Fundamentos de auditoría interna

Instituto de Auditores Internos de España

NUEVA EDICIÓN BASADA EN

"Fundamentos de la Auditoría Interna" de **Eduardo Hevia Vázquez** (2006)

Miguel Ángel Arévalo
Ricardo Brea
Eduardo Cuesta
Pedro Fominaya
Sergio Gómez Landero
Luis Hernández
Ana Minguet
Helena Redondo
Laly Serrano
Eduardo Villalobos

Instituto de Auditores Internos de España

Prólogo

Presentamos esta publicación desde el más profundo cariño y añoranza por la figura de **Eduardo Hevia,** presidente del Instituto de Auditores Internos de España entre 1988 y 1998, y presidente de honor hasta su fallecimiento, en 2018.

Bajo el título *Fundamentos de la Auditoría Interna,* queremos rendir homenaje a Eduardo con esta nueva edición actualizada basada en su obra homónima, que vio la luz en 2006. En ella, nos guiaba en un viaje a lo largo de todas las áreas que integran el proceso de la Auditoría Interna en una organización.

Ahora, gracias a esta exhaustiva actualización de contenido para hacerlo acorde a los tiempos y circunstancias actuales que vive nuestra profesión, Eduardo nos sigue acompañando en esta lectura. Partiendo de la definición actualizada de Auditoría Interna según el *Marco Internacional para la Práctica Profesional de la Auditoría Interna,* se tratan una gran variedad de asuntos que han evolucionado rápidamente durante los últimos años: el Gobierno Corporativo y el papel de Auditoría Interna; su relación con el control interno y la gestión del riesgo empresarial; la creación, organización y funcionamiento de departamentos de Auditoría Interna; los diferentes tipos de trabajos y la calidad de los mismos; o la importancia de la planificación y la elaboración de los informes de resultados.

Todas estas cuestiones se abordan en los capítulos que componen este libro junto a la incorporación de la tecnología y de nuevas metodologías de trabajo *(agile);* el papel de la Auditoría Interna en relación con el fraude; y los conocimientos y habilidades necesarias para el auditor interno o el creciente papel de Auditoría Interna en relación con tendencias como, por ejemplo, su papel en materia de desarrollo sostenible.

Ese camino que Eduardo emprendió lo continuamos ahora gracias a profesionales de primer nivel que han hecho que este homenaje sea una realidad: **Miguel Ángel Arévalo, Ricardo Brea, Eduardo Cuesta, Pedro Fominaya, Sergio Gómez Landero, Luis Hernández, Ana Minguet, Helena Redondo, Laly Serrano** y **Eduardo Villalobos.**

Gracias al trabajo de todos ellos esta publicación servirá como referencia al auditor interno de cualquier categoría. Aquí se conectan los conocimientos y experiencia del que fuera nuestro presidente con el profesional de hoy, que podrá disfrutar del espíritu de la publicación inicial adaptada a las circunstancias actuales de nuestra profesión, la Auditoría Interna, cuyo papel es cada vez más relevante y que ha sabido adaptarse al exigente entorno en el que lleva a cabo su actividad.

Instituto de Auditores Internos de España

Índice

La Auditoría Interna como profesión

Instituto de Auditores Internos de España

1. La profesión de auditor interno. Introducción

Para comprender gran parte de los conceptos y desarrollos de este manual, hay que partir de la concepción de Auditoría Interna como profesión de consultoría y gestión perfectamente diferenciada, con una trayectoria suficientemente prolongada en el tiempo y a lo largo y ancho del mundo que avala esta afirmación y que, para su desempeño, requiere de conocimientos y capacidades específicas.

En el pasado solía confundirse a la Auditoría Interna con la auditoría de cuentas, o auditoría externa. No obstante, la progresiva profesionalización de la función y el mayor grado de madurez de las organizaciones y del entorno socio-económico y regulatorio en el que desarrolla su actividad, ha hecho posible que se perciba a la Auditoría Interna como una realidad diferente de la auditoría de cuentas.

Hoy por hoy se reconoce a la Auditoría Interna como profesión que opera con un propósito y un alcance determinados, con un enfoque y una metodología específica, y dentro de un marco normativo y de guías y buenas prácticas emanadas y consensuadas por todos sus profesionales organizados institucionalmente a través del Instituto Global de Auditores Internos (IIA) y los Institutos locales establecidos en cada país. Todos estos elementos se desarrollan en los apartados siguientes.

2. Concepto de Auditoría Interna

2.1 Definición y características. Su evolución en el tiempo

En la actualidad, el propósito fundamental, la naturaleza y el alcance de la Auditoría Interna se encuentran definidos en el *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (en adelante MIPP), que veremos en detalle en el epígrafe siguiente y que define en qué debe consistir la Auditoría Interna en todas las organizaciones de cualquier parte del mundo:

" La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar los procesos de gestión de riesgos, control y gobierno".

El desarrollo y la mayor concreción de la anterior definición dependerán del país y de la organización a la que pertenezca la función de Auditoría Interna. En concreto, de aspectos tales como la cultura y el ordenamiento jurídico de cada país, la misión, visión y valores de la organización, su estrategia y objetivos, las políticas del Consejo de Administración

y de la Comisión de Auditoría, el estilo de Dirección y, sin duda, de la profesionalidad, criterios y personalidad del Director/a de Auditoría Interna.

No obstante, podemos decir que, en general, el trabajo de la Auditoría Interna dentro de las organizaciones consiste en revisar la fiabilidad e integridad de la información, el cumplimiento de políticas y regulaciones, la protección de los activos, el uso económico y eficiente de los recursos y el cumplimiento de las metas y objetivos operativos fijados por la Dirección.

Este trabajo se ejerce dentro de las organizaciones, pero sin responsabilidades de gestión para garantizar su independencia y objetividad, centrándose en los principales riesgos que puedan afectar a su empresa, supervisando que los controles existentes sean los adecuados para mitigar posibles riesgos, y que los procesos de gobierno sean eficaces y eficientes.

De esta forma, con su trabajo, el auditor interno proporciona aseguramiento al Consejo de Administración, a la Comisión de Auditoría y a la Alta Dirección sobre la eficacia de los sistemas de control interno y de gestión de riesgos.

En resumen, podemos decir que un departamento que desarrolle la función de Auditoría Interna profesionalmente tendrá las características siguientes:

- Actúa por delegación del Consejo de Administración (u órgano de gobierno equivalente) o de la Comisión de Auditoría.
- Está situado en el organigrama de la organización al mismo nivel que el resto de responsables o directores funcionales.
- Tiene mentalidad y visión gerenciales.
- Es independiente, es decir, está libre de condicionamientos que obstaculicen su capacidad de desarrollar su trabajo de forma imparcial, para lo cual depende funcionalmente del Consejo o de la Comisión de Auditoría y jerárquicamente del máximo ejecutivo de la organización.
- Sus funciones, atribuciones y responsabilidades se recogen en un estatuto aprobado por el Consejo de Administración u órgano equivalente.
- Se sitúa en el organigrama al mismo nivel que el resto de direcciones o en un nivel jerárquico funcional de máxima categoría.
- Planifica su actividad teniendo en cuenta los riesgos de la organización.
- Puede evaluar todas las actividades de la empresa y no tiene limitada su actividad a las áreas administrativas, contables y financieras.
- Elabora informes en los que emite recomendaciones, sin que tenga competencia para imponerlas ejecutivamente.

- Aporta valor a la organización.
- Y se configura cada vez más como un consultor interno.

De esta forma, Auditoría Interna se sitúa como una función que aporta valor, impulsando el perfeccionamiento constante de los sistemas de gestión de riesgos, control interno y gobierno de las organizaciones para mejorar y proteger su valor. Así deja atrás modelos de tiempos pasados que hoy resultarían del todo anacrónicos, modelos centrados en la vigilancia y en el antiguo concepto de intervención, en los que la Auditoría Interna se identificaba con "los ojos y los oídos de la dirección" como simple informador, desconfiado, que llegaba a ser intimidante en algún caso.

EVOLUCIÓN AUDITORÍA INTERNA

	Pasado	Presente
OBJETIVO FUNDAMENTAL	Asegurar la fiabilidad y exactitud de la información contable.	Asegurar un buen sistema gestión de riesgos, control y gobierno.
FORMACIÓN Y CAPACITACIÓN DEL EQUIPO	Eminentemente contable.	Personal altamente cualificado, con un conocimiento global de la organización y visión gerencial.
DEPENDENCIA JERÁRQUICA	Adscrita a las unidades financieras, de control o de intervención.	Doble dependencia funcional, del Consejo o de la Comisión de Auditoría, y administrativa del máximo nivel ejecutivo.
PLANIFICACIÓN	Realiza trabajos no específicos de auditoría, según las necesidades y «urgencias» momentáneas, sin una previa planificación anual de sus actividades.	Desarrolla su trabajo de acuerdo con la planificación autorizada y previamente distribuida en todo el ámbito de la organización.
ACTIVIDAD	Está centrada en el análisis de los registros de transacciones tratando de detectar errores o irregularidades. Dedica buena parte de su tiempo a colaborar con los auditores externos actuando como meros auxiliares de los mismos.	Formula opiniones y recomendaciones de manera independiente. Tiene una relación de colaboración con los auditados y participa en sus preocupaciones y problemas.
ATRIBUCIONES Y FACULTADES	Limitadas al campo administrativo-contable sin autoridad para auditar el resto de áreas funcionales de la organización.	Suficientes para auditar todas las actividades y áreas funcionales de la organización.

Esta **evolución de la actividad de Auditoría Interna** no solo se observa en la propia definición, también en muchos otros elementos, algunos de ellos ya citados, que se han comparado en la tabla anterior.

2.2 El contenido y el fundamento del valor de Auditoría Interna

Una vez sentadas las bases de la definición y de las características fundamentales de la profesión, podemos añadir que la característica más significativa de la Auditoría Interna es su capacidad para analizar, desde una posición de independencia y con objetividad y profesionalidad, actividades, organizaciones o situaciones en las que no tiene responsabilidades de gestión.

A esta capacidad fundamental de análisis se añaden capacidades o propiedades complementarias que configuran igualmente la función:

- Elabora informes con recomendaciones cuya aceptación está en función de su calidad y utilidad.
- Sus opiniones se apoyan en la evidencia o en la racionalidad de sus argumentos.
- Carece de fuerza ejecutiva para imponer sus recomendaciones: trata, por tanto, de convencer y no de imponer.
- En las organizaciones en las que desarrolla su actividad genera dinámicas de cambio y aceptación de nuevas ideas, métodos e iniciativas.
- A través de ella, el Consejo y la Alta Dirección ejercen su responsabilidad de supervisar el sistema de control interno y de gestión de riesgos y el cumplimiento de sus políticas y programas.
- Efectúa una permanente y sistemática evaluación del sistema de gestión de riesgos.
- Su universalidad y adaptabilidad la hacen aplicable a cualquier tipo de organización y de país.

Expuesto lo anterior, es necesario hacer una reflexión sobre la capacidad de la Auditoría Interna de aportar valor a las organizaciones, porque esto solo se produce cuando la actividad es desempeñada por auditores internos profesionales, es decir, cualificados, formados específicamente para este trabajo y con la necesaria experiencia.

En concreto, los profesionales de la Auditoría Interna deberían tener conocimientos y capacidades suficientes para:

- Realizar su trabajo desde la independencia que les debe proporcionar su total desvinculación de responsabilidades en las actividades o cuestiones que auditan.

- Tratar de conocer de forma suficientemente completa la realidad auditada (lo que es) para emitir un juicio objetivo, oportuno y acertado, y realizar recomendaciones (lo que debe ser) tan sólo cuando se está suficientemente seguro de la realidad investigada.
- Conocer de forma clara el negocio o actividad de la organización a la que sirven, tener una visión gerencial de la misma, con un conocimiento amplio del conjunto de sus funciones y actividades, de su cultura empresarial, sus sistemas y sus procesos.
- Expresar sus opiniones, recomendaciones y sugerencias, apoyándose en la racionalidad de sus argumentos y en la consistencia de los hechos.
- No solo señalar deficiencias, errores, irregularidades y fraudes, sino indicar también sus causas y la forma de que no se reproduzcan, además de reconocer las buenas prácticas y demás aspectos reseñables de las actividades auditadas.

Si los auditores internos cumplen los requisitos anteriores, existe una cultura de auditoría en toda la organización, y el Consejo y la Comisión de Auditoría tienen en cuenta las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna a la hora de utilizar sus servicios, el valor y eficiencia de la función estarán garantizados, y su utilidad se proyectará en los resultados de la organización.

2.3 Clases o tipos de servicios de Auditoría Interna

SERVICIOS DE ASEGURAMIENTO Y SERVICIOS DE CONSULTORÍA

La primera clasificación la encontramos en el Marco Internacional para la Práctica Profesional de la Auditoría Interna (en adelante MIPP), que distingue entre servicios de aseguramiento y de consultoría.

Según el MIPP, **los servicios de aseguramiento** comprenden la tarea de evaluación objetiva de las evidencias, efectuada por los auditores internos, para expresar opiniones o conclusiones respecto de una entidad, operación, función, proceso, sistema u otros asuntos. La naturaleza y el alcance de un trabajo de aseguramiento son definidos por el auditor interno.

En general, en los servicios de aseguramiento intervienen tres partes:

1. El propietario del proceso: la persona o grupo directamente implicado en la entidad, operación, función, proceso, sistema u otro asunto.
2. El auditor interno: la persona o grupo que realiza la evaluación.
3. El usuario: la persona o grupo que utiliza la evaluación.

En cambio, también según el MIPP, los **servicios de consultoría** son por naturaleza consejos y se realizan, por lo general, a pedido de un cliente. La naturaleza y el alcance del trabajo de consultoría están sujetos al acuerdo efectuado con el cliente, no son definidos unilateralmente por el auditor interno. Además, cuando desempeña servicios de consultoría, el auditor interno deberá mantener la objetividad y no asumir responsabilidades de gestión.

En general, en los servicios de consultoría intervienen solo dos partes:

1. El auditor interno: la persona o grupo que ofrece el consejo.
2. El cliente del trabajo: la persona o grupo que busca y recibe el consejo.

CLASIFICACIÓN ATENDIENDO A LA FINALIDAD

Además de la clasificación del MIPP, dependiendo de su finalidad, las auditorías pueden ser auditorías financieras, verificativas, informáticas, operativas o de gestión y técnicas. Esta clasificación no debe entenderse como algo rígido. Tampoco son categorías que se excluyan radicalmente. Se definen a continuación:

Auditorías financieras: se realizan con el fin de asegurar el adecuado registro contable de las operaciones, el cumplimiento de los principios y normas de contabilidad generalmente aceptados y las disposiciones legales y regulaciones contables, fiscales y financieras que son de obligado cumplimiento para las organizaciones. Los métodos utilizados son similares a los que emplean los auditores de cuentas externos y lo que se persigue es la integridad, transparencia y fiabilidad de la información financiera.

Auditorías verificativas o de cumplimiento: tratan de comprobar que las políticas, programas y normas de las organizaciones se cumplen satisfactoriamente en todo el ámbito de las mismas. No obstante, la visión y el análisis del auditor interno en este tipo de auditorías debe ir más allá de la simple verificación del cumplimiento, para comprobar adicionalmente que no hayan cambiado las condiciones bajo las que se establecieron dichas políticas, programas y normas.

Auditorías informáticas o del entorno TIC: analizan la utilidad, eficiencia y fiabilidad de los sistemas de información, la seguridad de los datos y sus archivos, así como el control interno de los servicios informáticos que elaboran y procesan tales datos.

Auditorías de gestión: auditan sistemas, métodos, procesos, estructuras organizativas, programas, etc., con la finalidad de mantener una gestión eficiente y óptima de los recursos de la organización.

Auditorías técnicas: auditorías de gestión que se desarrollan en áreas concretas (ambientales, de producción, ingeniería, calidad, etc.).

LA AUTOEVALUACIÓN DE CONTROL - CONTROL SELF ASSESMENT (CSA)

La Autoevaluación de Control o CSA (también se denomina «Autoevaluación de Control/Riesgo» o «CRSA» en inglés) merece una mención especial como tipo de servicio concreto que puede prestar la Auditoría Interna (aunque no exclusivamente, también la gerencia).

Consiste en un proceso a través del cual se examina y evalúa la efectividad del control interno y la razonabilidad de los procesos de gestión de riesgos con el objetivo de proporcionar seguridad razonable sobre el cumplimiento de los objetivos.

Los auditores internos también pueden utilizar esta metodología para obtener información relevante acerca de los riesgos y controles, necesaria para realizar el plan de auditoría basado en riesgos. Esta técnica, además, puede agregar valor a Auditoría Interna incrementando la implicación de las unidades operativas en el diseño y mantenimiento de los sistemas de gestión de riesgos y control, logrando así una mayor colaboración de los gerentes operativos y de sus equipos de trabajo.

En su forma más pura, el CSA permite obtener y comunicar información para mejorar la gestión de riesgos y el control, impulsa la colaboración y cooperación, y ayuda a la gerencia a crear una cultura más abierta y compartida en la organización. Su valor último es ayudar a la gerencia a alcanzar sus objetivos.

Los que emplean esta metodología utilizan una gran cantidad de técnicas y formatos diferentes. No obstante, la mayoría de los programas implantados comparten ciertas características y objetivos clave. En concreto, una organización que utiliza el CSA tendrá un proceso formal y documentado que permita participar de forma estructurada a los directivos y equipos de trabajo y su finalidad será la siguiente:

- Identificar factores de riesgo y exposiciones significativas.
- Evaluar los procesos de control que mitigan o gestionan esos riesgos.
- Desarrollar planes de acción que reduzcan los riesgos a niveles aceptables.
- Determinar la probabilidad de alcanzar los objetivos de negocio o ayudar a que lo sean.

Este sistema se basa fundamentalmente en integrar a los clientes de Auditoría Interna en el proceso de evaluación de control interno, a través de diversos métodos, dependiendo

del sector, el área geográfica, la cultura organizacional, el ambiente de control presente en la organización, etc.

Las tres formas principales de programas de CSA son los talleres de trabajo, las encuestas y los análisis producidos por la Dirección. Las organizaciones a menudo combinan más de un enfoque.

Las encuestas son un método económico para obtener información, especialmente si los participantes son muy numerosos o están muy dispersos como para participar en un taller. En su contra podemos decir que la información es de menor calidad que la obtenida en un taller.

En cuanto a los talleres de trabajo, el papel del auditor interno debe ser exclusivamente el de facilitador/coordinador. En ellos se suele reunir a distintos empleados de áreas concretas de la empresa, seleccionados por Auditoría Interna, para los siguientes aspectos:

- Determinar, entre otras cosas, si los procedimientos de control están funcionando eficazmente y están generando riesgos residuales dentro de un nivel aceptable.
- Analizar la diferencia entre cómo están funcionando los controles y cómo espera la gerencia que funcionen esos controles.
- Y evaluar, actualizar, validar, mejorar e, incluso, dirigir procesos y sus componentes.

Los análisis producidos por la Dirección a menudo tienen la finalidad de lograr un juicio informado y oportuno sobre características específicas de procedimientos de control y son generalmente realizados por un equipo de la organización. El auditor interno puede sintetizar este análisis con otra información para mejorar la comprensión sobre los riesgos y para compartir el conocimiento con los responsables de las unidades de negocio o funcionales, como parte del programa de CSA de la organización.

La participación de Auditoría Interna en los programas de CSA puede ser desde muy significativa, llegando a ser la propietaria de todo el proceso; o mínima, como parte interesada y consultor, o como último verificador de las evaluaciones generadas por los equipos; o puede situarse en un punto intermedio entre los dos extremos anteriores.

Para profundizar en esta metodología la Fundación para la Investigación del Instituto Global (IIA) ha publicado varios manuales al respecto y promueve una certificación sobre esta metodología (CCSA - Certificate in Control Self-Assesment), complementaria del CIA.

2.4 Los roles de Auditoría Interna en el modelo de las Tres Líneas

El Modelo de las Tres Líneas establece una serie de roles clave que deben encontrarse presentes en todas las organizaciones, independientemente de su actividad, estructura y características internas.

A este respecto, se señalan:

ROLES ATRIBUIDOS AL ÓRGANO DE GOBIERNO

- Rinde cuentas ante los *stakeholders* en materia de supervisión general de la organización.
- Adquiere el compromiso con los *stakeholders* para realizar un seguimiento de sus intereses y llevar a cabo una comunicación transparente con ellos sobre el logro de los objetivos.
- Proporciona una cultura que no solamente promueve los comportamientos éticos en la entidad, sino que también promueve la rendición de cuentas de las acciones y actividades desarrolladas.
- Se encarga de establecer las estructuras y procesos de Gobierno de la entidad.
- Delega en la Alta Dirección la responsabilidad de lograr los objetivos propuestos y, para ello, le asigna los recursos necesarios.
- Determina el apetito de riesgo y supervisa la gestión de riesgos.
- Supervisa el grado de cumplimiento de la organización con las expectativas legales, regulatorias y éticas.
- Establece y supervisa una Auditoría Interna independiente, objetiva y competente.

ROLES ASOCIADOS A LA ALTA DIRECCIÓN

- Roles de PRIMERA LÍNEA:
  - Dirigen las acciones necesarias y utiliza los recursos proporcionados por el Órgano de Gobierno para lograr los objetivos de la organización.
  - Mantienen un dialogo periódico con el Órgano de Gobierno para informar sobre los resultados obtenidos en relación con los objetivos de la entidad, así como también de los riesgos asociados.
  - Adoptan estructuras y procesos para la gestión de las operaciones y de sus riesgos.
  - Garantizan el cumplimiento de las expectativas legales, regulatorias y de carácter ético.

- Roles de SEGUNDA LÍNEA:
  - Dan soporte y apoyo en materias relacionadas con la gestión de los riesgos.
  - Analizan e informa sobre la adecuación y grado de eficacia de la gestión de riesgos.

ROLES DE AUDITORÍA INTERNA

- Rinde cuentas ante el Órgano de Gobierno, manteniendo su independencia de las responsabilidades de la Alta Dirección (no debe participar en decisiones de la operativa del negocio).
- Informa a la Alta Dirección y al Órgano de Gobierno sobre el aseguramiento y asesoramiento independiente que proporciona en materias de adecuación y eficacia, tanto del Gobierno de la entidad como de la gestión de riesgos.

ROL ATRIBUIDO A LOS PROVEEDORES EXTERNOS

- Proporciona soporte adicional en dos ámbitos concretos:
  - Protege los intereses de los *stakeholders* en relación con las expectativas legislativas y regulatorias.
  - Complementa los recursos internos de aseguramiento, a petición de la Alta Dirección y del Órgano de Gobierno.

3. El marco normativo de la profesión. *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (MIPP)

El objetivo del MIPP es proporcionar una guía coherente que facilite la interpretación y aplicación de conceptos, metodologías y técnicas fundamentales para la profesión. Delimitando la práctica actual de la Auditoría Interna, y considerando futuras expansiones, el Marco pretende ayudar a los profesionales a satisfacer las necesidades de un mercado que demanda, cada vez más, servicios de Auditoría Interna de alta calidad.

El auditor interno es, cada vez más, uno de los profesionales mejor cualificados dentro de su organización. Y es dentro de este entorno donde el Instituto de Auditores Internos busca homogeneizar la profesión a través del establecimiento del Marco y de la certificación de sus profesionales.

No obstante, al desarrollar su actividad en todo el mundo y en todo tipo de organizaciones, la realidad es que la Auditoría Interna se ejerce en entornos diversos y en empresas de distintos

tamaños, objetos y estructuras. Además, las leyes y costumbres son diferentes en cada país. Todas estas diferencias pueden afectar a la práctica de la Auditoría Interna, y de ellas dependerá en gran medida la implementación del Marco. Esta variará en función del entorno en el que desempeñe sus responsabilidades y tendrá presente que, en ningún caso, la aplicación del Marco puede entrar en conflicto con la legislación vigente.

El Marco se divide fundamentalmente en seis partes, de las cuales las 4 primeras son de aplicación obligada y las dos últimas de aplicación recomendada:

1. Misión y Definición de Auditoría Interna.
2. Código de Ética.
3. Principios Fundamentales para la Práctica Profesional de la Auditoría Interna.
4. Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.
5. Guías de Implementación.
6. Guías Complementarias.

MISIÓN DE AUDITORÍA INTERNA

Articula los objetivos que ésta aspira a alcanzar en la organización. Engloba todo el marco, para demostrar cómo los profesionales de Auditoría Interna deberían apoyarse en su conjunto para tratar de cumplir con la misión.

DEFINICIÓN DE AUDITORÍA INTERNA

Corresponde a la declaración del propósito fundamental, la naturaleza y el alcance de la Auditoría Interna.

CÓDIGO DE ÉTICA

Su propósito es promover una cultura ética en la profesión de Auditoría Interna. Un código ético es necesario en nuestra profesión, cuyos pilares se asientan en la confianza en el aseguramiento objetivo de la gestión de riesgos, control y gobierno de las empresas. (Anexo III).

PRINCIPIOS FUNDAMENTALES

Describen la eficacia de Auditoría Interna. Para que ésta sea considerada eficaz, los principios deben estar presentes y funcionando de forma eficaz. La forma de cumplir con los principios puede ser muy diferente de una organización a otra, pero no cumplir con alguno de ellos implica que una actividad de Auditoría Interna no es tan eficaz como debiera para cumplir su misión.

NORMAS

Constituyen los criterios mediante los cuales el desempeño de un departamento de Auditoría Interna es calificado. Representan cómo debe ser la práctica de la profesión. Están diseñadas para aplicarse en todo tipo de organizaciones donde se pueda encontrar un auditor interno.

GUÍAS DE IMPLEMENTACIÓN

Ayudan a los profesionales en el cumplimiento de las Normas Internacionales. Tratan de forma colectiva el enfoque de Auditoría Interna y la metodología, pero no detallan procesos o procedimientos. Incluyen consideraciones para la implementación de las Normas y demostrar su conformidad con ellas.

GUÍAS COMPLEMENTARIAS

No se vinculan directamente con el cumplimiento de las Normas. Complementan temas de actualidad, asuntos específicos y sectoriales, e incluyen procesos y procedimientos, herramientas y técnicas, programas, enfoques paso a paso y ejemplos de entregables. Forman parte de las Guías Complementarias todas las Guías para la Práctica, Guías del Sector Público, Guías Globales de Auditoría de TI (GTAGs) y Guías para la Evaluación del riesgo de TI.[1]

La importancia de este compendio para la profesión exige una continua revisión y actualización del mismo y este proceso es promovido por el Instituto de Auditores Internos, a través de la continua creación de comisiones de investigación. Además, en todo momento el Instituto mantiene informados a sus asociados de todos los cambios realizados en el Marco Internacional para la Práctica Profesional de la Auditoría Interna a través de su página web y otras vías de comunicación.

3.1 La Misión y la Definición de Auditoría Interna

La misión de Auditoría Interna, según el MIPP, es mejorar y proteger el valor de las organizaciones proporcionando aseguramiento objetivo, asesoría y conocimiento basado en riesgos.

La definición establece que la Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfo-

1. Instituto de Auditores Internos de España. Consulta los documentos de la Práctica Profesional de la Auditoría Interna en español y en inglés

que sistemático y disciplinado para evaluar y mejorar los procesos de gestión de riesgos, control y gobierno.

3.2 El Código de Ética

El propósito del Código de Ética del Instituto es promover una cultura ética en la profesión de Auditoría Interna.

Es necesario y apropiado contar con un código de ética de obligado cumplimiento para la profesión de Auditoría Interna, ya que ésta se basa en la confianza que se imparte a su aseguramiento objetivo sobre la gestión de riesgos, control y dirección.

El código está integrado por componentes esenciales:

A. **Principios relevantes** para la profesión y práctica de la Auditoría Interna.

B. **Reglas de Conducta:** son normas de comportamiento o guías de la conducta ética que deben observar los auditores internos. Son desarrollos prácticos de los Principios que ayudan a interpretarlos, pero que no pueden ser considerados taxativamente. De hecho, el Código especifica que el hecho de que una conducta particular no se halle contenida en las Reglas de Conducta no impide que ésta sea considerada inaceptable o como un descrédito y, en consecuencia, puede hacer que se someta a acción disciplinaria al socio, poseedor de una certificación o candidato a la misma.

Con la expresión "auditores internos", el Código de Ética se refiere a los socios del Instituto, a quienes han recibido –o son candidatos a recibir– certificaciones profesionales del Instituto y, en general, a todos los que presten servicios de Auditoría Interna.

Además, el Código de Ética se aplica no solo a los individuos, sino también a todas las entidades que presten servicios de Auditoría Interna.

Cabe señalar que, en caso de incumplimiento del Código de Ética por los socios del Instituto y por los que han recibido o son candidatos a recibir certificaciones profesionales del Instituto, este será evaluado y administrado de conformidad con los Estatutos y Reglamentos Administrativos del Instituto.

A. PRINCIPIOS

Se espera que los auditores internos apliquen y cumplan los siguientes principios:

· **Integridad.**La integridad de los auditores internos establece confianza y aporta la base para confiar en su juicio.

· **Objetividad.** Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso que va a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por otras personas.

· **Confidencialidad.** Los auditores internos respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización, a menos que exista una obligación legal o profesional para hacerlo.

· **Competencia.** Los auditores internos aplican el conocimiento, aptitudes y experiencia necesarios al desempeñar los servicios de Auditoría Interna.

B. REGLAS DE CONDUCTA

· Integridad

- Los auditores internos desempeñarán su trabajo con honestidad, diligencia y responsabilidad.
- Respetarán las leyes y divulgarán lo que corresponda de acuerdo con la ley y la profesión.
- No participarán a sabiendas en una actividad ilegal o de actos que vayan en detrimento de la profesión de Auditoría Interna o de la organización.
- Respetarán y contribuirán a los objetivos legítimos y éticos de la organización.

· Objetividad

- Los auditores internos no participarán en ninguna actividad o relación que pueda perjudicar o aparentemente perjudicar su evaluación imparcial. Esta participación incluye aquellas actividades o relaciones que puedan estar en conflicto con los intereses de la organización.
- No aceptarán nada que pueda perjudicar o aparentemente perjudicar su juicio profesional.
- Divulgarán todos los hechos materiales que conozcan y que, de no ser divulgados, pudieran distorsionar el informe de las actividades sometidas a revisión.

· Confidencialidad

- Los auditores internos serán prudentes en el uso y protección de la información adquirida en el transcurso de su trabajo.

- No utilizarán información para lucro personal o que de alguna manera fuera contraria a la ley o en detrimento de los objetivos legítimos y éticos de la organización.

· Competencia

- Los auditores internos participarán sólo en aquellos servicios para los cuales tengan los suficientes conocimientos, aptitudes y experiencia.
- Desempeñarán todos los servicios de Auditoría Interna de acuerdo con las Normas para la Práctica Profesional de Auditoría Interna.
- Mejorarán continuamente sus habilidades y la efectividad y calidad de sus servicios.

3.3 Los Principios Fundamentales para la Práctica Profesional de la Auditoría Interna

Los Principios Fundamentales, tomados en su conjunto, articulan la efectividad de la Auditoría Interna. Para que ésta sea eficaz, todos los Principios deben estar presentes y operar de forma efectiva. La manera en la que un auditor interno o la actividad de Auditoría Interna demuestran la efectividad de los Principios Fundamentales puede ser muy diferente de una organización a otra, pero el fracaso en el logro de cualquiera de los Principios implicaría que una actividad de Auditoría Interna no es todo lo efectiva que podría ser para el logro de la misión.

Auditoría Interna:

· Demuestra integridad.

· Demuestra competencia y diligencia profesional.

· Es objetiva y se encuentra libre de influencias (independiente).

· Se alinea con las estrategias, los objetivos y los riesgos de la organización.

· Está posicionada de forma apropiada y cuenta con los recursos adecuados.

· Demuestra compromiso con la calidad y la mejora continua de su trabajo.

· Se comunica de forma efectiva.

· Proporciona aseguramiento en función de los riesgos.

· Hace análisis profundos, es proactiva y está orientada al futuro.

· Promueve la mejora de la organización.

3.4 Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna

Las Normas, junto con el Código de Ética, son los elementos de cumplimiento obligatorio del MIPP.

Consisten en:

- Declaraciones de requisitos esenciales para el ejercicio de la Auditoría Interna y para evaluar la eficacia de su desempeño. Son internacionalmente aplicables a nivel de las personas y a nivel de las organizaciones.
- Interpretaciones que aclaran términos o conceptos dentro de las Normas.

El propósito de las Normas es:

- Orientar en la adhesión a los elementos obligatorios del Marco Internacional para la Práctica Profesional de la Auditoría Interna.
- Proporcionar un marco para ejercer y promover un amplio rango de servicios de Auditoría Interna de valor añadido.
- Establecer las bases para evaluar el desempeño de la Auditoría Interna.
- Fomentar la mejora de los procesos y operaciones de la organización.

Para comprender y aplicar las Normas correctamente, es necesario tener en cuenta los términos incluidos en el glosario del MIPP. Por ejemplo, en las Normas se diferencia entre la palabra "debe" y la palabra "debería": la primera se utiliza para indicar total obligatoriedad, y la segunda implica la aplicación del juicio profesional.

Las Normas se aplican a los auditores internos individualmente y a la actividad de Auditoría Interna. Todos los auditores internos son responsables de cumplir las Normas relacionadas con la objetividad, aptitud, cuidado profesional y las relevantes para el desempeño de su trabajo. Y los Directores de Auditoría Interna, además, son responsables de que la actividad de Auditoría Interna, en su conjunto, cumpla las Normas.

En el caso de que los auditores internos o la actividad de Auditoría Interna no puedan cumplir con ciertas partes de las Normas por impedimentos legales o de regulaciones, deberán cumplir todas las demás partes y efectuar la correspondiente declaración.

Las Normas se conforman en dos categorías principales:

- **Normas sobre Atributos y sobre Desempeño.**

  Las Normas sobre Atributos tratan las características de las organizaciones y las personas que prestan servicios de Auditoría Interna. Las Normas sobre Desempeño describen la naturaleza de los servicios de Auditoría Interna y proporcionan criterios de

calidad con los cuales puede evaluarse el desempeño de estos servicios. Ambas normas se aplican a todos los servicios de Auditoría Interna.

- Normas de Implantación

  Amplían las de Atributos y Desempeño, proporcionando los requisitos aplicables a los servicios de aseguramiento (A) y consultoría (C).

La elaboración y revisión de las Normas es un proceso continuo. El Comité de Normas Internacionales de Auditoría Interna realiza un extenso proceso de consulta y debate antes de emitir las Normas. Esto incluye la solicitud de comentarios en todo el mundo mediante el proceso de borrador de exposición. Todos los borradores de exposición se incluyen en la página web del Instituto Global de Auditores Internos (IIA) además de ser distribuidos a todos los Institutos de Auditores Internos locales.

4. Organizaciones profesionales de Auditoría Interna

4.1 Instituto de Auditores Internos de España (IAI)

El Instituto de Auditores Internos de España (IAI) es la organización que aglutina a los profesionales de la Auditoría Interna en España. Se constituyó el 29 de septiembre de 1983 y fue reconocido como miembro oficial del Global Institute of Internal Auditors el 29 de noviembre del mismo año con el número 200.

Es una asociación profesional sin ánimo de lucro que da servicio a cerca de 4.000 auditores internos de las principales empresas e instituciones, de todos los sectores económicos del país, bajo el lema de "Progresar Compartiendo".

Actúa como portavoz de la profesión de la Auditoría Interna ante instituciones nacionales e internacionales, otros organismos y medios de comunicación. Difunde en nuestro país las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna y proporciona formación, información y oportunidades de encuentro a sus socios sobre todos los aspectos relacionados con el trabajo diario del auditor interno.

Forma parte de la red internacional Global IIA, en la que se sitúa como uno de los 10 primeros del mundo. También forma parte de la Confederación Europea de Institutos de Auditores Internos (ECIIA en sus siglas en inglés) y mantiene frecuentes contactos con asociaciones similares de Iberoamérica para colaborar, asesorar o compartir documentos.

La misión del Instituto español es contribuir al éxito de las organizaciones impulsando la profesión como función clave del buen gobierno. Su visión es promover la profesión mediante la excelencia en el servicio a los profesionales y las organizaciones, la innovación constante en las actividades de aseguramiento y asesoría y la transmisión del valor y la relevancia de la función a los grupos de interés. Y sus valores son la independencia, la integridad, la innovación, la colaboración, la competencia profesional y la orientación al socio.

Pueden ser socios del Instituto todas las personas físicas y jurídicas que tengan interés en el desarrollo de su misión y fines, y se comprometan a cumplir el Código de Ética del MIPP, anteriormente expuesto.

4.2 Confederación Europea de Institutos de Auditoría Interna (ECIIA)

La Confederación Europea de Institutos de Auditoría Interna (ECIIA) aglutina a los Institutos de Auditores Internos de 34 países de Europa e Israel, con la misión fundamental de promover y desarrollar el ejercicio y la práctica de Auditoría Interna.

Sus objetivos son:

- Intercambiar conocimientos y experiencias entre sus miembros para estimular el cumplimiento de las normas profesionales de Auditoría Interna.
- Lograr la institucionalización de la función de Auditoría Interna como garantía de transparencia y buen gobierno corporativo de las organizaciones.
- Informar y divulgar en toda Europa la profesión de auditor interno y sus exigencias de formación y cualificación.
- Llevar a cabo estudios, análisis, conferencias y actos de todo tipo sobre la Auditoría Interna entendida como profesión.
- Mantener una continua corriente de comunicación con la comunidad europea.
- Apoyar a la profesión de auditor interno, en general, y relacionarse con otras organizaciones profesionales para la defensa de los auditores internos europeos y su integración profesional.

La ECIIA como tal desarrolla proyectos para enriquecer la profesión en el ámbito europeo y, anualmente, organiza una reunión internacional en uno de los países miembros. Esta reunión anual toma el nombre de Conferencia Europea de Institutos de Auditoría Interna.

4.3 The Global Institute of Internal Auditors (Global IIA)

The Global Institute of Internal Auditors (Global IIA), creado en 1941 y con sede en Lake Mary (Florida - EEUU), es la red internacional de auditores internos, que aglutina a más de 200.000 asociados en casi 200 países y tiene asociados cerca de 200 institutos locales en las principales áreas metropolitanas de los cinco continentes.

Podemos decir que el Global IIA es el portavoz de la profesión de Auditoría Interna en el mundo, autoridad y líder reconocido a nivel mundial, representante y defensor de la profesión, y principal formador de la misma.

Su misión es proporcionar un liderazgo dinámico para la profesión global de Auditoría Interna a través de las siguientes actividades (entre otras):

- Apoyar y promover el valor que los profesionales de Auditoría Interna aportan a sus organizaciones.
- Ofrecer oportunidades educativas y de desarrollo profesional integral, estándares y otras guías de práctica profesional y programas de certificación.
- Investigar, difundir y promover el conocimiento sobre la Auditoría Interna y su papel en el control, la gestión de riesgos y la gobernanza para los profesionales y las partes interesadas.
- Formar los profesionales y otras instancias relevantes en las mejores prácticas de Auditoría Interna.
- Crear redes de relación entre los auditores internos de todos los países para compartir información y experiencias.

Entre las actividades señaladas, remarcamos que el Instituto Global es el que actualiza, somete a consulta y aprueba el Marco Internacional para la Práctica Profesional de la Auditoría Interna por el que se guían los auditores internos de todo el mundo. Además, publica periódicamente declaraciones sobre Auditoría Interna, que actualizan el concepto de la profesión, su alcance y contenido funcional.

El Instituto Global cuenta con una Fundación de Investigación en Auditoría Interna dedicada a estudiar nuevas tendencias en el campo de la Auditoría Interna, favorecer estudios y grupos de trabajo, financiar becas y donaciones para ayudas de estudiantes, y subvencionar a las universidades y escuelas de negocios que tienen establecidos programas y cursos de especialización en Auditoría Interna.

Por último, indicamos como dato relevante que el Instituto Global ha determinado que el mes de mayo sea el mes de la concienciación sobre la importancia de la Auditoría Interna, celebrándolo con distintas actividades cada año y el siguiente logo.

El Control Interno

Instituto de Auditores Internos de España

1. Control, control interno y Auditoría Interna

Las Normas precisan en su glosario que el término "control" se refiere a cualquier acción tomada por la dirección de una organización, el Consejo y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidas. La Dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas.

En el mismo glosario se especifica que un "control adecuado" es el que está presente si la Dirección ha planificado y organizado (diseñado) las operaciones de manera tal que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica.

La palabra control se puede afinar con distintos adjetivos y complementos que sitúan la acción de controlar en distintas áreas o actividades. De esta forma podemos hablar de control administrativo, control de gestión, control contable, control de tecnología de la información, control financiero, etc. Todos estos tipos de controles, en su conjunto, constituyen el "sistema global de control" de una organización que podemos definir como el sistema de control de la organización cuyos componentes se relacionan entre sí con la finalidad común de alcanzar los objetivos establecidos por el Consejo de Administración y la Dirección.

El sistema global de control, como todo sistema de control, debe cumplir una serie de requisitos. Son los siguientes:

- Analizar y tener en cuenta la relación coste/beneficio.
- Tener capacidad de detectar con rapidez y precisión posibles desviaciones.
- Suministrar la información a los niveles adecuados para la toma de decisiones.
- Informar sobre las causas que producen las distintas situaciones.
- Ser flexible y de fácil comprensión.
- Ajustarse a las características y a la gestión de la organización.
- Respetar a las personas.

Al control general o global de una organización se le denomina "control interno" en contraposición a los controles externos que tienen origen fuera de la misma, como las leyes, reglamentos y regulaciones de todo tipo que la afectan.

La expresión control interno fue empleada por vez primera en 1949 en un estudio del American Institute of Certified Public Accountants (AICPA), titulado *Control interno: elementos de un sistema coordinado y su importancia para la dirección y los auditores externos.* Desde entonces, el término ha sido utilizado por los auditores internos para describir el conjunto de controles

existentes en un sistema, operación, actividad o unidad funcional de gestión, y para evaluarlos y ayudar a la organización en su mejora continua.

En concreto, la *Norma 2130-Control* establece que la actividad de Auditoría Interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua. Para implementar esta norma, de obligado cumplimiento, el MIPP recomienda la *Guía de Implementación 2130* cuya lectura completa recomendamos y de la que podemos subrayar los puntos siguientes:

El Director de Auditoría Interna y toda la actividad de Auditoría Interna deben demostrar que conocen los procesos de control de la organización, alertar a la Dirección sobre nuevas cuestiones de control y proporcionar recomendaciones y planes de acción que incluyan la implantación de acciones correctivas y su supervisión. La actividad de Auditoría Interna debe obtener suficiente información como para evaluar la eficacia de los procesos de control de la organización.

