de estos puntos, es necesario documentar adecuadamente todos los indicadores, sus fórmulas de cálculo, los datos que los integran y sus características.

Desarrollo de la plataforma / Adaptación de la herramienta de mercado

En base al análisis funcional y diseño técnico, hay que definir y aprobar un plan de implantación / ejecución del proyecto, que incluya:

- La definición de objetivos.
- La asignación de responsabilidades.
- Las necesidades de personal / equipos / licencias / espacio físico / comunicaciones.
- La metodología de desarrollo e implantación.
- El calendario
- Las actividades de seguimiento y reporte.

Algunas de las cuestiones clave a tener en cuenta en esta fase son:

- El seguimiento frecuente para el control de desvíos en tiempo y coste.
- El uso de prototipos –demostraciones– y contraste frecuente con usuarios finales.
- Se debe detallar y documentar incidencias que supongan un riesgo sobre los objetivos del proyecto en tiempo, forma y coste, indicando las soluciones adoptadas e informando a la Dirección.

Conexión con las aplicaciones / repositorios

La conexión con las fuentes de información depende del modelo elegido:

- **En los casos de acceso a la información mediante un repositorio**, hay que definir:
 - Los requerimientos de información (tablas, campos y formato esperado).
 - La periodicidad de carga de la información.
 - El tiempo de retención de la información.
 - Si los datos se añaden o sustituyen a los existentes.
 - Definición de responsable de la carga de la información.
 - Definición de información necesaria para realizar validaciones (por ejemplo, número de registros y totales sobre campos de importe).
- **Si el acceso es directo** a las aplicaciones, debemos acordar cómo se advierte al área

Análisis funcional y diseño técnico son los principales aspectos a tener en consideración a la hora de decidir y aprobar un plan de implantación de un proyecto de Auditoría Continua.

En análisis de la conexión con otras herramientas existentes, la gestión de incidencias y la realización de pruebas son cuestiones relevantes en el desarrollo de un sistema de Auditoría Continua.

de Auditoría Interna de las posibles incidencias en la información fuente.

El modo de acceso puede implementarse a bajo nivel, con conectores de bases de datos; o a alto nivel, con herramientas o aplicaciones específicas. En cualquier caso, se debe tener en cuenta:

- El impacto de la carga sobre los procesos de la compañía, especialmente si se usa repositorio.
- Problemas en la operativa, problemas de seguridad, etc.
- Velocidad del proceso de carga, que impacta en la ejecución posterior de los indicadores.
- Disponibilidad de la información, con la garantía de que toda la población auditada se encuentra actualizada en la fuente.
- Mecanismos para la gestión y reporte de incidencias en la carga.

Conexión con otras herramientas similares ya existentes

La conexión puede ser:

- **Saliente:** La herramienta nutre a aplicaciones externas como, por ejemplo, herramientas de seguimiento de controles (GRC, mapa de riesgos, etc.).
- **Entrante:** Otras herramientas similares nutren a la plataforma de Auditoría Continua, aportando información útil, por ejemplo, para algún indicador.

Cuando la herramienta nutre a otras aplicaciones hay que definir un procedimiento de exportación de información adecuado, que incluya un responsable, la definición de datos que se reportan, la periodicidad y las validaciones de integridad.

Gestión de incidencias

Las incidencias más habituales en este tipo de proyectos son:

- **Desviaciones en tiempo y coste.** Estos proyectos suele comenzar con una definición sencilla, que se complica conforme los indicadores evolucionan. El área de Auditoría Interna, como responsable del proyecto, define el nivel de complejidad de cada indicador, teniendo en cuenta que un buen diseño inicial evita sobrecostes, retrasos, y garantiza que la herramienta cumple las expectativas.
- **Lentitud de proceso,** originada por las tablas origen de la información y los procesos de conexión. El proceso de análisis de los indicadores puede, en ocasiones, requerir la extracción de bases de cierto tamaño, o consultas “pesadas” con un alto volumen de información. Por ello, es básico que se configure adecuadamente la forma de extracción y el formato del detalle generado. Es recomendable definir específicamente cada indicador, acotando la población de datos siempre que se pueda, por tiempo, por geografía, por unidad dentro de la organización, etc.

Pruebas

La fase de pruebas del desarrollo, que se integran en el proceso habitual de desarrollo establecido en la organización, se divide en:

- **Pruebas técnicas** para validar la integridad y coherencia del proceso. Son comunes en cualquier desarrollo técnico. Incluyen pruebas unitarias, pruebas completas de un indicador, pruebas de convivencia de los nue-

vos indicadores con el resto de sistemas, pruebas de velocidad de proceso de información en función de la información fuente, etcétera.

- **Pruebas de usuario o concepto**, que tienen por objetivo validar los resultados obtenidos. En la fase de diseño las define el área de Auditoría Interna. Las más habituales son:
 - *Formato de la información*: validar el formato de los campos del indicador como, por ejemplo, fechas o importes.
 - *Totalidad de la información*: validar que los resultados que contienen información sobre la población esperada, todas las zonas geográficas analizadas, todas las unidades de negocio analizadas, etcétera.
 - *Coherencia contable*: comprobar si la información se corresponde con los datos disponibles en los Estados Financieros u otras fuentes conciliadas contablemente.
 - *Coherencia*: validar que los datos obtenidos son conceptualmente coherentes, como por ejemplo, facturas vencidas que todavía no han sido emitidas.
 - *Coherencia entre indicadores*: validar que la población de los distintos indicadores es homogénea. Por ejemplo, el número de facturas pendientes de cobro en un determinado día debe ser la misma para todos los indicadores que utilicen esta información.
 - *Pruebas sobre el indicador en sí mismo*: verificar la utilidad de los datos obtenidos, percepción de rendimiento por parte del usuario, etcétera.
 - *Resultados*: validar que el objetivo del indicador se ha cumplido.

Estas pruebas ayudan a mejorar el diseño del indicador, ajustándolo y reduciendo el número de falsos positivos.

DESPLIEGUE

Implantación

Siempre que el proyecto se presente a la Dirección de forma adecuada y se diseñe en una plataforma apropiada, su implantación no tiene por qué ser complicada. El principal obstáculo es el limitado conocimiento de la nueva herramienta que tiene la organización. Hace falta formación impartida por el área de Auditoría Interna.