- Una evaluación competente de la eficacia de los controles debe incluir la evaluación de los controles en el contexto de los riesgos que pueden afectar al cumplimiento de objetivos en todos esos niveles. Para realizar estas evaluaciones, el auditor interno puede encontrar útil emplear una matriz de riesgos y controles que puede ayudar a la actividad de Auditoría Interna a:
  - Identificar los objetivos y los riesgos que pueden afectar a su logro.
  - Medir la gravedad de los riesgos, teniendo en cuenta el impacto y la probabilidad.
  - Comprobar que se da la respuesta apropiada a los riesgos significativos (p.ej. aceptar, seguir, mitigar, transferir o evitar).
  - Comprobar los controles clave que la Dirección utiliza para gestionar riesgos.
  - Evaluar la idoneidad del diseño de los controles para poder determinar si es apropiado realizar una prueba de la eficacia de los controles.
  - Probar controles que se considera que han sido diseñados adecuadamente, para evaluar si están realmente operando como se pretende.
- Al utilizar una matriz de riesgos y controles, la actividad de Auditoría Interna puede encontrar útil entrevistar a la Dirección; revisar los planes, las políticas y los procesos de la organización; emplear pruebas, encuestas, cuestionarios y flujogramas para obtener información sobre la idoneidad del diseño del control; y realizar inspecciones, conciliaciones, auditorías continuas y análisis de datos para probar la efectividad del control.
- Para evaluar la eficiencia de los controles, la actividad de Auditoría Interna habitualmente revisa si la Dirección mide y supervisa los costes y beneficios de los controles. Esto supone identificar si los recursos empleados en los procesos de control exceden de los beneficios, y si los

procesos de control provocan problemas importantes al negocio (p.ej. errores, retrasos o duplicación de trabajo).

- También puede ser útil para los auditores internos evaluar si el nivel de un control es adecuado para el riesgo que pretende controlar. Una herramienta que muchos auditores internos utilizan para documentar visualmente esta relación entre riesgos y controles es el mapa de riesgos y controles, en el que se señala gráficamente la gravedad del riesgo en relación con la eficacia del control.

El Director de Auditoría Interna puede recomendar la implementación de un marco de control si la organización no utiliza ninguno. Adicionalmente, los auditores internos pueden realizar recomendaciones que mejoren el entorno de control (p.ej. una pauta ética dada desde el máximo órgano de gobierno *–tone at the top–* que promueva una cultura del comportamiento ético y una baja tolerancia a los incumplimientos).

La actividad de Auditoría Interna puede dar pasos adicionales para promover una mejora continua de la efectividad del control con las acciones siguientes:

- Proporcionando formación sobre controles y procesos de autoevaluación continua.
- Impartiendo a la dirección sesiones sobre evaluación del control (o de riesgos y controles).
- Ayudando a la Dirección a establecer una estructura lógica para documentar, analizar y evaluar el diseño y la ejecución de los controles de la organización.
- Ayudando a desarrollar un proceso para identificar, evaluar y remediar deficiencias de control.
- Ayudando a la Dirección a mantenerse al tanto de nuevos problemas, leyes y regulaciones relacionadas con obligaciones de control.
- Supervisando los avances tecnológicos que pueden mejorar la eficiencia y la eficacia del control.

2. COSO: el Informe "Control Interno - Marco Integrado" *(el Marco)*

2.1 COSO y el objetivo de mejorar el control interno

Desde que en 1992 el *Committee of Sponsoring Organizations of the Treadway Commission* publicara el primer informe *COSO – Marco Integrado de Control Interno,* se viene reconociendo en el mundo su liderazgo a la hora de proporcionar herramientas para de-

sarrollar, fortalecer y mantener un marco de control interno eficaz y eficiente que ayude a todo tipo de organizaciones a cumplir sus objetivos.

Este informe ha pasado por distintas actualizaciones hasta el documento actual denominado *Control Interno - Marco Integrado* (en adelante *el Marco),* siempre con el fin de adaptarse a los cambios habidos tanto en las organizaciones y en su entorno operativo y de negocio, cada día más complejo, global y tecnológico, como en sus grupos de interés más conscientes y comprometidos. Hoy por hoy es una publicación de referencia para todos aquellos profesionales con responsabilidades en los sistemas de control interno que apoyan la toma de decisiones y el buen gobierno corporativo de las organizaciones.

El objetivo del *Marco* es ayudar a la dirección a mejorar el control en la organización, así como proporcionar al Consejo de Administración herramientas adicionales para mejorar la capacidad para supervisarlo. El sistema de control interno permite que la Dirección oriente sus esfuerzos en la consecución de los objetivos operativos y desempeño financieros de la organización, mientras opera de acuerdo con los límites establecidos en la legislación aplicable y minimiza sorpresas que puedan surgir. El control interno permite que una organización gestione con mayor eficacia los cambios que se produzcan dentro del entorno económico y competitivo, la Dirección de la organización, así como sus prioridades y modelos de negocio cambiantes.

2.2 El control interno según *el Marco*

El Marco define el control interno de la siguiente forma:

> *El control interno es un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable para la consecución de los objetivos relativos a las operaciones, a la información y al cumplimiento.*

Esta definición de control interno es intencionadamente amplia para posibilitar su aplicación a diferentes tipos de organizaciones, sectores y zonas geográficas, y también para que pueda implementarse en los distintos subapartados del control interno.

De esta forma, las organizaciones podrán centrarse de forma independiente, por ejemplo, en el control interno sobre la información financiera o en los controles relativos al cumplimiento de las leyes y regulaciones. De igual manera, podrán enfocarse en los controles de unidades de negocio concretas o actividades específicas de una organización.

Asimismo, esta definición permite una aplicación flexible para que una organización pueda implantar un sistema de control interno en toda la organización en su conjunto, o solamente a nivel de filial, división o unidad operativa, o función relevante, dependiendo de sus necesidades o circunstancias específicas.

Cabe señalar, además, que esta definición hace hincapié en determinados aspectos del control interno que los señalamos a continuación:

- Está orientado a la consecución de objetivos en una o más categorías separadas, pero con áreas comunes (operaciones, información y cumplimiento).
- Es un proceso que consta de tareas y actividades continuas; es un medio para llegar a un fin, y no un fin en sí mismo.
- Es llevado a cabo por las personas, no se trata solamente de manuales, políticas, sistemas y formularios, sino de personas y de las acciones que éstas aplican en cada nivel de la organización para desarrollar el control interno.
- Es capaz de proporcionar aseguramiento razonable, pero no seguridad absoluta, al Consejo y a la Alta Dirección de la organización.
- Es adaptable a la estructura de la organización, flexible para su aplicación al conjunto de la organización o a una filial, división, unidad operativa o proceso de negocio en particular.

Además de definir el control interno, *el Marco* establece que el sistema de control interno se compone de un total de **5 componentes** y **17 principios,** que recogen los conceptos fundamentales relacionados con cada componente. Los componentes son los siguientes:

- Entorno de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Actividades de supervisión.

Estos componentes son relevantes tanto para el conjunto de la organización, como para sus distintos niveles: sus filiales, divisiones, o cualquiera de sus unidades operativas, funciones, u otras subdivisiones que existan en la organización.

Existe una relación directa entre los objetivos (lo que una organización se esfuerza por lograr), los componentes (lo que se necesita para lograr los objetivos), y la estructura de la organización (las unidades operativas, entidades jurídicas y demás estructuras). La relación puede ser representada en forma de cubo.

A continuación, definimos los 5 COMPONENTES del control interno:

Entorno de Control
El entorno de control es el conjunto de normas, procesos y estructuras que constituyen la base sobre la que se desarrolla el sistema de control interno de la organización. El Consejo y la Alta Dirección son quienes establecen el Tone at the top sobre la importancia del control interno y las normas de conducta esperables.

Evaluación de Riesgos
La evaluación de riesgos implica un proceso dinámico e iterativo que se realiza para identificar y analizar los riesgos asociados al logro de los objetivos de la organización. Este proceso es la base que determina la forma de gestionar dichos riesgos. La Dirección tiene en cuenta los posibles cambios que pueden darse en el entorno externo, o en el propio modelo de negocio, que pueden impedir su capacidad para lograr los objetivos.

Actividades de Control
Las actividades de control son las acciones, establecidas por políticas y procedimientos que contribuyen a garantizar que se cumplen las instrucciones que da la Dirección para mitigar los riesgos que pueden afectar a la consecución de los objetivos. Las actividades de control se realizan en todos los niveles de la organización, en las diferentes etapas de los procesos de negocio y también en el entorno tecnológico.

Información y Comunicación
La información es necesaria para que la organización pueda desarrollar las responsabilidades de control interno que respaldan la consecución de sus objetivos. La comunicación se produce tanto interna como externamente, y proporciona a la organización la información necesaria para realizar los controles que forman parte del día a día de la organización. La comunicación permite a las personas comprender sus responsabilidades relacionadas con el del sistema de control interno y su importancia para lograr los objetivos.

Actividades de Supervisión
Las evaluaciones continuas, las evaluaciones aisladas o una combinación de ambas sirven para determinar si cada uno de los cinco componentes del sistema de control interno

–incluidos los controles para cumplir los principios de cada componente– están presentes y funcionan adecuadamente en la organización. Los hallazgos se evalúan y las deficiencias se comunican de forma oportuna, mientras que los asuntos más graves se reportan a la alta dirección y al consejo.

Estos cinco componentes son desarrollados en *el Marco* por 17 PRINCIPIOS que recogemos a continuación.

Entorno de Control

1. La organización muestra su compromiso con la integridad y los valores éticos.
2. El Consejo de Administración es independiente de la Dirección y supervisa el desarrollo y la ejecución del sistema de control interno.
3. La Dirección determina, con la supervisión del Consejo, las estructuras, las líneas de reporte y los niveles de responsabilidad y las funciones apropiadas para lograr los objetivos.
4. La organización muestra su compromiso por atraer, desarrollar y retener a profesionales competentes alineados con los objetivos de la organización.
5. La organización está integrada por profesionales que rinden cuentas por sus responsabilidades de control interno, ejercidas como parte del proceso de lograr sus objetivos.

Evaluación de Riesgos

6. La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.
7. La organización identifica los riesgos asociados a la consecución de sus objetivos en todos los niveles y los analiza para poder decidir cómo se deben gestionar.
8. La organización considera la probabilidad de fraude al evaluar los riesgos asociados a la consecución de los objetivos.
9. La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.

Actividades de Control

10. La organización selecciona y desarrolla actividades de control que contribuyen a la mitigación de los riesgos a niveles aceptables para lograr sus objetivos.
11. La entidad selecciona y desarrolla controles generales de tecnología para respaldar el logro de objetivos.
12. La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno, y de los procedimientos que ponen en práctica dichas políticas.

Información y Comunicación

13. La organización obtiene o genera y utiliza información relevante y de calidad para respaldar el funcionamiento del control interno.
14. La organización comunica la información internamente, incluidos los objetivos y las responsabilidades, por ser necesario para respaldar el funcionamiento del sistema de control interno.
15. La organización habla con los grupos de interés externos de los aspectos clave que afectan al funcionamiento del control interno.

Actividades de Supervisión

16. La organización selecciona, desarrolla y realiza evaluaciones continuas y/o puntuales para comprobar si los componentes del sistema de control interno están presentes y en funcionamiento.
17. La organización evalúa y comunica las deficiencias de control interno en el momento oportuno a los responsables de aplicar las medidas correctivas, incluyendo la Alta Dirección y el Consejo, según corresponda.

2.3 El papel de la Auditoría Interna en las actividades de Supervisión del *Marco*

Como indicamos anteriormente, Auditoría Interna debe evaluar la eficacia y eficiencia de los controles y promover la mejora continua del sistema de control interno *(Norma 2130),* obligación que tiene presente *el Marco* cuando desarrolla el concepto "Supervisión" y su principio asociado (16). Este principio se refiere a Auditoría Interna como posible proveedor de **evaluaciones independientes.**

En concreto, *el Marco* indica lo siguiente:

> *Las evaluaciones independientes a menudo son realizadas por el equipo de Auditoría Interna. Tener esta función, si bien es cierto que no es un requisito del control interno, es evidente que puede mejorar el alcance, la frecuencia y la objetividad de dichas revisiones […]*

Las evaluaciones independientes pueden incluir las **Evaluaciones de Auditoría Interna.** Los auditores internos son a menudo recursos objetivos y competentes, tanto si son empleados de la propia organización como profesionales externos. Y suelen realizar evaluaciones puntuales en el marco de sus obligaciones ordinarias, o previa solicitud específica de la Alta Dirección o del Consejo de Administración. Por lo general, cada año la función de Auditoría Interna desarrolla un plan de auditoría interna con proyectos seleccionados

siguiendo un enfoque de riesgos, alineado con los objetivos de la organización y las prioridades de los grupos de interés. Por ejemplo, las áreas de revisión pueden incluir el cumplimiento del código de conducta, el diseño del proceso de evaluación de riesgos, informes sobre la calidad de los datos, informes sobre transacciones y controles específicos, sobre cumplimiento de leyes y regulaciones aplicables, y sobre si se mantienen determinados estándares de calidad. Los informes se distribuyen a la Alta Dirección, al Consejo o a su Comisión de Auditoría, y a otros destinatarios que puedan tomar decisiones sobre las recomendaciones incluidas en los informes.

Auditoría Interna no sólo interviene en auditorías del área financiera, también puede realizar auditorías de seguridad, calidad, y medioambientales, entre otras.

Expuesto todo lo anterior, no hay que perder de vista que en este capítulo se han presentado muy brevemente los principales aspectos del Informe *Control Interno - Marco Integrado* con el único fin de dar a conocer su existencia y la relevancia que tiene este documento para los profesionales de la Auditoría Interna. No obstante, esta breve referencia debería completarse con una lectura reflexiva y en profundidad del informe completo.

Además, el profesional que esté interesado en acreditar sus conocimientos y experiencia en este ámbito puede obtener a través del IAI la certificación global en Control Interno avalada y ofrecida por los miembros de COSO.

La Gestión de Riesgos. COSO ERM

1. La gestión de riesgos como enfoque de COSO
2. El *Marco ERM* como estructura conceptual básica
3. Componentes y Principios del *Marco ERM*
4. Conclusión

Instituto de Auditores Internos de España

1. La gestión de riesgos como enfoque de COSO

Tras el éxito obtenido por el informe COSO de 1992, el organismo observó la tendencia por parte de los *stakeholders* de conceder a la gestión del riesgo un valor cada vez más relevante como pieza clave en la creación de valor de las organizaciones.

Ello hace pensar a COSO en la necesidad de un marco integrado de gestión de riesgos corporativos que defina las pautas y conceptos fundamentales, así como una terminología común en esta área. Este nuevo informe se publica en 2004 bajo el nombre de *Gestión de Riesgos Corporativos. Marco Integrado*, que logró una amplia aceptación en todo el mundo y en toda clase de organizaciones al ser visto como una ayuda fundamental para gestionar sus riesgos.

No obstante, los cambios habidos en la complejidad del riesgo y su continua evolución, así como el mayor conocimiento por parte de los Consejos de Administración y equipos directivos relacionados con la supervisión de la gestión del riesgo y su mayor demanda de información sobre este tema, hicieron conveniente actualizar el documento de 2004 en una nueva versión que pusiera de manifiesto la importancia de tener en cuenta el riesgo tanto en el proceso de definición de la estrategia como en la ejecución del desempeño. El resultado es el documento publicado en 2017 bajo el nombre de *Gestión de Riesgo Empresarial - Integrando Estrategia y Desempeño,* informe al que nos referiremos como *Marco ERM.*

Esta publicación es distinta y complementaria de la referida en el capítulo anterior, *Control Interno - Marco Integrado* de COSO, enfocada en el control interno y adecuada para diseñar, implantar, llevar a cabo y evaluar el sistema de control interno y para presentar informes posteriores.

2. El *Marco ERM* como estructura conceptual básica

El *Marco ERM* se enfoca más en el objetivo de ayudar a las organizaciones a gestionar sus riesgos de forma óptima, ofreciéndoles una estructura conceptual básica bajo la premisa de que todas las entidades afrontan riesgos en su búsqueda del valor y esos riesgos afectan a su capacidad de lograr la estrategia y los objetivos de negocio.

La primera parte del *Marco ERM* se centra en los conceptos y las aplicaciones relevantes en el ámbito de la gestión del riesgo empresarial, y la segunda parte desarrolla cinco componentes fáciles de comprender que mejoran las estrategias y la toma de decisiones, y pueden adaptarse a estructuras operativas y puntos de vista diversos.

En concreto la primera parte del *Marco ERM* aborda y desarrolla los siguientes aspectos:

DEFINICIÓN DE RIESGO E INCERTIDUMBRE

La estrategia y los objetivos de negocio de una entidad pueden verse afectados por potenciales eventos. La falta de previsibilidad completa existente en torno a que se materialice (o no) un evento y su impacto relacionado generan incertidumbre para cualquier organización. Existirá incertidumbre para cualquier entidad que se proponga alcanzar futuras estrategias y objetivos de negocio.

En este contexto, el riesgo se define como la posibilidad de que ocurran eventos y afecten a la consecución de la estrategia y a los objetivos de negocio.

Términos que amplían y respaldan la definición de riesgo.

- **Evento**. Acto o conjunto de actos que se materializan.
- **Incertidumbre.** El estado de no saber si los eventos potenciales pueden manifestarse o cómo pueden hacerlo.
- **Gravedad.** Medida que valora consideraciones tales como la probabilidad y el impacto generado por determinados eventos o el tiempo que se tarda en recuperarse de ellos.

DEFINICIÓN DE LA GESTIÓN DEL RIESGO EMPRESARIAL

La gestión del riesgo empresarial se define en la presente publicación como:

> *La cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo de cara a la creación, preservación y materialización de valor.*

Una mirada más en profundidad a la definición de la gestión del riesgo empresarial hace hincapié en su enfoque en la gestión del riesgo a través de:

- El reconocimiento de la cultura.
- El desarrollo de las capacidades.
- Las técnicas aplicadas.
- La integración de la estrategia establecida y el desempeño.
- La gestión del riesgo y su alineación con la estrategia y los objetivos de negocio.
- La relación con el valor.

ESTRATEGIA Y GESTIÓN DEL RIESGO EMPRESARIAL

La gestión del riesgo empresarial ayuda a una organización a comprender mejor:

- Cómo la misión, la visión y los valores clave forman la expresión inicial de qué tipo y nivel de riesgo es aceptable considerar al establecer la estrategia.

- La posibilidad de que la estrategia y los objetivos de negocio no estén alineados con la misión, visión y valores clave.
- El tipo y nivel de riesgo al que la organización se expone potencialmente al elegir una estrategia en particular.
- El tipo y el nivel de riesgo inherente a la ejecución de su estrategia y al logro de los objetivos de negocio y a la aceptabilidad de este nivel de riesgo, y en última instancia, del valor.

GESTIÓN DEL RIESGO EMPRESARIAL Y DESEMPEÑO

La evaluación del riesgo con respecto a la estrategia y los objetivos de negocio requiere que una organización comprenda la relación entre el riesgo y el desempeño, lo que en este Marco se denomina "perfil de riesgo". El perfil de riesgo de una entidad proporciona una visión global de los riesgos en relación con un nivel específico de la entidad (por ejemplo, a nivel corporativo, a nivel de unidad de negocio, a nivel funcional) o un aspecto del modelo de negocio (por ejemplo, producto, servicio, geografía).

LA IMPORTANCIA DE LA INTEGRACIÓN DE LA GESTIÓN DEL RIESGO EMPRESARIAL

La integración de la gestión del riesgo empresarial con las actividades y procesos del negocio se traduce en una mejor información que respalda la toma de decisiones y conduce a un mejor desempeño. Además, ayuda a las organizaciones a:

- Anticiparse a los riesgos antes o de manera más explícita, abriendo más opciones para gestionar los riesgos y minimizar el potencial de desviaciones en el desempeño, pérdidas, incidentes o fallos.
- Identificar y perseguir las oportunidades existentes y nuevas de acuerdo con el apetito de riesgo y la estrategia de la entidad.
- Comprender y responder a las desviaciones en el desempeño de manera más rápida y coherente.
- Desarrollar y reportar una visión más integrada y coherente del riesgo a nivel de cartera, permitiendo así que la organización asigne mejor los recursos limitados.
- Mejorar la colaboración, la confianza y el intercambio de información en toda la organización.

3. Componentes y Principios del *Marco ERM*

Como ya se ha expuesto, la segunda parte del Marco ERM desarrolla los cinco componentes que se interrelacionan con la gestión del riesgo empresarial y los principios que los integran.

La figura siguiente, denominada modelo de doble hélice, muestra estos componentes y su relación con la misión, visión y valores clave de la entidad. Las tres cintas del diagrama de Establecimiento de la Estrategia y de los Objetivos, Desempeño, y Revisión y Monitorización, representan los procesos más habituales que fluyen a través de la entidad. Las otras dos cintas, Gobierno y Cultura, e Información, Comunicación y Reporte, representan aspectos de apoyo a la gestión del riesgo empresarial.

La figura ilustra además que, cuando la gestión del riesgo empresarial se integra en el desarrollo de la estrategia, la formulación de objetivos de negocio y la ejecución y el desempeño puede aumentar el valor.

La gestión del riesgo empresarial no es estática. Se integra en el desarrollo de la estrategia, la formulación de objetivos de negocio y la implantación de esos objetivos a través de la toma de decisiones diarias.

Los cinco componentes son:

GOBIERNO Y CULTURA

El gobierno y la cultura forman conjuntamente una base para todos los demás componentes de la gestión del riesgo empresarial. El gobierno marca el tono en la entidad, reforzando la importancia de la gestión del riesgo empresarial y estableciendo responsabilidades de supervisión al respecto. La cultura se refleja en la toma de decisiones.

ESTABLECIMIENTO DE LA ESTRATEGIA Y DE LOS OBJETIVOS

La gestión del riesgo empresarial se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos de negocio. Con un conocimiento profundo del contexto empresarial, la organización puede comprender mejor los factores internos y externos y sus efectos en el riesgo. Una organización fija su apetito al riesgo en conjunción con la definición de estrategias. Los objetivos de negocio permiten poner en práctica la estrategia y configurar las operaciones y prioridades diarias de la entidad.

DESEMPEÑO

Una organización identifica y evalúa los riesgos que pueden afectar a la capacidad de una entidad para alcanzar la estrategia y los objetivos de negocio. Como parte de esa búsqueda, la organización identifica y evalúa los riesgos que pueden afectar a la consecución de dicha estrategia y los objetivos de negocio.

Prioriza los riesgos en función de su gravedad y teniendo en cuenta el apetito de riesgo de la entidad. La organización entonces selecciona las respuestas al riesgo y efectúa un seguimiento del desempeño considerando posibles cambios. De esta forma, desarrolla una visión de cartera sobre el nivel de riesgo que la entidad ha asumido para cumplir con su estrategia y conseguir los objetivos de negocio a nivel de entidad.

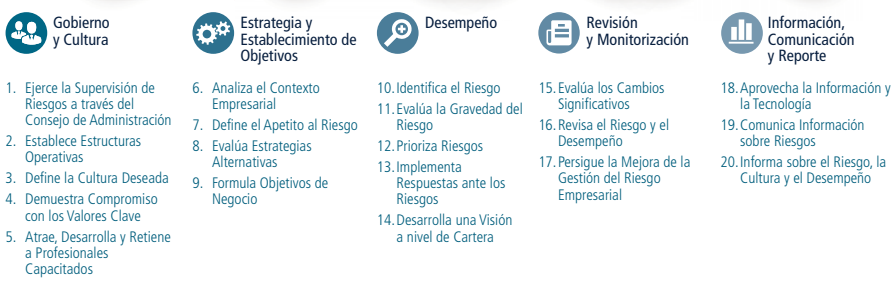
REVISIÓN Y MONITORIZACIÓN

Al examinar las capacidades y técnicas de gestión del riesgo empresarial y el desempeño de la entidad en relación con sus objetivos, una organización puede considerar en qué medida las capacidades y técnicas de gestión del riesgo empresarial han creado valor a lo largo del tiempo y seguirán haciéndolo cuando se produzcan cambios sustanciales.

INFORMACIÓN, COMUNICACIÓN Y REPORTE

La comunicación es el proceso continuo e iterativo de obtener y compartir información en toda la entidad. La Dirección utiliza información pertinente de fuentes internas y externas para facilitar la gestión del riesgo empresarial. La organización aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño.

Dentro de estos cinco componentes hay una serie de principios, como se ilustra en la siguiente figura. Los principios representan los conceptos fundamentales asociados a cada componente, y están redactados de la misma manera que lo harían las organizaciones como parte de las técnicas de gestión del riesgo empresarial de la entidad. Si bien estos principios son universales y forman parte de cualquier iniciativa eficaz de gestión del riesgo empresarial, la Dirección debe hacer valer su criterio al aplicarlos.



4. Conclusión

Una organización debe contar con medios adecuados para proporcionar a las partes interesadas de la entidad una expectativa razonable de que es capaz de gestionar el riesgo hasta un mínimo aceptable. Esto se logra evaluando las prácticas implantadas para la gestión del riesgo empresarial. Este tipo de evaluación es voluntario, a menos que la legislación o regulación lo establezca de otro modo.

El Marco proporciona criterios para llevar a cabo una evaluación y determinar si la cultura, las capacidades y las técnicas de gestión del riesgo empresarial abordan conjuntamente el riesgo de no lograr la estrategia de la entidad y los objetivos de negocio asociados. Durante la evaluación, la organización considera si:

- Los componentes y principios relativos a la gestión del riesgo empresarial están presentes y en funcionamiento.
- Los componentes relativos a la gestión del riesgo empresarial funcionan juntos de forma integrada.
- Los controles necesarios para poner en práctica los principios relevantes están presentes y en funcionamiento.

En estas tres consideraciones, el concepto "estar presente" significa que los componentes, principios y controles existen en el diseño e implantación de la gestión del riesgo empresarial para lograr la estrategia y los objetivos de negocio. "En funcionamiento" significa que están operando para lograr la estrategia y los objetivos de negocio. "De forma integrada" se refiere a las interdependencias de los componentes y a su funcionamiento conjunto.

Las organizaciones pueden poner un énfasis diferente en principios específicos y aplicarlos de manera diferente, dependiendo de los beneficios que una organización busque obtener a través de la gestión del riesgo empresarial. Cuando estos componentes, principios y controles de apoyo están presentes y en funcionamiento, la organización puede esperar dentro de lo razonable que la gestión del riesgo empresarial ayude a la entidad a crear, preservar y materializar valor.

En este capítulo se han presentado muy brevemente los principales aspectos del informe *Gestión de Riesgos Empresarial – Integrando Estrategia y Desempeño,* siendo recomendable que esta breve referencia se complete con una lectura reflexiva y en profundidad del informe completo.

También en este caso, el profesional que esté interesado en acreditar sus conocimientos y experiencia en este ámbito puede obtener a través del Instituto la certificación global en COSO ERM *(Enterprise Risk Management)* avalada y ofrecida por los miembros de COSO.

Creación, organización y funcionamiento de Auditoría Interna

Instituto de Auditores Internos de España

A la hora de crear una función de Auditoría Interna, el Instituto Global de Auditores Internos ofrece una serie de sugerencias y pasos recomendables que se indican a continuación.

1. Crear una función de Auditoría Interna: 16 pasos clave

Paso 1 · Establecimiento de la autoridad de Auditoría Interna

Establecer la autoridad de la actividad de Auditoría Interna y revisar su definición, así como las Normas Internacionales para la Práctica Profesional de Auditoría Interna (Normas) para familiarizarse con lo que se requiere.

Paso 2 · Entrevista de Liderazgo

Realizar entrevistas con la Alta Dirección y los presidentes del Consejo de Administración/Comisión de Auditoría, con el objeto de establecer un cauce de comunicación y entendimiento, de cara a garantizar que quienes ocupan los primeros puestos en la organización tengan una idea clara de la función de Auditoría Interna y calibrar con ellos sus expectativas.

Es necesario aprovechar esta oportunidad para tomar el pulso al entorno que define la cultura de la organización y abordar lo que la gerencia y el Consejo de Administración consideran los mayores riesgos para la entidad, teniendo en cuenta los posibles retos futuros junto con los problemas y oportunidades que ya se han identificado.

Desarrollar un sistema para catalogar la información obtenida, incluyendo la fecha y el nombre de la persona entrevistada, puede ser muy útil para asegurar la disposición de esta información en el futuro.

En relación con la determinación de la estructura más adecuada y la obtención de los recursos óptimos necesarios para la creación del área de Auditoría Interna, existen diversas consideraciones a tener en cuenta. Se recomienda evaluar la orientación y las consideraciones adicionales descritas en el Documento de Posición del IIA, *El papel de Auditoría Interna en el aprovisionamiento de la actividad de Auditoría Interna.*[1]

Paso 3 · Aprobación del Reglamento de funcionamiento de la Comisión de Auditoría

Redacte y someta a aprobación el Reglamento de funcionamiento de la Comisión de Auditoría. Ningún Reglamento puede abarcar todas las actividades que podrían ser apropiadas para una

1. Global Institute of Internal Auditors. IIA Position Paper: *The role of internal auditing in resourcing the internal audit activity.*

Comisión de Auditoría en particular, ni todas las actividades identificadas en un documento modelo serán relevantes para cada Comisión.

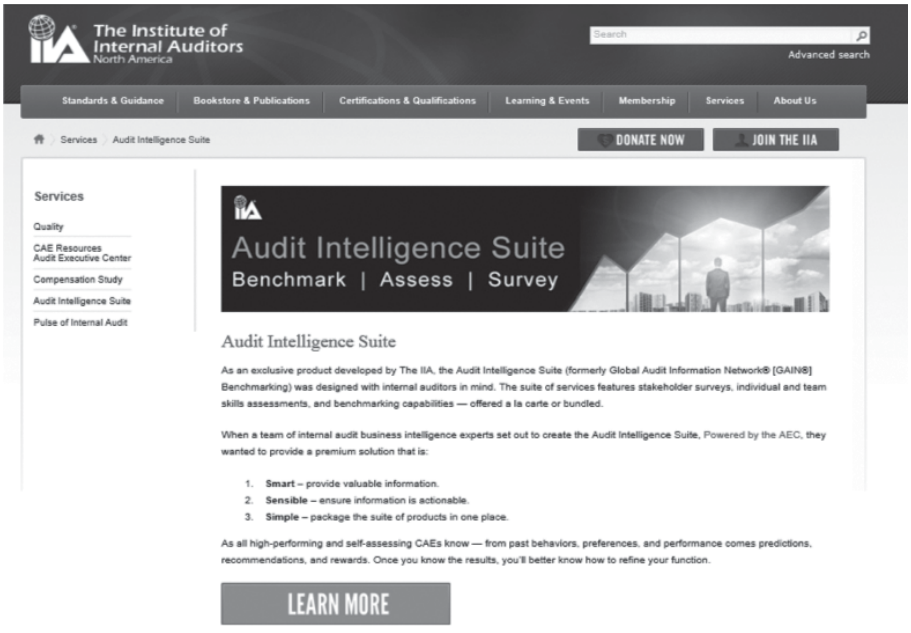
El Reglamento debe adaptarse a las necesidades de cada Comisión y a las reglas de gobierno corporativo definidas en la organización. El Instituto Global tiene a disposición de sus profesionales un modelo de Reglamento de la Comisión de Auditoría[2].

Paso 4 · Comprender las necesidades de evaluación comparativa

Es importante comprender las necesidades de "evaluación comparativa", es decir, las especificidades de la industria en la que opera la organización, la posible existencia de grupos especializados, obtención de información de organizaciones con el mismo tamaño de personal, etc.

Se recomienda obtener la opinión de la Alta Dirección en relación con la situación actual del mercado en el que opera la entidad (identificación de líderes y rezagados).

Como recoge la siguiente figura, el Instituto Global IIA pone a disposición de los profesionales la *Suite de inteligencia de auditoría*[3] para obtener más información al respecto.



2. Global Institute of Internal Auditors: Model Audit Committee Charter.

3. Global Institute of Internal Auditors. *Audit Intelligence Suite*

Es de especial relevancia conocer la cultura y la perspicacia comercial de la empresa. Ello proporciona una perspectiva general del entorno de control y de la madurez de riesgo de la compañía, lo que permitirá al auditor interno contar con información cualitativa relevante para determinar su enfoque y desarrollar el marco del departamento de Auditoría Interna.

Paso 5 · Revisión de políticas y procedimientos

Obtenga y revise las políticas y procedimientos con los que cuenta su organización, especialmente la Normativa Interna relativa al Gobierno Corporativo. Según el *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (MIPP), el Director de Auditoría Interna (DAI) debe desarrollar políticas y procedimientos para regular, estandarizar y documentar las actividades de Auditoría Interna.

Aunque no deben limitarse a la relación que se detalla a continuación, el conjunto de políticas debe cubrir, al menos: la elaboración del Plan Anual de Auditoría; el proceso de aprobación del mismo; el *Risk Assessment;* la ejecución de las auditorías; la elaboración de los informes de auditoría, el seguimiento de recomendaciones *(follow up),* el *reporting* a las diferentes partes interesadas, garantía de calidad, etc.

Las políticas y procedimientos deberán ser aprobados por la Comisión de Auditoría.

Paso 6 · Problemas de control

Es recomendable poner en común con los auditores externos los problemas de control interno más significativos, abiertos y cerrados, que pueden haber sido identificados durante las revisiones realizadas en el ejercicio de la actividad de Auditoría Interna.

Paso 7 · Desarrollo del "universo de auditoría"

El concepto de "universo de auditoría" hace referencia al listado de todas las entidades y áreas auditables.

Paso 8 · Mapa de procesos/operaciones principales

Es crítico realizar un mapeo de los principales procesos/operaciones dentro de la organización. También es necesario llevar a cabo reuniones con los responsables de los distintos departamentos involucrados en las operaciones, incluidos los de tecnologías de la información, para comprender sus riesgos y preocupaciones.

Paso 9 · Desarrollar la evaluación de riesgos (Risk Assessment)

Debe realizarse una evaluación de los riesgos de la organización, una evaluación a nivel macro, que incluya factores de riesgo tanto externos como internos.

Paso 10 · Desarrollar el Estatuto de la función de Auditoría Interna

Redacte y someta a aprobación el Estatuto de la función de Auditoría Interna. Es crítico asegurarse de que tanto la Alta Dirección como la Comisión de Auditoría revisan y aprueban el documento.

Para elaborar este Estatuto se pueden consultar las recomendaciones que incluye el *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (MIPP), el documento *Model Internal Audit Activity Charter* y el *World-Class Tools for Building an Internal Audit Activity,* 2nd Edition[4].

Con carácter adicional, siempre se recomienda consultar las webs del Instituto Global y el Instituto de Auditores Internos de España, ya que en ellas se recopilan diferentes recursos y muestras adicionales, siempre útiles para la labor del auditor interno.

Paso 11 · Elaborar el presupuesto

La Comisión de Auditoría es responsable de aprobar el presupuesto de Auditoría Interna. Este presupuesto debe ser adecuado y suficiente para atraer y retener a los profesionales necesarios, así como para proporcionar los recursos suficientes para que el área pueda desarrollar las actividades funcionales que tiene encomendadas.

Paso 12 · Desarrollar un Plan de Auditoría

Una vez realizada la evaluación de riesgos *(Risk Assessment),* el auditor interno dispondrá de la información necesaria para poder desarrollar un Plan de Auditoría que contemple tanto las actuaciones que se prevén llevar a cabo en ese periodo, como el alcance y el resto de información relevante.

Las revisiones planificadas en el período de tiempo asignado (generalmente un año) dependerán de los riesgos identificados, junto con los recursos y el personal de los que disponga Auditoría Interna.

4. Global Institute of Internal Auditors.1. *International standards for the Professional Practice of Internal Auditing (Standards).* 2. *Model Internal Audit Activity Charter.* 3. *World-Class Tools for Building an Internal Audit Activity,* 2nd Edition.

Es muy recomendable dejar tiempo en el Plan de Auditoría para poder incorporar las solicitudes de trabajos adicionales que lleguen desde la Dirección o la Comisión de Auditoría (la práctica habitual es dejar para este cometido un 10% del tiempo).

Paso 13 · Contratación del personal y desarrollo de un plan de capacitación

Auditoría Interna necesita contar con un equipo de personas cualificado cuyo número y perfiles dependerá enormemente de la dimensión y el tipo de organización de la que se trate, así como de las actividades de Auditoría Interna que puedan desarrollarse externamente. Además, es necesario desarrollar un plan para la capacitación del equipo, asegurándose de que el personal cubre la gama de conocimientos y experiencia necesarios, según la evaluación de riesgos que se ha determinado previamente.

Otra opción para considerar es la externalización de algunas partes del Plan de Auditoría a proveedores de servicios, o utilizar profesionales internos de otras áreas de la organización. Para profundizar sobre estos aspectos, se recomienda consultar el documento *El papel de la auditoría interna en el aprovisionamiento de la actividad de auditoría interna*[5].

Paso 14 · Garantizar la cooperación

Es importante tener siempre presente la necesidad de mantener una colaboración y un diálogo fluido con los principales *stakeholders*, desde las distintas áreas de la organización a otros grupos de interés relevantes. Un documento de interés para los auditores internos que trata esta cuestión, también del Instituto Global, es *All in a day's work*[6], el cual se recomienda consultar para profundizar en este asunto.

Paso 15 · Establecimiento de mecanismos de *reporting* de informes de mejores prácticas

Auditoría Interna tiene que sentarse con la Alta Dirección para definir mecanismos de *reporting* de informes de mejores prácticas, a efectos de garantizar la promoción de Auditoría Interna a lo largo de toda la organización.

Con carácter adicional, se debe desarrollar una metodología para efectuar el seguimiento de las recomendaciones de auditoría y realizar una medición del desempeño de los profesionales que forman del departamento.

5. Global Institute of Internal Auditors. IIA Position Paper: *The role of internal auditing in resourcing the internal audit activity.*
6. Global Institute of Internal Auditors. *All in a day's work.*

Paso 16 · Establecimiento de un programa de garantía de la calidad

Para llevar a cabo esta tarea, es recomendable consultar la guía práctica para establecer un programa de garantía de la calidad: *Practice Guide: Quality Assurance and Improvement Program*[7].

Es importante destacar también la relevancia del *Tone at the top,* un componente vital antes de establecer cualquier función, especialmente en el caso de Auditoría Interna. Los auditores internos necesitan el máximo apoyo de la Alta Dirección y del Consejo de Administración en el establecimiento y creación de la función de Auditoría Interna. Solo de esta manera se puede preservar la necesaria independencia y objetividad que caracterizan a esta función.

2. Crear una función de Auditoría Interna: otros aspectos relevantes

2.1 Estructura del departamento

Además de los detalles mencionados en el paso 2 (Entrevista de liderazgo), a la hora de determinar la estructura del departamento es importante tener en mente algunas preguntas importantes que ayudarán a moldear la función. Se citan a continuación algunas de esas cuestiones:

- ¿En qué parte de la estructura de la organización se ubicará Auditoría Interna?
- ¿A quién debe informar?
- ¿Quién tendrá la decisión de contratar o despedir auditores internos?

Finalmente, a los efectos de disponer de un área de Auditoría Interna actualizada y que verdaderamente aporte valor a sus *stakeholders* y al conjunto de la entidad, sería necesario alinear el departamento de Auditoría Interna con las actuales exigencias del entorno empresarial (dinamismo, digitalización, etc) y crear un área con la mayor agilidad y relevancia posible.

2.2 Desarrollo de la actividad del área

Para determinar el desarrollo de la actividad de Auditoría Interna hay que tener en cuenta algunos aspectos relevantes como:

AUDITORÍA INTERNA COMO ROTACIÓN

Es necesario buscar la aprobación ejecutiva para instituir un Programa de Rotación, entendido como una iniciativa de desarrollo profesional que permite a los no auditores in-

7. Global Institute of Internal Auditors. *Practice Guide: Quality Assurance and Improvement Program.*

corporarse a Auditoría Interna para posteriormente regresar a sus puestos asignados regularmente.

Gracias a esta iniciativa, el equipo de auditores internos podría incluir auditores tradicionales, así como también miembros del área de finanzas, de TI, de operaciones o de otras partes de la organización, que complementarán los conocimientos, experiencia y puntos de vista para dotar de una mayor calidad a los trabajos de Auditoría Interna.

Hacer que los miembros de otros equipos ganen experiencia en auditoría interna impulsará tanto el valor de esta función como una mejor concienciación y comprensión del riesgo en toda la organización. Por supuesto, la rotación puede y debe funcionar en ambos sentidos. El hecho de que los auditores internos pasen temporalmente a otros departamentos les permite obtener más experiencia y conocimiento sobre otras partes del negocio. Tendrán una mejor visión y perspectiva de la organización, aunque nunca deben perderse de vista los rasgos que definen a estos profesionales: independencia, integridad y objetividad.

EQUIPO DIVERSO CON UN PLAN DE RECURSOS DE ORIGEN COMPARTIDO

Una sólida función de Auditoría Interna tiende a complementar su equipo central con auditores invitados rotativos que trabajan con los expertos en la materia. Un grupo más diverso puede percibir y aportar puntos de vista diferentes y dar así respuesta a cuestiones de auditoría más amplias y complejas y proporcionar una mejor visión de la empresa en su conjunto. La diversidad en el equipo, y en la función, se traduce en mayores y diferentes experiencias y valiosas perspectivas.

CENTRARSE EN LAS COMPETENCIAS, NO SOLO EN LAS HABILIDADES

Las habilidades técnicas son ciertamente importantes para los profesionales de Auditoría Interna, pero las competencias y habilidades sociales *(soft skills)* marcan la diferencia cuando se trata de reaccionar ante necesidades cambiantes y trabajar en proyectos totalmente nuevos.

Auditoría Interna es una función que requiere desarrollar capacidades específicas para lidiar con la ambigüedad y el aprendizaje sobre la marcha. También se precisan altas dosis de creatividad para resolver cómo enfrentarse a desafíos inesperados.

La necesidad de interacción y diálogo fluido con los responsables o gestores de los procesos y otras partes interesadas brinda a los auditores la oportunidad de perfeccionar sus capacidades de gestión de relaciones y gestión de proyectos.

Gestionar esta comunicación es clave en Auditoría Interna, que debe saber cómo dar la información correcta a las personas adecuadas en el momento adecuado, para lograr un cambio positivo. Tampoco sobra el conocimiento de las cualidades de liderazgo, incluida

la perspicacia para comprender una situación y hacer recomendaciones prácticas que deben implementarse con éxito.

Un departamento que se concentre en las competencias clave, y no se quede solo en un conjunto de habilidades, tiene más probabilidades de convertirse en una fuente de valor para la empresa.

APOYO Y ENLACE A UN PROGRAMA ERM

Para poder auditar eficazmente los riesgos de toda la empresa, Auditoría Interna debe conocer esos riesgos. Esto significa que la función debe apoyar o ayudar a desarrollar un programa de Gestión de Riesgos Empresariales (ERM). Sin esto, Auditoría Interna corre el riesgo de tener un Plan de Auditoría que solo aborde los riesgos que ella misma conoce, no los principales riesgos que realmente afectan a la organización.

Para que funcione bien, un programa ERM debe promover la alineación entre las actividades de auditoría y los objetivos de negocio. Mantener esta alineación es un proceso continuo.

NADA ES NO AUDITABLE

Auditoría Interna puede tender a trazar una línea alrededor de lo que ya sabe auditar y declarar que nada más es auditable. Esto llevaría a perder la oportunidad de realizar auditorías muy relevantes para la organización.

Practicar la mentalidad de que "nada es no auditable" puede ser enriquecedor, pero también intimidante, por eso se necesitan competencias y un equipo diversificado.

No cabe duda de que es más fácil y seguro auditar las mismas cosas conocidas año tras año, pero descubrir cómo auditar algo nuevo, aun siendo retador, permitirá desarrollar competencias valiosas.

BUSQUE Y TENGA EN CUENTA A OTROS PROVEEDORES DE ASEGURAMIENTO

Los auditores internos viven su día a día pegados a los riesgos, lo que a veces puede llevar al error de pensar que son los únicos que entienden el riesgo y brindan seguridad. Pero no es así.

Un equipo de Auditoría Interna que esté bien integrado con otros departamentos aprovechará estas sinergias para trabajar y comprender a otros proveedores de aseguramiento. Adoptar esta mentalidad y esta metodología de trabajo permite proporcionar una mayor cobertura de riesgos.

GESTIÓN PROACTIVA DE LAS RELACIONES

Auditoría Interna no puede auditar de manera efectiva desde una torre de marfil. Es necesario bajar al suelo, recorrer el terreno. Hay que escuchar y hablar con las personas de la organización para aprender sobre ellas y comprender cómo se les puede ayudar con el trabajo, tanto a ellas como al negocio.

Al trabajar incansablemente para construir y mantener relaciones con todos los niveles de empleados y partes interesadas, los auditores internos tomarán más conciencia y tendrán mejor visión sobre lo que es más relevante en su organización.

VINCULAR OBJETIVOS INDIVIDUALES Y DE EQUIPO CON LAS PRIORIDADES ESTRATÉGICAS

A nivel individual y departamental, Auditoría Interna necesita ampliar sus aspiraciones más allá de cumplir con la descripción de su trabajo. Es importante saber cómo podrían alinearse los objetivos de Auditoría Interna con la estrategia de la organización y establecer objetivos específicos con métricas de rendimiento para su monitorización.

Si, por ejemplo, el objetivo de una entidad es la eficiencia operativa, quizás Auditoría Interna pueda centrar sus prioridades en crear un programa de auditoría más ágil para ahorrar costes.

CONSULTORÍA CON MENTALIDAD DE SERVICIO AL CLIENTE

No siempre se recuerda que el auditor interno es como un consultor: un profesional que da opiniones y consejos profesionales, o sirve como asesor.

Esta mentalidad de servicio al cliente posiciona a Auditoría Interna como un asesor de confianza que quiere aprender y conocer las actividades desarrolladas por los distintos profesionales y departamentos de la organización, con el objeto de ayudarlos a encontrar formas de mejorar.

El rol de consultor también puede ayudar al Director de Auditoría Interna a administrar el departamento como una empresa, creando un presupuesto y una planificación para cada proyecto, reservando un porcentaje de horas para cumplir con la gestión de peticiones específicas de otras áreas.

Cuando Auditoría Interna se ve a sí misma con rol de consultoría, puede ahorrar tiempo y costes, a la par que construye relaciones sólidas con sus propios clientes internos.

TECNOLOGÍA PARA AUTOMATIZAR PROCESOS

Como en otras funciones y departamentos de la organización, Auditoría Interna puede aprovechar la tecnología para automatizar las tareas manuales más repetitivas y liberar tiempo para realizar actividades de mayor valor agregado.

También puede ayudar a las organizaciones a identificar oportunidades para integrar la automatización en los procesos y funciones del negocio.

La automatización puede conducir a una mayor eficiencia en los controles de monitorización; mejor visibilidad para todas las partes interesadas y ahorros significativos de tiempo y costes que se pueden dedicar a proyectos que impulsen el valor de la organización.

Hacer las mismas evaluaciones y auditorías año tras año es costoso, pero más fácil que aventurarse en nuevas necesidades para, de esta manera, hacer la función de Auditoría Interna más ágil y relevante. Incluso asumiendo que esas nuevas auditorías no sean tan ágiles, en el sentido de rápidas, porque se está auditando algo que hasta ahora no se había afrontado, debido a que se situaba en el cajón de lo "no auditable". Este cambio de mentalidad y de visión requiere desarrollar un importante grado de tolerancia a la ambigüedad. Y también debe contar con el apoyo de la organización, de los clientes –los auditados– y de los grupos de interés, que deben entender que las auditorías nuevas no serán tan rápidas, pero sí más relevantes para la organización.

Los beneficios de este giro en la concepción de Auditoría Interna pueden ser significativos. Centrándose en las competencias, desarrollando relaciones sólidas, cultivando una mentalidad de servicio de consultoría, alineando las metas de Auditoría Interna con los objetivos de la compañía… Todo ello ayudará a desarrollar una función de Auditoría Interna que sea muy relevante y un departamento atractivo para los profesionales que quieren aprender y aportar valor al negocio desde su ámbito de actuación. Con un equipo adecuado y diverso, una función ágil y relevante posicionará a Auditoría Interna como líder dentro de la empresa.

Metodología de Auditoría Interna

Instituto de Auditores Internos de España

Antes de comenzar conviene dejar perfectamente identificados algunos conceptos que se manejan a lo largo de este capítulo, que recoge las técnicas utilizadas por los auditores internos; una de las cosas que los distingue de otros profesionales en el desarrollo de sus trabajos.

Precisamente, la unidad de Auditoría Interna debe recoger en su Manual de Procedimientos los procesos y técnicas a seguir que guían su actividad, tal y como establece la Norma 2040. Cada unidad deberá definir cuál es su propia metodología, de acuerdo con el entorno, cultura y modo de operar de la compañía. En organizaciones más innovadoras, con velocidad de respuesta al mercado y flujos de comunicación que requieren rapidez, Auditoría Interna necesita ofrecer conclusiones a un ritmo que acompañe al negocio, lo que exige adoptar metodologías de trabajo más ágiles (metodología *Agile*) para adecuar así los proyectos de auditoría a los objetivos de la compañía y ser generadores de valor.

Hay que distinguir entre las técnicas y los procedimientos de Auditoría Interna: las primeras no son exclusivas de la función, pero los segundos sí le son específicos y propios.

1. Técnicas de Auditoría Interna

En la actualidad, un departamento moderno y profesional de Auditoría Interna hace uso de diversas técnicas y no puede decirse que ninguna de ellas sea exclusiva y propia, porque los conceptos básicos en los que se apoya un auditor interno para sus investigaciones son el sentido común, la lógica y la razón.

El matiz diferenciador es que, cualquiera que sea la técnica empleada, el auditor interno debe perseguir la evidencia, el hecho probado, o llegar a conclusiones que sean de muy difícil rechazo en virtud de un razonamiento lógico impecable.

Auditoría Interna emplea principalmente las Tecnologías de Información (TI), el análisis continuo de información y la Estadística, pero también técnicas sociológicas, como encuestas, sondeos, entrevistas, y técnicas analíticas y matemáticas para el planteamiento y estudio de problemas que pueden concretarse en fórmulas, ecuaciones o identidades.

En relación con las TI, la automatización de los controles (auditoría continua), a través de la robótica o de la Inteligencia Artificial, así como el uso de herramientas para el análisis masivo de datos *(Big data* o *Data Mining),* son aspectos clave en el desarrollo de sus procesos y que no pueden quedarse fuera del ámbito de actuación de Auditoría Interna. El Capítulo X desarrolla el uso de estas tecnologías por parte de la función de Auditoría Interna.

Otra diferencia respecto a otros profesionales es que los auditores internos pueden y deben trabajar con una mentalidad objetiva y desde una posición de independencia para expresar su-

gerencias y recomendaciones, que serán o no aceptadas como útiles y oportunas para la organización, pero que, en principio, pueden hacer llegar a sus destinatarios libre y directamente.

Hay una serie de métodos de trabajo que son específicos de Auditoría Interna, entre los que citamos:

- Planificación y programación de trabajos e investigaciones obligatorias.
- Búsqueda de la evidencia o certeza de las conclusiones.
- Evaluación y determinación de los riesgos.
- Recogida de información en papeles de trabajo (PPTT) normalizados.
- Verificación sistemática de la información recogida.
- Pruebas de cumplimiento para asegurar la adecuación de los procedimientos.
- Pruebas en general para la comprobación de situaciones.
- Circularización o comprobación efectiva de información financiera y de todo tipo con el exterior de la organización.
- Cumplimiento de las normas.
- Uso de cuestionarios de control interno.

MÉTODOS Y PROCESOS DE TRABAJO ESPECÍFICOS DE AUDITORÍA INTERNA

Indagación.

Consiste en la averiguación mediante entrevistas directas con el personal del área auditada o con terceros que tengan relación con las operaciones de ésta (evidencias testimoniales).

Encuestas y cuestionarios.

Aplicación de preguntas relacionadas con las operaciones, para conocer la verdad de los hechos, situaciones u operaciones (evidencias documentales, testimoniales).

Observación.

Verificación ocular de operaciones y procedimientos durante la ejecución de las actividades objeto de revisión (evidencias físicas).

Comparación.

Análisis entre las operaciones realizadas y las definidas para determinar sus relaciones e identificar sus diferencias y semejanzas (evidencias analíticas).

Revisión selectiva.

Examen de las características importantes que debe cumplir una actividad, informe o documento, seleccionándose así parte de las operaciones que serán evaluadas o verificadas en la ejecución de la auditoría (evidencias analíticas).

Evaluación.
Conjunto de actividades que permiten documentar la forma en la que se ejecuta un procedimiento (evidencias documentales, testimoniales).

Rastreo/*tracking.*
Seguimiento de una operación, a través de la documentación respectiva, a fin de conocer y evaluar su ejecución (evidencias analíticas).

Revisión de cálculos matemáticos.
Verificación de la exactitud aritmética de las operaciones contenidas en los documentos (evidencias analíticas y documentales).

Confrontación.
Cotejo de la información contenida en los registros contra el soporte documental para confirmar la veracidad, exactitud, existencia, legalidad y legitimidad de las operaciones realizadas (evidencias analíticas y documentales).

Métodos estadísticos.
Muestreo estadístico o no estadístico, o combinación de ambas. Estos métodos aseguran que todas las operaciones tengan la misma posibilidad de ser seleccionadas y que la selección represente significativamente la población o universo (evidencias analíticas).

Confirmación.
Corroboración de la verdad, certeza o probabilidad de los hechos, situaciones, sucesos u operaciones mediante datos o información, obtenidos de manera directa y por escrito del personal que participa o ejecutan las tareas sujetas a verificación (evidencias documentales).

Comprobación.
Confirmación sobre la veracidad, exactitud, existencia, legalidad y legitimidad de las operaciones realizadas por la organización auditada, mediante el examen de los documentos que las justifican (evidencias documentales).

Conciliaciones.
Examen de la información emanada de diferentes fuentes con respecto a una misma operación o actividad, a efectos de hacerla concordante (evidencias analíticas).

Tabulación.
Agrupación de resultados importantes obtenidos en áreas, segmentos o elementos analizados, para soportar conclusiones (evidencias analíticas).

Comunicación.
Obtención de información directa y por escrito de un sujeto externo a la entidad auditada (evidencias testimoniales).

Análisis.
Separación de los elementos o partes que conforman una operación, actividad, transacción o proceso, con el propósito de establecer sus propiedades y conformidad con los criterios de orden normativo y técnico (evidencias analíticas).

Análisis de tendencias y comparación con los indicadores.
Permite medir la eficiencia y economía en la gestión de los recursos, la eficacia y efectividad de los bienes producidos o de los servicios prestados o el grado de satisfacción de las necesidades de los usuarios o beneficiarios (evidencias analíticas).

Análisis de soportes informáticos.
Evaluación de los elementos lógicos, programas y aplicaciones utilizados por el auditado (evidencias informáticas).

Inspección.
Examen físico y ocular de los activos tangibles o de hechos, situaciones, operaciones, transacciones y actividades aplicando la indagación, observación, comparación, rastreo, análisis, tabulación y comprobación (evidencias físicas).

Adicionalmente podrán utilizarse MÉTODOS AUXILIARES que complementen los procedimientos ya citados. Destacamos a continuación algunos de ellos:

Pruebas selectivas a criterio del auditor interno.
Se seleccionará una muestra representativa del universo a analizar con la finalidad de simplificar las labores de muestreo, verificación o examen. La cantidad y características de las unidades elegidas estarán vinculadas con el conocimiento que pueda tener el auditor interno del control interno vigente.

Pruebas selectivas por muestreo estadístico.
Se aplicarán métodos matemáticos para determinar el tamaño mínimo de la muestra que permita cuantificar el grado de riesgo que resulta de examinar sólo una parte del universo.

Tal y como mencionábamos anteriormente, el uso de nuevas tecnologías de minería de datos permite analizar poblaciones en su conjunto en lugar de utilizar muestras selectivas. El reto será adaptar a los equipos de Auditoría Interna para que cuenten con las habilidades y formación necesarias para el uso de las nuevas técnicas basadas en los sistemas de información.

El criterio profesional del auditor interno y su experiencia determinarán la combinación de prácticas y procedimientos, según los riesgos y otras circunstancias, con vistas a obtener la evidencia necesaria y la suficiente certeza para sustentar sus conclusiones y opiniones de manera objetiva.

2. Procedimientos de Auditoría Interna

En general, llamamos procedimiento a los pasos que deben seguirse para la ejecución de actividades repetitivas, y aplicado al terreno de la auditoría interna, sus procedimientos son aquellos que obligatoriamente han de emplear estos profesionales cuando hagan informes de auditoría, de conformidad con las normas que rigen la profesión. Reiterando que deberá ser cada unidad de Auditoría Interna quien deberá definir esos procedimientos, bajo el espíritu y criterios definidos por las Normas y en función del entorno y cultura de su organización, y siempre con el último objetivo de cumplir con la misión de la profesión, para la mejora y protección del valor de la organización.

Las mencionadas normas determinan los procedimientos **de planificación** (Norma 2200); **de desempeño del trabajo de Auditoría Interna** (Norma 2300); **de comunicación de resultados** (Norma 2400); **de seguimiento de recomendaciones** (Norma 2500); **de coordinación y confianza con otras líneas de aseguramiento** (Norma 2050) y de p**rogramas de aseguramiento y mejora de la calidad** (Norma 1300).

Tomando las normas como referencia y punto de partida, los procedimientos deben elaborarse por escrito en cada unidad de Auditoría Interna y en cada organización y ser incorporados al Manual de Auditoría.

El procedimiento para la iniciación y desarrollo de informes de auditoría se articula en torno a los siguientes hitos o pasos sucesivos:

- Determinación de su finalidad y objetivos.
- Precisar su alcance.
- Conseguir la información previa necesaria sobre lo que se audita.
- Planificación del trabajo a desarrollar para satisfacer la finalidad del informe y alcanzar sus objetivos.
- Llevar a cabo los trabajos de recogida de información y documentación, que puedan efectuarse antes de la presentación de los auditores *in situ.*
- Comienzo de la auditoría, presentación ante los auditados y cumplimiento de la planificación establecida.
- Análisis y síntesis de la información y documentación obtenida.
- Verificación de cuánto se ha recogido.
- Comprobación de que se han alcanzado los objetivos señalados y la finalidad del Informe.
- Conclusión y emisión de recomendaciones.
- Elaboración del borrador del informe.

- Revisión detallada del mismo por parte de Auditoría Interna.
- Distribución del borrador.
- Discusión del borrador y obtención del plan de acción por parte de los auditados.
- Distribución del informe final a la Comisión de Auditoría, a la dirección y a los auditados, según el procedimiento establecido.

En este procedimiento, que es el método profesional de Auditoría Interna, es posible diferenciar en el ciclo de la auditoría SEIS PASOS BÁSICOS:

1. Evaluación preliminar. Para la familiarización y conocimiento con y de lo que se audita.
2. Elaboración del programa de trabajo.
3. Presentación e información a los auditados *(Kick-off meeting).*
4. Trabajo de campo. Desarrollo de la planificación establecida y verificación de la información obtenida.
5. Elaboración del informe y discusión.
6. Seguimiento de las recomendaciones.

A la hora de desarrollar estos pasos, se puede optar por DOS FORMAS DIFERENTES DE PROCEDER:

- Por un lado, una ejecución del ciclo de auditoría aquí descrito de principio a fin, con una interacción principal con el auditado en el momento de la planificación (paso 3) y otra interacción final (paso 5) con la discusión del informe.
- Por otro lado, también se puede seguir la metodología *agile,* basada en acelerar los ciclos de la auditoría, con interacciones reiteradas con el auditado, de forma que el programa de trabajo se divide en ciclos completos de auditoría en sí mismos.

3. Ciclo de auditoría: análisis de los seis pasos clave

Veamos ahora en detalle cada uno de los seis pasos identificados anteriormente, diferenciando las dos metodologías que señalamos.

3.1 Evaluación preliminar (Familiarización)

Un auditor interno ha de conocer con cierta profundidad y certeza los riesgos que tienen o que pueden producirse en el área o actividad concreta que se audita, las funciones y

responsabilidades asignadas, la información de reporte que periódicamente envía a la dirección de la organización y la que recibe, su estructura orgánica, las normas y legislación que le afectan, entre otros aspectos. Supongamos que estamos auditando algo por primera vez: lo que se busca es un conocimiento lo más amplio y certero posible del entorno de control y de lo que se audita, para que el auditor sea capaz de hablar el mismo lenguaje de los auditados.

Con este bagaje, el auditor interno podrá adentrarse en campos de actividad sobre los cuales, por lo general, carece de conocimientos profundos. Sin esa familiarización previa, los auditados podrían no reconocer al auditor interno ninguna autoridad. Y llevar a cabo esa evaluación preliminar es lo que dice la Norma 1210 sobre aptitud y cuidado profesional. El equipo de auditoría, en su conjunto, debe reunir los conocimientos necesarios para llevar a cabo la evaluación del trabajo y, en caso contrario, subcontratar dichos servicios, siempre bajo los requisitos de independencia y competencia que recoge la Norma 2050.

Las técnicas sociológicas y de inteligencia emocional son necesarias porque permiten que el auditado perciba que el auditor que le entrevista entiende su lenguaje, conoce de lo que se está hablando y sabe lo que tiene que preguntar y el cómo y el por qué lo hace. Solo así la comunicación entre ambos fluirá sin obstáculos.

Esto, recogido en la metodología, es perfectamente válido también para los auditores internos que llevan tiempo ejerciendo en una misma organización y que, consecuentemente, tienen una visión de conjunto de sus actividades y conocen a sus responsables, así como el contenido funcional y procesos de cada unidad. Aunque estos auditores internos tengan mucho tiempo y trabajo ganado porque están familiarizados con la compañía, la velocidad de los cambios en el mercado y la innovación constante hace recomendable informarse previamente antes de iniciar una auditoría. No olvidemos además que los períodos que transcurren entre cada auditoría son, en general, largos. Y aunque fueran cortos, pueden producirse cambios relevantes en los riesgos que afrontan dichos procesos.

La familiarización, o recogida de información previa. no tiene que plantear excesivas dificultades a los auditores internos. Por ello citaremos, sin entrar a más detalles, algunas observaciones que nos parecen oportunas y útiles:

- Examinar toda la información que emite y que recibe el área, actividad, departamento auditado, etc.
- Analizar los sistemas informatizados y su conexión con la informática corporativa.
- Conocer posibles problemas de personal informándose en la unidad de personal y RRHH.
- Ver los presupuestos (gestión previsional) en lo referente a lo que se audita.

- Cerciorarse de que existen o no regulaciones que les afecten y en qué medida.
- Si hubo auditorías anteriores, verificar el cumplimento de las recomendaciones.
- Conocer los objetivos que la dirección de la organización ha elaborado para la unidad, área o actividad auditadas.

Son diversas las posibles técnicas que se pueden utilizar dentro de la metodología *agile* para ayudar a organizar y fomentar el entendimiento de los procesos. Una de ellas se conoce como *Canvas Project,* y Auditoría Interna puede utilizarla para obtener los elementos necesarios para la fase de familiarización. En esta fase, el auditor interno debe identificar los diferentes aspectos recogidos en el Panel:

- Descripción del área/proceso auditado, cuáles son sus objetivos y riesgos iniciales identificados.
- Qué importancia tiene para la compañía.
- Cuál es la proposición de valor de la auditoría.
- Qué sistemas principales se ven impactados, legislación implicada o requisitos financieros.
- Quiénes son sus principales clientes.
- Qué métricas utiliza para su seguimiento tanto el área, como los que utilizará Auditoría Interna para medir el éxito de la auditoría.
- Alcance definido para lograr el objetivo de la auditoría.
- Definición de los riesgos y controles y su priorización según la planificación de *sprints* (unidad de tiempo predefinida, normalmente dos semanas); siendo éste el embrión de lo que será el siguiente paso "programa de trabajo", que veremos a continuación.
- Principales partes interesadas de la auditoría.

3.2 Elaboración del Programa de Trabajo

Una vez finalizada la fase de evaluación preliminar o descubrimiento, el auditor debe desarrollar y detallar el programa de auditoría. Un programa de Auditoría Interna ha de reflejar los distintos pasos y operaciones necesarios para conseguir los objetivos establecidos en la planificación general de un informe de auditoría.

Su finalidad es servir de guía de los procedimientos a seguir durante el curso de la auditoría, y es como una especie de recordatorio de las sucesivas fases de la misma, a fin de no dejar nada a la improvisación, ni olvidarse de aspectos importantes a tener en cuenta mientras se efectúa el informe.

La **Norma 2200 - Guía de implementación 2201** indica que los programas deben:

- determinar los procedimientos para la recogida, análisis, interpretación y documentación de la información obtenida;
- establecer los objetivos de la auditoría;
- ídem el alcance y el grado de las pruebas necesarias para alcanzar los objetivos;
- identificar los aspectos técnicos, riesgos, procesos y transacciones que habrán de revisarse, y
- determinar la naturaleza y la extensión de las pruebas.

Los objetivos de un informe de auditoría son las finalidades que persiguen los auditores internos con los trabajos de información, estudios, investigación, análisis y verificación que llevan a cabo en el curso de la auditoría.

El alcance debe precisar hasta dónde se ha querido llegar con la auditoría correspondiente y el enfoque o perspectiva de los auditores; en suma, la amplitud y profundidad de los trabajos realizados. Los objetivos y los procedimientos utilizados en un informe –que son los medios para conseguir dichos objetivos– tomados en su conjunto delimitan el alcance de un informe de Auditoría Interna. En el Anexo 11 se indican ejemplos de programas de Auditoría Interna.

La forma de documentar el programa de trabajo, pudiera ser a través de un documento de planificación, o bien a través de la aplicación de metodología de trabajo *agile*, en lugar de definir un programa de trabajo exhaustivo para el cumplimiento de un objetivo final, se plantea el uso de un listado de historias de usuario, como unidad básica mínima que aporta valor a la auditoría, recogiendo riesgos/procesos *(backlog)* a ser evaluados como áreas concluíbles en sí mismas, de forma que el objetivo sea entregar comunicaciones finales parciales como mínimo producto viable (MPV), acortando así los tiempos de reporte y comunicación final.

El *backlog* de auditoría (el programa de trabajo), se conformará del listado de historias de usuario, las cuales deben tener suficiente detalle para ser analizadas y concluidas, incluyendo los riesgos, complejidad y relevancia.

3.3 Presentación e información a los auditados *(Kick-off meeting)*

Es un momento crucial del procedimiento de Auditoría Interna. De este paso depende en buena parte conseguir o no un clima de auténtica cooperación de los auditados, que son los que tienen que facilitar la información y documentación necesarias y –que no se olvide– son los que de verdad conocen con detalle y profundidad lo que se audita.

Una primera pauta de comportamiento del auditor es observar con la cortesía y educación propia de un invitado. Es cierto que la dirección de la organización ha concedido a los auditores internos la autoridad suficiente para llevar a cabo su trabajo, pero éste se realiza en el terreno del auditado, cuyas instalaciones y dependencias le pertenecen por delegación de la dirección. El auditor es, por tanto, un visitante y debe explicar el objeto de su visita, el tiempo que durará, las personas y sitios que visitará, quiénes le acompañarán, cuáles son los objetivos de la auditoría. Y lo explicará al jefe o responsable, en cada caso, según las distintas responsabilidades asignadas.

La información se iniciará con el comentario de la planificación prevista: objetivos, alcance y programa de la auditoría, asegurando que los auditados y su máximo responsable serán los primeros en recibir el borrador del informe con sus conclusiones y recomendaciones, para su análisis y discusión, antes de ser distribuido a la Comisión de Auditoría y a la Dirección.

Los auditores serán receptivos a las sugerencias y opiniones de los responsables de área auditada, en la medida en que éstas no alteren los objetivos de la auditoría. La cortesía, la buena educación, la empatía, es decir, ponerse en la situación de los auditados, y la flexibilidad, son necesarias para no añadir más dificultades a las que normalmente ocasionan las auditorías, en general, molestas e incómodas para los auditados.

En la metodología *agile,* las interacciones con el auditado se intensifican. En el momento de finalización de la etapa de descubrimiento, esta información será validada con el auditado, a través de la presentación, discusión y validación de la información contenida.

Adicionalmente, una vez definidas las historias de usuario (que conformarán el programa de trabajo) éstas son validadas con las partes interesadas (en este caso, el área auditada). Una vez aceptadas, se constituye para cada una el hito de *Definition of Ready,* como ítem del *backlog* que ha sido consensuado y está listo para ser evaluado, revisado, examinado…, pudiéndose pasar ya la siguiente fase, el trabajo de campo.

3.4 Trabajo de campo. Desarrollo de la planificación establecida y verificación de evidencias

Tradicionalmente, esta fase comenzaba en las propias oficinas de Auditoría Interna con el único objetivo de hacer la presencia de los auditores lo menos molesta posible y realizar ahí la mayor parte del programa, recopilando información y documentos. Sin embargo, las nuevas formas de trabajo *agile* requieren y potencian la toma de contacto de forma próxima con el auditado, para observar y conocer los riesgos que el proceso afronta,

orientar el trabajo a la creación de valor y establecer una comunicación continua con todas las partes interesadas.

La tecnología y las técnicas de minería de datos permiten a los auditores internos acceder a un caudal de conocimientos sobre las áreas auditadas, que después podrán consultar y verificar obviando consultas a los auditados y pérdidas de tiempo. De esta forma se acorta considerablemente el trabajo de campo y, en definitiva, se reducen los costes de la auditoría.

La planificación ha de estar cuidadosamente preparada, pero no tiene que ser inamovible, ni una pauta rígida de trabajo para el auditor interno que puede observar sobre la marcha la conveniencia de introducir en esa planificación nuevos pasos o, por el contrario, eliminar otros que estaban previstos.

Durante el desarrollo de una auditoría, un auditor interno con experiencia jamás debe aventurar opiniones negativas respecto a lo que en cada momento analiza y examina, porque siempre se mueve en desventaja en cuanto al conocimiento de lo que ve respecto a quienes llevan tiempo efectuando tareas y conocen muy bien el terreno. Otra cosa distinta es si tiene ya en mente claridad suficiente sobre alguna sugerencia de mejora y desea comprobar la oportunidad y receptividad de la misma con los auditados, exponiéndola simplemente como una posibilidad.

Especial atención exige el procedimiento de los **papeles de trabajo** (PPTT), que, una vez preparados por el auditor interno, deben registrar la información obtenida y los análisis efectuados, sirviendo de apoyo a las recomendaciones y conclusiones que se formulen.

La **Norma 2330** indica con detalle todo lo referente a los PPTT. Aquí solo vamos a señalar para qué sirven:

- Proporcionan el soporte principal del informe de auditoría.
- Ayudan a la planificación, ejecución y revisión de las auditorías.
- Permiten comprobar que se han alcanzado los objetivos de la auditoría.
- Facilitan las revisiones del trabajo realizado por terceros.
- Son imprescindibles para la discusión de los informes.
- Proporcionan un apoyo en circunstancias como reclamaciones, casos de fraudes y litigios judiciales.
- Son documentos fundamentales para los programas de garantía de calidad de la unidad de Auditoría Interna.
- Demuestran que ésta cumple las Normas de Auditoría Interna.
- Ayudan al desarrollo profesional de los auditores internos.

Lo que da valor al dictamen y opinión de los auditores internos es que se basan en los hechos y, por tanto, han de tener un alto grado de evidencia o certeza.

Pero gran parte de la información obtenida durante la realización de un informe de auditoría se ha conseguido por medio de entrevistas con los auditados en las que, en principio, es preciso distinguir la realidad (de las situaciones) de las opiniones (de los auditados), siempre subjetivas, por lo que los auditores han de verificar esa información.

La verificación consiste en comprobar su fiabilidad, en asegurarnos de su certeza.

¿CÓMO SE VERIFICA UNA INFORMACIÓN POR PARTE DE LOS AUDITORES INTERNOS?

No es posible enumerar los modos operativos de verificación, pues la información se concreta en formas y documentos muy diversos: entrevistas, diagramas funcionales, estudios, informes, etc. En cada caso, serán la profesionalidad y la experiencia de los auditores internos las que decidirán cómo dar por buena una información, utilizando el análisis comparativo, patrones normalizados, métodos estadísticos, bibliografía, cruces de opiniones de los entrevistados, recabarla de diferentes niveles jerárquicos o categorías. Y, desde luego, apoyándose en los propios registros y archivos del área auditada y de la organización.

Esta fase es vital –y de ninguna manera debería obviarse– para dar fuerza a las opiniones, sugerencias y recomendaciones de los informes. Aunque como es lógico nos referimos a la información que ya ha sido sintetizada por considerarse suficiente a los fines de los informes correspondientes.

Trabajar bajo metodología *agile* no varía las técnicas a desarrollar en el trabajo de campo. Sin embargo, las técnicas se estructuran en intervalos de tiempo definidos como *sprints* para organizar las tareas a realizar para cada historia de usuario y planificar su conclusión en dos semanas o el tiempo habilitado del *sprint*.

Durante los *sprints,* la unidad auditora interna deberá definir los puntos de seguimiento y supervisión (diaria, semanal, planificación o retrospectiva…) y concluir el valor aportado en cada *sprint* completando la fase de *Definition of Done*.

3.5 Elaboración del informe y discusión del mismo

El informe de Auditoría Interna es el resultado de los estudios, investigaciones y análisis efectuados durante la realización de una auditoría y ha de elaborarse con arreglo a las indicaciones que se expresan en la **Norma 2400 sobre Comunicación de los trabajos y las Guías de implementación 2410 y 2420,** que señalan los criterios que aplican a la

comunicación, no tanto en su forma (escrita, verbal, audiovisual…) siendo un mecanismo que permita dejar constancia de la misma.

Incluimos los informes dentro de la metodología de Auditoría Interna, porque están sujetos a una normativa específica y han de redactarse siguiendo un procedimiento determinado, desde su iniciación hasta su distribución en el ámbito de la organización.

El informe debe señalar los objetivos y el alcance de la auditoría realizada, la opinión de los auditores internos sobre el control interno del entorno auditado, las recomendaciones que hayan considerado conveniente formular y cualquier otra sugerencia o información oportuna y necesaria. Su estructura ha de estar normalizada, así como la forma de escribir las expresiones de uso más frecuente.

Se pueden encontrar más detalles a este respecto en el capítulo siguiente, dedicado a los informes de Auditoría Interna.

Sí es reseñable mencionar que, bajo la metodología *agile,* la conclusión de cada historia de usuario (como unidad mínima auditable) se constituye en el llamado *Definition of Done,* que establece el resultado del trabajo realizado para concluir el apartado definido en el programa de trabajo (historia de usuario). Este resultado es comunicado al área auditada, recogiendo sus observaciones, estado de los riesgos y recomendaciones emitidas para esa historia. Esta discusión, llamada *Punto de Vista,* dará paso a una revisión completa de la historia de usuario y del trabajo realizado, a la discusión sobre los puntos de vista, a recopilar la retroalimentación, entregables pendientes y establecer una nueva lista de actividades específicas que constituirán un nuevo *sprint*.

De esta forma, el informe final se irá componiendo de forma iterativa como compendio de las diferentes historias de usuario concluidas *(Definitions of Done)*. El producto entregable final deberá incluir, además, la opinión global y estado de los riesgos auditados.

3.6 Seguimiento de las recomendaciones

La expresión recomendaciones refleja a la perfección que Auditoría Interna no tiene autoridad ejecutiva para ordenar acciones concretas como resultado de un informe. De ahí que formule sus consejos y sugerencias por medio de recomendaciones, que tienen que cumplir determinados requisitos:

- Han de ser oportunas, viables y sustanciales.
- Deben dirigirse a personas o instancias identificables, que además tengan competencia suficiente para implantarlas.
- Tienen que ser claras y fácilmente comprensibles.

- En la medida de lo posible, debieran poder cuantificarse y evaluar su impacto en los resultados de la organización.

Las recomendaciones son el fruto de la auditoría, y se basan en las observaciones y conclusiones obtenidas por los auditores internos durante la realización de la misma.

En esas recomendaciones se concreta el valor de un informe de Auditoría Interna, hasta tal punto que, si no se cumplen, sería como decir que Auditoría Interna no tiene sentido en la organización. Por esto es fundamental efectuar su seguimiento, para lo cual el director o responsable de Auditoría Interna ha de establecer un procedimiento que incluya los siguientes tres aspectos:

- Un plazo de tiempo para su cumplimiento y el responsable de la implantación.
- Un mecanismo para verificarlo.
- Un canal de comunicación con la Comisión de Auditoría o el Consejo de Administración, para informar sobre incumplimientos, actuaciones no satisfactorias, etc., especificando los riesgos que se asumen.

Por todo ello, el cumplimiento de las recomendaciones de Auditoría Interna debe de ser uno de los objetivos prioritarios de la misma, y reflejarse como tal, es decir, debe ser medible, cuantificable, en la planificación anual de la función.

Comunicación de Resultados. Los informes de Auditoría Interna

Instituto de Auditores Internos de España

De un tiempo a esta parte, los informes de Auditoría Interna se han convertido en elemento esencial no sólo para los propios departamentos de Auditoría Interna, sino para toda la organización.

Son el vehículo que tiene la función para comunicar las conclusiones de los proyectos de Auditoría Interna contenidos en el plan anual. El objetivo fundamental es poner de relevancia si los riesgos se encuentran adecuadamente gestionados por la organización, y si no es así, identificar las mejoras potenciales en los procesos vía recomendaciones.

Además, un factor esencial que hay que destacar es el creciente número de destinatarios internos y externos que tiene el informe de Auditoría Interna, los llamados *stakeholders* o grupos de interés.

Por estos motivos, la elaboración del informe tiene que ser una actividad en la que, al igual que hemos realizado en las fases previas, apliquemos la máxima excelencia para que el resultado de todo nuestro trabajo se plasme de manera objetiva, clara y eficiente.

Los puntos que aborda este capítulo desarrollan estas ideas, que sirven como directrices generales a la hora de elaborar los informes de Auditoría Interna. No obstante, hay que tener presente también que los informes hay que adaptarlos a cada organización y a cada destinatario, elaborando si es preciso informes *adhoc* para que nuestro mensaje llegue al destinatario con la máxima eficiencia.

En general, el producto que vende Auditoría Interna es el informe, de ahí que éstos adquieran gran importancia y relevancia, entre otras razones, porque normalmente se remiten a la Comisión de Auditoría y al Consejo de Administración, así como a la Alta Dirección y son el medio de Auditoría Interna para dar a conocer sus opiniones y recomendaciones; en definitiva, son su vehículo de comunicación.

Por la importancia de los informes de Auditoría Interna, hay que prestar especial atención a su redacción y presentación. La minuciosidad y el examen de los informes una vez redactados y listos para ser distribuidos exige un cuidadoso procedimiento que elimine errores y fallos de cualquier clase y evite apresuramientos e improvisaciones.

Especial relevancia en este proceso, cuando se tiene el borrador de informe, es contrastarlo antes de su versión definitiva con los responsables que han estado involucrados en el proceso de auditoría. Este aspecto requiere una mención especial en este capítulo, ya que es esencial al presentar el informe definitivo frente a la Comisión de Auditoría que todos los elementos hayan sido contrastados. De esta manera, se evitan las posibles sorpresas de última hora, relativas a nueva documentación que surge o nuevas interpretaciones que hacen que determinadas conclusiones tengan un nuevo matiz.

Conviene tomar las siguientes precauciones:

- Revisar cifras y datos detenidamente.
- Leerlo por auditores que no lo hayan redactado ni intervenido en la auditoría.
- Comprobar la adecuación de opiniones y recomendaciones.
- Verificar su fundamentación documental y racional.

Toda la atención y cuidados que se dediquen a la redacción y presentación de un informe de Auditoría Interna no serán nunca excesivos y producirán, sin duda, los mejores resultados para Auditoría Interna y para la organización. Porque el informe refleja, condensa y divulga la opinión de los auditores y sus recomendaciones y es la prueba elocuente de su calidad y de su acierto, o de sus carencias, en el trabajo que han realizado.

1. Qué es un informe de Auditoría Interna

Un informe es el resultado de la información, estudios, investigaciones y análisis efectuados por los auditores internos durante la realización de una auditoría que, de forma normalizada, expresa por escrito su opinión sobre el área o actividad auditada en relación con los objetivos fijados, señala las debilidades de control interno, si las ha habido, y formula las recomendaciones pertinentes para eliminar las causas de tales deficiencias y establecer las medidas correctoras adecuadas.

El informe de Auditoría Interna *"es el medio principal para comunicar el resultado de la labor realizada y representa para el auditor interno la oportunidad de captar la atención de la dirección respecto a la fiabilidad, adecuación y suficiencia de la información sobre la que basa sus decisiones, promoviendo su confianza en el correcto funcionamiento de la organización. En caso necesario, ha de motivar a la acción mediante la exposición clara y convincente de aquellos aspectos que precisan mejorarse, proporcionando sugerencias sobre ahorros de coste, mejoras en el control, nuevos enfoques de gestión, etc."*

La **Norma 2400, Comunicación de los Resultados,** señala los requisitos o condiciones que los informes han de reunir y que resumimos a continuación.

1.1 Requisitos

La **Norma 2420 referente a la Calidad de la Comunicación** *establece que "las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas".*

En este punto, consideramos interesante destacar el artículo que el expresidente del Instituto Global de Auditores Internos Global (IIA), Richard Chambers, publicó bajo el título *Escribir un informe de auditoría impactante: 6 consejos para ser más persuasivo*[1], porque nos da una idea de la importancia del informe de auditoría en nuestra profesión.

Destacamos algunas ideas interesantes de ese artículo:

- **Finalidad.** La finalidad del informe de Auditoría Interna es persuadir a sus lectores para que puedan tomar medidas. En este contexto adquiere especial relevancia el estilo de escritura, que es lo que motiva a tomar esas medidas y dará lugar a una llamada a la acción para obtener resultados.

- **Lo bueno, si breve…** Los informes de Auditoría Interna son más persuasivos cuando se adaptan a las necesidades de nuestros grupos de interés. Si abrumamos con demasiada información, nuestros informes tendrán menos impacto. Si una palabra, idea o frase no contribuye directamente al punto, considere eliminarla.

- **Simplicidad.** Los mejores informes de Auditoría Interna expresan grandes ideas en pocas y pequeñas palabras, nunca pequeñas ideas en grandes palabras. Esto no significa tener que bajar el nivel en nuestros informes; pero sí significa una comunicación clara y efectiva, lo opuesto a la jerga legal.

  Existe evidencia convincente de que el lenguaje sencillo tiene más probabilidades de ser leído, comprendido y atendido en mucho menos tiempo: vende las ideas mejor. Es más probable que su escritura sea más persuasiva si no es pomposa, innecesariamente complicada o está cargada de jerga técnica.

- **Destacar las mejores ideas.** Mantener los textos y frases cortos y simples puede ayudar, pero también debemos organizar nuestros informes para resaltar las ideas más importantes. En ocasiones es apropiado utilizar un resumen ejecutivo, una tabla de contenido y/o un índice para ayudar al lector a encontrar fácilmente información del informe. Para informes más largos, un resumen ejecutivo es esencial. Los *stakeholders* tienen diferentes necesidades, por lo que debemos ayudar a los lectores individuales a acceder a la información específica que necesitan.

- **Considerar las implicaciones.** Todos tratamos de ser imparciales, pero a veces pasamos por alto la implicación de nuestras palabras. Si queremos que los lectores acepten nuestras ideas, nuestro tono debe ser objetivo, incluso cuando enviemos un mensaje negativo. Raramente persuadimos haciendo que alguien sienta hostilidad que le obligue a adoptar una actitud defensiva. Si nuestro informe parece parcial o injusto, es probable que el cliente desconecte.

1. Richard Chambers blog. Artículo: *Escribir un informe de auditoría impactante: 6 consejos para ser más persuasivo.*

- **Recuerda las Cinco C.** En este punto es importante destacar los cinco componentes de las observaciones y recomendaciones que tiene que contener un informe de Auditoría Interna:
  - Criterios (lo que debería ser).
  - Condición (el estado actual).
  - Causa (el motivo de la diferencia).
  - Consecuencia (efecto).
  - Planes de acción Correctiva / recomendaciones.

  Incluso utilizando la técnica de las cinco C, es posible que el informe no sea persuasivo. Pero sin las cinco C, las posibilidades de éxito se desplomarán. La descripción de las posibles consecuencias es particularmente importante, porque empuja a la gerencia a la acción. Indica quién se beneficiará, cómo se beneficiarán y por qué. A menudo, la persuasión se potencia si las consecuencias se describen en términos orientados a los negocios, con elementos medibles y marcos de tiempo específicos.

1.2 Elaboración de los informes

El proceso de elaboración de un informe de Auditoría Interna es complejo y delicado. Hay que tener presente que, por lo general, en ellos se señalan deficiencias y fallos de los controles, sistemas y procedimientos, de los que son responsables en última instancia los más altos niveles directivos de las organizaciones. Además, incluyen sugerencias y recomendaciones sobre cómo eliminarlos, lo que puede resultar aún más incómodo para quienes no se apercibieron de tales fallos y deficiencias.