La Auditoría Continua se implementa por módulos, según una planificación inicial y, a partir de pruebas piloto, es recomendable chequear a las unidades de negocio y, una vez validado el éxito, extender su alcance. Comprobado el correcto funcionamiento de la plataforma, se realizan los necesarios ajustes en la parametrización y pesos de los indicadores. Ajustes que se repetirán periódicamente para adaptarlos a la dinámica de la organización y sus procesos. Las revisiones permiten ajustar paulatinamente la herramienta y detectar y reducir las incidencias.

Comunicación a la organización

La Dirección y las áreas afectadas por los análisis deben considerar la Auditoría Continua como una herramienta de mejora del aseguramiento de la organización. Para el área de Auditoría Interna esta actividad es la evolución natural de su trabajo, de la misma forma que evolucionó desde la Auditoría Interna de cumplimiento, o tradicional, hasta un

Uno de los principales obstáculos en la implantación de un sistema de Auditoría Continua es el limitado conocimiento existente en la organización acerca de la nueva herramienta.

La puesta en marcha de una herramienta de Auditoría Continua requiere de un proceso de formación y comunicación adecuados, tanto para los miembros de Auditoría Interna como para los de los departamentos afectados por los objetivos y desempeño de sus sistemas.

trabajo basado en el análisis de riesgos. Ahora es posible avanzar hacia la Auditoría Continua. Y así debe transmitirlo.

Conviene estudiar detenidamente cómo se presentan los resultados finales de los trabajos de Auditoría Continua. Los informes periódicos deben tener una presentación “amigable” y deben centrarse sólo en los aspectos realmente relevantes, incorporando únicamente los indicadores que afecten significativamente a una actividad.

El reporting debe procurar, además, no invadir nunca las competencias de otras áreas de la organización (por ejemplo, Control de Gestión), debe enfocar sus contenidos dentro de los de la tercera línea de defensa y evitar que se considere a Auditoría Continua simplemente como una actividad complementaria de los análisis propios de otras áreas.

El lanzamiento de la plataforma de Auditoría Continua conlleva un proceso de formación y comunicación, tanto para los integrantes de la Dirección de Auditoría Interna como los de las áreas afectadas por los objetivos y desempeño de sus Sistemas.

Análisis de la situación tras el despliegue

Finalizado el proceso de despliegue del Sistema de Auditoría Continua, conviene analizar si se han conseguido los objetivos marcados y plantearse el cumplimiento de factores de éxito y fracaso para mantener vivo el impulso inicial y adelantarse a los posibles problemas.

La siguiente tabla resume la lista de desafíos y sus causas, y los factores de éxito en la implantación de un Sistema de Auditoría Continua.

RIESGO: FALLO EN LA ADOPCIÓN O APLICACIÓN DE MEJORAS

FACTORES DE FRACASO

- Soluciones demasiado complejas o poco prácticas.
- Soluciones desarrolladas en forma aislada por consultores o por un equipo externo.
- Mejores prácticas copiadas, pero no ajustadas para satisfacer la operación de la empresa.
- Soluciones no “asumidas” por los propietarios del proceso/equipo.
- Organización sin roles y responsabilidades claros.
- Gerencia que no demanda ni respalda el cambio.
- Resistencia al cambio.
- Pobre comprensión de la manera en que deben aplicarse los nuevos procesos o herramientas que han sido desarrollados.
- Habilidades y perfiles no coincidentes con los requerimientos del rol.

FACTORES DE ÉXITO

- Enfocarse en ganancias rápidas (quick wins) y proyectos manejables.
- Realizar pequeñas mejoras para probar el enfoque y asegurarse que funciona.
- Involucrar a los propietarios de los procesos y a otros terceros interesados en el desarrollo de la mejora.
- Asegurarse de que los roles y responsabilidades son claras y aceptadas, cambiando las descripciones de los roles y perfiles, si es necesario.
- Llevar la mejora desde la gerencia hacia abajo y a través de toda la empresa.
- Aplicar una formación adecuada, cuando sea necesario.
- Desarrollar los procesos antes de intentar automatizarlos.
- Reorganizar, si es necesario, para habilitar una mejor apropiación de los procesos.
- Hacer coincidir los roles (específicamente aquellos que son claves para el éxito) con las capacidades y características individuales.



RIESGO: DIFICULTAD PARA MOSTRAR O MEDIR BENEFICIOS

FACTORES DE FRACASO

- Metas y métricas no establecidas o sin funcionar efectivamente.
- Seguimiento de beneficios no aplicados después de la implementación.
- Pérdida de foco en los beneficios y el valor que se obtendrá.
- Pobre comunicación de los éxitos.

FACTORES DE ÉXITO

- Establecer metas claras, medibles y realistas (resultado esperable de la mejora).
- Establecer métricas prácticas de rendimiento (para monitorizar si la mejora está llevando al logro de las metas).
- Producir cuadros de mando que muestren la manera en que se mide el desempeño.
- Comunicar en términos del impacto en el negocio, los resultados y beneficios que se están obteniendo.
- Implementar ganancias rápidas (quick wins) y entregar soluciones en escalas de tiempo breves.

RIESGO: PÉRDIDA DE INTERÉS O MOMENTO

FACTORES DE FRACASO

- La mejora continua no es parte de la cultura.
- Gestión que no produce resultados sostenidos.
- Recursos focalizados en actividades de bombero y entrega de servicio, y no en la mejora.
- Personal sin motivación, que no puede ver el beneficio personal al adoptar y conducir el cambio.

FACTORES DE ÉXITO

- Asegurar que la gerencia comunica y refuerza regularmente la necesidad de servicios, soluciones y un buen gobierno confiables y robustos. Comunicar las mejoras logradas a todas las partes interesadas.
- Visitar nuevamente a las partes interesadas y obtener su respaldo para 'alimentar' el impulso.
- Si los recursos son escasos, aprovechar la oportunidad para implementar mejoras en el transcurso del trabajo, como parte de un proyecto de la rutina diaria.
- Focalizarse en tareas de mejora regulares y gestionables.
- Obtener asistencia externa, pero que permanezca comprometida.
- Alinear los sistemas de recompensa personales con las metas y métricas de mejora en el desempeño, tanto personales como organizacionales.

Fuente: COBIT 5

Y LUEGO... ¿QUÉ?