Partiendo de la consideración de que la precaución y la cautela siempre son necesarias, el auditor interno no ha de omitir en su informe todo aquello que estime fundamental para la correcta gestión de la organización, aunque pueda resultar molesto para algunos responsables, e incluso para los más altos niveles de la misma. Este es uno de los riesgos de la Auditoría Interna: decir lo que hay que decir, si bien de la manera menos molesta posible, sin excluir la reserva, confidencialidad y discreción necesarias, cuando así lo exijan las circunstancias y la categoría de las personas responsables de las actividades auditadas.

En este contexto, una buena aproximación para que el informe de Auditoría Interna sea más receptivo por parte de las áreas auditadas es que todos los aspectos positivos que se hayan identificado al realizar la auditoría *(best practices)* se pongan de manifiesto. Esta práctica, además de ser bien acogida por parte del área auditada, nos sirve para identificar mejores prácticas que en su caso podrán ser aplicadas en procesos/compañías similares que tengan el mismo problema.

Siempre es conveniente elaborar un **informe borrador** una vez llevadas a cabo las diferentes fases del programa de la auditoría para su comentario y discusión con los auditados. Se llama así, informe borrador, porque las opiniones, recomendaciones, conclusiones y observaciones no han sido aún contrastadas formalmente con la realidad auditada y, por tanto, no se ha discutido con los auditados. Su finalidad es servir de punto de partida de la reunión de discusión, antes de la definitiva publicación del informe. Este informe borrador se recomienda que incluya fecha de revisión, ya que es habitual que el contraste del informe de Auditoría Interna conlleve varias revisiones para corroborar que todas las conclusiones se encuentren consensuadas.

Tanto los borradores como los informes han de ser debidamente controlados en el momento de su emisión o distribución. En este sentido, es aconsejable que todas las páginas del informe incluyan la marca de agua de confidencialidad. Además, independientemente de los registros de control de difusión que Auditoría Interna tiene que mantener, es recomendable que en la carátula del informe incluya los destinatarios del informe de Auditoría Interna.

El archivo de apoyo de los informes (soporte), ya sea en papel o electrónico, recoge el conjunto de información, documentos, papeles de trabajo (PPTT), que han de conservarse después de realizada la auditoría, y debe comprender, entre otros, los siguientes aspectos o elementos:

- PPTT.
- Memorándum o notas redactadas por los auditores internos.
- Documentos, impresos, fotocopias, etc., utilizados.
- Planificación y programa de la auditoría.
- Borrador del informe.
- Informe definitivo.
- Auditores que han efectuado la auditoría.
- Tiempo empleado.
- Plan de acción previsto.
- Cualquier otra información pertinente.

1.3 La discusión de los informes

La **Norma 2440 Difusión de Resultados** establece que *"el Director de Auditoría Interna debe difundir los resultados a las partes apropiadas".* Esto significa que, previamente, debe revisar y aprobar la comunicación final del trabajo antes de su emisión y decidir a quiénes y cómo será distribuida dicha comunicación. El Director de Auditoría Interna retiene la responsabilidad última, aunque delegue estas tareas.

El auditor interno debe discutir las conclusiones y las recomendaciones con los niveles directivos apropiados antes de emitir el informe final escrito. Es importante tener en cuenta dos aspectos.

1. La discusión de las conclusiones y recomendaciones se realiza, generalmente, durante el desarrollo de la auditoría y/o en reuniones posteriores a su finalización (entrevistas finales). Otra técnica consiste en la revisión del borrador de los informes de Auditoría Interna por el responsable de cada área auditada. Estas discusiones y revisiones sirven para asegurar que no ha habido equívocos o malas interpretaciones de los hechos, al proporcionar al auditado la oportunidad de clarificar detalles concretos y expresar su punto de vista sobre las observaciones, conclusiones y recomendaciones.

2. Aunque el nivel de los participantes en las discusiones y revisiones puede variar dependiendo de las organizaciones y de la naturaleza del informe, generalmente deben estar incluidas aquellas personas conocedoras del detalle de las operaciones, y aquellas que pueden autorizar la puesta en marcha de la acción correctora.

La discusión de los informes se realiza en la REUNIÓN DE DISCUSIÓN, fundamentalmente para discutir sus recomendaciones, que son la esencia de los mismos.

En esta reunión es necesario considerar una serie de aspectos que son básicos para el éxito de la misma:

- **Transparencia.** Nada tendría que escribirse en el borrador que no haya sido comentado previamente con los auditados en cuanto se refiera a las recomendaciones y sugerencias.

- **Prioridad de información.** Quien primero ha de ser informado sobre la auditoría es el responsable directo con el que los auditores internos han trabajado y de quien han recogido la información en el desarrollo del programa de la auditoría.

- **Valoración de las recomendaciones.** Deben de exponerse en función de su importancia y de las consecuencias que de su no implantación pueden derivarse para la organización.

- **Ejecutividad.** Los informes son eficaces en la medida en que generan actuaciones inmediatas, que se ponen en marcha desde el momento posterior a su discusión.

- **Orden.** Es necesario que la reunión transcurra ordenadamente, centrándose los participantes en el análisis de lo fundamental, que son las recomendaciones y conclusiones del informe.

- ***Vender* el informe.** Se trata de la mejor aceptación del informe, de su "venta", y no de dar lectura a un documento, por lo cual la reunión ha de ser convenientemente prepa-

rada por los auditores. Transparencias, gráficos, programas informáticos, etc., con los puntos esenciales que se quieren destacar, suponen tantos a favor de los auditores, sin perjuicio de la imprescindible base de apoyo que son los PPTT, y de los documentos que vayan a ser utilizados.

Las recomendaciones son el momento más delicado de la reunión, en el que con frecuencia se originarán diversidad de puntos de vista y opiniones.

En la reunión de discusión se establecerá el plan de acción al que se comprometen los auditados, que conviene quede reflejado en el acta de la reunión, indicando para cada recomendación quién se responsabilizará de la misma y el plazo límite para su implantación.

En los supuestos en los que el auditor considere necesario no ceder en la esencia de una recomendación y se produzca una disparidad de opiniones entre él y el auditado, el auditado deberá dejar constancia por escrito en los informes en el apartado comentarios para cada una de las recomendaciones los motivos de su desconformidad.

1.4 Seguimiento de las recomendaciones

La auditoría no finaliza con la emisión del informe y su difusión a los diferentes *stakeholders*. Hay que organizar un proceso de seguimiento de las recomendaciones para garantizar que todos los aspectos incluidos en el informe, llegada su fecha de implementación, han sido solventados correctamente. Para ello, el auditor interno pedirá evidencias de que la recomendación ha sido implantada para concluir que la debilidad que motivó la inclusión de la recomendación en el informe de Auditoría Interna ha sido subsanada.

Este aspecto es esencial en el proceso de auditoría, ya que –tal como venimos comentando a lo largo del capítulo– nuestro objetivo es proporcionar aseguramiento de que los riesgos están siendo controlados.

Por este motivo es muy importante montar un procedimiento mediante el cual podamos informar a la Comisión de Auditoría del grado de implantación de las recomendaciones que contienen los informes de Auditoría Interna emitidos. Dependiendo el tipo de organización, la periodicidad del seguimiento se realizará trimestral o semestralmente. No aconsejamos realizar un seguimiento superior al semestral ya que, con toda probabilidad, en ese periodo de tiempo se producirán vencimientos de recomendaciones que necesitan ser implantadas, y por lo tanto revisadas por el equipo de Auditoría Interna.

Especial atención en este proceso tienen que conllevar las recomendaciones con impacto alto / medio, cuya no implementación o implementación no correcta en la fecha acordada,

puede generar un problema desde el punto de vista de auditoría. Si nos encontramos con esta situación, hay que averiguar en primer lugar el motivo de la no implementación en fecha y, dependiendo del caso concreto, se podrá plantear una nueva fecha de implementación si el riesgo durante ese periodo de tiempo se puede asumir. De lo contrario, este hecho se tendrá que escalar a la Comisión de Auditoría para que sea consciente de que hay un riesgo que no se está gestionando adecuadamente por parte de la organización.

Auditoría de Gestión

1. Antecedentes de la auditoría operativa
2. Evolución de la auditoría operativa
3. Naturaleza de la auditoría operativa
4. Concepto de la auditoría de gestión
5. Definiciones
6. El auditor como consultor de la Alta Dirección

Instituto de Auditores Internos de España

Deberíamos empezar por aparcar la expresión "auditoría operativa", pues tal como indicamos en el primer capítulo, Auditoría Interna hoy se hace sobre operaciones, actividades, funciones y estructuras. Incluso las auditorías verificativas no pueden limitarse a comprobar que se cumplen las normas y procedimientos establecidos, sino que también han de analizar su necesidad, racionalidad y conveniencia, o sea, sus procedimientos operativos.

Entendemos que, lo que hasta ahora se ha venido llamando **auditoría operativa,** no es más que el tipo o forma de hacer auditoría que hoy efectúan los modernos departamentos de Auditoría Interna, sobre los sistemas, procesos, estructuras, políticas, programas, planes y actividades similares y que, sin duda, podemos llamarlas auditorías de gestión, pues la gestión descansa sobre todas las acciones de la dirección de una organización, que intenta planificarla, coordinarla, controlarla, administrarla y dirigirla eficientemente.

En cualquier caso, estas auditorías son el principal desempeño de Auditoría Interna que, superando el campo económico-financiero y contable, examinan de forma periódica y permanente el conjunto de funciones que integran la gestión de una organización, para comprobar su eficacia y buen funcionamiento, proponer mejoras y suprimir deficiencias y disfunciones, en un clima de mutua cooperación con los auditados y no de desconfianza y confrontación.

Y llamaríamos **auditorías de gestión** a aquellas que analizasen la gestión global de una organización y de su equipo de dirección, incluido su Consejo de Administración examinando la calidad de sus controles de su gestión, por medio de los resultados obtenidos a corto plazo, de sus planes estratégicos, de sus políticas y de sus programas. Se trataría de comprobar la eficiencia con que se están gestionando los recursos de la organización, si se están cumpliendo los principios del buen gobierno corporativo, su viabilidad de desarrollo futuro y su competitividad.

Lógicamente, si la finalidad de una auditoría es analizar y evaluar la gestión de los administradores y directores de una organización, será muy difícil que sea la propia unidad de Auditoría Interna quien la ejecute, aunque esté mejor preparada que cualquier otra instancia externa y pese a que, como un informe de Auditoría Interna que es, el destinatario y único poseedor del mismo sería el Consejo de Administración, en el supuesto de que fuera este órgano quien lo hubiera solicitado.

En la realidad, este tipo de auditorías se lleva a cabo cuando lo disponen los accionistas mayoritarios de una organización, o cuando la auditoría corporativa de un grupo empresarial audita a sus empresas filiales.

En el Anexo 11 se incluye un posible programa de una auditoría de esta naturaleza.

1. Antecedentes de la auditoría operativa

El término "auditoría operativa" (AO) fue utilizado por primera vez por auditores internos progresistas en los años cincuenta para describir el trabajo que estaban realizando con el objetivo de buscar la mejora de las operaciones que auditaban. El enfoque constructivo, las técnicas y los resultados positivos que caracterizan a la AO fueron empleados en principio en la fabricación, comercialización y marketing, pero son igualmente aplicables a las actividades públicas, instituciones financieras, económicas, organizaciones de servicios y a cualquier organización de suficiente tamaño para mantener una Auditoría Interna como función separada o específica.

La auditoría operativa se caracteriza por el enfoque y la mentalidad del auditor interno, no por métodos distintos. Puede ser una ampliación de las normales actividades de Auditoría Interna, esto es: financieras o de revisión de ciclos. La auditoría operativa aplica las habilidades, conocimientos y técnicas de los auditores internos a los específicos controles operativos que existen en los negocios. El sentido común y una buena visión personal de las actividades del negocio son los activos fundamentales de un buen auditor operativo, forma o tipo de auditoría que caracteriza a las modernas auditorías internas.

Fue en 1947 cuando se reconoció que el alcance de la Auditoría Interna podía extenderse a la revisión de las operaciones y ello se hizo en la ***Declaración de Responsabilidades de los Auditores Internos*** (ver Anexo 2) que describió la naturaleza y objetivos de la Auditoría Interna como sigue: *"La Auditoría Interna es una actividad de valoración, independiente dentro de una organización, para la revisión de la contabilidad, finanzas y otras operaciones como un servicio a la dirección. Es un control de dirección que funciona midiendo y evaluando la efectividad de otros controles. El objetivo global de la Auditoría Interna es asistir a todos los miembros de la dirección en la efectiva ayuda de sus responsabilidades, suministrándoles análisis objetivos, valoraciones, recomendaciones y comentarios pertinentes relativos a las actividades revisadas. El auditor interno, por tanto, debería estar interesado en cualquier fase de la actividad del negocio que pueda ser un servicio a la dirección".*

2. Evolución de la auditoría operativa

La extensión de las responsabilidades del auditor interno a las operaciones es una lógica evolución de la inicial delegación de responsabilidades al auditor para la protección de los intereses de la compañía. La Auditoría Interna protectora es una función que existe en cualquier negocio. Por ejemplo, en una tienda donde dos dependientes trabajen, el propietario está continuamente alerta a cómo éstos están realizando sus deberes. El propietario, casi involuntariamente, vigilará

para ver que las ventas se hacen adecuadamente, que los justificantes de las mismas se preparan correctamente, que las ventas en efectivo se registran en caja, que las mercancías se colocan con el debido orden en los estantes, que los clientes son tratados con corrección por los empleados, en suma, que todo esto lo hacen los empleados para que la tienda consiga beneficios. Cuando vigila el registro de caja, el propietario está haciendo Auditoría Interna protectora; cuando observa cómo son tratados los clientes, está haciendo en realidad auditoría operativa.

Cuando un negocio se desarrolla hasta el punto de que el dueño ya no puede vigilar personalmente todo lo que se hace, delega alguna de estas funciones de auditoría a los subordinados. Esta primera delegación es apta para reforzar la responsabilidad de los controles que protegen al negocio contra el fraude, despilfarros o pérdidas, los controles protectores. Esto es lógico porque estos controles pueden establecerse definitivamente y reforzarse con poca necesidad de juicio y conocimiento para determinar que se aplican adecuadamente. Por ejemplo, asumir procedimientos para el registro de ventas en efectivo. Si éstos son registrados como determina la observación, son correctos; si no son registrados así, están equivocados. Poco juicio o sentido del negocio se requiere para verificar y evaluar esta situación.

Sin embargo, cuando el tamaño y complejidad de las operaciones de los negocios aumentan, las auditorías internas van más allá de las simples situaciones en que su evaluación se basa en un claro y obvio correcto o incorrecto. La atención de los auditores puede estar y está enfocada en el cumplimiento de los procedimientos y en la efectividad de cómo la auditoría puede contribuir a la mejora de la unidad auditada y a la salud del negocio entero. Junto con la especialización del trabajo del personal que opera en los departamentos, está la asignación de responsabilidades funcionales a los distintos departamentos. Cada departamento desempeñará las tareas asignadas de la mejor forma posible, pero ellas son solamente una parte del trabajo total de la organización.

Como resultado, es a veces difícil para cualquier director o jefe de un departamento tener una visión objetiva con una adecuada perspectiva del conjunto de la organización. El ejecutivo estará interesado casi enteramente en la dirección del área de la organización que se le ha asignado, incluso aunque fuese posible una operatividad más efectiva por medio de una mejor coordinación y comunicación con otros departamentos.

El éxito de los negocios es una conjunción de esfuerzos en equipo. El auditor interno es el miembro de un equipo que examina los controles que la dirección general y departamental ha establecido sobre las operaciones. El auditor interno evalúa la manera en que tales controles funcionan para conseguir la más efectiva y beneficiosa operatividad del equipo.

En resumen, el trabajo del auditor es asegurar a la dirección que los controles que gobiernan las operaciones están adecuadamente concebidos y efectivamente administrados y que ayudan

a la consecución de los beneficios de la organización. Si esta seguridad no puede darse, el auditor debe recomendar medidas correctoras hasta donde sus capacidades le permitan. Si la situación va más allá de la experiencia y competencia del auditor, deberá comunicar sus resultados recomendando estudiar el problema más ampliamente.

3. Naturaleza de la auditoría operativa

La naturaleza de la auditoría operativa está adecuadamente ilustrada por el punto de vista expresado por dos altos ejecutivos de dos grandes compañías, que estaban participando en reuniones con sus equipos de auditoría y cuyo diálogo reproducimos a continuación.

– Ejecutivo 1. *"Yo quiero que ustedes asuman que son los propietarios de estos negocios y que éstos y sus beneficios les pertenecen. Antes de que ustedes recomienden un cambio, antes de que critiquen una operación, pregúntense si ustedes lo harían si el negocio fuera suyo".*

– Ejecutivo2. *"Quiero que ustedes, auditores internos, miren su trabajo como si estuvieran haciendo las cosas que la Dirección haría si tuviera tiempo para hacerlas".*

Ambos puntos de vista son lo mismo: el auditor interno deberá pensar como piensa un director general. La Dirección tiene solamente un interés secundario en el control protector; su principal interés está relacionado con las actividades, y los controles que afectan a dichas actividades son la esencia de la auditoría operativa.

Como se señaló anteriormente, la auditoría operativa debería considerarse como una óptica o visión, análisis y pensamiento, no un tipo distinto y separado de auditoría, que se caracteriza por técnicas y programas especiales. Una concepción errónea muy común entre los auditores internos es que existe una clara distinción entre auditoría operativa y auditoría financiera. Ellos esperan manuales especiales que les digan cómo hacer auditoría operativa, cuando todo lo que realmente se necesita es un cambio en su propia forma de enfoque y análisis.

La Auditoría Interna tradicional estaba en su mayoría dirigida a la valoración y análisis de los controles protectores, a menudo ajustándose a dogmáticas normas de control financiero. La auditoría operativa comienza por familiarizarse con las operaciones actuales y los problemas operativos o de funcionamiento, continuando con el análisis de los controles para asegurar que éstos son adecuados para proteger a la organización. Sin embargo, esto es sólo el principio de la auditoría.

4. Concepto de la auditoría de gestión

En los tres epígrafes anteriores hemos seguido el libro *Cadmus Operational Auditing,* de David S. Kowalecyk, porque explica sencilla y claramente los antecedentes, evolución y naturaleza de la auditoría operativa y que, en adelante, llamaremos auditoría de gestión, insistiendo en el hecho de que ésta es la auditoría que en la actualidad realizan las unidades de Auditoría Interna modernas, servidas por profesionales cualificados como auditores internos. Una auditoría incomparablemente más amplia que el análisis de los controles establecidos, puesto que el contenido funcional de una unidad de Auditoría Interna hoy se desarrolla a partir de su alcance, que es el asegurar, en la medida de lo posible, el sistema de control interno de las organizaciones.

Teniendo en cuenta que, según la concepción más reciente de control interno, este es un proceso que trata de conseguir los tres objetivos básicos –fiabilidad[1] de la información, eficiencia operativa y cumplimiento de leyes y regulaciones externas e internas–, podemos deducir la amplitud de funciones y responsabilidades de Auditoría Interna en la actualidad, y cómo toda o casi toda la actividad auditora de una unidad de Auditoría Interna es auditar las operaciones en las que se basa la gestión de las organizaciones.

Este fue, precisamente, el origen de la auditoría moderna, la necesidad de extender la función de auditoría a todo el conjunto de las operaciones y actividades de las empresas, y ello en virtud de una serie de razones, entre las que destacamos las siguientes:

- Necesidad de cubrir todas las áreas de riesgo de las organizaciones y no tan sólo las administrativas o económico-financieras.
- Satisfacer la demanda de información objetiva y fiable que precisan las direcciones sobre lo que sucede en el conjunto de su organización, respecto a los objetivos de la organización, al cumplimiento de normas, directrices, políticas, leyes y regulaciones.
- Por lo general, las personas responsables de la línea operativa de las organizaciones no disponen de tiempo para dedicarse a comprobar la eficacia y eficiencia de los controles y la utilización óptima de los recursos, ni por otra parte conocen bien las técnicas y métodos de análisis que se emplean.
- La mayoría de las organizaciones importantes están obligadas por ley a someterse a auditorías de cuentas efectuadas por compañías auditoras externas, lo que contribuye a cubrir los riesgos de tipo contable o económico-financiero.

Resumiendo, si se compara todo lo que venimos escribiendo sobre auditoría de gestión con lo que hemos expuesto sobre concepto, filosofía y definiciones de Auditoría Interna sin más adje-

1. Fiabilidad entendida como calidad del dato y en consonancia con el concepto de *Data Governance* en las organizaciones.

tivos, el lector comprobará que no se diferencian en nada. En apoyo de cuanto afirmamos, exponemos en el epígrafe que sigue diversas definiciones sobre auditoría de gestión.

Una última observación: no hemos estado nunca de acuerdo en que la auditoría de gestión, la moderna Auditoría Interna, consista simplemente en un cambio de visión y mentalidad del auditor y no en métodos diferentes a los de las auditorías clásicas.

Hacer Auditoría Interna en la actualidad exige técnicas y programas específicos, habilidades y condiciones profesionales concretas, que no son en absoluto necesarias para realizar auditorías financieras y, sobre todo, una amplísima cultura empresarial y de organización y economía de la empresa. A este respecto, el auditor interno moderno debe formarse y evolucionar hacia una auditoría que va más allá de los márgenes establecidos; una auditoría interna que evoluciona hacia la combinación temprana de conceptos como el de auditoría integrada en los procesos (auditoría preventiva) y el de la auditoría continua.

5. Definiciones

Comenzaremos por nuestra propia definición: *Examen realizado por auditores, y según las técnicas y métodos de auditoría, del conjunto o de parte de las áreas, funciones o actividades de una organización, comprobando la eficiencia y adecuación de su sistema de control interno.*

- L. B. Sawyer da una primera y breve definición de la auditoría de gestión diciendo que es una revisión que comprende las actividades, sistemas y controles dentro de una empresa, para conseguir economía, eficiencia, efectividad u otros objetivos.

  Y más adelante señala que se precisa otra definición para describir la amplitud de evaluaciones que contempla la Auditoría Interna moderna, para lo cual da la definición que, de forma resumida, indicamos a continuación: *"Una sistemática y objetiva evaluación realizada por auditores internos, de las diferentes operaciones y controles de una organización, para determinar si se siguen políticas y procedimientos aceptables, si se siguen las normas establecidas, si se utilizan los recursos eficientemente y si se han alcanzado los objetivos de la organización".*

- Willian P. Leonard, que fue el primero que despertó en nosotros el interés por la auditoría de gestión, en su libro *The Management Audit* –traducido al español por la Editorial Diana, de México, con el título de *Auditoría Admistrativa*– la define de la siguiente manera: *"Un examen completo y constructivo de la estructura organizativa de una empresa, institución o departamento gubernamental, o de cualquier otra entidad, de sus métodos de control, medios de operación y del empleo que dé a sus recursos humanos y materiales"*

· Finalmente, la publicación de la Generalidad de Cataluña, *Tecniques d'Auditoría Operativa Aplicades a l'Administració Pública,* de la que son autores **Jordi Mas** y **Carles Ramió,** la define de la siguiente forma: *"La auditoría operativa o de gestión analiza los sistemas, los procedimientos, las estructuras, los recursos humanos y materiales y los programas de los diferentes complejos de organización de la Administración Pública. Es decir, el campo de actividad de esta auditoría incluye todas las funciones que integran la gestión pública, para verificar su buen funcionamiento, proponer mejoras y modificar los comportamientos disfuncionales".*

Todas las definiciones anteriores están identificando los objetivos y el alcance de la función de Auditoría Interna moderna. A lo largo de este capítulo se han expuesto razones suficientes para afirmar que la auditoría operativa es auditoría sobre áreas de gestión y que ésta es, a su vez, la moderna Auditoría Interna, por lo que, tal como expresábamos al comienzo , realmente no hay más que dos clases de auditorías, que constituyen dos profesiones diferentes: Auditoría Externa o de Cuentas y Auditoría Interna, ambas con la exigencia de independencia para sus auditores, lo que significa que la independencia no es suficiente para distinguirlas.

6. El auditor como consultor de la Alta Dirección

La unión de las palabras auditoría y consultoría, por lo general, produce cierta confusión y, en ocasiones, se nos ha preguntado qué sentido puede tener esta relación, lo que nos mueve a tratar de clarificar la situación en que Auditoría Interna actúa como puede hacerlo una compañía externa de consulta.

Hay que señalar que el ejercicio de la función de consulta y asistencia técnica no desvirtúa el contenido funcional de una unidad de Auditoría Interna, sino que refuerza la imagen del auditor que trata de prestar a la organización otro servicio más, porque está en condiciones para hacerlo mejor que nadie, en principio.

La Asociación Española de Empresas de Consultoría define la consultoría en dirección y organización como *"la prestación de consejos y asistencia independiente sobre asuntos de dirección y organización. Normalmente incluye identificación y estudio de problemas y/o de oportunidades, recomendando acciones apropiadas y ayudando a implantar tales recomendaciones".* Y recomendar acciones apropiadas es la tarea en la que se concretan los informes de Auditoría Interna.

En la mayoría de las grandes organizaciones de hoy, buena parte de los trabajos que se encargan a los consultores externos podrían ser efectuados por los propios profesionales de éstas, porque las conocen suficientemente y porque están preparados para ello. Sin embargo, las direcciones recurren a ellos, entre otras razones no siempre confesables, porque piensan que la visión in-

dependiente y objetiva del consultor externo es garantía de falta de prejuicios, y porque creen que el consultor acumula experiencia, especialización y conocimientos diversos que no poseen sus empleados. Este es el camino que nos conduce a comprender la nueva imagen del auditor-consultor, ya que la objetividad y la falta de prejuicios son exigencias que garantizan, entre otras, la profesionalidad del auditor interno. Si a éstas unimos la independencia y un conocimiento global, profundo y gerencial de la organización en la que prestan sus servicios, creemos que, salvo para aplicaciones de muy alta especialización, Auditoría Interna se encuentra en inmejorables condiciones para llevar a cabo este tipo de trabajo.

Existen también otras razones por las que recomendamos que Auditoría Interna efectúe de cuando en cuando trabajos de consulta. Algunas de ellas son:

- Auditoría Interna no debe ser ajena a la contratación de servicios externos, que cuando adquieran cierta importancia tendrían que ser auditados.
- El consultor aplica "recetas" y su análisis es obligadamente superficial, pues su tiempo es limitado.
- El consultor no tiene la preocupación indeclinable de asegurar en lo posible el control interno y evitar riesgos.
- El consultor tiende a complacer al cliente.
- Sus estudios y proyectos quedan en la mayoría de las veces al arbitrio del cliente.
- El coste del consultor externo es incomparablemente más alto que el del servicio que pueda prestar la Auditoría Interna.
- El auditor-consultor ha de profundizar hasta conseguir la evidencia o certeza de que su investigación y conclusiones se apoyan sobre bases sólidas.
- El auditor-consultor conoce la organización y su sector de actividad y su tiempo no es, hasta cierto punto, un factor condicionante.
- Su independencia no está presionada por aspectos comerciales o de intereses ajenos al bien de la organización
- El seguimiento de sus recomendaciones es obligado por las *Normas para el Ejercicio Profesional de la Auditoría Interna.*

Sin embargo, esta capacidad del auditor interno para realizar auditorías de consulta no debe entenderse como una total dedicación de su tiempo a esta actividad, sino como una manera de trabajar esporádicamente para resolver problemas de carácter confidencial o especial, así como situaciones que podríamos llamar delicadas o especialmente difíciles para ser tratadas desde el exterior de la organización.

En cualquier caso, los servicios de consultoría están actualmente incluidos en la definición oficial de Auditoría Interna proporcionada por el Instituto global (IIA), tal como hemos indicado en el Capítulo I. Asimismo, las Normas 1000C1; 1130C1; 1130C2; 1210C1; 1220C1; 2010C1; 2120C1; 2120C2; 2120C3; 2130C1; 2201C1; 2210C1; 2210C2; 2220C1; 2220C2; 2240C1; 2410C1; 2440C1; 2440C2 y 2500C1, así como las Guías de Implementación correspondientes contienen una exhaustiva información sobre los diferentes aspectos de los servicios de consultoría en relación con Auditoría Interna.

En la actualidad, el papel del auditor interno como consultor se está viendo especialmente reforzado en procesos de cesiones o adquisiciones de empresas, a través de las diligencias debidas, implantación de nuevos sistemas, etc.

Planificación de Auditoría Interna

Instituto de Auditores Internos de España

1. Introducción

En al capítulo V ya se describió cómo debe planificarse cada trabajo de auditoría, desde que se comienza hasta que se escribe el informe. Pero la **gran pregunta** a la que suele enfrentarse un departamento de Auditoría Interna es **¿cuáles son los trabajos de auditoría que debo hacer en mi compañía con los recursos disponibles durante, por ejemplo, el próximo año?**

En este capítulo vamos a dar respuesta a esa pregunta, ofreciendo una serie de pautas para identificar trabajos que acaban culminando en lo que tradicionalmente se denomina "Plan de Auditoría Interna". Ése es el documento en el que se recogen todos los trabajos que un departamento de Auditoría Interna va a realizar en un periodo de tiempo determinado. Abordamos ahora cómo se suele elaborar un plan de auditoría y qué debe contener.

2. Conceptos básicos del plan de Auditoría Interna

Responsabilidad del plan

La responsabilidad de elaborar el plan de auditoría recae en la Dirección de Auditoría Interna. Y, para su elaboración, el Director de Auditoría Interna (DAI) se suele apoyar en los auditores con mayor experiencia y conocimiento de la organización.

¿Cuánto tiempo cubre el plan de auditoría?

No hay una respuesta correcta. Es el DAI el que debe tomar esa decisión según la naturaleza de la organización para que el plan recoja el inventario de todos los trabajos a realizar por Auditoría Interna en un periodo de tiempo determinado. En los últimos tiempos, suele ser bastante frecuente que las unidades de Auditoría Interna elaboren dos planes de auditoría distintos: uno a corto plazo y otro a largo. De esta forma, pueden encontrar un equilibrio adecuado entre ofrecer al Consejo de Administración una visión a largo plazo (más estratégica) con una visión más a corto plazo (táctica/operativa). Las duraciones más habituales en las compañías que siguen esta visión largo/corto son:

- Plan a corto plazo: 6 meses o 1 año.
- Plan a largo plazo: entre 3 y 5 años.

¿Quién debe aprobar el plan de auditoría?

Las mejores prácticas indican que el plan de auditoría debe aprobarlo la Comisión de Auditoría. Aunque también suele ser muy conveniente su presentación y aprobación por parte del Consejo de Administración.

¿Cómo decido los trabajos a realizar? El mapa de riesgos.

Es la cuestión de mayor complejidad a la hora de elaborar el plan y no se puede resolver de forma sencilla. Conviene aflorar otro concepto: **el mapa de riesgos.**

Mapa de riesgos es el resultado que se obtiene del proceso que se sigue para identificar las actividades o procesos sujetos a riesgo de una compañía, de forma que pueda tener inventariado cuáles son los riesgos a los que está expuesta y la importancia de éstos. El mapa de riesgos es una herramienta fundamental para elaborar el plan de auditoría de una compañía, ya que los riesgos de mayor importancia deberían ser los más vigilados y, en consecuencia, los más auditados por el equipo de Auditoría Interna.

3. Cómo elaborar un plan de Auditoría Interna

La elaboración del plan de auditoría es una tarea que conlleva una dificultad elevada. Apuntamos las pautas generales que debe seguir Auditoría Interna para elaborar tanto un plan a largo plazo como a corto plazo.

Se suelen distinguir varias fases.

Aunque en la figura anterior se presenta un diagrama por fases, es importante destacar que no se trata de tareas secuenciales que se ejecutan una detrás de otra. Más bien lo contrario: casi se podrían pintar como tareas paralelas que se van retroalimentando unas a otras. Por tanto, el DAI no debe preocuparse de si, cuando esté formalizando el plan en un documento, descubre que hay cuestiones que no le encajan, o que le faltó incluir algún elemento en el universo de auditoría.

3.1 Elaborar el universo de auditoría

¿QUÉ ES EL UNIVERSO DE AUDITORÍA?

El primer paso a la hora de elaborar el plan debería ser la elaboración del Universo de Auditoría que es, simplemente, un listado de todos los posibles trabajos de auditoría que se pueden realizar.

UNIVERSO DE AUDITORÍA

A continuación presentamos un detalle de los principales procesos de megocio de la organización.

Planificación Estratégica
- Planificación estratégica.
- Comunicación partes interesadas.
- Metas y objetivos organizacional.
- Riesgos y preocupaciones.

Mercados de Capital
- Financiamiento (estructura cap.)
- Administración Riesgo de crédito.
- Manejo liquidez.
- Pago deudas.
- Relaciones con bancos.

Adquisiciones/Retiros
- Análisis Flexibilidad.
- Adquisiciones/Retiros.
- Joint Ventures.
- Due dilligence.

Cadena de Suministros
- Relación/integración suplidores.
- Contratos.
- Controles Tecnológicos.
- Manejo mercancía.
  - Aprobación.
  - Transportación.
  - Planificación & reemplazo.

Administración y Recursos
- Manejo materia prima.
- Contrato contingencias.
- Mantenimiento maquinarias.
- Higiene & seguridad.
- Pagos productos y servicios.
- Embarque & recepción.

Construcción/Desarrollo
- Selección lugar.
- Presupuesto proyecto, planificación y ejecución.
- Selección contratista.
- Ofertas/estimación proceso.
- Construcciones/mejoras.
- Monitoreo construcción (cambio órdenes, administración proceso, aprobación facturas).
- Contabilización proyectos.

Administración y Consejo
- Reuniones Consejo/Comité.
- Reuniones equipo directivo.
- Gobierno corporativo.
- Educación control interno.
- Auditoría Interna.
- Servicios legales.
- Cumplimiento regulatorio.

Finanzas & Contabilidad
- Cuentas por pagar.
- Facturación & cobros.
- Cuentas por cobrar.
- Opción Acciones & Comp. Ejec.
- Desembolsos de capital.
- Compras menores.
- Activos fijos.
- Presupuesto.
- Contabilización.
- Cierre contable.
- Informes internos & externos.
  - Revelación controles.
- Estados de gastos.
- Tesorería.
  - Administración activos.
  - Estructura deuda.
  - Manejo efectivo.
- Inversiones.
- Nómina.
- Impuestos.
- Cumplimiento regulatorio.
- Dividendos.
- Partes relacionadas.

Gestión de Riesgo
- Implementación Sistema ERM.
- Seguros.
- Pérdidas/obsolescencia inventario.
- Reclamaciones gerenciales.

Legal/Impuestos
- Contratos/arrendamientos.
- Manejo litigios.
- Prevención fraude.
  - Educación y previsión.
  - Código de Ética.
  - Línea de denuncias.
  - Responsabilidad penal organización.

Sistema información
- Estategia/Planificación.
- Desarrollo sistemas.
- Administración proyectos.
  - Selección/des. Programas.
- Mantenimiento sistemas TI.
- Administración red.
- Seguridad/Privacidad..
- Plan continuidad negocio.
- Información/adm. Registros.
- Ayuda escritorio.

Recursos Humanos
- Reclutamiento/contratación/terminación.
- Programa entrenamiento.
- Compensación & incentivos.
- Administración plan incentivos.
- Evaluaciones desempeño.
- Relación con empleados.

Fuente: Ejemplo 1 de Nahun Frett: http://nahunfrett.blogspot.com

Cómo se puede observar, el concepto es muy simple: una mera lista de todos los trabajos que Auditoría Interna considera que podría realizar en un periodo. Hay que resaltar que en el universo habrá trabajos que, finalmente, no se realizarán. Más adelante veremos cómo se toma esa decisión.

¿DE DÓNDE OBTENGO LA INFORMACIÓN PARA ELABORAR EL UNIVERSO?

Es una pregunta muy común que le puede surgir al DAI. Existen múltiples fuentes de información y herramientas para elaborar el universo. A continuación, se citan algunas:

- **Mapa de riesgos** de la compañía. Probablemente, esta sea la fuente más relevante para elaborar el universo de auditoría.
- **Normativa de aplicación** para la compañía, ya que determinadas leyes y normas obligan a los departamentos de auditoría a realizar algunos trabajos concretos de auditoría.

- **Manuales de procedimientos** de la organización (para conocer los procesos y actividades que se realizan).
- **Entrevistas** con los ejecutivos y gerentes de la compañía (con el mismo fin que el anterior: conocer los procesos y actividades).
- **Marcos de control,** como COSO, COBIT[1] …

¿CÓMO SE TRASLADA TODA ESA INFORMACIÓN AL UNIVERSO?

Conviene recordar que esta tarea de elaboración del universo consiste en agrupar los riesgos en trabajos de auditoría concretos donde se revisarán esos riesgos y los controles que tiene la compañía para minimizarlos. Es decir, el DAI debe decidir cómo va a organizar los trabajos de auditoría interna para revisar todos los riesgos relevantes.

Por ello, la elaboración del Universo es, probablemente, la tarea más compleja de toda la elaboración del plan de Auditoría. Básicamente, hay que tener en cuenta que esta tarea encaja más en lo que se podría definir como un "arte", en lugar de una ciencia. No existen guías, recetas, pasos, tareas, ni *checklist.* Tan solo conocimiento del negocio de la compañía, experiencia y sentido común.

Algo que puede servir de ayuda antes de elaborar el Universo es que el DAI realice una reflexión estratégica sobre varias cuestiones:

- ¿Prefiero hacer trabajos largos o cortos? ¿La organización (y la Comisión de Auditoría) prefiere recibir pocos informes de auditoría, pero opinando sobre "mega-procesos"? ¿o prefiere recibir un mayor número de informes, pero centrado en procesos más cortos o subprocesos?
- ¿Prefiero ver los riesgos de forma aislada o dentro de un proceso de negocio?
- ¿Cómo puedo agrupar los riesgos en trabajos para que sea más eficiente realizar cada uno de los trabajos de auditoría? (teniendo en cuenta cómo están configurados los equipos de trabajo en Auditoría Interna).

También resulta conveniente que se involucre en su elaboración a los miembros con más experiencia del departamento de Auditoría Interna.

RELACIÓN ENTRE EL MAPA DE RIESGOS Y EL UNIVERSO DE AUDITORÍA

Existen algunas unidades de Auditoría Interna que consideran que el universo de auditoría es directamente el mapa de riesgos de la compañía. Es decir, cada riesgo del mapa se traslada tal cual al universo de auditoría. Dicho enfoque también resulta válido y es perfectamente aplicable.

1. *Control Objectives for Information and related Technology*, guía de mejores prácticas presentada como *framework*, dirigida al control y supervisión de tecnología de la información.

No obstante, otras unidades de Auditoría Interna consideran que el universo de auditoría debe ser algo más que el inventario de riesgos. Es decir, que cada elemento del universo debe ser un trabajo donde se pretenden revisar varios riesgos de la misma compañía. En este libro vamos a seguir este último enfoque.

La principal diferencia entre ambos enfoques suele ser que, en el primero, Auditoría Interna no se preocupa de cómo va a auditar cada uno de los riesgos en el largo plazo. Es decir, el plan a largo plazo se parecerá poco al plan a corto a plazo, ya que:

- En el **plan a largo plazo** están todos los riesgos, pero no están organizados en forma de trabajos concretos.
- En el **plan a corto** Auditoría Interna decide cómo organizar los trabajos para auditar los riesgos que toque revisar en ese periodo.

Supongamos que tenemos una organización que ha elaborado planes anuales y trienales. Si pasan tres años y observamos todos los trabajos que ha realizado Auditoría Interna veremos que:

- En las unidades que no trasladan tal cual los riesgos al universo, sino que los transforman en trabajos, los nombres de los informes que se han emitido coincidirán, en su gran mayoría, con el universo.
- En cambio, en las unidades que trasladan tal cual los riesgos al universo, se podrá ver que no existe esa similitud, ya que en el universo tenemos riesgos, y, en cambio, en cada informe se habrán auditado varios riesgos.

3.2 Elaborar el plan a largo plazo

Llegados a este punto, hemos terminado de construir el universo de auditoría. Es decir: tenemos una lista de todos los trabajos que, según la Dirección de Auditoría Interna, sería posible realizar.

Pero en todas las compañías, los recursos de Auditoría Interna son finitos y normalmente escasos. Por lo tanto, se necesita realizar una tarea de **priorización** para realizar con mayor frecuencia aquellos trabajos del universo que están sujetos a un mayor riesgo para la organización y no auditar aquellos que representan un riesgo bajo.

Y en eso consiste la realización del plan a largo plazo: decidir con qué periodicidad vamos a auditar cada uno de los elementos[2] del universo de auditoría: ¿cada 6 meses? ¿cada año? ¿cada dos años? Coloquialmente, entre auditores internos, a veces también se llama ciclo a esta cantidad.

2. Un elemento es cada uno de los trabajos que hemos dado de alta en el Universo de Auditoría.

Ej: Pregunta en una conversación informal: "¿Cuál es vuestro ciclo de auditoría?" Respuesta: "Tres años". Esta conversación entre auditores internos significa que, al menos, cada tres años se auditan todos los procesos que tengan algún riesgo relevante.

PRINCIPALES PASOS A LA HORA DE ELABORAR EL PLAN A LARGO PLAZO

En la elaboración del plan a largo plazo se podrían distinguir dos tareas:

- Definir las periodicidades con las que se van a auditar los elementos.
- Construir (y aplicar) una metodología para asignar una periodicidad a cada elemento del universo.

En los siguientes tres apartados veremos en qué consiste cada una de las tareas.

DEFINIR LAS PERIODICIDADES CON LA QUE SE VAN A AUDITAR LOS ELEMENTOS

Esta tarea consiste, básicamente, en hacer (y responder) a varias preguntas:

- ¿Cada cuánto tiempo quiere Auditoría Interna auditar los elementos que tengan más riesgo?
- ¿Y los que tengan menos?
- ¿Cuántos niveles de riesgo va a tener la metodología de priorización de trabajos?

En definitiva, esta tarea es algo "tan simple" como construir una tabla como la siguiente:

NIVEL DE RIESGO	CADA CUÁNTO SE AUDITA
MA (Muy Alto)	Cada año
A (Alto)	Cada 2 años
M (Medio)	Cada 3 años
B (Bajo)	Cada 4 años
MB (Muy Bajo)	No se audita

El lector se puede hacer muchas preguntas a la hora de acometer esta tarea: ¿existe alguna guía o criterio para construir esta tabla? ¿Cuántos niveles debería haber? ¿Cuál debería ser la periodicidad mínima o máxima? Pues bien, no existe ningún criterio específico que haya que seguir. En este sentido, esta decisión debe estar marcada por el apetito de riesgo tanto de la compañía como del propio departamento de auditoría.

CONSTRUIR UNA METODOLOGÍA PARA ASIGNAR UNA PERIODICIDAD A CADA ELEMENTO DEL UNIVERSO

El segundo paso consiste en construir una metodología para asignar un nivel de riesgo a cada elemento del universo. Y, en consecuencia, una periodicidad de auditoría.

En este caso, conviene comenzar ilustrando esta tarea con un ejemplo de qué aspecto podría tener el resultado final de construir esta metodología:

ID	Elemento del Universo	F_1	F_2	…	F_n	Rotación Resultante
1	Auditoría de …	MA	A	A	A	Cada año
2	Auditoría de …	A	M	B	B	3 años
3	Auditoría de …	A	B	A	MA	2 años
4	Auditoría de …	A	A	A	B	2 años
5	Auditoría de …	B	B	B	M	No se audita
6	Auditoría de …	M	M	M	B	4 años
7	Auditoría de …	B	B	A	B	4 años

Obsérvese cada columna de la tabla:

- En la tabla debe haber una fila por cada elemento del universo.
- Las dos primeras columnas se utilizan para identificar cada elemento del universo.
- Las siguientes (desde F_1 hasta F_n) representan cada uno de los factores de riesgo que se quieran modelizar.
- La última columna representa la rotación resultante para cada trabajo. En el siguiente apartado se verá cómo se puede realizar el cálculo.

¿QUÉ SON LOS FACTORES DE RIESGO? ¿Y CÓMO SE CALCULA LA ÚLTIMA COLUMNA?

Los factores de riesgo son los elementos que se van a utilizar para caracterizar el nivel de riesgo que representa el elemento auditado. Y depende de cada departamento de auditoría interna el establecer cuáles son esos factores de riesgos.

No obstante, conviene poner un par de ejemplos clásicos que se pueden utilizar como factores de riesgos: el nivel de riesgo y el nivel de control de ese elemento auditable. De esta forma, se podría construir una tabla como la siguiente para, mediante la combinación de ambos factores, calcular la periodicidad del trabajo:

NIVEL DE RIESGO	NIVEL DE CONTROL			
	BAJO	MEDIO	ALTO	MUY ALTO
MUY ALTO	1	1	2	2
ALTO	2	2	2	3
MEDIO	3	3	4	4
BAJO	4	0	0	0

Cada año
Cada 2 años
Cada 3 años
Cada 4 años
No se audita

La celda ■ representa un elemento auditable cuyo nivel de riesgo observable por auditoría es MUY ALTO; y cuyo nivel de control es BAJO. Por tanto, estos los elementos los auditaremos todos los años (que es lo que representa el 1).

La celda ■ representa un elemento auditable cuyo nivel de riesgo observable por Auditoría Interna es BAJO; y cuyo nivel de control es MUY ALTO. Por tanto, estos elementos no se van a auditar (que es lo que representa el 0).

El ejemplo anterior ilustra cómo calcular la periodicidad de la auditoría en una metodología que solo tenga dos factores de riesgo. En el caso de que quieran incluir más factores de riesgos, se puede articular un sistema de pesos para calcular la periodicidad de los trabajos.

¿CÓMO SE ASIGNAN LOS VALORES A CADA FACTOR DE RIESGO?

Llegados a este punto conviene hacerse una pregunta que puede generar intensos debates en las unidades de Auditoría Interna. ¿Cómo se establece el nivel de riesgo y el nivel de control de cada elemento del universo? ¿Mediante fórmulas matemáticas que partan del mapa de riesgos de la entidad y transformen los valores del mapa en nuestros valores de la matriz? ¿O mediante criterio experto?

Se podría decir que ambas opciones son perfectamente correctas. No obstante, quizá la opción más adecuada para la mayoría de los departamentos de Auditoría Interna sea la fijación mediante criterio experto. No debemos olvidar que la elaboración del plan requiere de la implicación de los profesionales de Auditoría Interna con mayor grado de experiencia. Y dicha experiencia y criterio tienen un gran valor, que no merece la pena "ocultar" bajo fórmulas matemáticas.

Además, tampoco debemos olvidar que, en un escenario ideal, el mapa de riesgos que se utiliza para comenzar la elaboración del plan trienal ha sido construido por la dirección de la entidad, y no por Auditoría Interna. Por tanto, la dirección de la compañía puede estar sobrevalorando o infravalorando algunos riesgos. La utilización del criterio experto permite que Auditoría Interna pueda salvar las posibles discrepancias de valoración que tenga con los directivos, utilizando su propio criterio.

Tengamos en cuenta que, si un riesgo está infravalorado por la Dirección y utilizamos fórmulas matemáticas para determinar la rotación de los trabajos de auditoría, dichos riesgos se auditarán con una periodicidad menor de la necesaria. Por tanto, si el día de mañana ocurre un problema en ese proceso, la organización también responsabilizará a Auditoría Interna del problema. Y poner como excusa que "el directivo responsable de ese proceso infravaloró los riesgos" sonará precisamente a la palabra que hemos utilizado: a una excusa que no le valdrá al Consejo de Administración ni a la Comisión de Auditoría.

Es cierto que los defensores de usar fórmulas matemáticas también argumentarán que si Auditoría Interna piensa que algún riesgo está infravalorado, la obligación de auditoría es recomendar que se modifique la valoración de los riesgos en el mapa de riesgos de la compañía.

Por tanto, se pueden encontrar argumentos a favor de usar criterio experto o de usar fórmulas matemáticas. Y todos estos argumentos convierten esta cuestión en un apasionante debate.

3.3 Elaborar el plan a corto plazo

Antes de hablar del plan a corto plazo, conviene recopilar y ver en qué punto nos encontramos en esta parte de la metodología. Repasemos. Hemos construido el universo de auditoría. Es decir, una lista con todos los posibles trabajos que podría llevar a cabo Auditoría Interna. Y hemos decidido con qué periodicidad tenemos que realizar cada trabajo del universo. Es decir, tenemos una estrategia a largo plazo para revisar todos los riesgos de la compañía de una forma organizada.

Así que, llegados a este punto, hay que saltar de la estrategia (plan a largo plazo) a la táctica (plan a corto plazo). Es decir, hay que coger todos los elementos del plan a largo plazo y decidir cuáles de ellos se van a realizar, por ejemplo, durante el próximo año.

¿CÓMO SE SELECCIONAN LOS TRABAJOS DEL PLAN ANUAL?

Esta parte de la metodología es realmente sencilla, comparada con las dos fases anteriores. Es tan simple como hacer lo siguiente:

- Incorporar a la hoja de cálculo[3] en la que tengamos inventariado el universo de auditoría la fecha de la última auditoría.
- Añadir una columna en la que se muestre cuál es el año en el que, como máximo, debemos hacer la siguiente auditoría de ese elemento. A este campo se le puede llamar "año de la próxima auditoría".
- Seleccionar los trabajos que, obligatoriamente, se tienen que auditar el año siguiente.

Veamos un ejemplo. Supóngase que estamos a final de 2019 y se está elaborando el plan anual. Y supóngase que se tiene un elemento del universo de auditoría cuya última auditoría se realizó en ese año 2019. Entonces:

- Si su periodicidad es igual a 1, obviamente, lo tendremos que incorporar en el plan anual 2020.

3. La gestión de los elementos del universo de auditoría y los planes de auditoría se puede realizar mediante una hoja de cálculo. Aunque una base de datos o una pequeña aplicación permitirán una mejor gestión.

- Si su periodicidad es igual a 2, no tendremos que hacer esa auditoría hasta 2021.
- Si su periodicidad es igual a 3, no tendremos que hacer esa auditoría hasta 2022.
- Si su periodicidad es igual a 4, no tendremos que hacer esa auditoría hasta 2023.

Por tanto, siguiendo el ejemplo, lo único que hay que hacer es incorporar al plan anual todos los elementos del universo de auditoría cuyo año de próxima auditoría sea 2020. Una vez hecho, si el Director de Auditoría Interna considera que aún tiene recursos disponibles, podría incorporar trabajos de otros años.

REFLEXIÓN SOBRE UNA DE LAS GRANDES VENTAJAS DE LA PLANIFICACIÓN COMBINADA (LARGO Y CORTO PLAZO)

Una gran ventaja de este método es que permite compartir con los *stakeholders* una visión estratégica de auditoría a largo plazo, pero con un enfoque de trabajos muy concreto. Una pregunta muy típica que le puede trasladar el CEO, un consejero o supervisor al Director de Auditoría Interna es: ¿cuándo tienes previsto auditar el proceso x?

Con una metodología de este tipo, no sólo es fácil responder a esa pregunta, sino que se puede demostrar la respuesta acudiendo al plan a largo plazo. Y, además, como veremos en el siguiente apartado, esa información se facilita al Consejo de Administración.

3.4 Formalización de los planes en un documento y presentación al Consejo

Una vez que ya se han tomado todas las decisiones relevantes y se han decidido los trabajos a realizar y las periodicidades, llega el momento de plasmarlo todo en un documento y presentarlo a las partes interesadas.

QUÉ DEBE CONTENER EL DOCUMENTO

No existe un formato estándar que sea necesario seguir para presentar los planes de auditoría. Tanto el formato como el contenido es una decisión del DAI. No obstante, sí se pueden ofrecer algunos consejos a seguir o prácticas que se observan usualmente.

En general, el plan a largo plazo y el plan a corto plazo se suelen presentar en dos documentos separados, y en formato presentación o documento de texto.

El plan a largo plazo suele ser un documento más corto que el plan a corto y puede contener:

- Una nota metodológica de cómo se ha construido, es decir, una explicación de la metodología, de los factores de riesgo utilizados y de cómo se combinan entre sí.

- Una tabla (o estructura similar) donde se enumeran todos los trabajos del plan, que incluye:
  - Un ID único que facilita la trazabilidad.
  - El nombre del trabajo.
  - La periodicidad del trabajo.
  - La identificación de los riesgos que se revisarán en ese trabajo (aunque sea en un primer nivel de agregación general).

El plan a corto plazo suele ser un documento más extenso. La información que se puede incluir en este tipo de plan es:

- Una descripción más detallada de los trabajos que se van a realizar. Es decir, en el plan a largo es común que solo se enumeren los trabajos, pero no se ofrezca una descripción detallada de en qué consiste el trabajo. En cambio, en el plan a corto plazo se suele describir el objetivo de cada uno de los trabajos.
- También se incluyen algunos apartados que están relacionados con el cumplimiento de las normas. Se puede incluir información sobre la independencia de Auditoría Interna, o sobre la suficiencia del presupuesto y los recursos disponibles.
- También suele ser frecuente incluir información sobre los proyectos internos de auditoría.

¿QUIÉN DEBE APROBAR EL PLAN DE AUDITORÍA?

En general, los planes de auditoría deben someterse a la aprobación de la Comisión de Auditoría o del Consejo de Administración de la compañía.

Además de ese proceso de aprobación, los planes son documentos valiosos que conviene compartir con otras partes de interés de la organización. Suele ser frecuente y valioso compartirlo con la Alta Dirección, con el auditor de cuentas y con los organismos de supervisión de la compañía.

Cualificación y formación del auditor interno

Instituto de Auditores Internos de España

Las *Normas Internacionales para el ejercicio de la Auditoría Interna*[1] detallan los aspectos más relevantes que identifican tanto la cualificación como la formación que debe tener el auditor interno. El texto recoge que el Director de Auditoría Interna (DAI) debe asegurar que los recursos de Auditoría Interna sean apropiados, suficientes y eficazmente asignados para cumplir con el plan aprobado.

- **Apropiados.** Hace referencia a la combinación de conocimientos, aptitudes y otras competencias necesarias para llevar a cabo el plan.
- **Suficientes.** Se refiere a la cantidad de recursos necesarios para cumplir con el plan. Los recursos están eficazmente asignados cuando se utilizan de forma tal que optimizan el cumplimiento del plan aprobado.

En la **NORMA SOBRE ATRIBUTOS 1200 - APTITUD Y CUIDADO PROFESIONAL** se indica que *"los trabajos deben cumplirse con aptitud y cuidado profesional adecuados".*

En concreto, se establece:

1210-APTITUD

"Los auditores internos deben reunir los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades individuales. La actividad de Auditoría Interna, colectivamente, debe reunir u obtener los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades.

Interpretación:
La aptitud es un término general que se refiere a los conocimientos, habilidades y otras competencias requeridas a los auditores internos para llevar a cabo eficazmente sus responsabilidades profesionales. Incluye tendencias, temas emergentes y la consideración de las actividades actuales para posibilitar asesoramiento relevante y formulación de recomendaciones. Se alienta a los auditores internos a demostrar su aptitud obteniendo certificaciones y cualificaciones profesionales apropiadas, tales como la designación CIA y otras designaciones ofrecidas por el Instituto de Auditores Internos y otras organizaciones profesionales apropiadas."

- 1210. A1 - *"El Director de Auditoría Interna debe obtener asesoramiento y asistencia competentes en el caso de que los auditores internos carezcan de los conocimientos, las aptitudes u otras competencias necesarias para llevar a cabo la totalidad o parte del trabajo."*
- 1210. A2 - *"Los auditores internos deben tener conocimientos suficientes para evaluar el riesgo de fraude y la forma en que se gestiona por parte de la organización, pero no es de*

1. Instituto de Auditores Internos. *Normas Internacionales para la práctica profesional de la Auditoría Interna.*

esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección o investigación del fraude".

- 1210.A3 - *"Los auditores internos deben tener conocimientos suficientes de los riesgos y controles clave en tecnología de la información y de las técnicas de Auditoría Interna disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado. Sin embargo, no se espera que todos los auditores internos tengan la experiencia de aquel auditor interno cuya responsabilidad fundamental es la auditoría de tecnología de la información."*

- 1210.C1 - *"El Director de Auditoría Interna no debe aceptar un servicio de consultoría, o bien debe obtener asesoramiento y asistencia competentes, en caso de que los auditores internos carezcan de los conocimientos, las aptitudes y otras competencias necesarias para desempeñar la totalidad o parte del trabajo."*

1220-CUIDADO PROFESIONAL

"Los auditores internos deben cumplir su trabajo con el cuidado y la aptitud que se esperan de un auditor interno razonablemente prudente y competente. El cuidado profesional adecuado no implica infalibilidad."

- 1220.A1 - *"El auditor interno debe ejercer el debido cuidado profesional al considerar:*

  El alcance necesario para alcanzarlos objetivos del trabajo:
  - *La relativa complejidad, materialidad o significatividad de asuntos a los cuales se aplican procedimientos de aseguramiento.*
  - *La adecuación y eficacia de los procesos de gobierno, gestión de riesgos y control.*
  - *La probabilidad de errores materiales, fraude o incumplimientos.*
  - *El coste de aseguramiento en relación con los beneficios potenciales."*

- 1220.A2 - *"Al ejercer el debido cuidado profesional, el auditor interno debe considerar la utilización de auditoría basada en tecnología y otras técnicas de análisis de datos."*

- 1220.A3 - *"El auditor interno debe estar alerta a los riesgos materiales que pudieran afectar los objetivos, las operaciones o los recursos. Sin embargo, los procedimientos de aseguramiento por sí solos, incluso cuando se llevan a cabo con el debido cuidado profesional, no garantizan que todos los riesgos materiales sean identificados."*

- 1220.C1 - *"El auditor interno debe ejercer el debido cuidado profesional durante un trabajo de consultoría, teniendo en cuenta lo siguiente:*
  - *Las necesidades y expectativas de los clientes, incluyendo la naturaleza, oportunidad y comunicación de los resultados del trabajo;*
  - *La complejidad relativa y la extensión de la tarea necesaria para cumplir los objetivos del trabajo; y*
  - *El coste del trabajo de consultoría en relación con los beneficios potenciales."*

1. Competencias y facilitadores del auditor interno

En relación con las competencias

El Instituto de Auditores Internos ha definido un Marco de competencias aplicable a los profesionales que desarrollan esta actividad. En concreto, se indican una serie de habilidades principales que deberían identificarse en los componentes del equipo, desde el personal de *staff* hasta los *managers* y el Director de Auditoría Interna.

Estas habilidades se distribuyen de la siguiente manera:

- PROFESIONALIDAD: Competencias requeridas para demostrar la autoridad, credibilidad y conducta ética esencial para una actividad de Auditoría Interna de valor. Se centra en las siguientes áreas de conocimiento:
  - Misión de Auditoría Interna.
  - Estatuto de Auditoría Interna.
  - Independencia organizativa.
  - Objetividad individual.
  - Comportamiento ético. Promueve y aplica la ética profesional.
  - Debido cuidado profesional.
  - Desarrollo profesional.

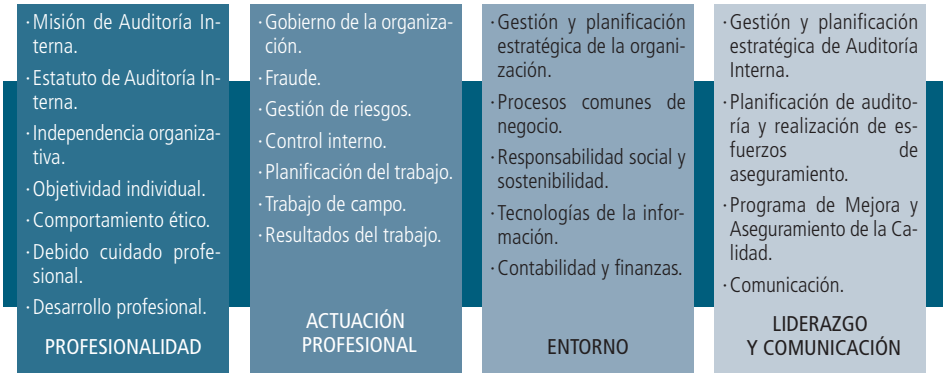
- ACTUACIÓN PROFESIONAL: Competencias requeridas para planificar y llevar a cabo trabajos de auditoría interna, de acuerdo con las Normas. Se centra en las siguientes áreas de conocimiento:
  - Gobierno de la organización.
  - Fraude.
  - Gestión de riesgos.
  - Control interno.
  - Planificación del trabajo.
  - Trabajo de campo.
  - Resultados del trabajo.

- ENTORNO: Competencias requeridas para identificar y gestionar los riesgos específicos del sector y el entorno en el que opera la organización. Se centra en las siguientes áreas de conocimiento:
  - Gestión y planificación estratégica de la organización.
  - Procesos comunes de negocio.
  - Responsabilidad social y sostenibilidad.
  - Tecnologías de la información.
  - Contabilidad y finanzas.

LIDERAZGO Y COMUNICACIÓN: Competencias requeridas para proporcionar una dirección estratégica, comunicar de manera efectiva, mantener relaciones y gestionar el personal y los procesos de Auditoría Interna. Se centra en las siguientes áreas de conocimiento:
- Gestión y planificación estratégica de Auditoría Interna.
- Planificación de auditoría y realización de esfuerzos de aseguramiento.
- Programa de Mejora y Aseguramiento de la Calidad.
- Comunicación.

De esta manera, los Directores de Auditoría Interna deben asegurarse de que el equipo participante en cada uno de los encargos posee la experiencia, conocimientos y autoridad necesarios para llevar a cabo este tipo de auditorías.

A continuación, se muestra el cuadro resumen del Marco de Competencias de Auditoría Interna del Instituto Global[2]



Con carácter adicional a lo anterior, y teniendo en consideración la penetración de las nuevas tecnologías en el mundo actual, los conocimientos y competencias digitales se presentan con claves y necesarios para los profesionales de Auditoría Interna. La re/evolución digital está aquí para quedarse.

En concreto, los departamentos de Auditoría Interna deben considerar la inclusión entre sus profesionales de los siguientes perfiles:

- **Expertos en procesos digitales.** Aportan *know-how/expertise* específico en relación con los procesos y *feedback* a los analistas de datos.
- **Expertos en datos.** Gestionan la ingesta de distintas fuentes de datos, ejecutando la transformación y limpieza de los mismos.

2. *The Global IIA's Internal Audit Competency Framework:* https://na.theiia.org/standards-guidance/Pages/Internal-Audit-Competency-Framework.aspx

- **Analista de datos.** Identifica la metodología más acertada de análisis de datos, permitiendo la transformación de las necesidades detectas en conocimiento de las estructuras de los datos que pueden ser susceptibles de procesamiento.

En relación con los facilitadores

A partir de la experiencia obtenida por distintos departamentos de Auditoría Interna en el desarrollo de actividades relativas a la auditoria de riesgos estratégicos, se han identificado 4 facilitadores ligados con experiencias de éxito:

- CONTINUA DEMOSTRACIÓN DEL VALOR AÑADIDO A APORTAR POR AUDITORÍA INTERNA
  La percepción de que el área entrega un retorno perceptible, una vez generada, debe mantenerse en el tiempo mediante el desarrollo de trabajos de aseguramiento relativos a la gestión del riesgo estratégico y actuando como socio consultor de las áreas de negocio.

- ACCESIBILIDAD
  La demostración de generación de valor añadido junto con la determinación del Director de Auditoría Interna de construir y mantener relaciones fluidas y estables con la gerencia y el Consejo de Administración de la entidad se traslada en la obtención de un valioso conocimiento de lo que está ocurriendo en el conjunto de la organización y de los posibles giros estratégicos e iniciativas que pudieran tomarse en el futuro próximo.

- LENGUAJE COMÚN
  Resulta especialmente destacable la importancia de trasladar adecuadamente el significado del término "controles internos" a la terminología de funciones transversales como Sistemas y a los propietarios de procesos críticos, asegurando de esta manera, su correcto entendimiento y la aplicación a nivel organizativo.

- PARTICIPACIÓN
  Las funciones líderes de Auditoría Interna tienden a ser altamente activas y participativas, pasando una cantidad significativa de tiempo en los lugares en los que se desarrolla la actividad empresarial (tiendas, fábricas, etc). Este enfoque les permite obtener un entendimiento profundo y no sesgado de las vulnerabilidades y la gestión por parte de la gerencia.

2. Certificaciones profesionales existentes en la actualidad

2.1 Certificaciones emitidas por el Instituto de Auditores Internos

El Instituto de Auditores Internos de España recomienda las Certificaciones Internacionales del *Global Institute of Internal Auditors,* por ser las certificaciones reconocidas a nivel mundial y acreditar las habilidades y conocimientos inherentes a cada actividad.

- Las certificaciones *Certified Internal Auditor (CIA) y Certified Risk Management Assuranc*e (CRMA) avalan a los profesionales de la Auditoría Interna.
- El Certificado COSO en Control Interno acredita la experiencia en el diseño, implementación y seguimiento de un sistema de control interno.
- El Certificado COSO-ERM acredita los conocimientos necesarios para el diseño, implementación y seguimiento de un sistema de Gestión del Riesgo Empresarial (ERM) según el marco definido por COSO.
- El *Qualification in Internal Audit Leadership* (QIAL) constituye el mayor reconocimiento a la capacidad de liderazgo en Auditoría Interna.
- La certificación QA –*Quality Assesment*– avala las Direcciones de Auditoría Interna y certifica que trabajan conforme a las Normas Internacionales de Auditoría Interna.

¿Por qué certificarse?

Se trata de Certificaciones profesionales de reconocimiento internacional cuya obtención avala ante la Alta Dirección, la Comisión de Auditoría, otros profesionales y clientes externos e internos la suficiencia de conocimientos y, lo que es todavía más importante, la homogeneidad en la práctica de la profesión.

CIA - CERTIFIED INTERNAL AUDITOR

CONTENIDOS DEL EXAMEN

PARTE 1 · 125 Preguntas de opción múltiple / 2 horas y 30 minutos

1. Guía Obligatoria (Normas Internacionales).
2. Control Interno / Riesgo.
3. Realización de trabajos de Auditoría Interna.
4. Herramientas y técnicas de Auditoría Interna.

PARTE 2 · 100 Preguntas de opción múltiple / 2 horas

1. Gestión de la función de Auditoría Interna.
2. Gestión de trabajos de Auditoría Interna individuales.
3. Riesgos de Fraude y controles.

PARTE 3 · 100 Preguntas de opción múltiple / 2 horas

1. Gobierno y ética del negocio.
2. Gestión de Riesgos.
3. Estructura organizacional y Riesgos y Procesos del Negocio.
4. Comunicación.
5. Principios y gestión de liderazgo.
6. Tecnologías de la información y continuidad del negocio.
7. Gestión Financiera.
8. Análisis de Negocio.

CRMA - CERTIFICATION IN RISK MANAGEMENT ASSURANCE

Acredita la habilidad profesional para proporcionar aseguramiento sobre los procesos claves de la gestión de riesgos, e informar a la Alta Dirección y a la Comisión de Auditoría sobre la importancia de una adecuada gestión de riesgos.

CONTENIDOS DEL EXAMEN CRMA · 100 Preguntas opción múltiple/ 2 horas

DOMINIO I - Gestión de Riesgos y Buen Gobierno.

DOMINIO II - Fundamentos de la Gestión de Riesgos.

DOMINIO III - Aseguramiento y control de la gestión de riesgos: el papel del auditor interno.

DOMINIO IV - Evaluación y asesoramiento en la gestión de riesgos: el papel del auditor interno.

COSO CONTROL INTERNO

Certificado global en el Marco Integrado de Control Interno, que acredita experiencia en el diseño, implementación y seguimiento de un sistema de control interno.

Dirigido a profesionales de cualquier nivel vinculados a cualquier área de control (Auditoría Interna, Gestión de Riesgos, Control Interno, Auditoría de Cuentas, etc.). Está avalado y ofrecido por los miembros de COSO: *American Institute of Certified Public Accountants (AICPA), el Institute of Management Accountans (IMA) y The Institute of Internal Auditors (IIA).*

COSO ENTERPRISE RISK MANAGEMENT

Certificado global en el Marco de Gestión de Riesgos de COSO, que acredita conocimientos y experiencia en el diseño, implementación y seguimiento de un sistema de gestión de riesgos (ERM).

Dirigido a profesionales de cualquier nivel vinculados a cualquier área de control (Auditoría Interna, Gestión de Riesgos, Control Interno, Auditoría de Cuentas, etc.). Está avalado y ofrecido por los miembros de COSO: *American Institute of Certified Public Accountants (AICPA), el Institute of Management Accountans (IMA) y The Institute of Internal Auditors (IIA).*

QIAL - QUALIFICATION IN INTERNAL AUDIT LEADERSHIP

La necesidad de innovación en Auditoría Interna exige un nuevo tipo de líder para dirigir equipos de Auditoría Interna de alto nivel y rendimiento. Mientras aporta valor alineado con las necesidades de los grupos de interés, domina y es parte integrante de las actividades de control, seguimiento y supervisión, y conoce los riesgos de la organización, los prioriza y alinea sus actividades de acuerdo con esas prioridades (el enfoque top-down risk), y además maneja las expectativas de un mercado en constante evolución.

El IIA ha desarrollado la *Qualification in Internal Audit Leadership* (QIAL®) para acreditar a los profesionales que marcan tendencia en la Profesión.

2.2 Otras Certificaciones relevantes

CISA - CERTIFIED INFORMATION SYSTEMS AUDITOR

Se trata de una certificación para auditores que tiene reconocimiento a nivel mundial. La certificación CISA cuenta con el respaldo de la Asociación de Control y Auditoría de Sistemas de Información (ISACA) y, para poder obtener dicha certificación, hay que cumplir una serie de requisitos impuestos por este organismo.

A través de la certificación CISA se reconocen los conocimientos y aptitudes de un profesional en diferentes áreas establecidas. Es el caso de la auditoría en sistemas de información, las operaciones, soporte y mantenimiento de estos sistemas, el gobierno y mantenimiento de la tecnología de la información, la protección de la información y finalmente, la adquisición, ejecución y desarrollo de estos sistemas a los que estamos haciendo referencia. Todos aquellos que quieran convertirse en un CISA podrán demostrar que son capaces de evaluar las vulnerabilidades de dichos sistemas, elaborar informes, establecer controles y por supuesto mostrar las habilidades y conocimientos en auditorías, así como dar a conocer su experiencia dentro de este sector.

CFE - CERTIFIED FRAUD EXAMINER

Los CFE's son expertos antifraude que han acreditado su conocimiento mediante la experiencia y la aprobación del examen que incluye temas como transacciones financieras fraudulentas, investigación de fraudes, elementos legales del fraude, y prevención y disuasión de fraudes. Y se mantienen actualizados con formación continua acreditada.

La designación como CFE es reconocida por organizaciones privadas y gubernamentales alrededor del mundo, y acredita al profesional que la adquiere su conocimiento especializado en materia de prevención, detección e investigación de fraudes.

Es emitida por ACFE, *Association of Certified Fraud Examiners.* Se trata de la organización antifraude más grande del mundo y el principal proveedor de capacitación y educación antifraude.

Auditoría Interna y las Tecnologías de la Información y Comunicación

Instituto de Auditores Internos de España

1. La Información

La información es la base cultural y sociológica del mundo en que vivimos. Es también instrumento de gestión y elemento de comunicación. La información activa y viva se renueva y fluye a velocidades vertiginosas a través de las autopistas de la información alrededor del mundo.

El mundo se ha empequeñecido, las noticias corren y se propagan a gran velocidad, cualquier acontecimiento en Saigón es noticia inmediata en Nueva York. El mundo se ha globalizado y se ha unido a través de poderosas redes de comunicaciones.

1.1 La información y las personas

La persona consume información, necesita información para comunicarse, hablar, formarse, desarrollarse y vivir en el mundo de hoy. Las personas intercambian, a través de los sistemas de comunicación, conocimientos científicos, progresos técnicos, ideas, inquietudes, problemas, necesidades, sentimientos, juegos. La información es hoy calidad de vida, es dinero y es poder. El subdesarrollo radica en perder el tren de la información global, que es el tren de la cultura y el poder.

Los medios de comunicación canalizan, filtran e interpretan los datos, la influencia activa de los medios se traduce en la mediatización o acción mediática, que no es más que la influencia del medio sobre la información, y que actúa sobre las conciencias sociales, los criterios, las costumbres y las políticas, mediatizando la propia cultura y propiciando la gran paradoja de nuestro tiempo: hoy el poder reside en los medios.

1.2 La información y las empresas

Si la información hoy es necesaria para la persona tanto más lo será para la empresa. La información en las empresas es la base de la gestión y la toma de decisiones, para lo cual deberá ser veraz, oportuna e íntegra.

- **Veraz** significa que sea cierta y fiable, reflejo de la realidad.
- **Oportuna,** que esté disponible tanto en el tiempo como en el espacio, es decir, actualizada y que se disponga de ella allí donde sea necesaria.
- **Íntegra** significa que sea consistente y segura, en definitiva, que esté protegida.

La información –que es dinero y poder– es, en definitiva, un bien patrimonial de la empresa, tal vez el fundamental y, por ello, debe ser protegida.

Al margen de esto, la tecnología y la informática se han constituido en un elemento clave y diferenciador en el desarrollo de las empresas y en su progreso y competitividad.

1.3 La auditoría y la información

La creación institucional de la Agencia de Protección de Datos (APD), la entrada en vigor del Reglamento General de Protección de Datos (RGPD) y la promulgación de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDP y GDD) –cuyo objetivo es hacer a las personas dueñas de su propia información– corrobora la idea de la propiedad, valor y confidencialidad de la información. La promulgación de la Circular de la Ley del Mercado de Valores (LMV) sobre la obligación de las empresas de guardar la confidencialidad de hechos relevantes en las compañías cotizadas y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), obligan a las empresas, desde el punto de vista legal –a veces con fuertes sanciones– a garantizar la seguridad y protección de la información.

La información en la empresa se encuentra, por lo general, organizada y debidamente estructurada y dirigida a cada empleado que la necesita para desarrollar su trabajo para tomar decisiones y actuar. A la información de la empresa, considerada como un todo organizado, se le llama sistema de información.

Una actividad fundamental de Auditoría Interna consiste en garantizar la integridad, fiabilidad y confidencialidad del sistema de información de la empresa, que es patrimonio fundamental y base para la toma de decisiones. La información se materializa a través de distintos soportes. El soporte fundamental, que en la mayoría de las empresas llegará a ser el único, es el informático. Pero no debemos olvidar los otros soportes, los que se materializan en soportes físicos, que requieren también controles, medios de protección y auditorías que verifiquen su correcto funcionamiento y que sean garantía última de su integridad.

Los riesgos éticos, morales y económicos derivados del incumplimiento legal deben ser objeto de preocupación y dedicación de la empresa y muy especialmente de la Auditoría Interna.

2. Auditoría Interna y las Tecnologías de la Información y Comunicación (TICs)

La relación entre Auditoría Interna y la informática se canaliza a través de dos vertientes. La primera se basa en la misión de la Auditoría Interna consistente en garantizar la integridad del sistema de información, y en la circunstancia de que el soporte principal del sistema sea informático, por lo que Auditoría Interna debe auditar la informática. La segunda se basa en que la propia Auditoría Interna, para realizar su función, analiza y verifica la información empresarial que generalmente está en soporte informático, por lo que en su trabajo habitual necesita herramientas informáticas.

De lo anterior se deduce que Auditoría Interna debe relacionarse con la informática. Estas relaciones frecuentes, y cada vez más intensas, entre la auditoría y la informática las reducimos a dos grupos fundamentales:

- La auditoría informática. Auditoría Interna en el ejercicio de su misión, para lo que realizará auditorías informáticas.
- La informática en auditoría. Auditoría Interna como una unidad más de la empresa que utiliza la informática para realizar su propio trabajo en una doble faceta: para hacer auditorías y para su propia gestión.

2.1 La auditoría informática

Entendemos por auditoría de las TIC aquella actividad auditora que trata de evaluar la adecuada utilidad, eficiencia, fiabilidad y salvaguarda de la información mecanizada que se produce en una determinada empresa o institución, así como el control interno de los servicios que la elaboran y procesan.

Los objetivos de la auditoría informática son:

- Verificar el control interno de la función informática, lo que significa información fiable, que es la necesaria en el momento oportuno y que sirve de base para tomar decisiones importantes. Es decir, que la información ha sido obtenida de registros reales, ha sido procesada adecuadamente, no existe posibilidad de manipulación y es la demandada por el usuario.
- Eliminar o reducir al máximo la posibilidad de pérdida de la información por fallos en los equipos, por fallos en los procesos o por gestión inadecuada de los archivos de datos (eficiencia operativa).
- Detectar y prevenir fraudes por manipulación de la información o por acceso de personas no autorizadas a transacciones que originen trasvases de fondos.
- Comprobar el cumplimiento de leyes y regulaciones.

AUDITORÍA DE LA FUNCIÓN INFORMÁTICA

Es la auditoría que se realiza a la función informática como un área empresarial especializada en la gestión y administración de la información, que está al servicio del sistema de información, al que debe dar soporte y garantizar su eficacia e integridad.

Lo primero que el auditor debe constatar es si existe una definición estratégica de los objetivos de la función informática, si están definidas las políticas y misiones fundamentales de la informática en consonancia y sintonización con los de la empresa. En definitiva,

si existe un plan informático en el que se determinen claramente qué es lo que la empresa exige a la informática y cuáles son las actuaciones principales y los costes para realizarlas. El auditor debe verificar si existe el plan y si se sigue y se cumple.

Posteriormente la atención de la auditoría se debe dirigir hacia el centro de proceso de datos y hacia los sistemas informáticos que éste produce, y que posteriormente explota. El centro de informática es un área específica de riesgo, no sólo por el coste de los equipos y recursos humanos cualificados que la informática necesita, sino también por la importancia que la seguridad, eficiencia y el adecuado diseño de los sistemas informáticos tiene para la correcta gestión de la empresa.

La finalidad de la auditoría de la función informática es, en definitiva, verificar la existencia de control interno en el ejercicio de la función y en el centro de proceso de datos.

En síntesis, un programa de trabajo consistiría en analizar:

- La organización y gestión de las actividades de la unidad de informática.
- Plan informático.
- Los sistemas informáticos en fase de desarrollo.
- El mantenimiento de los sistemas informáticos.
- La explotación de los recursos informáticos.
- El potencial de software del ordenador, adaptándole a las necesidades actuales y futuras previstas de la empresa.
- La seguridad.
- Los sistemas de comunicaciones.
- Uso de los ordenadores y dispositivos móviles.
- Uso de Internet y la ciberseguridad.
- Correo electrónico y redes sociales.
- Comercio electrónico y canales digitales.
- La función de almacenamiento y la administración de las bases de datos.
- El cumplimiento de la legislación vigente.

AUDITORÍA DE LOS SISTEMAS INFORMÁTICOS

Un sistema informático es el conjunto de programas desarrollados para dar una solución informática a una función concreta, dentro de un área de actividad empresarial. Por ejemplo, contabilidad, nóminas, gestión de proveedores, reservas de plazas, facturación, etc. Pero en un mundo cada vez más digitalizado, la tecnología y la informática cubren prác-

ticamente todos los aspectos de la actividad de una compañía y, por ende, son objetos de revisión por parte de Auditoría Interna.

Se trata de auditar los sistemas informáticos desde una doble perspectiva:

- **De eficacia,** que consiste en verificar si el sistema cumple con la funcionalidad que se le exige, y
- **de seguridad,** para ver si los controles aplicados garantizan la integridad de los procesos y los datos.

Por tanto, la finalidad de la auditoría de un sistema informático es la de evaluar en qué medida se está garantizando el control interno y la seguridad de los datos y programas con la utilización de la aplicación, así como el rendimiento de la misma en relación a la finalidad con la que fue diseñada, en términos de coste-eficiencia.

Para ello es necesario, en primer lugar, llegar a conocer el proceso, detectar los controles existentes y probar su funcionamiento.

El desarrollo del trabajo sería el siguiente:

- Definir los objetivos.
- Analizar la eficacia del sistema, su eficiencia y utilidad.
- Identificar el proceso, procedimientos administrativos, flujo de información, etc.
- Analizar la organización existente alrededor del sistema, segregación de funciones, etc.
- Analizar la aplicación respecto a los:
  - Controles de entrada/Controles de acceso.
  - Controles de procesamiento.
  - Controles de salida.
  - Controles generales (equilibrio global del procesamiento y de los archivos maestros).
- Identificar los controles operativos y hacer pruebas sustantivas o de cumplimiento.
- Identificar fallos de control.
- Detectar riesgos.
- Proponer recomendaciones.

Hay que poner de manifiesto que el desarrollo de los sistemas informáticos también ha sufrido modificaciones con la llegada de las nuevas tecnologías, especialmente de Internet, y ahora se desarrollan las denominadas *Apps,* aplicativos a través de los cuales se interactúa con los clientes, proveedores o empleados a través de internet y que frecuentemente utilizan procedimientos y metodologías diferentes para su desarrollo de las usadas tradicionalmente , como es el caso de la metodología *Agile*.

2.2 La informática en auditoría

El auditor interno no puede ignorar el potencial que puede suponer para él el uso de la informática como instrumento de trabajo para realizar las auditorías y como herramienta de ayuda para la gestión de la función de auditoría.

Auditoría Interna en su trabajo se enfrenta al enorme volumen de datos que manejan hoy día las empresas y muchas áreas a auditar, lo que hace prácticamente imposible acometer trabajos de auditoría con el rigor que requiere la profesión y sin pérdidas innecesarias de tiempo si no se utilizan herramientas informáticas.

INFORMÁTICA PARA AUDITAR

La auditoría sobre la gestión de una determinada unidad de la empresa requiere no sólo el análisis de la estructura de la misma y de sus funciones, sino también el de la información que maneja y el soporte de la misma. Si esta información está mecanizada, es conveniente auditar el sistema informático que la soporta.

Mediante la aplicación de programas apropiados la auditoría podría seleccionar así la información y datos, relación de datos entre ficheros, cálculo de valores medios y desviaciones, detectar desajustes en la información, etc.

El objetivo es crear un conjunto de aplicaciones y herramientas informáticas para Auditoría Interna, de manera que ésta pueda disponer directamente de la información, ficheros o datos y manejarlos de acuerdo con los objetivos fijados en su programa de trabajo. Obtener informes específicos, con la selección de datos necesarios, cruzar información entre distintos ficheros, calcular totales por algún concepto, así como desviaciones respecto a valores establecidos, etc. De esta manera, se aumenta el alcance de la información y la autonomía en el manejo de la misma.

Se trata de aplicaciones informáticas específicas para cada empresa, y a veces para cada auditoría, por lo que para poder utilizar las aplicaciones desarrolladas en ocasiones sucesivas se deben emplear sistemas abiertos, muy flexibles y de fácil adaptación a las nuevas necesidades y a los cambios.

En la mayoría de los casos, la utilidad de la informática en la auditoría estará en función del volumen de datos a tratar. En grandes empresas puede ser muy útil en la revisión de las áreas de gestión de patrimonio, presupuestos, financiera, ventas, clientes, compras, etc.

En el mercado existen varios paquetes que permiten realizar una elevada variedad de este tipo de pruebas y, además, incluyen otras posibilidades novedosas como la utilización de la Ley de Benford en la detección de fraudes.

La adquisición de estas herramientas es una alternativa que manejan ciertas empresas frente al diseño de un paquete a medida. Estas herramientas permiten, mediante el establecimiento de determinados indicadores, la realización de pruebas a distancia que permiten agilizar el trabajo de una posible visita in situ posterior.

Fundamentalmente el trabajo a realizar puede seguir dos orientaciones distintas, que en algunos casos serán complementarias y que señalamos seguidamente:

- Evaluación de los datos

  Los auditores deben tener acceso a todos los datos, y con mayor motivo, a los informáticos. Los datos en informática se almacenan en grandes ficheros generalmente organizados en forma de bases de datos que se caracterizan por su gran volumen y por las facilidades de acceso que proporcionan.

  Debido al gran volumen de datos que, por lo general, la auditoría debe verificar y de las facilidades de acceso, lo más usual es analizar por muestreo –o sobre el total de la población– de todos los registros de un fichero o base de datos perteneciente al área en cuestión, estimando una serie de valores y críticas (o fundamentales como sobre existencias o número de roturas en el caso de almacenes, morosos en el caso de clientes, etc.).

  Para ello se pueden utilizar programas para analizar el conjunto, diseñar una muestra, o bien seleccionarla manualmente. El muestreo no tiene por qué ser aleatorio y, en cualquier caso, habrá que diseñar los programas que calculen los valores que se hayan definido.

  Si no se han realizado pruebas sobre la totalidad de los datos, es necesario extrapolar los resultados obtenidos al conjunto de la población. Normalmente, para evitar sesgos de extrapolación, ésta deberá seguir una determinada sistemática para ello. La utilización de la informática es entonces muy recomendable.

  En áreas de alto riesgo, el auditor debe comprobar tanto los datos de entrada como los procesos para asegurarse de la fiabilidad de dicha información.