Administración de la plataforma

Una vez implantado el modelo de Auditoría Continua, la administración de la plataforma requiere de los siguientes trabajos:

- **Crear nuevos indicadores.** La evolución de la organización puede exigir crear nuevos indicadores o ajustar los existentes a las

nuevas situaciones o riesgos. De aquí la necesidad de retroalimentación.

- **Gestionar la información de los afectados.** Es muy importante que los receptores reciban puntualmente la información y sugerencias sobre puntos de mejora, sobre todo en la fase inicial. Estas sugerencias deben analizarse desde un punto de vista global, porque algunas áreas parciales del negocio podrían no contar con información

Administrar la plataforma, medir la rentabilidad del proceso e incorporar mejoras en Auditoría Interna para asegurar la correcta utilización de la herramienta de Auditoría Continua son las principales actividades a realizar una vez puesta en marcha dicha aplicación.

suficiente para valorar el proyecto en su conjunto. No obstante, siempre debe quedar constancia y trazabilidad de las sugerencias, tanto para el "cliente interno", como para el resto de participantes.

- **Distribuir los resultados.** El principal activo de un sistema de Auditoría Continua es la gestión automática y simultánea de múltiples puntos de control. Se realizan análisis periódicos (diarios, semanales, mensuales) y se comunican inmediatamente las incidencias o problemas a los responsables de las áreas afectadas. Posteriormente, el área de Auditoría Interna emite un reporte donde detalla las acciones adoptadas para subsanarlos. La plataforma se configura como una aplicación corporativa de acceso público con Cuadros de Mando que facilitan su gestión.

Medición de la rentabilidad

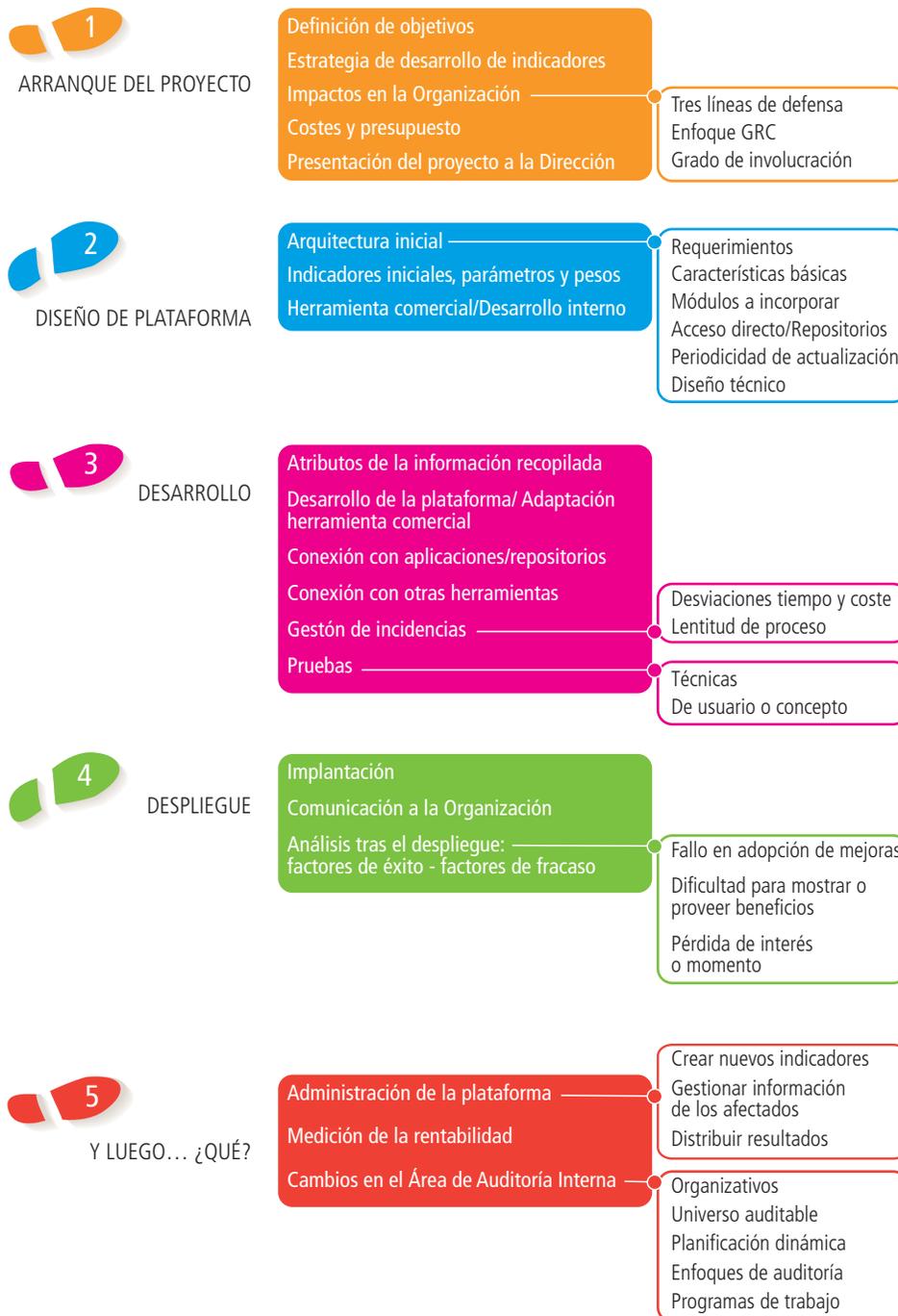
En general, el principal beneficio de los modelos de Auditoría Continua es la clara y evidente mejora de la eficiencia y eficacia en el trabajo de Auditoría Interna, una mayor cobertura del aseguramiento, la detección temprana de incidencias, la reducción de gastos de viaje y la mejora del entorno global de control. Es

necesario registrar y medir estos beneficios para poner en valor las inversiones realizadas de cara a la organización.

Cambios en el área de Auditoría Interna

- **Organizativos.** Incorporación de nuevas habilidades y competencias en el equipo de Auditoría Interna: perfiles profesionales con conocimientos de Sistemas de Información.
- **Universo auditable.** Las técnicas de Auditoría Interna no se basan únicamente en pruebas de cumplimiento, aumenta la importancia de las pruebas sustantivas y el análisis de toda la población de datos.
- **Planificación dinámica.** Al disponer de un sistema de indicadores y alertas, se revisa el Plan de Auditoría Interna con una periodicidad mayor.
- **Enfoques de Auditoría Interna.** Mayor disciplina y unificación en la forma de realizar el trabajo de auditoría interna en todo el equipo.
- **Programas de trabajo.** Las pruebas se enfocan hacia los Sistemas de Información y no tanto hacia el papel o hacia los informes finales generados por los usuarios.

IMPLANTACIÓN DE UN MODELO DE AUDITORÍA CONTINUA · CONSIDERACIONES





Caso práctico

MODELO DE AUDITORÍA CONTINUA EN FLEXI ACER

DESCRIPCIÓN DE LA EMPRESA

EMPRESA

FLEXI ACER.

(se trata de una empresa ficticia. Los datos que se incluyen en este supuesto práctico no han sido extraídos de ninguna empresa real).

DESCRIPCIÓN

Trabaja de forma industrial con componentes de acero para construir mobiliario urbano (por ejemplo, papeleras, barandillas, etc). Tienen la sede en Málaga, plantas de fabricación en Málaga, Madrid, Barcelona y México y filiales comerciales internacionales en Alemania, Italia, México, EEUU y Argentina.

En total, factura alrededor de 1.000 Millones de Euros anuales, especialmente fuera de España. Tiene un total de 2.500 empleados repartidos por Europa y América.

SITUACIÓN

La caída de ventas, como efecto de la menor actividad industrial, ha impactado en su cuenta de resultados. Esto ha provocado:

- **Aumento del nivel de fraude interno.** El esquema retributivo establecido al personal de sus filiales se basa en incentivar el resultado obtenido en las mismas, lo cual ha llevado a múltiples intentos de fraude por parte de responsables en diferentes filiales,

que han procurado enmascarar la cifra de ventas o diferir pérdidas, ocultando determinados indicadores que afectan al resultado, o difiriendo costes de un ejercicio a otro.

- **Reducción del margen de beneficio.** La necesidad de detener la caída de negocio ha llevado a acuerdos de dudosa rentabilidad y caídas de márgenes, hasta dejar la cuenta de algunas filiales en situación comprometida, que puede afectar a la viabilidad de la organización.
- **Cambios en la organización.** Ante la necesidad de aumentar el entorno de control en la estructura de la Sociedad, y de reducir el nivel de gastos, se están agrupando las actividades realizadas en filiales, mediante la centralización de servicios en Agrupación de Interés Económico (AIE) que prestan su apoyo a las distintas filiales del Grupo.

ENTORNO DE CONTROL

Basado en un esquema de tres líneas de defensa:

- **1ª Línea: Gestión operativa realizada.**
 - Desde las distintas áreas operativas de cada una de las filiales.
 - Desde las áreas operativas de fases del negocio centralizado en AIE.
 - Desde las áreas de central que gestionan la realización de funciones a nivel Grupo.
- Son Finanzas, RR HH, TI y Administración.

- **2ª línea: a nivel Grupo.** La Sociedad dispone de las siguientes áreas de control que afectan a la matriz y a todas las filiales del Grupo:
 - Control Financiero y de Gestión.
 - Seguridad en la Información.
 - Gestión de Riesgos Corporativos.
 - Calidad.
 - Cumplimiento.
 - Control Interno.
- **3ª línea: Auditoría Interna.**
 - Ubicado en la Sede Central, formado por 3 auditores más un Director de Auditoría Interna.
 - Dedican más del 50% de su tiempo a visitas presenciales en las distintas sedes, validando procedimientos y realizando revisiones periódicas.
 - Depende directamente del CEO.
 - Reporta a un Comité de Auditoría, integrado por Consejeros independientes de la sociedad.

HERRAMIENTAS PARA EL CONTROL INTERNO

La 2ª línea de defensa dispone de las siguientes herramientas y aplicaciones para un adecuado seguimiento del sistema de Control Interno.

- **Mapas de procesos.** Identifica en tres niveles los distintos procesos que componen la Sociedad. A nivel 1, serían:
 - Asesoría Jurídica.
 - Atención al Cliente.
 - Comercial.
 - Comunicación.
 - Contabilidad.
 - Inmuebles y logística.
- **Mapas de Riesgos.** La Sociedad agrupa a sus distintos responsables de áreas en "responsables de riesgos" encargados de definir y valorar los riesgos que les afectan. De esta forma, configura un mapa de riesgos, basado en tres niveles, que incluyen:
 - Descripción del riesgo.
 - Causas.
 - Controles mitigantes.
 - Valoración antes de controles.
 - Valoración después de controles. (la valoración se basa en un esquema de probabilidad e impacto).

- Fiscal.
- Inversiones financieras.
- Planificación y análisis de gestión.
- Recursos humanos.
- Sistemas de Información.
- Gestión de Riesgos.
- Supervisión y Control Interno.
- Proveedores.
- Ventas.
- Facturación y cobro.

A primer nivel, clasifica los riesgos en los siguientes grupos:

- Crédito (de cobro, ...).
- Financiero (tipo de interés, valoración inversiones, ...).
- Operacional.
- Regulatorio.
- Negocio.

- **Sistemas de Información.** Dispone de:
 - Data Warehouse, con información de todas las variables que considera para seguimiento de la actividad de todas las unidades de la Organización.



- *Work Flow* en la Intranet, con asignación de funciones a todos los empleados de la organización, identificando acciones ante determinados aspectos programados.
- Paquete contable integrado en SAP, que cuenta con un módulo de gestión de almacenes y materiales. Algunas unidades pueden utilizar otro sistema, aunque la empresa está en un proceso de unificación de los mismos.
- Para gestión de costes y márgenes operativos cuentan con un sistema de Business Intelligence (BI) de reciente implantación.
- Aplicativo de Auditoría Interna enfocado a un esquema de programas de trabajo y realización de informes, enfocado a los sistemas tradicionales de Auditoría Operativa.
- Para procesos con sistemas de Auditoría Continua desarrollado, identificamos indicadores.
- Conexión con otras herramientas: ver cómo afectan los nuevos desarrollos.
- Reporting a funciones clave.
- Seguimiento realizado sobre indicadores:
 - Por áreas responsables (Monitorización Continua).
 - Por Auditoría Interna (Auditoría Continua).
- Sistema para determinar nuevos indicadores y actualización de los existentes.