  El examen de los justificantes no puede sufrir mayor mecanización que la de disponer de programas que permitan hacer un muestreo representativo, según las condiciones de la información a analizar.

- Revisión de los programas

  Por lo que se refiere a las pruebas de procesos, se puede optar entre las siguientes opciones:

  - **Revisión directa de los programas.** Aparte de la complejidad de revisar programas desarrollados por otras personas, este sistema no suele ser el más adecuado porque,

por lo general, requiere un gran conocimiento de lenguajes de programación, con los que los auditores normalmente no están habituados a trabajar.

- **Prueba de datos reales** con un programa sencillo de simulación propio. Puede ser útil cuando se disponga de las habilidades y capacidades para llevarlo a cabo.
- **Preparación de un juego de datos de prueba.** Consiste en la creación de un conjunto de datos diseñado por el propio auditor interno que recoja las distintas situaciones que puedan darse en la realidad y de los cuales conozca con certeza el resultado del proceso. Estos datos serán cargados en el sistema a analizar y se compara la información de salida con los resultados obtenidos, previamente calculados.
- **Utilización de modelos de contraste**. Se trata de la comparación de determinadas magnitudes reales con valores teóricos o valores medios de la empresa, sector, etc.

Una vez analizado el proceso, detectados sus controles y evaluado el grado de control interno, se debe realizar una serie de pruebas de cumplimiento o sustantivas que verifiquen que esos controles están operando.

Para ello se pueden utilizar programas de simulación que analicen datos reales y muestren si, tras el paso por un determinado control, el resultado es el que se obtuvo en la realidad.

Asimismo, y de cara a las recomendaciones, se pueden diseñar nuevos controles y/o modificar los existentes, viendo rápidamente su efecto sobre el procedimiento sometido a revisión.

Cada vez es más frecuente la auditoría sobre un proceso completo, en el que se realiza un análisis integral del mismo, en el que la mayoría o gran parte de sus funciones o actividades están soportadas por sistemas informáticos. En este tipo de trabajos suelen colaborar tanto auditores informáticos como otro tipo de auditores, obteniéndose una revisión general de cómo funciona y está controlado el proceso. Todo ello suele ser de gran utilidad para los auditados.

INFORMÁTICA PARA GESTIONAR LA AUDITORÍA

Cuando Auditoría Interna está adecuadamente organizada y trabaja con planificación previa, tiene unos programas que cumplir, prioridades en los mismos, recursos humanos limitados, información que manejar, recomendaciones que seguir, etc.

Como ayuda a la gestión de auditoría, se puede desarrollar o adquirir un sistema mecanizado para dar soporte informático a la planificación y control de las auditorías y a otros trabajos y actividades realizados.

En este sentido, lo correcto es que, a fines del ejercicio, Auditoría Interna publique una memoria resumen sobre todas las actividades efectuadas durante el año, lo que exige disponer de una amplia documentación sobre:

- Trabajos realizados.
- Situación de recomendaciones.
- Planificación a corto plazo.
- Planificación a largo plazo.

En cuanto a la planificación a largo plazo, es frecuente encontrar en publicaciones, artículos sobre sistemas mecanizados que ajustarían dicha planificación en función del tiempo disponible y de las áreas de riesgo.

Se trata de introducir el análisis de riesgos en la planificación de Auditoría Interna, de manera que sea el ordenador quien defina todas las áreas a auditar, determinando la prioridad con que se han de efectuar los trabajos.

Determinadas empresas han desarrollado programas de gestión integral del proceso de auditoría que permiten unificar el archivo de la función de Auditoría Interna incluso en direcciones de Auditoría Interna en distintos continentes o mantener informada a la Comisión de Auditoría del estado de implantación de las recomendaciones vía web.

RECURSOS INFORMÁTICOS

Los recursos son de tres tipos: recursos humanos, equipos y formación.

- Recursos humanos

  Para la elaboración y diseño de un plan informático de auditoría es necesario contar, al menos, con una persona o un equipo con conocimientos sobre metodologías de análisis y programación sobre los sistemas operativos, así como de otras herramientas informáticas.

  Esta persona puede pertenecer al departamento de Auditoría Interna o ser cedida por la unidad de informática, si la empresa dispone, para ello, del personal suficiente, o bien contratada del exterior.

  En el caso de utilizar personal de la empresa, la primera duda sería relativa a la selección del individuo en cuestión. ¿Es más conveniente formar un auditor en informática o un informático en auditoría?

  En principio parece que resulta mucho más rápido formar como auditor a un experto en informática que a la inversa, sin que ello suponga que los auditores no deban adquirir una cierta formación informática y que, incluso, lleguen a ser auditores especialistas en esta rama si tienen esa vocación. Lo ideal sería disponer de un informático

que tenga deseos de cambiar su forma de trabajo, pero que no pierda en ningún momento el interés por el área de donde procede, continuando su especialización en ella y procediendo a su formación como auditor.

Todos los auditores deben colaborar en el desarrollo del plan, así como en las auditorías informáticas que progresivamente se vayan realizando.

- Equipos

Se debe disponer de ordenadores portátiles, en definitiva, el *hardware* de Auditoría Interna conviene que tenga una estructura mínima que permita, por otra parte, desarrollar una informática de auditoría propia.

Actualmente, es muy amplia la gama de posibilidades donde poder escoger. Una vez más nos encontramos con la limitación del tamaño de cada empresa y el interés de la Dirección. En cualquier caso, Auditoría Interna debe poder disponer de los equipos de la empresa, ya que en ellos reside la información y de ellos debe extraerla para su tratamiento.

En esos equipos deben desarrollarse las aplicaciones informáticas de auditoría para el análisis de los datos de carácter general de la empresa. Por ello, es interesante que la unidad de auditoría pueda disponer de ordenadores personales conectados al servidor principal o corporativo, con posibilidad de acceso para consultar cualquier tipo de ficheros. De esta forma podrán analizar la información almacenada en el ordenador utilizando el sistema operativo y el *software* de la empresa.

Respecto al sistema informático para la propia gestión de Auditoría Interna, así como para satisfacer sus necesidades concretas de trabajos de auditoría, conviene disponer de ordenadores personales con *software* específico ya desarrollado, de los que existe alguna oferta en el mercado.

La solución óptima para una auditoría de tamaño medio sería una combinación de ordenadores personales con capacidad de conectarse a la red y al ordenador principal o corporativo y ordenadores personales portátiles, con posibilidad de conectarse a la red y a Internet, en el caso de que existan delegaciones o filiales que auditar.

- Formación

La necesidad de que los auditores utilicen en su trabajo las tecnologías informáticas al máximo nivel requiere que se familiaricen con la terminología empleada en los centros de proceso de datos y que tengan una serie de conocimientos cuya extensión puede depender de lo que se vaya a requerir de ellos. Por tanto, se puede hablar de dos niveles principales de formación: básica y conveniente.

- **Formación básica.** Su objetivo sería el de familiarizar al auditor con la informática y darle una visión de cómo la automatización puede incidir en su trabajo. Se trataría de unos conocimientos mínimos que el auditor podría ir ampliando en función de sus necesidades:
  - Conocimientos básicos sobre *hardware*, saber lo que es un ordenador, sus funciones, los soportes de información y sus características (velocidades, volúmenes, tipos de acceso, etc.).
  - Conocimientos básicos sobre el *software,* cómo son los sistemas operativos, los compiladores, definición de ficheros y sus características, comunicaciones, sistemas de teleproceso, etc.
  - Conocimiento sobre las funciones principales que se realizan en un centro de proceso de datos y la organización del mismo.
  - Conocer las estructuras y manejo de datos, las relaciones entre datos, clasificaciones, selecciones, tipos de acceso, formas de proceso, definición de registros, definición de bases de datos, etc.
  - Conocimientos generales de los sistemas de aplicación más extendidos (hojas de cálculo, tratamiento de textos, presentaciones, conocimientos generales de las aplicaciones desarrolladas en la empresa, gestores de bases de datos, etc.).
  - Seguridad, perfilado, controles de acceso y nociones relativas a la ciberseguridad, *backups* y recuperaciones.

- **Formación conveniente.** Nos referimos a un auditor especializado en auditoría informática. Aparte de los mencionados anteriormente, debería llegar a poseer conocimientos básicos sobre:
  - Análisis de sistemas, programación, procedimientos y metodologías más empleadas.
  - Desarrollo orgánico de aplicaciones, organización de datos, funciones y procesos de generación de informes, etc.
  - Algún lenguaje de alto nivel o algún generador de informes para realizar aplicaciones o informes para auditoría.
  - Manejo y cuidado de ordenadores personales, sobre todo en lo que se refiere a la utilización de las herramientas de ofimática.

Para el proceso continuo de formación y actualización se puede ir consultando información y realizando cursos como los de COBIT, ITIL o el SANS Institute, entre otros.

Tenemos que tener presente que, en la actualidad, estamos asistiendo a una serie de realidades que están cambiando nuestro mundo y nuestra manera de trabajar y tene-

mos que ser conscientes de que han surgido nuevas tecnologías como *machine learning, big data, artificial intelligence, smart contract, blockchain…* Y esto está produciendo un proceso de digitalización de los departamentos de Auditoría Interna desde un doble punto de vista:

- Tenemos que saber cómo auditar estas nuevas realidades, obtener los *skills* adecuados para poder realizar nuestro trabajo.
- Es imprescindible realizar un proceso de transformación: una de las palancas fundamentales para realizarlo es a través del *Data Analytics*, para ello tenemos que mejorar nuestro *performance* a través de los datos.

3. El fraude informático

Entendemos por fraude informático toda acción que origine un perjuicio para la empresa, entidad o persona, en beneficio de un tercero y utilizando para ello medios informáticos o manipulando indebidamente los mismos.

Los activos que son objeto, y a su vez objetivo, del fraude informático son los datos y las aplicaciones informáticas.

Las acciones fraudulentas más comunes que se pueden cometer sobre estos activos son:

SOBRE LOS DATOS

- **Consulta indebida.** Consiste en acceder y disponer de información no permitida, reservada o confidencial.
- **Apropiación de información.** Se considera la enajenación masiva de datos o ficheros completos para su posterior uso o divulgación.
- **Modificación no permitida de datos.** Consiste en la alteración indebida de los datos con ánimo de lucro. Esta es la tipología más frecuente del fraude informático y una de las más dolosas.

SOBRE LAS APLICACIONES INFORMÁTICAS

- **Acceso indebido.** Consiste en disponer o usar sin consentimiento una determinada aplicación informática. Normalmente se utiliza como vía de acceso a los datos (consulta o modificación).
- **Apropiación indebida de aplicaciones** para uso, manipulación o comercialización.
- **Modificación ilícita de aplicaciones.** Consiste en modificar algún programa de proceso con el fin de obtener un beneficio; este tipo de fraude informático es el más característico y espectacular.

3.1 Tipología o forma del fraude informático

El fraude informático utiliza diversas vías y se reviste de múltiples y variadas formas, alguna de las cuales vamos a contemplar. Para cada una de ellas intentaremos exponer el método y posteriormente el objeto que persiguen.

- **Fraude a través de los procedimientos.** Se introducen datos falsos utilizando los procedimientos administrativos existentes para la captura y flujo de la información, y aprovechando las debilidades y faltas de control en el sistema.
- **Utilización delictiva de terminales en ordenadores personales.** Aprovechando la falta de precaución o de controles físicos, se obtiene de esta forma acceso a las aplicaciones y a los datos.
- **Accesos indebidos a aplicaciones.** Por falta de claves de protección, o porque éstas sean conocidas, fáciles, o por mala organización y gestión del sistema de claves.
- **Acceso a través de las líneas o redes de teleproceso.** Se accede al ordenador principal y a sus recursos, o a las claves de programas o a la información transmitida a través de la red.
- **Uso indebido de los programas de utilidad.** Permiten el acceso o modificación de cualquier dato.
- **Posibilidad de cambio no autorizado en programas o aplicaciones.** Por falta de controles o procedimientos adecuados de desarrollo y mantenimiento de los sistemas informáticos.
- **El uso de ordenadores personales conectado a los ordenadores principales.** Al facilitar el acceso a las bases de datos corporativas, permitiría la extracción de información y el traspaso de esta a disquetes y otros soportes comunes.

El rápido desarrollo de las tecnologías de la información hace que surjan, de manera igualmente veloz, nuevas tipologías de fraude, lo que implica la necesidad de prestar una especial vigilancia a esta área. Un aspecto destacado, a tener en cuenta, es la posibilidad de fraudes a través de Internet, ya que es muy habitual la conexión de las empresas a Internet y la relación con los clientes, empleados y proveedores a través de este medio, abriendo la posibilidad de acceso a nuestros sistemas informáticos.

3.2 Medidas preventivas

Son aquel conjunto de acciones, controles y procedimientos que tratan de disuadir, evitar o dificultar el fraude informático. Entre estas medidas señalaremos:

- **Establecer procedimientos administrativos** para la entrada de datos, que sean lo más sensibles posibles; controlados; facilidad para detectar pérdidas, duplicaciones, falsifi-

caciones; documentación de fácil interpretación; relación biunívoca transacción/documento fuente; procedimiento único, aunque las vías de entrada sean múltiples.

- **Poder dividir el total empresarial** en unidades de negocios más pequeñas, con subdivisiones jerárquicas y asignación de responsabilidades, más fáciles de controlar.
- **Controles de acceso a los datos.** Los podemos clasificar en: controles físicos como acceso a locales, a ordenadores y a terminales, y controles lógicos, claves referidas a terminales, a las personas que acceden y a las funciones a realizar y a los datos a procesar.
- **Establecer procedimientos de asignación y gestión de claves** que garanticen los accesos y asignen responsabilidades concretas a las personas concretamente.
- **Prohibir terminantemente la existencia de ventanas y puentes falsos** en las aplicaciones.
- **Control de las líneas de comunicaciones**, sobre los accesos, transmisiones y flujos; encriptación de la información transmitida; claves complejas, renovables y largas.
- **Procedimientos de control en las funciones de desarrollo y mantenimiento** de aplicaciones informáticas: realizando pruebas exhaustivas, validaciones e inspecciones sobre las aplicaciones nuevas o modificadas; emplear una metodología muy modular en el desarrollo de aplicaciones, de forma que se puedan desarrollar y mantener por módulos sencillos y fácilmente revisables.
- **Limitar y controlar el uso, sobre ficheros corporativos,** de los programas de utilidad.
- **Establecer procedimientos para la utilización de los ordenadores personales**, asignando responsabilidades sobre la custodia de los datos corporativos.
- **Selección adecuada del personal,** cuidar la política de recursos humanos y relaciones laborales, rotación razonable, remuneración justa y buen ambiente laboral, unido a castigos ejemplares cuando se detecten infracciones.

3.3 Medidas correctivas

Son aquellas medidas que tienen por objeto la detección del fraude informático. El fraude informático es muy difícil de descubrir, pero cada vez existen más medios disponibles para perseguirlo. Relacionaremos los más característicos:

- **Diseño de informes que verifiquen la integridad, coherencia y consistencia de la información,** interrelacionando ficheros, conformando, cuadrando cuentas y verificando cantidades totales.

- **Programas que calculen ratios y relaciones entre valores críticos,** alarmas por cuotas o topes establecidos.
- **Seguimiento diario del uso del ordenador,** de los procesos ejecutados, de los recursos empleados, disponiendo de informes de ayuda que detecten las excepciones.
- **Existencia de *pistas de auditoría*** sobre los datos principales, de manera que permanezca la huella de cualquier cambio o acceso sobre los mismos.
- **Verificación periódica de los datos,** utilizando las pistas de auditoría y técnicas de muestreo verificativo.
- **Utilización de juegos de ensayo y procesos de simulación.**
- **Disponer de un servicio de auditoría informática** que verifique el correcto funcionamiento de los controles.

Nuestra intención no tiene otra finalidad que la de sensibilizar a los auditores internos sobre este riesgo permanente que afecta a la sociedad actual, intentando alarmar a los moderados y moderar a los alarmistas.

4. Los ordenadores personales (PC's)

El ordenador personal o PC es un aparato o máquina lógico-pensante utilizado como instrumento de oficina o artilugio doméstico. Su presencia es, hoy día, tan común y familiar como lo pueda ser la televisión o el móvil. Cualquier hogar medio, cualquier oficina o puesto de trabajo dispone de un PC. Los PC's están dotados de unas características especiales como eficacia, flexibilidad, independencia, facilidad de manejo, etc., que le confieren esa funcionalidad propia capaz de otorgar envidiables prestaciones a su propietario. Estas **características inherentes al PC son la antítesis de la seguridad,** por lo que *a priori* afirmamos que los PC's, por su propia naturaleza, no son seguros.

Los riesgos a los que nos referiremos a continuación, inherentes a los PC's como instrumentos de trabajo en las empresas, son riesgos graves y trascendentes que pueden afectar, de manera muy directa, al patrimonio y a la operatividad. Tales riesgos son:

- **Falta de formación de los usuarios.** Esto se traduce en el uso de herramientas poco adecuadas, técnicas poco apropiadas, falta de eficacia, quebraderos de cabeza...
- **Descoordinación en la adquisición de equipos.** Esto da lugar a diversidad y variedad de material informático, compra de PC's caros e incompatibles, sin posibilidad de compartir programas, ni formación, ni procedimientos.

- **Descoordinación también en el uso.** Empleo de *software* diferente, y también incompatible, diversos usuarios/propietarios con disparidad de criterios y procedimientos, con distinta formación, o sin ninguna. Añadamos también el riesgo de adquisición de *software* pirata, o poco control en copias, y cesión de programas con el problema consiguiente de la infección vírica.

- **Personalismo del PC.** El ordenador personal, como su mismo nombre indica, va dirigido a las personas, fomenta el individualismo y aislacionismo por su propia naturaleza, sus usuarios son propietarios. Puede producir un desarrollo desmadrado, y una duplicidad de esfuerzos, que llevado todo ello a sus últimas consecuencias, puede producir un caos desmedido de información, programas, datos, usuarios y herramientas.
  Aunque los PC's pueden disponer de un sistema de seguridad, en su esencia, la seguridad es opuesta a la propia filosofía y naturaleza del PC, tanto es así que cualquier norma o procedimiento destinados a proteger la seguridad e integridad de la información son mal aceptadas, difícilmente adaptadas y peor practicadas.

- **Falta de documentación.** Por lo general, no se documentan los programas desarrollados en PC; esta circunstancia es propia del individualismo ya mencionado. Estos programas dependen para su ejecución y comprensión de su autor/propietario.

- **Pérdida de datos y programas.** Originados por la falta de profesionalidad de los usuarios/propietarios, que puede generar una catástrofe como la de perder datos fundamentales, y sobre todo programas, que se traduce en la pérdida de horas de esfuerzo y de trabajo intelectual.

- **Pérdida de datos y programas por carecer de procedimientos de resguardo.** Carecer de la generación de copias de seguridad oportunas.

4.1 Medidas para controlar los riesgos en los PC's

Enumeramos las medidas básicas de aplicación obligada:

- **Coordinación en la compra de PC's.** La adquisición de cualquier ordenador personal debe estar controlada por una unidad, generalmente informática, encargada de la compra, gestión, inventario y mantenimiento.
- **Control en la compra del *software*** para PC's. Esta medida es muy importante y fundamental, ya que coordina esfuerzos, ahorra recursos, evita problemas legales y contaminación por virus.
- **Protección física de los PC's** a base de llaves cerrojos, vigilancia de recintos y cierres de puertas de despacho.
- **Normas, procedimientos y recomendaciones sobre el uso** y manejo de los PC's en lo que se refiere a:
  · Utilización, manejo, mantenimiento y resguardo del aparato.

  - Método para resolución de problemas o averías, tanto lógicas como físicas.
  - Copias de seguridad, alcance y frecuencia de las mismas.
  - Ubicación y resguardo de las copias de seguridad.
  - Documentación. Obligatoriedad de documentar aplicaciones de trascendencia y valor empresarial.
  - Control y esmerada verificación y validación con el fin de garantizar la integridad de la información compartida.
- **Formación.** Cursos de utilización, programación, uso de paquetes de *software.* Cursos oportunos y bien dirigidos, adecuando la materia a las personas y funciones.
- **Existencia de una unidad de sistemas de información capaz de coordinar todo el flujo** de datos hacia los cargos y funciones directivas, y de toda aquella información que se considere básica y crítica para la toma de decisiones.
- **Estrictas normas para el tratamiento y seguimiento** de la información corporativa que reside en los PC's.

La lista de las medidas es aún mayor que la de los riesgos, pero mientras que éstos son esporádicos y gratuitos, las medidas deben de ser constantes además de costosas. El auditor interno debe vigilar y velar por la eficaz implantación de estas medidas.

Todo esto, que es válido para los PC's, sirve de igual manera para los ordenadores portátiles, tabletas y móviles, que son de uso cotidiano tanto a nivel personal como profesional. Adicionalmente, hay que añadir el riesgo de que a través de estos dispositivos nos conectamos, generalmente vía Internet, a los sistemas informáticos de las empresas con lo que el riesgo de acceder de manera remota a la misma información que se utiliza en el trabajo diario, en un entorno más controlado y seguro.

5. Internet y el comercio electrónico

En estos ajetreados tiempos tecnológicos que corren no es necesario presentar a nadie Internet. Todo el mundo la conoce y, de alguna manera, la ha utilizado o padecido. La Red se ha colado de repente en nuestro trabajo y en nuestras vidas, cambiando comportamientos, organizaciones y procesos, ayudando en algunos casos y no tanto en otros.

Tampoco vamos a descubrir, a estas alturas, las notables excelencias de Internet y la importancia que va adquiriendo día tras día, de manera que ha llegado a convertirse en el fenómeno más importante y de mayor incidencia desde finales del pasado milenio. Internet ofrece enormes facilidades para la comunicación, para la información y para el comercio, es medio de intercambio de ideas, cultura, acuerdos y bienes de todo tipo y condición, en un entorno cada vez más

abierto y que a través de la Red se expande a velocidad extraordinaria sin más fronteras que las económicas y tecnológicas.

Abordaremos también en este trabajo los aspectos comerciales de Internet, el llamado comercio electrónico, pues consideramos que, atendiendo a su importancia y a los riesgos generados, es objeto de una atención específica posterior. Nos ocuparemos, pues, de la Red Internet como tal, como fue en su concepción y misión inicial: medio de información y comunicación y del comercio electrónico que se apoya y se basa en la propia Red.

5.1 La Red Internet

Las ventajas que aporta la Red en el mundo de la información y comunicación son inmensas y, además, van incrementándose día a día a medida que Internet va extendiéndose y ganando en potencia y velocidad. Relacionemos sus ventajas que, por otro lado, son sus principales características:

- **Comunicación.** Es la característica más importante de la Red. Su principal función. A través de la comunicación permite la conexión, para intercambio de información inmediata entre cualquiera de los puntos de esta.
- **Información.** Por la Red fluyen noticias y todo tipo de información de forma abierta y actualizada para la consulta desde todos los puntos de la Red.
- **Expansión.** Salvo actuaciones puntuales llevadas a cabo en sus territorios por regímenes políticos muy concretos (China, Corea del Norte, por ejemplo), Internet es una red abierta y potente y va creciendo y aumentando su potencia y velocidad muy rápidamente, aumentando su volumen y capacidad, y extendiéndose no sólo en cuanto a puntos de comunicación posible, sino también en cuanto a contenidos de información que fluyen por la Red.
- **Libertad.** Es la característica más propia de la Red Internet, que nació con esa vocación. La Red no tiene propietario, ni más leyes que las tecnológicas, ni más ideología que la del libre mercado, por encima de los Estados y las naciones. El individuo, convenientemente tecnificado, el llamado *internauta*, es el rey y dueño de la Internet.
- **Coste.** La Red es muy barata. Gratis en su conexión –aunque hay que disponer de un terminal de acceso, ya sea PC, tablet o móvil– y prácticamente gratis en su uso en virtud de la aplicación en todos los países de tarifas planas específicas. Además, los costes van bajando aceleradamente.
- **Oportunidades.** Internet ofrece cantidad de posibilidades de ocio, de negocio, de relaciones personales, culturales o comerciales, posibilidades que van desde la simple relación personal al conocimiento científico, artístico, utilización de medios de imagen, sonido, etc.

5.2 Riesgos en Internet

Nuestro propósito no es otro que enfocar el impacto de la Red Internet desde el punto de vista de Auditoría Interna, considerando este nuevo invento y artilugio universal como un instrumento de trabajo, olvidándonos tanto de triunfalismo inútiles como del obstinado derrotismo, para descubrir y analizar con rigor los riesgos que se pudieran derivar del uso de la Red, sin olvidar las indiscutibles ventajas que aporta.

RIESGOS PARA LAS PERSONAS

Aunque la Red parece un instrumento inofensivo, se han detectado riesgos y daños a nivel personal derivados de su uso y que atentan a la propia personalidad e intimidad de las personas:

- **Riesgos que atentan a la personalidad.** Derivados del uso abusivo de la Red. Afecta a personas que solo viven «en» y «para» Internet, y que a través de ella se relacionan en un mundo virtual olvidando cualquier conexión con el mundo real. Son personas con adición a Internet, que se ven atrapadas y absorbidas por la Red.

- **Riesgos de confidencialidad.** En la Red, cada persona es una clave y cada clave es personal al estar referida e íntimamente relacionada con una persona. La clave está viva en la Red, pues actúa, navega, consulta, publica y compra. A través de la clave, y por la actividad que despliega se puede conocer la personalidad que va unida a esa clave.

- **Riesgos de espionaje.** La Red es abierta y pública, por lo que es sencillo espiar siguiendo el rastro y los movimientos de las claves. Incluso existen unos instrumentos llamados *cookies* que son utilizados como cebos, de manera que las personas que acceden a ellos son posteriormente espiadas impunemente.

RIESGOS PARA LA EMPRESA

En la empresa, además de los riesgos que afectan a las personas que la integran, hay que añadir otros de carácter institucional que inciden sobre la organización y sus intereses de negocio.

- **Uso de Red Internet.** El uso descontrolado de Internet puede dar lugar a abusos desmedidos que afectan tanto al tiempo de trabajo remunerado que el empleado dedica a la Red descuidando sus obligaciones profesionales, como de actividad en la que el empleado realiza operaciones en la Red que nada tienen que ver con las funciones y responsabilidades que tiene encomendadas. Estos abusos indiscriminados y generalizados pueden ocasionar grave daño para las empresas.

- **Publicación en la Red.** Normalmente, las empresas disponen de una página web cuyo objeto principal es darse a conocer en la Red. Es la imagen al exterior que la organización quiere comunicar, es como el escaparate virtual al mundo de las comunicaciones. La mala utilización de esta herramienta, la mala administración o la falta de controles en la publicación puede ocasionar un grave daño a la empresa, al proporcionar una visión deformada o distinta de la diseñada por la política de imagen corporativa. En este sentido, también hay que hacer referencia al uso y aparición en las denominadas redes sociales, que pueden llegar a provocar importantes riesgos para las empresas, fundamentalmente reputacionales.

RIESGO DE LOS VIRUS

Los virus son muy populares, tristemente populares, por sus efectos nocivos sobre los ordenadores personales (PCs), son un riesgo y últimamente un riesgo unido a la Red. Se dividen en clases en razón al objeto de su actuación, y son:

- **Inocuos o jocosos.** No realizan ningún daño, solo tratan de jugar, desconcertar o sorprender. Forman parte de este grupo los virus llamados *gusanos* que saltan de un ordenador a otro.

- **Destructivos.** Su objeto es destruir, pueden destruir no sólo ficheros, sino el sistema operativo o incluso la propia placa de ordenador dejándolo inservible y destruyendo toda la información del disco duro. Son los vulgarmente llamados *bombas lógicas.* Ejemplo de este tipo de virus son el *Chernobyl* y el *Melissa.*

- **Espías.** Son los más corrientes y los que atentan más directamente a la seguridad del ordenador. Su objeto es colocarse entre el usuario y el ordenador y manejar y controlar las operaciones espiando contraseñas, procedimientos y controles. Son los popularmente llamados *Caballo de Troya,* pues actúan de la misma forma que el famoso caballo de "La Ilíada".

La transformación digital que hoy se vive en el sector empresarial, empujado por la evolución vertiginosa de las tecnologías de la información, nos lleva a un horizonte de cambios que no imaginábamos hace unos años, vinculado con el omnipresente tema de la ciberseguridad.

INTERNET DE LAS COSAS

Hay que hacer una mención aparte a lo que se denomina *Internet de las Cosas* (IoT en sus siglas en inglés), que se refiere a la interconexión digital de los objetos cotidianos a través de Internet. Es, en definitiva, la conexión a Internet más con objetos que con personas, pero a través de los cuales se puede acceder a la red de las empresas. Todos estos

dispositivos pueden parecer inofensivos para la ciberseguridad de nuestras redes y empresas, pero no es así. Al ser dispositivos conectados a Internet, son susceptibles de ser accedidos y comprometidos, además no suelen contar con los mismos estándares de calidad de seguridad de fábrica que otros dispositivos de red. Estos dispositivos suelen incluir deficiencias de seguridad como:

- Usuarios y contraseñas de acceso por defecto y sin mecanismos que obliguen al usuario a cambiarlas por otras más seguras.
- Páginas web de control y configuración insegura o accesibles en remoto.
- Inexistencia de cifrado en las comunicaciones, falta de personalización en la configuración de la seguridad.
- Falta de soporte y actualizaciones de los fallos de seguridad detectados tanto en el *software* de control como en el *firmware* de los dispositivos.

Esto hace que sean una presa fácil para los ciberdelincuentes, que buscan este tipo de dispositivos como punto de entrada a las redes de las empresas o a otros puntos de la red que se encuentran más protegidos. El ataque y compromiso de estos dispositivos puede dar lugar a consecuencias graves para la seguridad como:

- Ser añadidos a una *red zombi* que pueda realizar ataques de denegación de servicio (DDoS), como es el caso de la red *Mirai*, que en 2016 dejó sin servicio a varias de las empresas más importantes a nivel mundial durante varias horas.
- Ser utilizado como puente o punto de entrada para atacar otros equipos de la misma red, para poder robar información o comprometer servidores para realizar otras acciones delictivas.
- Reconfigurar los dispositivos y cambiar sus condiciones de utilización. Se podría manipular los termostatos del CPD para elevar su temperatura y producir una seria avería en los servidores ahí alojados.

Se debe ser consciente del problema que suponen estos dispositivos para la seguridad de nuestras empresas, así como las consecuencias que puede acarrear su deficiente instalación, configuración y mantenimiento. Para ello debemos tomar todas las medidas de precaución que nos permitan estos dispositivos, y debemos tratarlos como cualquier otro elemento que tengamos conectado a nuestras redes, incluyéndolos dentro de las políticas de seguridad y del Plan de Seguridad (PDS) de la empresa.

Se necesita ser precavido con los dispositivos que conectamos a nuestras redes corporativas, ya sea a través de cable o por medio de una red wifi, por inofensivo que parezca. Cualquier dispositivo conectado a la red es susceptible de ser atacado y comprometido, y más si no dispone de las medidas de seguridad suficientes. Hay que reducir el riesgo que suponen para las empresas, tomando conciencia del riesgo existente

y de sus posibles consecuencias. Por tanto, es un aspecto que debe ser incluido en los trabajos que se deben realizar por parte de Auditoría Interna.

CONTRATACIÓN DE SERVICIOS

Siempre hay que tener presente el riesgo que supone la utilización de servicios externos, el llamado *outsourcing* con sus diferentes modalidades y que tan extendido está en las áreas de sistemas de información.

También existe riesgo en la **contratación de servicios en la nube** *(Cloud computing)* es un modelo de prestación de servicios a través de una red (Internet), que permite a las empresas acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma flexible y pagando únicamente por el consumo efectuado. Existen tres grandes tipologías de servicios a contratar en la nube, los basados en:

- **La infraestructura como servicio** (infraestructura *as a service o IaaS)*, en la que se entrega almacenamiento básico y capacidades de cómputo como servicios estandarizados de la red. El proveedor se encarga de la administración y la empresa tiene el control sobre los sistemas operativos, almacenamiento, aplicaciones y componentes de red.
- **La plataforma como servicio** *(platform as a service o PaaS),* en lo que la empresa no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede instalar nuevas aplicaciones.
- **El *software* como servicio** *(software as a service o SaaS)* se caracteriza por ofrecer una o varias aplicaciones como servicio, en la que la empresa no tiene el control, se consume en función de su uso y elimina la necesidad a la empresa de instalar la aplicación en sus dispositivos, evitando asumir el coste de soporte y el mantenimiento del *hardware* y el *software.*

Hay cuatro modelos para implementar una nube:

- **La nube pública** es mantenida y gestionada por un proveedor no vinculado con la empresa. En este tipo de nubes, tanto los datos como los procesos de varias empresas comparten los servidores, sistemas de almacenamiento y otras infraestructuras de la nube.
- **La nube privada** es una buena opción para las empresas que necesitan alta protección de datos. Las nubes privadas están en una infraestructura bajo demanda, dedicada para una sola empresa que controla qué aplicaciones deben ejecutarse y dónde.
- **La nube híbrida** que combina los modelos de la nube pública y privada.
- **La nube comunitaria** se define como aquella que se organiza con la finalidad de servir a una función o propósito común, es administrada por las empresas constituyentes o por terceras.

Principales riesgos de la contratación de servicios en la nube

- La dependencia del proveedor de servicios en la nube.
- La disponibilidad del servicio está sujeta a la disponibilidad de acceso a la red (Internet).
- La información sensible del negocio no reside en las instalaciones de la empresa.
- La continuidad del proveedor de servicios en la nube depende de su situación financiera.
- La disponibilidad de servicios diferentes al catálogo de servicios estandarizados podría tardar meses o incluso no ser factibles.
- La actualización continua de las aplicaciones puede impactar negativamente en su utilización por falta de conocimientos.
- La posible degradación en el servicio por una gestión inadecuada de la demanda por parte del proveedor.
- La información podría quedar expuesta a terceros afectando a su privacidad.

Hay que recordar que la responsabilidad última es de las empresas contratantes y no de los proveedores. Estos riesgos varían en función de la tipología de servicios *(IaaS, PaaS, SaaS)* y del modelo de implementación de la nube (privada, híbrida, pública, comunitaria). Cuestiones fundamentales son determinar qué información es susceptible de estar en la nube, que proveedor es el más indicado contratar y las auditorías de los servicios contratados.

6. Actuación de Auditoría Interna

Ante esta situación creada por nuevas tecnologías, Auditoría Interna debe actuar, por un lado, como un usuario más de las mismas beneficiándose en todo lo que sea posible para mejorar su propio trabajo y la gestión de este. Pero, por otro lado, Auditoría Interna, en razón a su misión, debe ser consciente de todos los riesgos que hemos mencionado que afectan tanto a las personas como a las empresas, por lo que deberá comprobar si existen los procedimientos, controles y salvaguardas que organicen el funcionamiento y uso de la Red, para posteriormente verificarlos y analizar si son los más idóneos para cubrir los riesgos derivados.

AUDITORÍA INTERNA DEBERÁ COMPROBAR SI:

- **Existen en la organización normas o procedimientos que regulen el uso de Internet,** en lo que se refiere a:
  - Autorización del servicio Internet. Autorización del acceso a la Red. Quién autoriza y cómo se autoriza.

  - El alcance de cada autorización. Definir los entornos de Red a los que cada usuario está autorizado a entrar.
  - Definir las operaciones que cada usuario pueda realizar.
  - Restricciones de uso, o bien horario o de limitación de tiempo.

- **Existen en la organización normas o procedimientos que regulen la publicación de información corporativa en Internet,** en lo que se refiere a:
  - Autorización de quién debe publicar en Internet. Autorización de la publicación corporativa en la Red. Quién autoriza y cómo se autoriza.
  - Quién debe controlar y gestionar las publicaciones.
  - Definición de los procesos de publicación.
  - Seguimiento de los accesos o visitas, atención e impacto de las publicaciones.

- **Existen en la organización procedimientos para evitar la contaminación por virus,** tales como:
  - Existencia de antivirus con aplicación constante el PC y servidores y constantemente actualizados.
  - Comprobación de que los procesos de uso se ajusten a las limitaciones propias de los antivirus.
  - Autorización para *bajarse* información de la Red al PC. Análisis o filtrado de la información que se *baja.*
  - Control antivirus de la información recibida por correo electrónico.

- **Verificar si existe una función de control que garantice y supervise el cumplimiento de las normas y procedimientos anteriores** y que realice el seguimiento del uso de la Internet en la organización.

- **Comprobar que las normas y procedimientos aplicados, así como su seguimiento y control, son suficientes y adecuados** para cubrir los riesgos expuestos en los apartados anteriores.

Como complemento a estas comprobaciones vinculado con la ciberseguridad, se debería revisar:

- La seguridad del servidor web y de sus páginas.
- La calidad sobre el código de las aplicaciones informáticas que se utilizan, tanto si ha sido desarrolladas por terceros o *in-house.*
- *Hacking ético,* que hace referencia a la simulación de uno o diversos tipos de ciberataques usando técnicas de *hacking.*
- Ingeniería social, para comprobar el nivel de conocimiento que los empleados tienen sobre actividades como *phishing, malware* o *ransomware* y de la utilización de las contraseñas.
- El mapa de red de la empresa y cómo esta se conecta a Internet.

Esta es, a nuestro juicio, la responsabilidad y la posición de Auditoría Interna ante los riesgos generados por el uso de Internet que, como se puede apreciar, son numerosos e importantes.

En este sentido, se está produciendo la incorporación en los equipos de auditoría, o subcontratando la actividad, de especialistas en esta materia para conformar trabajos de *Red Team,* para realizar tests de intrusión, en los que se pueden ver vulnerabilidades y fallos en la estructura tecnológica de una organización.

El objeto de este trabajo ha sido el de intentar enviar un mensaje claro a las organizaciones y a sus Auditorías Internas para que, en función a la misión que les ha sido encomendada y de la importancia que en la actualidad tienen las nuevas tecnologías, se ocupen y preocupen de controlar la actividad y el uso de los medios en este mundo tecnológico, ya de por sí un tanto descontrolado.

7. El comercio electrónico

Uno de los grandes beneficios que presenta Internet es el comercio electrónico, propulsor de un mercado único e integrado, de un mercado global de acceso rápido y fácil a millones y millones de vendedores y de clientes para comprar cualquier clase de artículos, a precios universalmente competitivos, en este supermercado ágil y transparente.

Esta es la teoría progresista y optimista que alumbró el nacimiento ambicioso del comercio electrónico a finales del siglo pasado, con el mensaje subliminal de que aquello era el futuro y el camino, y que no había otro, ni para el comprador, ni para el vendedor, ni para el mercado. Se decía que aquel que no estuviese en la Red y en el mercado electrónico no existía.

7.1 Inconvenientes y soluciones del comercio electrónico

El tiempo le está dando la razón. El comercio electrónico ha crecido de manera exponencial desde su nacimiento. Pese a las razones que se esgrimían en su contra, como la inseguridad, el riesgo de fraude, fenómenos culturales o de costumbres y a otros de logística.

Ante la inicial desconfianza en el mercado electrónico y a su medio y una vez analizados, ha sido preciso implantar medidas para solventarlos, e intentar dotar, al mercado y al medio electrónico, de algunas cualidades fundamentales de las que carecía y que citamos a continuación.

LA SEGURIDAD DE LA RED

Internet ha dejado de ser abierto y libre. En el inmenso campo de la información han empezado a surgir parcelas acotadas y con propietario, que no permiten el acceso a extraños.

De esta forma la tecnología de Internet proporciona la comunicación, la autopista de la información, pero hacia lugares cerrados y protegidos, es decir, seguros, se ha creado la posibilidad de realizar comunicaciones seguras a través de la Red, de manera que garantizan la confidencialidad e integridad de la información que por ella circula.

LA AUTENTICACIÓN DE LAS PERSONAS

En el comercio es fundamental que el comprador sea el comprador y el vendedor sea el vendedor; es decir, que se produzca una identificación inequívoca de las partes. Los fraudes en el comercio por suplantación de la identidad han sido incontables. Cuando el mundo financiero irrumpió en la Red, cuando las transacciones electrónicas comenzaron a mover grandes cantidades de dinero, entonces fue necesario asegurarlas en origen y destino, garantizar y autentificar quién realiza un pago y a quién. Así nació la autenticación electrónica, basada en la firma electrónica, la cual, mediante la utilización de un código personal e intransferible, avalado por una entidad estatal o financiera, autentifica que la persona es quien realmente dice ser, con más garantías que la propia firma tradicional.

LA ADECUACIÓN DEL MERCADO

El Mercado Electrónico se está adaptando a las circunstancias, a la demanda y a las ventajas que le proporcionan el entorno y el medio, como no puede ser de otra manera. Para ello se ha organizado en tiendas o/y centros comerciales suficientemente acreditados por marcas o por entidades financieras, es como comprar en tiendas de élite en vez de *tiendas en barrios marginales*. De esta forma, el mercado se limita y se estrecha, pero se asegura. Por otro lado, el mercado electrónico cada vez se abre más a ofrecer servicios y bienes que se pueden suministrar directamente a través de la Red y que son los que mejor se adaptan a la infraestructura y recursos logísticos necesarios para el suministro.

LA INTEGRIDAD DE LOS PAGOS

El pago a través del número de la tarjeta de crédito en una Red abierta y accesible no es una garantía, por lo que se han arbitrado fórmulas más seguras que acrediten si el dinero existe realmente y cuál es su dueño. La solución más segura adoptada es la *tarjeta inteligente,* que lleva incorporado un *chip* y que admite un código secreto y un dinero límite de gasto.

7.2 Acción de Auditoría Interna

Ante esta situación creada por las nuevas tecnologías, Auditoría Interna debe actuar con moderación, cautela y mesura, y con el rigor en el análisis de las ventajas y de los riesgos que cualquier nueva situación implica.

En relación con el comercio electrónico, Auditoría Interna, por razón a su misión, deberá ser consciente de todos los riesgos que se han mencionado que afectan tanto a las personas como a las organizaciones, por lo que deberá comprobar si existen los procedimientos, controles y salvaguardas que organicen el funcionamiento y uso del comercio en la Red, para posteriormente verificarlos y analizar si son los más idóneos para cubrir los riesgos.

AUDITORÍA INTERNA DEBE COMPROBAR SI

- **Existen en la organización normas o procedimientos que regulen el uso del comercio electrónico en la entidad,** en lo que se refiere a:
  - Autorización de la compra o venta a través de la Red. Autorización al mercado electrónico. Quién autoriza y cómo se autoriza y cómo se controla y se revisa.
  - El alcance de cada autorización. Definir los entornos o los mercados a los que cada persona autorizada puede acceder, así como de Red a los que cada usuario está autorizado a entrar.
  - Definir las operaciones que cada persona autorizada pueda realizar y los límites en cuanto tipo de operación y cuantía de estas.
  - Restricciones de uso, o bien horario o de limitación de tiempo.
  - Instrumentos, procedimientos y controles para comprobar el resultado de la compra o de venta electrónica, el bien, su calidad, la fecha de entrega o el pago realizado.
  - Medios de seguridad y controles necesarios para verificar que se cumplen con rigor los procedimientos establecidos.