Estos son los aspectos previos considerados, antes de definir la implantación de un modelo de Auditoría Continua. Para desarrollarlo, hace falta revisar el trabajo que realizan todos los implicados, pues existe el riesgo de duplicar áreas.

Ahora, en base a este supuesto, se detalla la implantación de un modelo de Auditoría Continua, mediante:

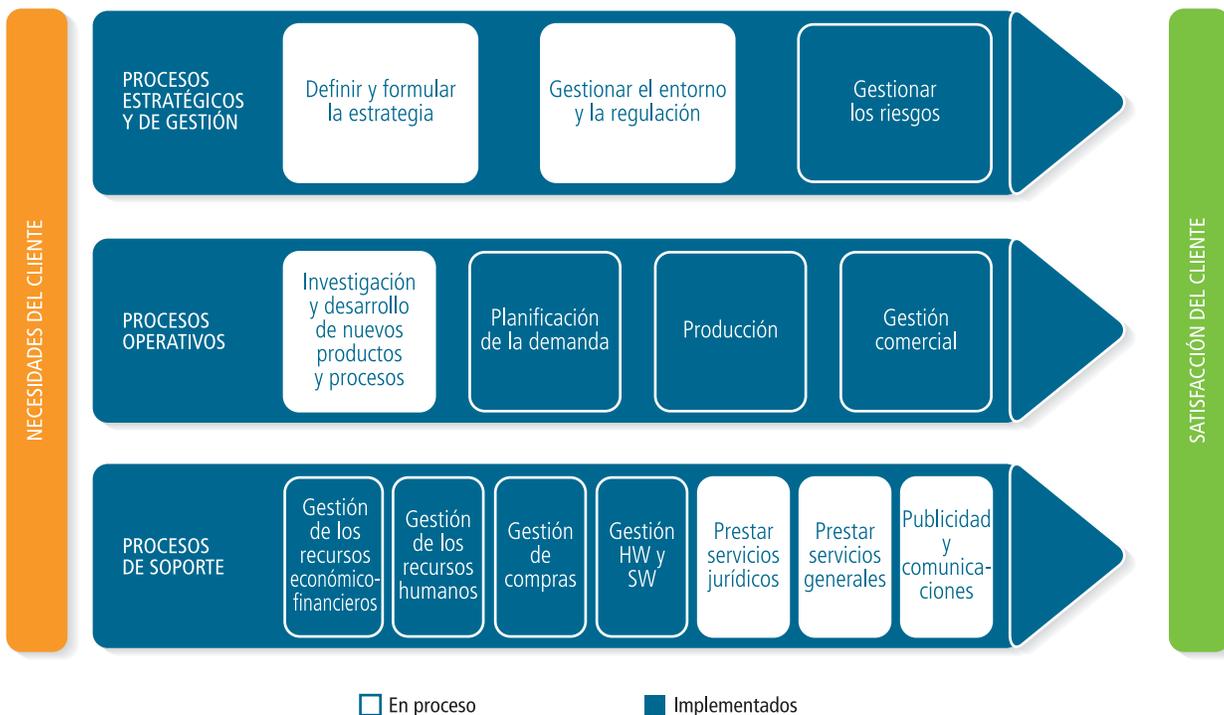
- Descripción de procesos.
- Asignación de riesgos.
- Departamentos responsables. Vemos cómo afecta la existencia de cambios organizativos.
- Identificamos el nivel de madurez de Auditoría por procesos.

MAPA DE PROCESOS

La Dirección de FLEXI ACER ha implantado un modelo de gestión orientado a procesos, donde las necesidades y la satisfacción del cliente forman el eje de la estrategia del negocio.

En el proceso de implantación del modelo de Auditoría Continua, la Dirección de Auditoría Interna decide seguir un enfoque "incremental" e "iterativo". En el alcance inicial del modelo se incluyen aquellos procesos relacionados con los riesgos más críticos del negocio y susceptibles de ser automatizados mediante las herramientas disponibles en FLEXI ACER.

La Dirección de Auditoría Interna dispone de un proceso de monitorización que identifica los cambios en el perfil de riesgo de la compañía o en sus procesos para adaptar los indicadores, y los indicadores incluidos en el modelo de Auditoría Continua.



En la actualidad, han sido implementados dentro del modelo de Auditoría Continua de FLEXI ACER los procesos señalados en el gráfico anterior.

El resto de procesos se siguen cubriendo mediante un enfoque de auditoría “tradicional” (cíclicas, *ad-hoc*, presenciales). Periódicamente, la Dirección de Auditoría Interna evalúa la posibilidad de incluir algunos de los procesos que faltan en el modelo de Auditoría Continua. Para ello contempla los riesgos asociados, las limitaciones tecnológicas o la naturaleza del proceso.

Para los procesos incluidos dentro del modelo de Auditoría Continua, adicionalmente a la supervisión continua del perfil de riesgo y la efectividad de los controles, se realizan audi-

torías complementarias con un enfoque “tradicional”, que cubren aspectos específicos de alta criticidad o no susceptibles de automatización.

MODELO DE AUDITORÍA CONTINUA IMPLEMENTADO EN FLEXI ACER

La plataforma de auditoría continua implementada en FLEXI ACER tiene dos años de antigüedad y presenta las siguientes características:

- El diseño de la plataforma fue realizado por la Dirección de Auditoría Interna. Posteriormente, su desarrollo e implantación fue subcontratado a una consultora especiali-



zada, en conjunción con el Departamento de Tecnología de FLEXI ACER. El Departamento de Tecnología se encarga del mantenimiento y la incorporación de nuevas funcionalidades.

- La plataforma utiliza la información existente en un repositorio para evaluar los diferentes indicadores. Este repositorio se actualiza cada noche con un volcado directo de las tablas existentes en el entorno de producción.
- La plataforma admite la incorporación de indicadores dinámicos que son definidos, desarrollados y parametrizados por los usuarios de Auditoría Interna. No es necesaria la involucración del área de tecnología para incorporar un nuevo indicador (salvo que sea necesario incorporar al repositorio alguna tabla nueva no considerada hasta ese momento).