- **Existen en la organización los medios técnicos necesarios para garantizar la confidencialidad, integridad y autenticación de las transacciones** en el comercio electrónico, tales como:
  - Comprobar que los mercados a los que se acude y que la contraparte de la compra, o de la venta, está debidamente identificada acreditada por entidades responsables de reconocido prestigio.
  - Verificar que cada persona autorizada para operar en el mercado electrónico dispone de una firma electrónica personal y certificada por la autoridad competente.
  - Comprobar que las transacciones financieras y comerciales se realizan a través de un canal seguro.
  - Verificar la existencia de un banco o entidad financiera que acredite y respalde la operación comercial.
  - Controlar el pago, la integridad del dinero electrónico o de la transferencia.
  - Control antivirus de la información recibida.

- **Verificar si existe una función de control que garantice y supervise el cumplimiento de las normas y procedimientos anteriores** y que realice el seguimiento del uso del comercio electrónico en la organización.

- **Comprobar que las normas y procedimientos aplicados, así como su seguimiento y control, son suficientes y adecuados** para cubrir los riesgos expuestos en los apartados anteriores.

Esta es, a nuestro juicio, la responsabilidad y la posición de Auditoría Interna ante los riesgos generados por la utilización de comercio electrónico que, como toda herramienta nueva y potente, está sometida a altos riesgos de integridad y sobre todo de fraude.

El objeto de este trabajo ha sido el de intentar enviar un mensaje claro a las organizaciones y a sus Auditorías Internas para que, en función a la misión que les ha sido encomendada, y de la importancia que en la actualidad tiene el uso de las nuevas tecnologías, se ocupen y preocupen en controlar la actividad del comercio electrónico complejo en cuanto la forma y el medio y fuente de irregularidades y de fraudes.

Auditoría Interna y el fraude

1. Qué entendemos por fraude
2. Tipología del fraude
3. Síntomas o indicadores del fraude
4. Los estímulos del fraude
5. Líneas básicas de una política antifraude
6. Disuasión del fraude
7. Posición de Auditoría Interna
8. Normas del Instituto de Auditores Internos

Instituto de Auditores Internos de España

1. Qué entendemos por fraude

Cuando hablamos de fraude nos referimos al fraude en la empresa realizado por empleados de la organización. Sin ninguna preocupación doctrinal o jurídica, a los efectos de este manual, entendemos por fraude el acto cometido –bien directamente o mediante cooperación– por cualquier empleado, directivo, consejero, accionista u otras personas relacionadas con la empresa, que origina un perjuicio a la misma en beneficio de los defraudadores.

Es decir, con intención engañosa y por acción u omisión, alguien no defiende los intereses de la empresa que moral y éticamente estaba obligado a defender, anteponiendo sus propios intereses al de la compañía. Es importante destacar que cuando decimos intención engañosa, el concepto incluye la existencia de acciones tendientes a ocultar o dificultar la posibilidad de identificación de las acciones indebidas.

Los ejemplos son innumerables: apropiación de bienes, dinero o valores, ocultación de información, transmisión de información confidencial al exterior para debilitar la posición competitiva de la empresa, falsificación de marcas o contrahechura, falsificación de documentos, sustracciones y robos, etc.

Las posibilidades de fraude son hoy tan numerosas y diversas que no es posible llegar a determinarlas, sobre todo considerando que la dependencia de la informática en los procesos ha abierto un nuevo abanico de riesgos que debe ser analizado con las particularidades propias de la tecnología.

El fraude se transformó en un riesgo que se ha materializado en casi la totalidad de las organizaciones y, hoy por hoy, ninguna organización puede considerarse libre de él. Es responsabilidad de la gestión de la empresa considerarlo como un acto de alta probabilidad de ocurrencia y arbitrar los recursos para actuar contra él.

Existe también el fraude en beneficio de la propia organización, como, por ejemplo, venta o asignación de activos ficticios o con engaño, fraudes a terceros, que suele ser el más importante (fraude indirecto), fraude fiscal, pagos ilegales (comisiones, sobornos, etc.), errores intencionados en la información pública, ocultaciones contables, etc. En este capítulo nos centraremos en el fraude de los empleados.

2. Tipología del fraude

No es posible hacer una enumeración exhaustiva de los innumerables tipos de fraude que pueden cometerse en el mundo actualmente, teniendo en cuenta que a medida que el proceso de innovación tecnológica tiene más injerencia en los procesos de negocio, surgen nuevas moda-

lidades que los defraudadores potenciales pueden aprovechar para llevar a cabo nuevas formas de fraude.

Sin embargo, apuntamos una relación de tipos o formas de fraude más frecuentes en las empresas, listado que es susceptible de una constante modificación y diversificación según sea la organización y su sector de actividad. Por otra parte, este es un manual para auditores internos, básicamente; y es desde la perspectiva de una unidad de Auditoría Interna desde la que se abordan los tipos de fraude que los auditores deben tratar de impedir, sin olvidar que esta es una tarea colectiva de una organización y no exclusiva de los auditores internos. Señalamos a continuación los fraudes más frecuentes en las corporaciones.

APROPIACIÓN INDEBIDA, HURTO O ROBO

- Robo o hurto de mercancías, herramientas, productos, materiales, prendas, etc.
- Apropiación o divulgación y venta de información confidencial.
- Uso indebido del nombre, imagen, representación o del saber hacer de la organización.
- Apropiación de aplicaciones informáticas *(software),* proyectos, métodos, secretos tecnológicos o investigaciones.
- Uso indebido del tiempo de trabajo, de herramientas e instrumentos, de ordenadores, teléfonos y otros medios de comunicación y útiles de la organización.

FALSIFICACIÓN O MANIPULACIÓN DE LA INFORMACIÓN

- Falsificación de documentos internos de pagos al personal como nóminas, dietas, gastos, ayudas sociales, etc.
- Modificación indebida de registros informáticos.
- Falsificación de documentos en beneficio de un tercero externo, como desviar pagos a otra cuenta, manipular ingresos, etc.
- Falsificar albaranes y vales de entradas y salidas de almacenes y similares.
- Manipular y alterar información sobre horas de trabajo, enfermedad, vacaciones.
- Falsificación de cheques, talones y tarjetas de crédito.
- Malversación de fondos.

RECIBO DE COMISIONES Y SOBORNOS

- Compras de productos o servicios a empresas en las que participan empleados de la empresa compradora, o son propietarios ellos o sus familiares.
- Contratos de servicios y obras innecesarios o no utilizados.
- Contratos realizados en clara desventaja para la organización.

- Contratos en condiciones aparentes excesivamente ventajosas.
- Recepción de obras, productos, mercancías, etc., no acordes con las estipulaciones de los contratos.
- Penalidades por incumplimiento no ejecutadas.
- Contratos con cláusulas de difícil o imposible cumplimiento.
- Contratos y operaciones fraudulentas en seguros.

3. Síntomas o indicadores del fraude

Los síntomas son señal de que algo puede suceder, un fenómeno revelador de una enfermedad. Exigen atención especial y estar muy alerta para evitar mayores males, deteniendo el proceso perturbador. Igual que los médicos, los auditores internos necesitan conocer los síntomas para diagnosticar si existe o no peligro para el cuerpo aquejado, en este caso, la empresa u organización de que se trate. Para los auditores internos, la preocupación por los síntomas o indicadores debe comenzar en los programas de trabajo, incluyendo pasos pensados para detectar indicios de fraude, especialmente en áreas de riesgo. Citamos a continuación algunos de los más significativos:

- Pérdida de documentos.
- Ausencia de justificantes o documentación soporte de las operaciones.
- Excesivas justificaciones o excusas.
- Situaciones frecuentes de incumplimiento de las normas.
- Quejas de proveedores por falta de información para enviar ofertas.
- No existen conciliaciones de control de las operaciones.
- Operaciones que se anulan repetidamente.
- Con frecuencia se reclaman pagos no efectuados.
- Devoluciones de pedidos que los clientes dicen no haber solicitado.
- Excesivos cargos por retraso a los proveedores.
- Reiteradas cancelaciones de cargos por retrasos.
- Efectos no cobrados ya vencidos o cancelados.
- Déficits en los inventarios.
- Incumplimiento de las especificaciones sobre mercancías, productos o servicios suministrados.
- Merma en las entregas.
- Utilización de documentos y copias en lugar de originales.

- Lugar de entrega distinto al apropiado (oficinas, centros de fabricación, plantas, ubicación de instalaciones).
- Pagos duplicados, confirmación de pagos sin cancelar o sin indicación de pagado.
- Facturas que se presentan como duplicados o copias.
- Las facturas están en papel en blanco, no en impresos o documentos oficiales.
- Partidas antiguas pendientes de conciliaciones de control.
- Proveedores con nombres y direcciones comunes.
- Desorden manifiesto en las áreas o actividades auditadas.
- Cambio de dirección seguido de una solicitud de pago.
- Aumento o disminución radical de gastos o transacciones al final del ejercicio.
- Repentinos pagos de operaciones o cuentas atrasadas.
- La dirección del proveedor es la misma que la de un empleado.
- Cualquier ejecución demasiado buena para ser creída.

Los síntomas indicados pueden ser detectados por auditores expertos si actúan sensibilizados en la detección de posibles fraudes. Si ponemos el foco en las personas, en sus hábitos, también se pueden percibir otros indicadores de fraude que se deben tener en consideración. Apuntamos los más relevantes:

- Un nivel de vida que no corresponde con el sueldo o salario de la persona en lo que se refiere a signos de riqueza, gastos excesivos, incrementos patrimoniales no justificables, etc.
- Los que están en situación económica grave: deudas, quiebras de negocios particulares, etc.
- Los resentidos por no estar situados en la organización al nivel que ellos creen que deberían tener.
- Los incumplidores sistemáticos de normas y políticas establecidas por la dirección.

En este sentido, una medida elemental que, sin embargo, no se emplea con seriedad y rigor, por lo general, es la de analizar con el debido detalle y cuidado los antecedentes del personal de nuevo ingreso, *(business intelligence* aplicado en la contratación de recursos).

4. Los estímulos del fraude

En muchas organizaciones no existe una mentalidad adecuada a la realidad del tiempo que vivimos en lo que respecta a la prevención y detección del fraude. Por eso, los auditores internos han de tener muy presentes algunas situaciones que pueden actuar como incentivos para los defraudadores potenciales y activos:

- Inexistencia de un posicionamiento firme de la empresa con respecto al fraude.

- Sistemas de control inoperantes.
- Carencia de políticas y de normas específicas que regulen actuaciones en casos de fraude, atribuciones y responsabilidades.
- Falta de información y de formación sobre la cuestión.
- Insuficiente segregación de funciones.
- Indefinición de funciones y atribuciones.
- Permisividad que no sanciona automáticamente al defraudador.
- Mal ejemplo de «los de arriba».
- Despreocupación por los controles.
- La creencia de que la confianza es un mecanismo de control.
- El temor al escándalo.
- Los «paños calientes», en general.

5. Líneas básicas de una política antifraude

La lucha contra el fraude no es una función que corresponda a uno u otro servicio, unidad o departamento de una organización, sino que exige una actuación coordinada y global dentro de la misma, partiendo de una declaración formal del Consejo de Administración y de la Dirección por la que se comprometen a:

- Prohibir cualquier tipo de actividad ilegal, incluyendo las que beneficien a la propia organización.
- Definir las responsabilidades de quienes han de llevar a cabo y dirigir las investigaciones y establecer los informes correspondientes al Comité de Auditoría o al Consejo (normalmente Auditoría Interna y los servicios de seguridad).
- Exigir que cualquier empleado que crea que se está cometiendo un fraude de graves consecuencias para la organización, lo comunique a sus superiores o a los responsables de las investigaciones directamente, quienes deberán guardar el más absoluto secreto respecto al denunciante.
- Establecer que toda sospecha sea investigada y comunicada por escrito a la Comisión de Auditoría o al Consejo.
- Prohibir cualquier acción que pueda estimarse como represalia contra denunciantes, testigos y declarantes y castigar los actos de encubrimiento.
- Exigir a la Dirección la observancia de la ley, reglamentos, normas de la Administración Pública, normas internas, y otorgar el apoyo y la información necesarios para la realización de las investigaciones a Auditoría Interna y a los servicios de seguridad.

- Tratar a los sospechosos y perpetradores de fraude de manera similar y consecuente, sin consideración a la posición que ocupen en la organización, ni a la importancia de la función que realicen.
- Asumir la responsabilidad de conocer los riesgos de fraude y de establecer controles adecuados para su prevención y detección.
- Elaborar y difundir en la organización un Código de Conducta en el que se determinen claramente las obligaciones y responsabilidades del personal, con independencia de cualquier otro compromiso legal, político o económico (Anexo 14).

6. Disuasión del fraude

La disuasión del fraude es responsabilidad de la Dirección. La responsabilidad de los auditores internos es examinar y valorar la adecuación y eficacia de las acciones adoptadas por la dirección para el cumplimiento de esta responsabilidad.

La disuasión consiste en llevar a cabo acciones encaminadas a evitar la realización del fraude y a limitar los riesgos si éste se ha llevado a cabo. El principal mecanismo para la disuasión del fraude es el control, y la responsabilidad principal de la Dirección es establecer y mantener un control efectivo.

Para cumplir con sus responsabilidades en la disuasión del fraude, Auditoría Interna deberá determinar si concurren o no los siguientes aspectos:

- El ambiente de la organización favorece la conciencia de control.
- Se fijan objetivos realistas.
- Si existen políticas corporativas escritas (por ejemplo: un Código de Conducta) que describen las actividades prohibidas y las acciones a tomar cuando se descubre cualquier violación.
- Están vigentes normas apropiadas de autorización de las transacciones.
- Los activos están convenientemente salvaguardados y especialmente en áreas de alto riesgo.
- Los canales de comunicación proporcionan información adecuada y fiable a la dirección.
- Es necesario recomendar la mejora de los controles para la disuasión del fraude.

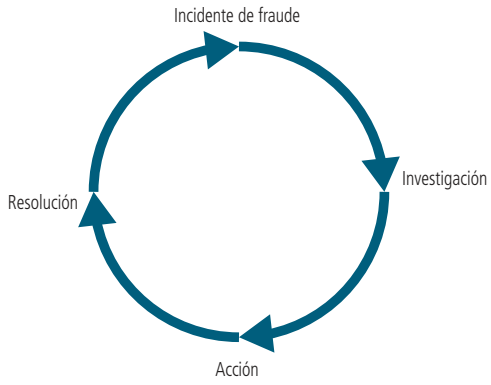
7. Posición de Auditoría Interna

Aunque la responsabilidad de la disuasión del fraude pertenece a la Dirección de las organizaciones, que es a quien corresponde fijar el posicionamiento ético de la empresa en este tema y

establecer los sistemas de control de estas, los auditores internos (como Tercera Línea) son responsables del examen y estimación de la adecuación y eficacia de las medidas tomadas por la Dirección para cumplir con tal responsabilidad. En este sentido, lo primero que Auditoría Interna debe tener es una idea muy clara de los fraudes e irregularidades graves cometidos a lo largo de un cierto período, cuyo plazo de tiempo ha de determinar la propia Auditoría Interna. Es decir, escribir la historia del fraude en la organización, dónde se ha producido, qué importancia ha tenido, cuáles han sido las medidas tomadas, etc. Todo ello, conjuntamente, con la tarea de identificar y analizar los riesgos de fraude propios del entorno donde opera la empresa (por tipo de actividad, por región o país donde opera, por tipo de operativa interna de la empresa, etc).

Para llevar a cabo estos cometidos, Auditoría Interna tiene que estar debidamente formada e impuesta en este campo y ser capaz de mentalizar a la Dirección, en el supuesto de que no haya Comisión de Auditoría, recomendando y, en su caso, efectuando una serie de medidas elementales para luchar con éxito contra el fraude.

MODELO DEFECTUOSO



MODELO EFICAZ

Entre esas medidas citamos a continuación las más relevantes:

- Ser consciente de que el fraude está instalado potencialmente en cualquier organización.
- Proponer la elaboración de un Código de Conducta.
- Analizar los procesos y determinar las áreas de riesgos graves y puntos críticos de fraude.
- Conocer y poner en práctica medidas específicas de detección de fraudes.
- Solicitar la autoridad necesaria para actuar en los casos de investigación de fraudes con la ejecutividad necesaria para coordinar todas las actuaciones y redactar el correspondiente informe a la Comisión de Auditoría o al Consejo de Administración.

En esta línea de actuación, Auditoría Interna tiene que conocer cuál es la situación real de la organización en lo que atañe a la prevención del fraude, para lo cual sería conveniente que se formulase algunas preguntas como las que citamos:

- ¿Dispone la organización de normas escritas que recoja las medidas que se han de tomar en caso de denuncias de fraude y de actuaciones sospechosas?
- ¿Existe un Código de Conducta que defina las conductas inaceptables para todos los niveles y categorías del personal de la organización, sin consideración de la responsabilidad que ostenten?
- ¿Han sido las normas o el código difundidos para conocimiento de todo el personal?
- ¿Hay constancia escrita de la aceptación de estas normas por parte de empleados y directivos?
- ¿Existe alguna cláusula de comportamiento ético o aceptación de las normas antifraude de la empresa en los contratos firmados con los proveedores de la organización?
- Entre las competencias de la Auditoría Interna ¿figura la de investigar denuncias de posibles fraudes u operaciones o actividades sospechosas?
- ¿Se ha asignado esta responsabilidad a algún otro departamento?;
- ¿Se despide o castiga automáticamente a los infractores de la normativa sobre conductas inaceptables sin consideración de su cargo, eficiencia, años de servicio, etc.?
- ¿Recibe la Comisión de Auditoría o el Consejo de Administración un informe escrito de todos los casos que se producen y se conocen?
- Cuando se limita el alcance de un informe de auditoría o se les niega el acceso a los datos a los auditores, ¿Se comunican estas excepciones a la Comisión de Auditoría o al Consejo?
- ¿Hay cauces establecidos para que el personal formule denuncias cuando alguien sospecha que se está defraudando?

Las preguntas anteriores solamente son un ejemplo de las que formularse para que los auditores internos tengan clara idea del entorno en materia de lucha contra el fraude, y les pongan en situación de informar al comité o al consejo sobre el particular.

8. Normas del Instituto de Auditores Internos

El *Marco Internacional para la Práctica Profesional de la Auditoría Interna* promovido por el Instituto de Auditores Internos global desarrolla las normas, e interpretaciones concretas y consejos para la práctica sobre el riesgo de fraude, que recogen los aspectos más relevantes a tener en cuenta desde el punto de vista de la supervisión y control de esta materia, empezando por los propios elementos que definen la profesión. A continuación, recogemos los puntos más relevantes.

1210 APTITUD

- 1210.A2 - *"Los auditores internos deben tener conocimientos suficientes para evaluar el riesgo de fraude y la forma en que se gestiona por parte de la organización, pero no es de esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude".*

1220 CUIDADO PROFESIONAL

- 1220.A1 - *"El auditor interno debe ejercer el debido cuidado profesional al considerar:*
  - *El alcance necesario para alcanzar los objetivos del trabajo.*
  - *La relativa complejidad, materialidad o significatividad de asuntos a los cuales se aplican procedimientos de aseguramiento.*
  - *La adecuación y eficacia de los procesos de gobierno, gestión de riesgos y control.*
  - *La probabilidad de errores materiales, fraude o incumplimientos.*
  - *El coste de aseguramiento en relación con los beneficios potenciales".*

2060 - INFORME A LA ALTA DIRECCIÓN Y AL CONSEJO

"El Director de Auditoría Interna debe informar periódicamente a la Alta Dirección y al Consejo sobre la actividad de Auditoría Interna en lo referido al propósito, autoridad, responsabilidad y desempeño de su plan, y sobre el cumplimiento del Código de Ética y las Normas. El informe también debe incluir cuestiones de control y riesgos significativos, incluyendo riesgos de fraude, cuestiones de gobierno y otros asuntos que requieren la atención de la Alta Dirección y/o el Consejo.

Interpretación:

La frecuencia y el contenido del informe están determinados por el Director de Auditoría Interna en colaboración con la Alta Dirección y el Consejo. La frecuencia y el contenido del informe dependen de la importancia de la información a ser comunicada y la urgencia de las acciones a seguir por parte de la Alta Dirección y/o el Consejo.

Los informes del Director de Auditoría Interna dirigidos a la Alta Dirección y el Consejo deben incluir información sobre:

- *El estatuto de Auditoría Interna.*

- *La independencia de la actividad de Auditoría Interna.*
- *El plan de auditoría y su progreso.*
- *Necesidad de recursos.*
- *Resultados de las actividades de auditoría.*
- *Nivel de cumplimiento con el Código de Ética y las Normas y planes de acción para afrontar incumplimientos significativos.*
- *La respuesta de la dirección que, a juicio del Director de Auditoría Interna, podría resultar inaceptable para la organización.*

Estos y otros requerimientos de comunicación para el Director de Auditoría Interna están referenciados en las Normas".

2120 GESTIÓN DE RIESGOS

- 2120.A2 - *"La actividad de Auditoría Interna debe* ***evaluar la posibilidad de ocurrencia de fraude*** *y cómo la organización maneja y gestiona el riesgo de fraude".*

2210 OBJETIVOS DEL TRABAJO

- 2210.A2 - *"El auditor interno debe considerar la* ***probabilidad de errores, fraude, incumplimientos*** *y otras exposiciones significativas al elaborar los objetivos del trabajo".*

Auditoría Interna y la calidad

Instituto de Auditores Internos de España

1. Consideraciones generales

Según el Diccionario de la Real Academia Española, *calidad* es la propiedad o conjunto de propiedades inherentes a una cosa que permiten apreciarla como igual, mejor o peor que las restantes de su especie. En un sentido absoluto, buena calidad significa superioridad o excelencia, por lo que hablar de calidad y de programas y normas de calidad aplicadas a Auditoría Interna, exige una concepción adecuada de esta función, tal como hemos indicado en el capítulo "La Auditoría interna como profesión"

La calidad es un imperativo que surge en la fase de crecimiento y desarrollo profesional de la Auditoría Interna, posterior a la etapa de nacimiento y adolescencia, empleando la terminología que se usa para seguir la evolución de las empresas. Es decir, que primero hay que conseguir un departamento de Auditoría Interna que satisfaga las necesidades y características de la organización a la que sirve, con todas sus potenciales capacidades dispuestas para el cumplimiento eficaz de sus funciones y la consecución de sus objetivos. Después estaremos en condiciones de preocuparnos por la calidad aplicada al ejercicio de la función.

La preocupación por la calidad es algo que está ya presente en la mayoría de las organizaciones, cualquiera que sea su actividad y su mercado, y no se limita tan sólo a los productos o servicios de una empresa, sino a todas sus operaciones y actividades.

En lo que se refiere a la calidad aplicada al ejercicio de la función, el Instituto de Auditores Internos de España dispone de programas de aseguramiento y mejora de la calidad que están regulados en la Norma 1300. Ésta señala explícitamente: *"El Director de Auditoría Interna debe desarrollar y mantener un programa de aseguramiento y mejora de la calidad que cubra todos los aspectos de la actividad de Auditoría Interna".*

2. Programas de aseguramiento y mejora de la calidad: *Quality Assurance and Improvement Program*

La finalidad de un programa de aseguramiento y mejora de la calidad, tal y como lo definen las Normas, es proporcionar una cierta seguridad a la Comisión de Auditoría, al Consejo de Administración y a la Alta Dirección, incluido, por supuesto, el del propio departamento de Auditoría Interna. Se trata de asegurarse de que el trabajo de auditoría interna se realiza conforme a las Normas, al Estatuto de Auditoría Interna, a otras normas aplicables y a las expectativas de la Comisión de Auditoría y la Alta Dirección.

Un programa de esta naturaleza se compone de **evaluaciones internas y externas.**

La interpretación de la Norma 1300 menciona que un programa de aseguramiento y mejora de la calidad está concebido para permitir una evaluación del cumplimiento de las Normas por

parte de la actividad de Auditoría Interna y de la aplicación y cumplimiento del Código de Ética por parte de los auditores internos. Adicionalmente, este programa también evalúa la eficiencia y eficacia de la actividad de Auditoría Interna e identifica oportunidades de mejora. En las últimas modificaciones del *Marco Internacional para la Práctica Profesional de la Auditoría Interna* se promueve, incluso, la participación del Consejo de Administracion, dando así la oportunidad al Director de Auditoría Interna de alentar la supervisión del Consejo en el programa de aseguramiento y mejora de la calidad.

Para calificar al departamento, un instrumento fundamental es su Estatuto de Auditoría Interna, cuya valoración debe hacerse en los términos que indica la serie de Normas 1300 con sus correspondientes Guías de Implementación, referidas al nivel del departamento dentro de la organización y a otra serie de requisitos que éste debería cumplir.

Citamos algunos ejemplos de Normas y de criterios potenciales de medición que hay que tener en cuenta para evaluar la actuación del departamento de Auditoría Interna:

- Código de Ética del auditor interno y su ratificación anual.
- Objetivos, políticas y procedimientos de la organización aplicables al departamento de Auditoría Interna.
- Leyes, reglamentos y normas de la Administración Pública o de quien establezca los requerimientos de Auditoría Interna e información.
- Métodos para identificar las actividades a auditar, la evaluación de riesgos y para determinar la frecuencia y alcance de las auditorías internas.
- Documentos de planificación de Auditoría Interna, en particular los propuestos a la Alta Dirección y al Consejo.
- Organización y estructura del departamento, la descripción de puestos de trabajo y los planes de desarrollo profesional de los auditores internos.

2.1 Supervisión

La supervisión del trabajo de los auditores internos tiene como fin comprobar que se realiza de conformidad con las Normas, las políticas del departamento y los programas de Auditoría Interna. La supervisión correcta es el elemento más importante de un programa de aseguramiento y mejora de la calidad y la base de apoyo de las evaluaciones internas y externas posteriores.

La responsabilidad por desarrollar y mantener un programa de aseguramiento de la calidad se describen en la NORMA 1300, que hace recaer esta responsabilidad sobre el Director de Auditoría Interna. Éste debe asegurar que las auditorías internas están

debidamente supervisadas. La supervisión o seguimiento continuo es un proceso que comienza con la planificación y continúa a través de las fases de examen, evaluación, informe y seguimiento de las recomendaciones pendientes originadas en las auditorías internas realizadas.

La **supervisión continua** incluye los siguientes aspectos:

- Asegurar que los auditores internos poseen los conocimientos y técnicas requeridas.
- Dar instrucciones adecuadas durante la planificación de la auditoría interna y la aprobación del programa de la misma.
- Comprobar la ejecución del programa.
- Examinar los papeles de trabajo y comprobar que soportan debidamente las evidencias, conclusiones, observaciones, recomendaciones, e informes de auditoría interna.
- Garantizar que los informes sean precisos, objetivos, claros, concisos, constructivos, completos y oportunos.
- Alcanzar los objetivos de la Auditoría Interna.
- Seguimiento de las recomendaciones.
- Proporcionar oportunidades de formación a los auditores internos, debiendo esta quedar registrada documental y adecuadamente archivada.
- Comparar la función de la Auditoría Interna con las mejores prácticas internacionales.
- Analizar la percepción de la Auditoría Interna por el resto de la organización.
- Proporcionar herramientas de marketing de la función hacia la organización.

La supervisión se extiende al desarrollo del personal de auditoría, a la evaluación del desempeño, a los controles de tiempos y gastos y a otros temas administrativos similares.

2.2 Evaluaciones internas (Norma 1311)

Las evaluaciones internas deben incluir el seguimiento continuo del desempeño de la actividad de Auditoría Interna y autoevaluaciones periódicas o evaluaciones por parte de otras personas dentro de la organización con conocimientos suficientes de las prácticas de Auditoría Interna.

Las evaluaciones internas es lo que se ha llamado *auditoría de la Auditoría Interna,* y **son efectuadas, de manera continua o periódica, por el propio departamento de Auditoría Interna,** generalmente por quien o quienes designe el responsable del mismo. Los grandes departamentos –dicen las Normas– pueden tener una persona encargada del programa

de aseguramiento y mejora de la calidad o con denominación y responsabilidades similares. Los **objetivos** de esta revisión son:

- Examinar y evaluar el grado de supervisión existente.
- Verificar el cumplimiento de las Normas.
- Verificar el cumplimiento de las políticas y normas internas.
- Conocer el grado de confianza en Auditoría Interna por parte de la Alta Dirección, de la Comisión de Auditoría y de los propios auditados.
- Medir la eficacia y adecuación del departamento y la calidad del trabajo que hace.
- Comprobar el seguimiento de las recomendaciones y su cumplimiento.

Según la **NORMA 1320,** el Director de Auditoría Interna debe comunicar los resultados del programa de aseguramiento y mejora de la calidad a la Alta Dirección y al Consejo. Se deben incluir el alcance y las frecuencias de las evaluaciones (tanto internas como externas), la cualificación e independencia de los evaluadores considerando posibles conflictos de interés, las conclusiones y planes de acciones correctivas.

Como un proceso de seguimiento continuo, puede aportar formación, intercambio de ideas y coherencia al personal del departamento, así como seguridad a su director o responsable, que es quien debe iniciar y controlar dicho proceso y nombrar a los auditores internos que lo llevarán a cabo. Para ello deberá asegurarse de que:

- El equipo o la persona sean suficientemente cualificados.
- Dispongan del tiempo y de los medios adecuados.
- Estén dotados de la necesaria independencia y autonomía.
- Se informe sobre esta operación al personal de Auditoría Interna.
- Se compromete seriamente a tomar medidas correctoras si fuesen necesarias.

2.3 Evaluaciones externas (Norma 1312)

La evaluación externa tiene, en principio, los mismos objetivos que la evaluación interna que, de forma global, se resumen en evaluar la calidad de los trabajos del departamento, aportando dos aspectos nuevos. Por un lado, examinar la calidad y adecuación de la dirección del departamento. Y, por otro, todo lo relativo a cuestiones del personal, tales como integración y motivación, promociones y ascensos, líneas de carrera, agravios comparativos, procesos de formación y actualización de conocimientos, frustraciones, etc.

Según las Normas, las evaluaciones externas deben hacerse, al menos, cada cinco años, aunque también indican –si los recursos no lo permiten– hacer más hincapié en la supervisión y en la evaluación interna. Se trata de dos fases del programa de aseguramiento y mejora de la calidad cuyo no cumplimiento es imperdonable en los depar-

tamentos de tipo medio y grande, una responsabilidad directa de la Comisión de Auditoría, del Consejo, de la Alta Dirección y del propio director o jefe de la unidad de Auditoría Interna.

En estos casos, corresponde al jefe de la unidad analizar cada año las causas que impiden la revisión externa.

Las evaluaciones externas deben ser efectuadas por personas con la debida cualificación, que sean independientes de la organización y que no tengan con ella conflictos de intereses ni reales ni aparentes. La exigencia de cualificación personal –entendida a efectos de interpretación de las Normas– es que sean auditores profesionales, capaces de acreditar una experiencia concreta como auditores internos, sin que ello pueda ser reemplazado por pertenecer a una compañía auditora de cuentas o consultora, con todo el prestigio de que éstas gocen, si así se les reconoce.

En este sentido, las propias Normas señalan que quienes lleven a cabo las evaluaciones externas pueden ser auditores internos externos, suministradores de servicios externos, independientes, lo que significa que no están bajo el control de la organización a la cual pertenece Auditoría Interna, ni relacionados con ella o con su departamento de auditoría.

Al finalizar una revisión de esta clase, la persona o equipo revisor ha de emitir un informe por escrito que contenga una opinión sobre el cumplimiento de las Normas por el departamento, el Estatuto y otras normas aplicables, con apropiadas recomendaciones de mejora relativas a cuantas cuestiones hemos indicado anteriormente. Este informe será entregado, normalmente, a la Comisión de Auditoría del Consejo, expresión que venimos usando para indicar que, si no existiera la primera, será el Consejo de Administración el receptor de la información y la Alta Dirección.

Hay que decir que las revisiones externas, dentro del contexto de un programa de garantía de la calidad total, deberían ser precedidas por las fases de supervisión y de revisión interna, cuya autorización corresponde al Director de Auditoría Interna. La propuesta de realizar una revisión externa debe someterse a la Comisión de Auditoría del Consejo y a la Alta Dirección, en su caso, por el director del departamento, explicando las finalidades que se persiguen y lo que preceptúan las Normas, para que resulten positivas para todos. A este respecto, dichas Normas señalan que **las revisiones limitadas de los auditores de cuentas,** centradas fundamentalmente en sus auditorías de los estados financieros, **no constituyen revisiones externas de un programa de calidad total para un departamento de Auditoría Interna.**

Asimismo, el personal del departamento tendría que ser convenientemente informado sobre el particular, haciéndole comprender la importancia de la revisión para evitar sus-

ceptibilidades y recelos y conseguir el adecuado clima de cooperación y participación con los revisores externos y evitar fricciones y posibles problemas.

En definitiva, se trata de implicar activa y positivamente a todas las partes interesadas en un proceso de esta naturaleza y de sacar el máximo provecho de la revisión externa, cuyos **principales objetivos** son:

- Determinar la eficacia y eficiencia de la Auditoría Interna, con especial atención a la importancia y cumplimiento de sus recomendaciones.
- Analizar la adecuación de sus medios a las funciones y objetivos que se le asignan.
- Verificación de las áreas de riesgo que cubre por medio de sus planificaciones anuales.
- Calidad de sus trabajos y grado de supervisión interna (de la dirección del departamento, del comité de auditoría y de la alta dirección).
- Imagen del departamento en la organización.
- Política de recursos humanos: rotación o permanencia en el departamento, selección y formación del personal, promociones y ascensos, motivación e integración, etc.

Aunque las Normas especifican que las revisiones externas se hagan cada cinco años, al menos, pueden darse según las propias Normas circunstancias especiales que justifiquen un intervalo diferente, entre las que se incluyen:

- Revisiones impuestas por el Consejo.
- La relativa estabilidad del Estatuto, de la organización, del personal y de las actividades a auditar.
- La naturaleza, alcance, independencia y resultados globales de las revisiones internas.

A partir del año 2005, el Instituto de Auditores Internos de España ha formado un equipo de profesionales altamente cualificados para realizar estas evaluaciones externas, y las principales empresas del país ya se están implicando en este proceso, no sólo por ser una exigencia de las Normas que garantiza la eficacia y eficiencia del departamento, sino que, además, proporciona un instrumento de marketing muy valioso para Auditoría Interna de cara a que el resto de la organización perciba el valor que aporta esta función.

3. Normas ISO 9000 y Auditoría Interna

En este epígrafe ofrecemos una visión muy simplificada de otra vertiente de la calidad, que se ha considerado un nuevo reto profesional para Auditoría Interna: la auditoría de los sistemas de la calidad, regulada por la familia de Normas ISO 9000, establecidas por la Organización Internacional de Normalización (ISO, por su siglas en inglés) para asegurar y gestionar con criterios de calidad las empresas y organizaciones, en general.

Para su desarrollo, seguimos la publicación del Instituto que lleva por título *La Auditoría Interna y la ISO 9000,* cuyo autor es Alfredo Hierro Cuenca, un libro de imprescindible conocimiento y manejo para los auditores que pretendan auditar sistemas de calidad de conformidad con las normas internacionalmente aceptadas. Recomendamos la lectura de esa publicación para profundizar en estos aspectos dada su enorme valía.

Prueba de ello es que el Comité Europeo de Normalización (CEN) las ha hecho suyas con la denominación de normas EN 29000, y en España, la Asociación Española de Normalización y Certificación (AENOR) ha procedido de idéntica manera llamándolas normas UNE 66-900.

Las razones de su difusión y general aceptación son que sus indicaciones y recomendaciones las hacen aplicables a cualquier tipo de organización, por ello son una obligada referencia cuando se habla de calidad y auditoría.

Para las normas ISO, el **aseguramiento de la calidad** es el conjunto de acciones planificadas y sistemáticamente implantadas dentro del sistema de la calidad, y demostrables, si es necesario, para proporcionar la confianza adecuada de que una entidad cumplirá los requisitos para la calidad.

Y **gestión de la calidad** es el conjunto de actividades de la función general de la dirección que determina la política de la calidad, los objetivos y las responsabilidades y se implanta por medios tales como la planificación de la calidad, el control, el aseguramiento y la mejora de la calidad en el marco del sistema de la calidad.

Las ISO definen un **sistema de la calidad** como la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la calidad. Con el eficaz funcionamiento del sistema se busca que los productos o servicios de la organización satisfagan las necesidades y expectativas de sus clientes, que la organización haya tenido en cuenta las exigencias sociales y del entorno, y prever los problemas antes que detectarlos.

Es justamente la obligación y la necesidad de asumir la responsabilidad de llevar a cabo auditorías de los sistemas de la calidad, como cualquier otro sistema de gestión de las organizaciones, lo que queremos poner de relieve con nuestros comentarios sobre calidad y Auditoría Interna. En este sentido, las ISO conciben las auditorías de la calidad como un examen metódico e independiente para determinar si los resultados relativos a la calidad cumplen las disposiciones establecidas, están implantadas de forma efectiva y son adecuadas para alcanzar los objetivos.

El sistema de calidad debe ser evaluado internamente según las ISO por la propia organización, utilizando técnicas de Auditoría Interna por personas cualificadas que sean independientes y no tengan responsabilidades sobre las áreas o actividades auditadas.

Por otro lado, las características que las ISO señalan para los auditores de calidad son –como ha demostrado contundentemente Alfredo Hierro en la publicación ya mencionada– casi las mismas que se exigen a los auditores internos en el *Marco Internacional para la Práctica Profesional de la Auditoría Interna.*

Se puede concluir que los departamentos profesionalizados de Auditoría Interna son los indicados para llevar a cabo auditorías internas de los sistemas de la calidad en todas sus categorías, de cumplimiento, de eficacia, de mejora y de aseguramiento externo, en este caso a efectos registrales de normalización.

Auditoría Interna y el desarrollo sostenible

1. La hoja de ruta para el desarrollo sostenible
2. La información no financiera (INF)
3. Los sistemas de gestión

Instituto de Auditores Internos de España

1. La hoja de ruta para el desarrollo sostenible

Las organizaciones empresariales se han enfocado tradicionalmente hacia la generación de valor financiero para los accionistas. Sus sistemas de información estaban dirigidos a medir los resultados de los negocios a través de los ingresos y los gastos devengados, la caja generada derivada de las entradas y salidas de fondos, y el patrimonio de los accionistas, como diferencia entre el valor de los activos y el de los pasivos.

Sin embargo, la supervivencia de las empresas en el largo plazo requiere, además, generar valor y un impacto positivo en otros grupos de interés –especialmente empleados, clientes, proveedores, financiadores– y también en la sociedad en la que desarrollan sus actividades. Esto implica conocer y dar respuesta a sus expectativas, que no solo son económicas, sino que también tienen que ver con la ética que practican en sus negocios y con su conducta desde un punto de vista medioambiental y social. Es decir, las empresas tienen que asumir su responsabilidad social ante otras organizaciones y personas que pueden verse afectadas por sus negocios, y que cada día tienen más protagonismo en los mercados y en la regulación.

En las últimas décadas se ha ido extendiendo la idea de que los modelos económicos tradicionales son cortoplacistas, generan desigualdades, contribuyen a un uso abusivo de los finitos recursos del planeta e impactan negativamente en el clima, por lo que comprometen el futuro y la calidad de vida de las siguientes generaciones. Como resultado de esta visión, y de los datos que la avalan, las empresas que quieren liderar sus mercados están llegando al convencimiento de que el desarrollo económico será sostenible, o no será.

Los analistas, conscientes de la sensibilidad de los inversores a todos aquellos aspectos que puedan afectar al valor y a la sostenibilidad de los negocios, han desarrollado metodologías de clasificación e índices que recogen, de forma general, tres ámbitos que popularmente se denominan ESG (por sus iniciales en inglés) o ASG (por sus iniciales en español):

- **Ambiental.** Incluye aspectos como el cambio climático, la contaminación, la economía circular, el uso sostenible de los recursos (principalmente materias primas, energía y agua) o la biodiversidad.

- **Social.** Incluye aspectos relativos al personal, a los proveedores, al servicio al cliente o a la sociedad, en general; así como las políticas y prácticas de contratación, formación, evaluación, remuneración, relaciones laborales, igualdad, diversidad, conciliación, seguridad y salud, accesibilidad, quejas y reclamaciones, contribución social o derechos humanos.

- **Gobierno.** Incluye aspectos relativos a los derechos de los accionistas, modelo de gobierno, composición y perfil de los miembros de los órganos de gobierno, ética, prevención del fraude y la corrupción, gestión de riesgos o transparencia.

La Organización de las Naciones Unidas, y algunos de los organismos que la estructuran, han sido muy activos en promover el desarrollo sostenible como concepto global. Sobresale el **Pacto Mundial** *(Global Compact),* iniciativa internacional presentada en el Foro de Davos de 1999, que promueve implementar 10 Principios universalmente aceptados para promover el desarrollo sostenible en las áreas de derechos humanos y empresa, normas laborales, medioambiente y lucha contra la corrupción en las actividades de las empresas. Mas de once mil organizaciones de todo el mundo son firmantes de este pacto.

Pero, probablemente, el concepto más integral del desarrollo sostenible es el ofrecido por Naciones Unidas en los **Objetivos de Desarrollo Sostenible (ODS).** Ésta es una iniciativa adoptada en 2015 por todos los Estados Miembros que plantea **17 objetivos para hacer frente a los retos más relevantes del planeta en materia económica, ambiental y social con horizonte 2030.**

Los impulsores de esta iniciativa son conscientes de que estos objetivos no pueden lograrse sin la colaboración de las administraciones públicas, los ciudadanos y las empresas, quienes están asumiendo ya compromisos de forma voluntaria que contribuyen a alcanzar algunas de las metas planteadas en dicho marco. Estas iniciativas se centran en aprovechar nuevas oportunidades de negocio, como las relativas a la descarbonización de la economía, pero también en mitigar riesgos financieros, operacionales o reputacionales, como las relativas a la prevención de la corrupción. Según los últimos estudios publicados, **los objetivos más asumidos por las empresas en sus planes de negocio son los objetivos número 8 · Trabajo decente y crecimiento económico, número 5 · Igualdad de género y número 3 · Salud y bienestar,** aunque es destacable también la asunción progresiva de compromisos relativos a los objetivos número 13 · Acción por el clima, número 7 · Energía asequible y no contaminante y número 12 · Producción y consumo responsables.