Existe un administrador en el área de Auditoría Interna que incorpora estos nuevos indicadores (o modifica sus parámetros) una vez han sido aprobados por la Dirección de Auditoría Interna. La descripción y detalle de los mismos se recoge en una ficha que se cumplimenta desde la propia plataforma.

- La periodicidad de ejecución de cada indicador es parametrizable y depende de la importancia del mismo. En cualquier caso, dicha periodicidad es –como mínimo– de un día.
- La plataforma cuenta con una serie de módulos que permiten, entre otras funciones, gestionar y/o incorporar indicadores, consultar resultados, asignarlos (de forma manual o predefinida) a los auditores internos para su análisis, comunicarse directamente

con las unidades auditadas para solicitar mayor información, seguimiento centralizado de ocurrencias, acceso a históricos, etcétera.

En base a los procesos incorporados por FLEXI ACER en el modelo de Auditoría Continua, se muestran los indicadores establecidos para dos de los procesos de negocio:

Gestión de Compras

- Proveedores duplicados.
- Campos faltantes en el maestro de proveedores.
- Pedidos creados tarde/a posteriori (en el momento de la primera recepción de mercancía o factura).
- Pedidos parciales (o troceados, sin controles de autorización adicionales para pedidos de importe o criticidad más elevada).
- Facturas afloradas con retraso (*facturas en el cajón*).
- Facturas conformadas (validadas, autorizadas) con retraso.
- Facturas que superan cierto importe y no han sido apropiadamente autorizadas.
- Facturas duplicadas.
- Partidas con potenciales problemas de corte de operaciones.
- Partidas abiertas de proveedor por un período de tiempo muy largo.
- Porcentaje de facturas sin referencia a pedido de compra.
- Pagos a proveedores en paraísos fiscales.
- Pagos a personal vinculado a la empresa (por ejemplo, con misma dirección o cuenta bancaria que el empleado).

Gestión de Hardware y Software

- Volumen de personal externo que accede a información sensible de los clientes.
- Usuarios del entorno de desarrollo que accede al área de producción.
- Aplicaciones que registran más de X solicitudes de mantenimiento correctivo en Z días.
- Tiempo medio de resolución de incidencias superior a Z días.
- Desviaciones en proyectos respecto a la planificación inicial superiores a Z días.

- Volumen de intentos de acceso a ficheros de passwords.
- El rendimiento de determinados servidores inferior a un X%.
- Usuarios con actividad fuera de horas normales de trabajo.
- Usuarios con muy baja actividad (o nula) (Son potencialmente innecesarios).

La ficha para incorporar nuevos indicadores o modificar la definición de los existentes presenta el siguiente formato:

Ficha Indicador (A cumplimentar como paso previo a su creación o modificación)							
Cabecera	<table border="1" style="width: 100%;"> <tr> <td>Identificador indicador: A-S-005</td> <td>Tipo indicador: Alarma</td> <td>Ámbito: Prueba sustantiva</td> </tr> <tr> <td colspan="3">Título indicador: Aplicaciones que presentan un alto mantenimiento correctivo</td> </tr> </table>	Identificador indicador: A-S-005	Tipo indicador: Alarma	Ámbito: Prueba sustantiva	Título indicador: Aplicaciones que presentan un alto mantenimiento correctivo		
Identificador indicador: A-S-005	Tipo indicador: Alarma	Ámbito: Prueba sustantiva					
Título indicador: Aplicaciones que presentan un alto mantenimiento correctivo							
Resumen	<table border="1" style="width: 100%;"> <tr> <td>Departamento asignado: Auditoría tecnológica</td> <td>Área auditada: Tecnología</td> </tr> <tr> <td>Tipo Riesgo: Tecnológico</td> <td>Epígrafe: Función de Desarrollo</td> </tr> </table> <p>Breve descripción del indicador: Aplicaciones que registran más X solicitudes de mantenimiento correctivo en Z días</p>	Departamento asignado: Auditoría tecnológica	Área auditada: Tecnología	Tipo Riesgo: Tecnológico	Epígrafe: Función de Desarrollo		
Departamento asignado: Auditoría tecnológica	Área auditada: Tecnología						
Tipo Riesgo: Tecnológico	Epígrafe: Función de Desarrollo						
Detalle	<p>Riesgo evaluado: Que una aplicación presente un volumen de mantenimiento correctivo alto en un breve periodo de tiempo, puede ser un síntoma de que dicha aplicación no ha sido lo suficientemente probada (o no lo ha sido algún cambio realizado sobre la misma). En cualquier caso, denota el riesgo de que dicha aplicación esté generando un volumen de errores superior al habitual, lo que puede dar lugar a problemas de integridad en la información, dificultades operativas, etc.</p> <p>Parámetros indicador: * Volumen de solicitudes de mantenimiento realizadas en un periodo dado * Días que componen el periodo evaluado</p> <table border="1" style="width: 100%;"> <tr> <td>Periodicidad de ejecución: Diaria</td> <td>Importancia: Media</td> <td>Versión indicador: 1.0</td> </tr> <tr> <td>Aprobación diseño: Director Auditoría</td> <td>Fecha de aprobación: 10/05/2013</td> <td>Fecha de última revisión: 10/05/2013</td> </tr> </table>	Periodicidad de ejecución: Diaria	Importancia: Media	Versión indicador: 1.0	Aprobación diseño: Director Auditoría	Fecha de aprobación: 10/05/2013	Fecha de última revisión: 10/05/2013
Periodicidad de ejecución: Diaria	Importancia: Media	Versión indicador: 1.0					
Aprobación diseño: Director Auditoría	Fecha de aprobación: 10/05/2013	Fecha de última revisión: 10/05/2013					
Gestión Resultados	<p>Información a mostrar: * Código de la aplicación * Tiempo de resolución medio * Identificador solicitudes pendientes * Volumen de solicitudes * Solicitudes pendientes</p> <p>Cómo revisar cada ocurrencia: * Analizar la tipología de solicitudes pendientes. Evaluar si se concentran en alguna transacción u operativa concreta cuyo mal funcionamiento se considere de riesgo relevante (gestión de saldos, facturación, informes financieros, atención al cliente, etc.) * Envío de correo automático desde la aplicación de auditoría a distancia al personal del departamento de Desarrollo para solicitar más información. Posible entrevista adicional</p> <p>Información adicional a solicitar: * Tipología de errores, causas identificadas hasta el momento, transacciones afectadas y posible impacto (y/o impacto real de haberse materializado)...</p> <p>Comunicación resultados si es una incidencia real: * Dirección de auditoría * Dirección de negocio implicada en el uso de la aplicación</p>						



MODELO DE EJECUCIÓN Y MANTENIMIENTO CONTINUO DEL MODELO DE AUDITORÍA CONTINUA

Modelo de Ejecución

Se distinguen dos tipos de ejecución de indicadores de Auditoría Continua:

- **Análisis Continuo:** los indicadores se ejecutan de forma automática una vez a la semana y se almacena el detalle de los resultados en el directorio compartido de Auditoría Interna. Además, se dispone de un cuadro de mando funcional que permite analizar la evolución de un indicador a lo largo del tiempo y separar para su análisis las excepciones relevantes.

Con motivo de la reunión semestral de la Comisión de Auditoría de Flexi Acer, Auditoría Interna prepara un resumen ejecutivo de la evolución del modelo de Auditoría Continua y de las excepciones detectadas.

- **Análisis "ad hoc":** los indicadores se ejecutan a petición del usuario, que puede seleccionar la ventana temporal de trabajo, la sociedad o sociedades del alcance, y los indicadores que ejecuta. Este modelo es habitualmente un paso previo a la auditoría de una filial de Flexi Acer, así se dispone del máximo de información antes de la inspección física.

Mantenimiento del Modelo

Se ha definido un responsable de Auditoría Interna como responsable del modelo de indicadores de Auditoría Continua. También se ha definido un interlocutor del área de sistemas responsable de la alimentación de la información necesaria y de la gestión de las mejoras continuas del modelo.

En general, los usuarios del modelo disponen de un perfil estándar, que permite parametrizar ejecuciones y ejecutar indicadores. El responsable de Auditoría Interna y el responsable del área de sistemas disponen de capacidad de administración, lo que permite realizar

CUADRO DE MANDO UTILIZADO POR FLEXI ACER PARA PRESENTAR LOS RESULTADOS DEL MODELO DE AUDITORÍA CONTINUA

			Valor Objetivo según AI	2013 H2							
			TOTAL	España	Francia	Alemania	Italia	América del Sur			
								Argentina	Brasil	Uruguay	
Pedidos creados tarde	en momento recepción	Delegada	1%	2%	4%	1,4%	0%	0%	0%	0%	0%
		Centralizada	1%	0%	0%	0,6%	0%	0%	0%	0%	0%
	respecto fecha factura	Delegada	1%	3%	0%	4%	2%	0%	0%	0%	0%
		Centralizada	1%	0,9%	0%	1,2%	0%	0%	0%	0%	0%
Pedidos parciales		Directa	15%	13%	7%	13%	0%	0%	0%	0%	40%
		Delegada	1%	2%	2%	4%	0%	0%	0%	0%	0%
Facturas afloradas con retraso (>6 meses)			1%	0,4%	1%	0,6%	0,1%	0%	1%	0%	0,7%
Facturas conformadas con retraso (>1 mes)			5%	2%	2%	5%	3%	1%	1%	0%	1%
Facturas FI registradas sin pedido			2%	0,8%	0,4%	1%	0%	1%	0,5%	0,2%	0%
Facturas duplicadas			Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple
Corte de operaciones			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Partidas abiertas de proveedor			Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple
Análisis apuntes manuales			Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple
Plazo pago s/ política			Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple	Cumple

EVOLUCIÓN DE INDICADORES



tareas de gestión de usuarios y resolución de incidencias.

Se dispone de un flujo de resolución de incidencias de ejecución del modelo, completamente integrado con el proceso de resolución de incidencias de Flexi Acer y con responsables asignados.

Independientemente de las modificaciones realizadas asociadas al mantenimiento correctivo (resolución de incidencias), el modelo de Auditoría Continua será revisado cuando:

- Se produzcan cambios relevantes en los procesos de negocio de Flexi Acer o en el

enfoque de Auditoría Interna, que obliguen a una evolución del modelo para adaptarlo a los nuevos requerimientos funcionales.

- Si el responsable de la ejecución detecta que algún indicador no funciona de forma adecuada (por ejemplo, detectando un número elevado de falsos positivos).
- Se produzcan cambios tecnológicos significativos que permitan incorporar mejoras o adaptaciones a la implementación técnica.
- Como máximo, el modelo completo debe ser actualizado a los tres años.





Anexos

GLOSARIO

Aseguramiento Continuo

El aseguramiento continuo puede lograrse mejor mediante una combinación de responsabilidades de seguimiento continuo de la Dirección y las actividades de supervisión continua de Auditoría Interna.

Auditoría Continua

GTAG 3 lo define como todo método utilizado por los auditores para realizar actividades relacionadas con la auditoría de forma (más) continua. Es la secuencia de actividades que abarcan desde la evaluación continua de control hasta la evaluación continua de riesgos (todas las actividades en la secuencia control-riesgo).

Auditoría a distancia

Es aquella auditoría que pretende facilitar el seguimiento de los diversos riesgos sin necesidad de realizar una visita *in situ* a la ubicación física objeto de la auditoría.

Falso positivo

Cuando una ocurrencia, normalmente ligada a un indicador tipo alarma, no refleja realmente una situación anómala o atípica. Normalmente no se debe a un fallo en la configuración o programación del indicador, sino a que éste no está lo suficientemente elaborado o su umbral de tolerancia es muy bajo.

GTAG - Global Technology Audit Guide

Guía de Auditoría de Tecnología Global, emitida por el Instituto Internacional de Auditores Internos.

Indicador

La base de un sistema de auditoría continua es la ejecución de una serie de consultas, análisis y pruebas que –en esta guía – se han denominado “indicadores”. Los indicadores pueden tener diversas finalidades, por lo que hay diferentes tipos:

- Alarmas. Alertas sobre situaciones atípicas cuyo origen podría ser (o no) la materialización de un determinado riesgo. Es el tipo de indicador más frecuente.
- *Key Performance Indicators* (KPI) y *Key Risk Indicators* (KRI). Ratios e indicadores clave. Por ejemplo, el volumen de horas de mantenimiento correctivo que, anualmente, se realiza sobre una aplicación.
- Pre-auditorías. La ejecución de una determinada prueba de auditoría (por ejemplo, el recálculo de la facturación de un servicio) o la obtención de información general (por ejemplo, listados de clientes).
- Excepciones. Avisos sobre fallos en el funcionamiento de una transacción, un control, etc.

Indicador Fijo / Indicador Dinámico

- En un modelo de Auditoría Continua basado en indicadores fijos, cada vez que se desea incorporar un indicador es necesario programarlo “a medida” dentro de la plataforma. Normalmente la programación la lleva a cabo el departamento de tecnología, un proveedor externo o la empresa que ha desarrollado la herramienta de Auditoría Continua utilizada.
- En cambio, los indicadores dinámicos se pueden ir incorporando a la plataforma mediante la parametrización de determinados elementos existentes en la misma, para que no sea necesario modificar su programación (salvo que se quiera

incorporar más “elementos” al conjunto de los existentes).

Los indicadores fijos son fáciles de incorporar al principio y si son muchos, pero se vuelve muy “tedioso” añadirlos de forma esporádica, lo que hace que poco a poco la evolución de la plataforma se ralentice o se detenga.

En cambio, cuesta mucho al principio diseñar una plataforma que permita indicadores dinámicos (especialmente cuando urge dar resultados que justifiquen la inversión) pero, si se consigue, será relativamente sencillo ir adaptando los indicadores a la evolución de los riesgos.

Monitorización continua o Supervisión continua

Abarca los procesos que la dirección implementa para garantizar que las políticas, los procedimientos y los procesos de negocio funcionen eficazmente. Implica la responsabilidad de la dirección en cuanto a evaluar la idoneidad y eficacia de los controles.

Ocurrencia

Resultado o resultados que devuelve cada indicador.

Servicios de aseguramiento

El Glosario del *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (MIPP) define Servicios de aseguramiento como “Un examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización”. Por ejemplo: trabajos financieros, de desempeño, de cumplimiento, de seguridad de sistemas y de diligencia debida (due diligence).

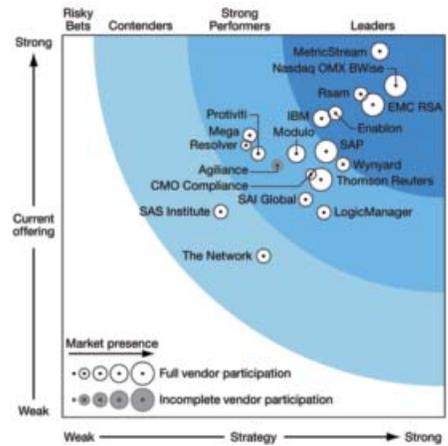
Umbral de tolerancia

Es el grado de sensibilidad del indicador. Cuanto más bajo sea, mayor volumen de ocurrencias generará (y viceversa). Lo ideal es que el umbral de tolerancia determine el volumen de personal necesario para analizar los resultados obtenidos, aunque lo habitual es que sea al revés (en función del personal disponible se ajusta el umbral).

EJEMPLOS DE HERRAMIENTAS DE MERCADO

En cuanto a las herramientas comerciales disponibles en el mercado, es más frecuente encontrar soluciones de propósito general, que soluciones específicas de Auditoría Continua.

En esta sección tratamos de reflejar estudios de mercado sobre plataformas GRC, que en su gran mayoría incluyen funcionalidades que soportan los procesos de Auditoría Continua, adicionalmente a otros procesos de aseguramiento.



Fuente: Forrester Research Q1 2014. *The Forrester Wave: Governance, Risk, and Compliance Platforms*



Fuente: *Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms*, 2013.



BIBLIOGRAFÍA

- *Auditoría Continua y Supervisión Continua. Presente y futuro.* Estudio de KPMG en la región EMA. Diciembre 2012.
- *Auditoría Continua y Supervisión Continua. Resultado del estudio en España.* KPMG. 2010.
- *Auditoría tecnológicamente avanzada: Auditoría a distancia y Auditoría Continua.* Partida doble, nº. 204. **Manuel Mendiola.** Noviembre 2008.
- *Beyond Continuous Auditing.* **Norman Marks.** December 2010.
- "Consejo para la práctica 2320-4: Aseguramiento Continuo". *Marco Internacional para la Práctica Profesional de la Auditoría Interna.*
- *Continuous monitoring and continuous auditing. From idea to implementation.* Deloitte. 2010.
- *Continuous process monitoring: your primary processes, structurally in control.* EY. 2011.
- *Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, 2013.*
- *GTAG-3-Guía de Auditoría de Tecnología Global. Auditoría continua: implicaciones para el aseguramiento, la supervisión y la evaluación de riesgos.* **David Coderre.** Octubre 2005.
- *Guía Práctica: Marco de relaciones de Auditoría Interna con otras funciones de Aseguramiento.* Instituto de Auditores Internos de España. Diciembre 2013.
- *Implementing a continuous audit process.* The Institute of Internal Auditors. December 2010.
- *The Forrester Wave: Governance, Risk, and Compliance Platforms.* **Christopher McClean, Nick Hayes and Renee Murphy.** January 27, 2014.
- *Transforming Internal Audit: A Maturity Model from Data Analytics to Continuous Assurance.* KPMG.

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-29726-2014

ISBN: 978-84-941921-8-0

Diseño y maquetación: desdezero, estudio gráfico

Impresión: IAG, SL



Los crecientes desafíos y responsabilidades a los se enfrentan los Consejos de Administración, los Comités de Auditoría y la Dirección de las compañías demandan contar con un sistema de aseguramiento sobre la eficacia del control y la gestión de riesgos, fiable, sostenible y continuo.

Implantar un modelo de Auditoría Continua permite a la Dirección de Auditoría Interna mejorar la calidad del aseguramiento que proporciona a la Alta Dirección y al Consejo de una manera proactiva, proyectiva y continua.

Esta guía hace un exhaustivo análisis de todas las cuestiones relevantes a considerar y no olvidar cuando se emprende la implantación de un modelo de Auditoría Continua, sus beneficios y desafíos.

La riqueza de este análisis radica en su flexibilidad, los autores presentan todas las opciones posibles con sus ventajas e inconvenientes para que cada Dirección de Auditoría Interna pueda valorar cuál de ellas se adapta mejor a la cultura, al marco de Gobierno, Riesgo y Cumplimiento y a la realidad de su organización.