Paralelamente al desarrollo de las iniciativas voluntarias, como los ODS, han ido creciendo los **requerimientos regulatorios** para las empresas, tanto en el ámbito medioambiental como en el social. Estos requerimientos son muy dispares en las distintas jurisdicciones y pueden implicar

nuevos riesgos de cumplimiento, especialmente difíciles de gestionar en entornos multinacionales. Esa asimetría en regulación se intensificará notablemente ante las nuevas propuestas europeas alrededor de las **6 prioridades fijadas por la Comisión Europea para el periodo 2019-2024:**

1. **Pacto Verde Europeo,** que tiene como objetivo que Europa sea el primer continente neutro en carbono en 2050, avanzando hacia una economía circular y conservando la biodiversidad. Para su desarrollo se ha definido un plan de acción que incluye, entre otras, una futura Ley del Clima, un plan de inversiones y la movilización de financiación por más de 100 billones de euros en el periodo 2021-2017.
2. Una Europa adaptada a la nueva **Era Digital** que garantice que la tecnología está al servicio de las personas, abra nuevas oportunidades a las empresas y facilite la transición a una economía baja en carbono.
3. Una economía **al servicio de las personas,** que cree empleos de calidad.
4. Una **Europa más fuerte** en el mundo, que defienda el multilateralismo y un orden mundial basado en normas por medio de un papel más activo y una voz más firme de la UE en el mundo.
5. Promoción del **modo de vida europeo,** protegiendo el Estado de Derecho y los derechos fundamentales, garantizando que todas las propuestas de la Comisión respeten la Carta de los Derechos Fundamentales de la Unión Europea.
6. Un **nuevo impulso a la democracia europea,** de forma que los europeos desempeñen un papel más destacado en el proceso de toma de decisiones y más activo en el establecimiento de las prioridades europeas.

En este contexto, Auditoría Interna se enfrenta al reto de ayudar a sus organizaciones a avanzar con seguridad en el nuevo paradigma de desarrollo sostenible, para lo cual debe convencer a los Administradores y a la Dirección de que se encuentra preparada para llevar a cabo esta labor, bien por sus propios medios, bien con la colaboración de especialistas, actuando como asesores o propiamente como función de aseguramiento.

Los auditores internos tienen la oportunidad de ampliar el soporte que ofrecen a la Alta Dirección y a los Administradores de sus organizaciones, bien directamente o bien a través de las Comisiones de Auditoría, de fortalecer sus capacidades y conocimiento del negocio y de asegurar el cumplimiento de su finalidad de una manera más integral a través de trabajos orientados a:

- Definir y aplicar de forma consistente la metodología para el análisis de materialidad, incorporando en dicho análisis a los grupos de interés que impactan o pueden verse impactados por las actividades de la empresa.
- Identificar qué información es clave para explicar la creación de valor de la empresa y su sostenibilidad futura, así como para cumplir con la regulación, y qué estándares o criterios son los más adecuados para su obtención.

- Implantar sistemas de información que proporcionen información fiable, puntual y construida siguiendo los estándares o criterios aprobados.
- Mejorar los procedimientos y los controles internos.
- Revisar de forma crítica las oportunidades y los riesgos a los que se enfrenta la empresa en todos los ámbitos.
- Revisar los planes de negocio para ver cómo tienen en cuenta los riesgos y oportunidades sociales y medioambientales.
- Mejorar la calidad y la conectividad de la información financiera y no financiera, para poner de manifiesto los factores que afectan al desempeño de la organización y su impacto social y medioambiental.
- Aplicar el concepto de auditoría continua a los sistemas de gestión ESG más críticos para la consecución de los objetivos de la empresa.
- Trabajar de forma coordinada con otros prestadores de servicios de aseguramiento de los sistemas de gestión o de la información no financiera.

2. La información no financiera (INF)

En 2014 se aprobó la Directiva Europea 2014/95/UE, que modificó la Directiva 2013/34/UE en lo que respecta a la divulgación de información no financiera e información sobre diversidad de las grandes empresas de interés público con más de 500 empleados, que entró en vigor en 2017. A esta Directiva le ha seguido la publicación, por parte de la Comisión Europea, de unas directrices para presentar dicha información no financiera con el objetivo de orientar a las compañías en su divulgación de una manera homogénea.

Esta Directiva, aun siendo un buen punto de partida, presenta múltiples interrogantes que aún hay que contestar para construir un marco de información no financiera sólido. Así lo ha reconocido también la Comisión Europea en su Pacto Verde Europeo, al proponer una revisión de dicha Directiva que se ha iniciado en febrero de 2020, con el lanzamiento de una consulta pública para recabar opiniones sobre las modificaciones necesarias.

Esta normativa responde a la creciente demanda de información y transparencia en materia de información de gobierno corporativo, social y medioambiental de los inversores y de otros grupos de interés, así como a la necesidad de asegurar la coherencia y la comparabilidad de dicha información en el ámbito europeo.

En España, la transposición de la Directiva se ha realizado en dos pasos. El primero, a través del Real Decreto-Ley 18/2017, de 24 de noviembre, en materia de información no financiera y di-

versidad por el que se modifican el Código de Comercio, el texto refundido de la Ley de Sociedades de Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio, y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas. El segundo, a través de la Ley 11/2018 de Información no financiera y Diversidad, que modifica los mismos textos que el mencionado Real Decreto.

La publicación de información no financiera es una práctica que comenzó a generalizarse en algunos sectores en la década de los 90 del siglo pasado, a través de informes de responsabilidad social corporativa o de sostenibilidad, y que ha seguido desarrollándose en el siglo XXI, pero sin alcanzar aún el grado de madurez de la información financiera. Asimismo, algunas empresas ya preparaban informes anuales integrados, a través de los cuales se quería facilitar a los distintos grupos de interés una visión integral de la estrategia y el desempeño en los negocios tanto a nivel financiero como no financiero.

La ley española exige a las empresas que cumplan ciertas condiciones[1], como la preparación de un Estado No Financiero que debe incluirse en el Informe de Gestión o en un informe separado incorporado por referencia al Informe de Gestión, que sirva para comprender los siguientes aspectos:

- La evolución, los resultados y la situación de la empresa.
- El impacto de las actividades de la empresa en relación con cuestiones relativas a:
  - Aspectos medioambientales.
  - Aspectos sociales.
  - Personal.
  - Respeto a los Derechos Humanos.
  - Lucha contra la corrupción y el soborno.

El Estado no Financiero debe incluir:

- Una breve descripción del modelo de negocio de la compañía.
- Una descripción de las políticas que aplica la compañía en cada una de las cuestiones y resultados de su aplicación.
- Los principales riesgos relacionados con estas cuestiones y cómo la empresa gestiona dichos riesgos.
- Indicadores clave de resultados no financieros, que se consideran relevantes para la actividad empresarial desarrollada.

Esta ley ha dejado fuera una de las temáticas más significativas de la información no financiera: la de gobierno corporativo. Esto es entendible cuando se trata de empresas cotizadas,

1. En el ejercicio 2018 la ley aplicó a sociedades o grupos con más de 500 empleados que, o bien eran entidades de interés público, o bien eran considerados grandes (dos años consecutivos cumpliendo dos de los tres criterios siguientes: activos superiores a 20 millones de euros, cifra anual de negocios superiores a 40 millones o número medio de empleados superior a 250). No obstante, el límite de 500 empleados se bajará a 250 en un plazo de tres años desde la entrada en vigor de la Ley, es decir, en 2021.

ya que para ellas existen requisitos de información de gobierno corporativo desde hace tiempo bajo el principio de "cumplir o explicar", requisitos que se complementan con las prácticas recomendadas por el Código de Buen Gobierno de entidades cotizadas (véase capítulo siguiente). En todo caso, sería conveniente que Auditoría Interna asegure que el modelo de gobierno es adecuado, considerando la naturaleza de la organización, la complejidad de sus operaciones, las expectativas de sus grupos de interés y los compromisos asumidos con dichos grupos.

Las directrices no vinculantes sobre la metodología para la presentación de informes no financieros difundidas mediante la Comunicación de la Comisión 2017/C 215/01, consideran diversos marcos internacionales generales o específicos para algunas de las cuestiones a divulgar, y distan mucho de ser el equivalente a las *Normas Internacionales de Información Financiera* (NIIF) en el ámbito de la información financiera. En España contamos también con la *Guía para la elaboración del informe de gestión de las entidades cotizadas* de la Comisión Nacional del Mercado de Valores (CNMV), guía que fue preparada antes de la nueva regulación y que no contempla todos los elementos que ésta ha introducido.

La información corporativa que las empresas ponen a disposición del mercado debe ser relevante y suficiente para permitir la toma de decisiones, para lo cual es imprescindible disponer de un buen análisis de materialidad. Auditoría Interna puede ser de mucha utilidad si asegura que el análisis de materialidad ha tenido en cuenta a todos los grupos de interés, que se han identificado las áreas o cuestiones realmente importantes para el negocio, que estas áreas son coherentes con las identificadas por el resto de las empresas del sector y que hay un responsable de fijar objetivos y medir el desempeño de la organización en cada una de estas áreas.

Asimismo, Auditoría Interna puede desarrollar un papel clave como garante de la fiabilidad de la información no financiera, facilitando la toma de decisiones por la Dirección y la tarea de supervisión de los Administradores y de la Comisión de Auditoría, en su caso.

Dado que la Ley española –no así la Directiva europea– requiere que la información no financiera sea verificada por un prestador independiente de servicios de verificación, aunque sin hacer más precisiones sobre el tipo de verificación a realizar o los estándares a utilizar, Auditoría Interna puede asesorar a la Dirección en el tipo de verificación a efectuar, los estándares más recomendables y los requisitos que debe cumplir el verificador.

Parece evidente que, en la medida en que la información no financiera se ha incorporado a los canales establecidos para la información corporativa regulada de las organizaciones y para su formulación por el máximo Órgano de Administración, ésta deberá ganar en madurez y fiabilidad. Aquí es donde Auditoría Interna puede jugar un papel decisivo, incorporando al universo a auditar los distintos aspectos que componen su gestión para mejorar la confianza de los grupos de interés internos y externos en la información y facilitar el cumplimiento de sus responsabilidades al Consejo de Administración.

Para posibilitar la asunción de este papel, desde el Instituto de Auditores Internos de España, y como iniciativa de su laboratorio de ideas LA FÁBRICA DEL PENSAMIENTO, se publicó en 2018 el documento *Auditoría Interna y la Información no Financiera*, donde se describe en detalle el posible rol de Auditoría Interna como consultor o como asegurador, las competencias necesarias o las consideraciones tecnológicas, entre otros aspectos. Su lectura puede ser muy útil a quien tenga interés en ampliar conocimientos en esta materia.

Resumidamente, en dicho documento se concluye que los auditores internos que participen en este tipo de trabajos deberían combinar conocimientos, experiencia y competencia técnica en las áreas relevantes de la INF que les permitan entender los procesos y la información generada por la entidad al elaborar la INF. El nivel de conocimientos necesario que el equipo del proyecto requiere, incluye conocimientos sobre, al menos, los siguientes aspectos:

- Análisis de materialidad.
- Identificación y gestión de los impactos del negocio, de los riesgos y de las oportunidades de la empresa en cada una de las dimensiones de la sostenibilidad.
- Estrategia y modelos de negocio de la empresa.
- Gestión ambiental.
- Gestión de recursos humanos.
- Seguridad y salud laboral.
- Derechos humanos.
- Modelos de cumplimiento y prevención del fraude y la corrupción.
- Estándares medioambientales, laborales o sociales utilizados.
- Sistemas de información.
- Estándares y criterios para la elaboración de la INF.
- Técnicas de Auditoría Interna.

Es importante destacar que muchos de los indicadores y elementos que se utilizan en la información ambiental y social tienen carácter cualitativo y, en el caso de los cuantitativos, algunos responden a estimaciones con un alto nivel de incertidumbre y otros a criterios de cálculo inmaduros o no generalmente aceptados. Estos factores exigen que los auditores internos deban tener un cuidado especial a la hora de:

- Planificar la tipología de los trabajos a realizar (consultoría o aseguramiento).
- Involucrar a profesionales, propios o de terceros, con experiencia y conocimientos actualizados de la materia y que apliquen un sano escepticismo profesional.
- Concluir sobre la conveniencia y corrección de los criterios o estándares utilizados.
- Evaluar cuidadosamente la suficiencia de las evidencias obtenidas.
- Emitir recomendaciones prácticas que permitan mejorar las políticas, procedimientos y sistemas medioambientales y sociales, así como la calidad de la información.

Asimismo, aunque los recursos son siempre limitados y Auditoría Interna tiene la obligación de ser eficiente, sería conveniente considerar en el Plan de Auditoría Interna la posibilidad de interactuar con representantes de los grupos de interés más relevantes de la empresa para contrastar de manera directa que se han identificado apropiadamente sus expectativas y que la información que está facilitando la empresa es pertinente y suficiente.

Finalmente, debemos ser conscientes del peso creciente de la regulación de sostenibilidad en las empresas y en los mercados, especialmente en Europa. Así, durante el primer semestre de 2021, hemos conocido las nuevas obligaciones de información de la regulación de la Taxonomía (Reglamento (EU) 2020/852 y los actos delegados que lo desarrollan); la propuesta de Directiva sobre Informes de Sostenibilidad presentada en abril de 2021, que sustituirá a la actual Directiva de Información no Financiera; así como el lanzamiento del desarrollo del estándar europeo para la preparación de dichos Informes de Sostenibilidad (ESRS), encargado por la Comisión Europea al *European Financial Reporting Advisory Group* (EFRAG).

En este entorno tan exigente y cambiante, Auditoría Interna puede contribuir a que su organización esté adecuadamente informada, preparada y cuente con los recursos necesarios para cumplir estos nuevos requerimientos en tiempo y forma.

3. Los sistemas de gestión

Los sistemas de gestión son uno de los instrumentos de los que dispone la Dirección de las organizaciones para ejecutar su política de sostenibilidad o de responsabilidad social. Pueden implantarse como sistemas específicos de un área concreta –gestión ambiental, de la calidad, de la energía, de riesgos, de seguridad, de cumplimiento, de innovación, de recursos humanos u otros– o como sistemas integrados.

Si bien son muchas las organizaciones que han emitido estándares en todo el mundo, los de mayor implantación son los desarrollados por *International Organization for Standardization* (ISO), a nivel mundial, y por la Asociación Española de la Normalización (AENOR), a nivel español.

En esencia, los **ELEMENTOS CLAVE** de la mayor parte de los sistemas de gestión son:

- La organización o estructura a la que se asignan las distintas responsabilidades, funciones y atribuciones.
- Las relaciones con otras partes interesadas.
- Los objetivos y compromisos.
- Los planes y programas para abordar riesgos y oportunidades.
- Los recursos necesarios.

- Las políticas y principios básicos.
- Los procesos, métodos y procedimientos del sistema que aseguren el cumplimiento de la regulación interna y externa.
- Los controles internos y los planes de mitigación para los riesgos identificados.
- La documentación, los datos y los informes internos y externos del sistema.
- Las revisiones para la mejora continua.

Además, **algunos de estos sistemas están regulados y tienen como requerimiento la realización de una auditoría interna con cierta regularidad.** Es el caso de las auditorías ambientales requeridas por el Reglamento (CE) 1221/2009 del Parlamento Europeo y del Consejo, relativo a la participación voluntaria de organizaciones en un sistema comunitario de gestión y auditoría medioambientales (EMAS), cuyos anexos han sido actualizados por el Reglamento (UE) 2017/1505 de la Comisión de 28 de agosto de 2017. Precisamente en su Anexo III se regula la Auditoría Interna ambiental y se detallan los pasos que debe incluir el procedimiento de auditoría del sistema, pasos que son aplicables a cualquiera de los sistemas de gestión de la sostenibilidad, con los necesarios matices que requiera cada materia:

- Comprensión de los sistemas de gestión.
- Valoración de los puntos fuertes y débiles de los sistemas de gestión.
- Recogida de pruebas para demostrar si el sistema está funcionando o no.
- Evaluación de los resultados de la auditoría.
- Preparación de las conclusiones de la auditoría.
- Comunicación de los resultados y conclusiones de la auditoría.

La implantación de Sistemas de Gestión eficaces está actualmente entre las prioridades de muchas organizaciones, por lo que una revisión periódica de Auditoría Interna de dichos sistemas debe ayudar a identificar problemas en su desarrollo, medir progresos y recomendar mejoras para que el sistema evolucione de forma eficiente.

Gobierno Corporativo y Auditoría Interna

Instituto de Auditores Internos de España

1. Concepto de Gobierno Corporativo

Una definición aproximativa al concepto de Gobierno Corporativo podría ser la de un conjunto de normas y principios que rigen el adecuado y equilibrado funcionamiento de los Órganos de Gobierno de una sociedad, asegurando su organización eficaz, transparente y justa, a fin de salvaguardar el interés social, y con el objetivo de maximizar el valor de la empresa a medio y largo plazo.

Otra definición sería que el Gobierno Corporativo es una combinación de procesos y estructuras diseñadas para ayudar a la organización a alcanzar sus objetivos. Estos procesos y estructuras se encuentran influenciadas no solo por los riesgos que afectan a la organización, sino también por los esfuerzos que se realizan para mitigar los riesgos conocidos y detectar los desconocidos.

El Consejo de Administración establece estructuras y procesos que determinan el Gobierno Corporativo dentro de la organización, tomando en consideración las perspectivas de los inversores, reguladores y gerencia, entre otros.

El Consejo de Administración debe revisar y monitorizar la estrategia de la compañía y la exposición a los riesgos operacionales, financieros y de cumplimiento. Adicionalmente, colabora con la Alta Dirección para definir el apetito al riesgo, las tolerancias al riesgo y alinear éstas con las prioridades estratégicas de la organización.

El modelo de buen Gobierno Corporativo, entendido como el conjunto de normas, principios y recomendaciones de actuación de las sociedades, trata de evitar, entre otras, las situaciones de conflictos de intereses en pro del interés social.

El Gobierno Corporativo guarda relación directa con los programas de cumplimiento y, como hemos visto en el capítulo anterior, con criterios de Responsabilidad Social Corporativa y los asuntos ESG. De hecho, en muchas ocasiones los sistemas de Gobierno Corporativo son respuestas a las exigencias normativas en estas materias, que cristalizan en políticas y procedimientos internos.

Todas las iniciativas en el ámbito del Gobierno Corporativo han sido desarrolladas sobre la base comúnmente aceptada de que la gestión de las empresas debe ser responsable, eficaz y transparente con el fin de lograr la confianza de los inversores y maximizar la creación de valor. El Gobierno Corporativo debe jugar un papel fundamental como instrumento para lograr tal fin y evitar situaciones vividas en los últimos años.

2. Principales iniciativas legislativas internacionales y nacionales

2.1 Principios de la OCDE

Dentro de las iniciativas de índole internacional hay que subrayar los *Principios de Buen Gobierno Corporativo* aprobados en 1999 por la Organización para la Cooperación y el Desarrollo Económico (OCDE). Se trata de normas no vinculantes y buenas prácticas internacionales, con una Guía para su implantación, que incluyó una serie de directrices sobre los derechos de los accionistas, revelación de datos, o funciones de los Consejos de Administración, entre otros.

Estos principios fueron objeto de una profunda revisión en 2004. Sin embargo, la crisis financiera posterior puso de manifiesto graves deficiencias. Por esta razón, en 2008 se aprobó un Plan de Acción para desarrollar un conjunto de recomendaciones en áreas como la política de remuneración, la gestión del riesgo, las prácticas del Consejo y el ejercicio de los derechos de los accionistas, así como para proponer instrumentos para la mejora en la aplicación de las recomendaciones ya publicadas.

Estos principios de Gobierno Corporativo establecen las líneas de evolución y desarrollo que, de forma común, deberían seguir los estados y las sociedades para una adecuada regulación del Gobierno Corporativo y, en particular:

- Garantizar un marco eficaz de Gobierno Corporativo.
- Amparar y facilitar el ejercicio de los derechos de los accionistas.
- Garantizar un trato equitativo a todos los accionistas incluidos los minoritarios y extranjeros.
- Reconocer los derechos de los grupos de interés establecidos por la ley o a través de acuerdos mutuos y fomentar la cooperación activa entre sociedades y sus grupos de interés.
- Garantizar la divulgación oportuna y precisa de todas las cuestiones materiales relativas a las sociedades, incluida la situación financiera, los resultados, la titularidad y el Gobierno de la empresa.
- Garantizar la orientación estratégica de la empresa, el control efectivo de la Dirección Ejecutiva por parte del Consejo y la responsabilidad de este frente a la empresa y accionistas.

2.2 Unión Europea

La Comisión Europea considera prioritario el desarrollo del Gobierno Corporativo, especialmente tras la crisis financiera de 2008.

Destacan las siguientes iniciativas legislativas:

- **Recomendación sobre la estructura y transparencia de las retribuciones de los administradores de las sociedades cotizadas** (3177/2009/CE) como complemento a las dos anteriores emitidas en diciembre de 2004 (913/2004/CE) y febrero de 2005 (162/2005/CE).
- **Libros verdes en materia de Gobierno Corporativo.**
- **Plan de Acción: derecho de sociedades europeo y Gobierno Corporativo;** un marco jurídico moderno para una mayor participación de los accionistas y la viabilidad de las empresas (diciembre 2012)
- Directiva 2014/95/UE del Parlamento europeo y del Consejo, de 22 de octubre de 2014, que modifica las Directivas 78/660/CE y 83/349/CEE en lo que respecta a la **divulgación de información no financiera e información sobre diversidad por parte de determinadas grandes empresas y grupos.**
- Directiva 2014/56/UE del Parlamento europeo y del Consejo, de 16 de abril de 2014, que modifica la Directiva 2006/43/CE, sobre **auditoría legal de las cuentas anuales y consolidadas.**

2.3 España

El desarrollo en nuestro país ha sido progresivo. El avance más significativo se ha producido mediante los Códigos de Buen Gobierno de las sociedades cotizadas, de cumplimiento voluntario y el posterior desarrollo de algunas de sus recomendaciones.

EL CÓDIGO DE BUEN GOBIERNO DE LAS SOCIEDADES COTIZADAS

La Comisión Nacional del Mercado de Valores (CNMV) aprobó el 18 de febrero de 2015 el *Código de Buen Gobierno de las Sociedades Cotizadas*[1], fruto del trabajo de una Comisión de Expertos en materia de Gobierno Corporativo que comenzó sus trabajos en mayo de 2013. Posteriormente, en 2016, la CNMV elaboró una *Guía técnica de buenas prácticas para la aplicación del principio "cumplir o explicar"*[2]. Y ya en 2020 se introdujeron algunas novedades reseñables[3] que comentamos más adelante. Primero, repasamos los elementos más destacados del código de 2015.

1. CNMV. *Código de Buen Gobierno de las sociedades cotizadas.* 1995.
2. CNMV. *Guía técnica de buenas prácticas para la aplicación del principio cumplir o explicar.* 2016.
3. CNMV. *Código de Bueno Gobierno de las sociedades cotizadas* revisado en 2020.

Los **PRINCIPIOS MÁS RELEVANTES** establecidos son los siguientes:

- **Aspectos generales,** entre los que destaca:
  - Cuando coticen varias sociedades pertenecientes a un mismo grupo deben establecerse las medidas adecuadas para proteger los intereses legítimos de todas las partes involucradas y solventar los eventuales conflictos de intereses.
- **Junta General de accionistas,** entre los que destaca:
  - La Junta General debe funcionar bajo principios de transparencia y con información adecuada.
- **Consejo de Administración,** entre los que destacan:
  - El Consejo de Administración asumirá, colectiva y unitariamente, la responsabilidad directa sobre la administración social y la supervisión de la dirección de la sociedad, con el propósito común de promover el interés social.
  - El Consejo de Administración se reunirá con la frecuencia necesaria para el correcto desarrollo de sus funciones de administración y supervisión y con la presencia de todos o una amplia mayoría de sus miembros.
  - Los consejeros contarán con información suficiente y adecuada para el ejercicio de sus funciones y tendrán derecho a obtener de la sociedad el asesoramiento preciso.

Las **PRINCIPALES RECOMENDACIONES** establecidas son las siguientes:

- Recomendaciones **relativas a la Junta General,** entre las que destacan:
  - Las sociedades cotizadas deben publicar en su página web con antelación suficiente a la celebración de la Junta General Ordinaria los informes que de forma preceptiva o voluntaria realice.
  - La sociedad debe facilitar el ejercicio de los derechos de asistencia y participación en la Junta General de accionistas en igualdad de condiciones a la totalidad del conjunto accionarial.
- Recomendaciones **relativas al Consejo de Administración,** entre las que destacan:
  - Que todos los consejeros expresen claramente su oposición cuando consideren que alguna propuesta de decisión sometida al Consejo puede ser contraria al interés social.
  - Que el Consejo de Administración tenga una composición equilibrada, con una amplia mayoría de consejeros no ejecutivos y una adecuada proporción entre consejeros dominicales e independientes, representando estos últimos al menos la mitad de los mismos.
  - Que las sociedades establezcan reglas que obliguen a los consejeros a informar y, en su caso, a dimitir en aquellos supuestos que puedan perjudicar al crédito y reputación de la sociedad y, en particular, les obliguen a informar al Consejo de Adminis-

tración de las causas penales en las que aparezcan como imputados, así como de sus posteriores vicisitudes procesales.

- Que los acuerdos contractuales incluyan una cláusula que permita a la sociedad reclamar el reembolso de los componentes variables de la remuneración, cuando el pago no haya estado ajustado a las condiciones de rendimiento o cuando se hayan abonado atendiendo a datos cuya inexactitud quede acreditada con posterioridad.

- Recomendaciones **relativas a la Comisión de Auditoría,** entre las que destacan:
  - Que los miembros de la Comisión de Auditoría, y de forma especial su presidente, se designen teniendo en cuenta sus conocimientos y experiencia en materia de contabilidad, auditoría o gestión de riesgos, y que la mayoría de sus miembros sean consejeros independientes.
  - Que, bajo la supervisión de la Comisión de Auditoría, se disponga de una unidad que asuma la función de Auditoría Interna que vele por el buen funcionamiento de los sistemas de información y control interno y que funcionalmente dependa del presidente no ejecutivo del Consejo o del de la Comisión de Auditoría.
  - Que la Comisión de Auditoría sea informada sobre las operaciones de modificaciones estructurales y corporativas que proyecta realizar la sociedad para su análisis e informe previo al Consejo de Administración, sobre sus condiciones económicas y su impacto contable y, en especial, en su caso, sobre la ecuación de canje propuesta.

I- Recomendaciones **relativas a la/s Comisión/es de Nombramientos y Retribuciones,** entre las que destacan:
  - Que las sociedades de elevada capitalización cuenten con una Comisión de Nombramientos y con una Comisión de Remuneraciones separadas.
  - Que la Comisión de Retribuciones consulte al presidente y al primer ejecutivo de la sociedad, especialmente cuando se trate de materias relativas a los consejeros ejecutivos y altos directivos.

REVISIÓN DEL CÓDIGO DE BUEN GOBIERNO DE LAS SOCIEDADES COTIZADAS

La revisión parcial del Código de Buen Gobierno de las sociedades cotizadas llevada a cabo en 2020 se centró en cuatro **EJES PRINCIPALES:**

- Fomento de la presencia de mujeres en los Consejos de Administración.
- Mayor relevancia de la información no financiera y la sostenibilidad.
- Más atención a los riesgos reputacionales y en general no financieros.
- Clarificación de aspectos relativos a la remuneración de consejeros.

La revisión actualizó y adaptó varias recomendaciones del Código a diversas modificaciones legales aprobadas desde su publicación y aclara el alcance de otras que habían

suscitado ciertas dudas; asimismo, supuso novedades relevantes en áreas como la diversidad de género en los Consejos de Administración, la información y riesgos no financieros, la atención a aspectos medioambientales, sociales y de gobierno corporativo, o las remuneraciones.

Se pueden consultar los detalles concretos de las recomendaciones revisadas por la CNMV en el portal del supervisor[4].

2.4 Marco Normativo relativo a las sociedades no cotizadas

La Ley 31/2014 fue aprobada con el objetivo de implantar en nuestro ordenamiento mejoras en el sistema de Gobierno Corporativo tanto de compañías cotizadas como no cotizadas, sobre la base de las propuestas realizadas por la Comisión de Expertos en materia de Gobierno Corporativo.

La Ley 31/2014 incluye medidas concretas que afectan a los órganos de gobierno de las sociedades de capital: la Junta General, con el fin de reforzar su papel y abrir cauces para fomentar la participación accionarial; y el órgano de administración (principalmente el Consejo de Administración), al objeto de impregnar de mayor transparencia el desarrollo de sus competencias y garantizar el tratamiento equitativo de todos los accionistas, la gestión de los riesgos o la independencia o la mejora de la participación y profesionalización de los consejeros.

CON RESPECTO A LAS COMPETENCIAS DE LA JUNTA GENERAL DE LAS SOCIEDADES

Las competencias de la Junta General se han visto ampliadas con la modificación de los artículos 160 y 161 de la Ley de Sociedades de Capital. En concreto, el artículo 161 amplía la posibilidad de la Junta General de participar en la gestión que anteriormente se encontraba prevista exclusivamente para sociedades de responsabilidad limitada.

CON RESPECTO A LOS ÓRGANOS DE ADMINISTRACIÓN DE LAS SOCIEDADES

En relación con el órgano de administración, la Ley 31/2014 ha transformado sustancialmente su régimen, con el fin de obtener una mayor transparencia en la gestión social mediante, principalmente, la independencia y profesionalización de sus miembros. Las modificaciones de mayor relevancia son las que atañen a las siguientes materias:

- RÉGIMEN DE RESPONSABILIDAD

  Los administradores de las sociedades mercantiles, de conformidad con el artículo 236 de la Ley de Sociedades de Capital, son responsables frente a la sociedad, frente a los

4. CNMV. Nota de prensa: *La CNMV aprueba la reforma del Código de Buen Gobierno de las sociedades cotizadas.* Junio 2020.

socios o accionistas y frente a los acreedores de posibles daños que puedan causar por actos u omisiones que sean contrarios a la Ley o a los estatutos sociales, así como aquellos realizados incumpliendo los deberes inherentes al desempeño de su cargo, siempre que media dolo o culpa.

Todos los miembros del Órgano de Administración que hubiera adoptado el acuerdo o realizado el acto lesivo responderán solidariamente, salvo los que prueben que, no habiendo intervenido en su adopción y ejecución, desconocían su existencia o, conociéndola, hicieron todo lo conveniente para evitar el daño o, al menos, se opusieron expresamente a aquel.

- CONSEJO DE ADMINISTRACIÓN

Se impone al Consejo de Administración la obligación de reunirse, al menos, una vez por trimestre.

En materia de delegación de facultades por parte del Consejo de Administración se establecen las siguientes especialidades:

- En la propia delegación debe indicarse el contenido y alcance de las facultades delegadas, incluyendo los límites en el ejercicio de las mismas.
- Aquellos consejeros en los que se deleguen funciones ejecutivas y, principalmente, el consejero delegado, deberán suscribir un contrato con la sociedad, que deberá ser aprobado por dos tercios de sus miembros, debiendo abstenerse el consejero afectado de participar en la deliberación y votación del acuerdo. El contrato aprobado, que debe incluir necesariamente todos los conceptos retributivos que percibirá el consejero, así como los derechos, obligaciones y funciones asumidas, deberá incorporarse como anejo al acta de la sesión.

Por su parte, el artículo 529.ter de la Ley de Sociedades de Capital establece un particular régimen de facultades indelegables en sede de sociedades cotizadas:

- Aprobar el Plan estratégico o de negocio.
- Determinar la política de control y gestión de riesgos.
- Determinar la política de Gobierno Corporativo de la sociedad y del grupo del que sea entidad dominante.
- Aprobar la información financiera que, por su condición de cotizada, debe hacer pública periódicamente.
- Definir la estructura del grupo de sociedades del que la sociedad sea entidad dominante.
- Aprobar las inversiones u operaciones de todo tipo que, por su elevada cuantía o especiales características, tengan carácter estratégico o especial riesgo fiscal.

- Aprobar la creación o adquisición de participaciones en (i) entidades de propósito especial, (ii) domiciliadas en países o territorios que tengan la consideración de paraísos fiscales, y cualquier otra transacción que pudiera afectar a la transparencia de la sociedad y su grupo.
- Aprobar, previo informe de la Comisión de Auditoría, las operaciones que la sociedad o sociedades de su grupo realicen con consejeros.

- DEBERES DE LOS ADMINISTRADORES
  - **Deber de diligencia.** Los administradores desempeñarán su cargo con la diligencia de un "ordenado empresario".
  - **Deber de lealtad.** Exigencia de que el administrador desempeñe las funciones que tiene encomendadas, en todo momento, actuando de buena fe y velando por el interés de la sociedad, anteponiendo el interés social al suyo propio o al de alguna persona especialmente relacionada con él.

3. Protección de la discrecionalidad empresarial en la toma de decisiones *(Business judgement rule)*

La razón de ser de esta regla se encuentra en la necesidad de garantizar a los administradores de las sociedades una esfera de libertad en su actuación, con el fin de que sus posibles errores en la toma de decisiones empresariales no deriven de forma automática en una infracción de sus deberes y, por tanto, en responsabilidad, toda vez que en la gestión de cualquier negocio interviene un factor de riesgo relevante que escapa el control absoluto de los administradores.

El legislador ha incluido, a través de la reforma del artículo 226 de la Ley de Sociedades de Capital, un estándar de actuación en virtud del cual los administradores, en caso de que se cumplan determinados requisitos, puedan adoptar las decisiones empresariales que estimen convenientes, sin que su actuación pueda ser considerada como negligente (que no pueda considerarse que se ha actuado mediando dolo o mala fe), independientemente del éxito o fracaso empresarial de dicha decisión.

La protección de la discrecionalidad empresarial únicamente resulta de aplicación en relación con el deber de diligencia, evitando la revisión judicial de las decisiones estratégicas y de negocio.

No significa que se excluya por completo la responsabilidad del administrador, sino que la actuación del administrador queda amparada siempre y cuando se siga una forma de proceder concreta en la adopción de dichas decisiones estratégicas y de negocio. Para que se entienda

cumplido el estándar de diligencia es necesario que el administrador haya actuado "con información suficiente y con arreglo a un procedimiento de decisión adecuado".

De esta forma, se trata de que – con carácter previo a la toma de decisión en cuestión– el administrador haya recabado por todos los medios pertinentes (y si fuera necesario contar con el asesoramiento técnico de expertos en la materia de que se trate) toda la información necesaria que un administrador diligente hubiera recabado antes de adoptar la decisión.

4. Instrumentos de Gobierno Corporativo

4.1 Comisiones especializadas

El Consejo de Administración podrá constituir en su seno comisiones especializadas, determinando su composición, designando a sus miembros y estableciendo las funciones que asume cada una de ellas.

La Ley de Sociedades de Capital establece con carácter obligatorio la creación de la Comisión de Auditoría y la Comisión de Nombramientos y Retribuciones, que estarán compuestas exclusivamente por consejeros no ejecutivos y al menos dos de ellos han de ser independientes, de entre los que se elegirá al presidente.

COMISIÓN DE AUDITORÍA

Entre otras, las funciones legalmente encomendadas a este órgano son las siguientes:

- Supervisar la eficacia del control interno de la sociedad, la auditoría interna y los sistemas de gestión de riesgos
- Supervisar el proceso de elaboración y presentación de la información financiera y presentar recomendaciones para salvaguardar su integridad

COMISIÓN DE NOMBRAMIENTOS Y RETRIBUCIONES

Entre otras, las funciones legalmente encomendadas a este órgano son las siguientes:

- Evaluar competencias, conocimientos y experiencia necesarios en el Consejo de Administración.
- Elevar al Consejo de Administración las propuestas de nombramiento de consejeros independientes y restantes consejeros para su designación por cooptación o para su sometimiento a la decisión de la Junta General, así como las propuestas para su reelección o separación por la Junta.
- Informar las propuestas de nombramiento y separación de altos directivos y las condiciones básicas de los contratos.

NORMAS ORGÁNICAS

Las sociedades anónimas cotizadas deberán aprobar un Reglamento de normas de régimen interno y funcionamiento del Consejo de Administración, de acuerdo con los artículos 528 y 529 de la Ley de Sociedades de Capital que contendrá las medidas concretas tendentes a garantizar la mejor administración de la sociedad.

El Reglamento deberá regular, entre otros, los siguientes aspectos:

- Composición del Consejo.
- Estructura del Consejo.
- Comisiones del Consejo.
- Funcionamiento del Consejo.
- Información del consejero.
- Deberes y retribución de los consejeros.

El reglamento será objeto de comunicación a la CNMV (Comisión Nacional del Mercado de Valores), acompañándose del documento en que conste. Efectuada esta comunicación se inscribirá en el Registro Mercantil con arreglo a las normas generales y, una vez inscrito, se publicará en la CNMV.

5. Informe Anual de Gobierno Corporativo

El Informe Anual de Gobierno Corporativo se encuentra regulado en el artículo 540 de la Ley de Sociedades de Capital. Estas entidades deben hacer público, con carácter anual, un informe de Gobierno Corporativo. Dicho documento se comunicará a la CNMV.

El informe debe ofrecer una explicación detallada de la estructura del sistema de gobierno de la sociedad y de su funcionamiento en la práctica, con el siguiente contenido mínimo:

- Estructura de la propiedad.
- Cualquier restricción a la transmisibilidad de valores o al derecho de voto.
- Estructura de la administración de la sociedad.
- Operaciones vinculadas de la sociedad con sus accionistas, administradores, cargos directivos y operaciones intragrupo.
- Sistemas de control de riesgos, incluido el fiscal.
- Funcionamiento de la Junta General, con información relativa al desarrollo de las reuniones que celebra.
- Grado de seguimiento de las recomendaciones de Gobierno Corporativo, o en su caso, la explicación de la falta de seguimiento de dichas recomendaciones.

6. La función de Auditoría Interna en relación con el Gobierno Corporativo

El documento del IAI Global *El rol de Auditoría Interna en el Gobierno Corporativo*[5] desarrolla el enfoque propuesto por el Instituto de Auditores Internos en relación con este tema.

Este documento pone de manifiesto las siguientes ideas principales:

- El rol de Auditoria Interna en el ámbito del Gobierno Corporativo es crítico.
- Auditoría Interna proporciona aseguramiento objetivo y entendimiento acerca de la efectividad y eficiencia de la gestión de los riesgos, el control interno y los procesos de Gobierno Corporativo.
- Un destacado apoyo por parte del Consejo de Administración y la Alta Dirección se apoya en relaciones construidas en la confianza mutua y la interacción del Director de Auditoría Interna de manera frecuente, oportuna y relevante con éstos.
- Una vibrante y ágil función de auditoría interna puede ser un indispensable recurso que soporte un robusto Gobierno Corporativo.
- En la medida que los riesgos crecen en número y complejidad, el rol de Auditoría Interna abarcará áreas como el gobierno del riesgo, la cultura y el comportamiento empresarial, la sostenibilidad y otras variables no financieras.

Con carácter adicional a lo anteriormente indicado, el documento destaca que Auditoría Interna ocupa una posición de privilegio a la hora de proporcionar aseguramiento cuando el nivel de recursos, competencia y estructura se encuentran alineados con la estrategia organizacional y se siguen los estándares establecidos por el Instituto de Auditores Internos.

Resaltar que Auditoría Interna está en una posición óptima y adecuada cuando se encuentra libre de influencias. Funcionando de esta manera, las actividades se llevan a cabo por profesionales que poseen una profunda apreciación de la importancia de un Gobierno Corporativo fuerte y un conocimiento en profundidad del negocio y de los procesos y sistemas de la organización, así como un deseo de colaborar en el éxito organizacional.

Finalmente, enfatizar que una función de Auditoría Interna madura puede ayudar a la organización en la identificación temprana de tendencias y llamando la atención sobre desafíos emergentes antes de que se conviertan en crisis.

5. The Global IIA. *Position Paper: Internal Auditing's role in Corporate Governance.*

Anexos

Anexo 1 · Publicaciones recomendadas

- EDUARDO HEVIA. *Manual de Auditoría Interna. Enfoque operativo y de gestión.* Grupo Océano Barcelona.
- EDUARDO HEVIA. "Manual de Auditoría Interna". *Expansión.*
- EDUARDO HEVIA. "Manual de Auditoría de Gestión". *Expansión*
- COSO. *Control Interno - Marco Integrado.* COSO
- EDUARDO HEVIA. *Concepto moderno de la Auditoría Interna.* IAI
- IAI. *Marco Internacional para la Práctica Profesional de la Auditoría Interna.* IAI
- EDUARDO HEVIA; JOSÉ JUAN LAFUENTE. *Cómo luchar contra el fraude en la empresa.* IAI
- CNMV. *Código de buen gobierno para entidades cotizadas.* CNMV
- COSO. *Gestión del Riesgo Empresarial - Integrando Estrategia y Desempeño.* COSO
- COSO. *Enterprise Risk Management - Applying enterprise risk management to environmental, social and governance-related risks.* COSO

Anexo 2 · Declaración de Responsabilidades de Auditoría Interna[1]

La finalidad de esta declaración es proporcionar, de forma resumida, un conocimiento general de la actuación y de las responsabilidades de Auditoría Interna. Para una orientación más específica, se debe acudir a las Normas Internacionales para la Práctica Profesional de la Auditoría Interna (las Normas).

Objetivo y Alcance

Auditoría Interna es una función de valoración independiente establecida dentro de una organización para examinar y evaluar sus actividades como un servicio a la organización. El objetivo de la auditoría interna es asistir a los miembros de la organización en el cumplimiento efectivo de sus responsabilidades. Con esta finalidad Auditoría Interna les proporciona análisis, valoraciones, recomendaciones, consejo e información sobre las actividades revisadas. El objetivo de la auditoría incluye la promoción de un control efectivo a un coste razonable. Los miembros de la organización asistidos por Auditoría Interna son tanto la dirección como el Consejo de Administración.

El alcance de los trabajos desarrollados por Auditoría Interna debe abarcar el examen y evaluación de la adecuación y efectividad de los sistemas de organización o control interno y la calidad de ejecución en la realización de las responsabilidades asignadas. Los auditores internos deben:

- Revisar la fiabilidad e integridad de la información financiera y operativa y de los medios utilizados para identificar, evaluar, clasificar y comunicar dicha información.
- Revisar los sistemas establecidos para asegurar que estén de acuerdo con aquellas políticas, planes, procedimientos, leyes y reglamentos que pudieran tener un efecto significativo en las operaciones e informes, determinando si la organización los está aplicando.
- Revisar los medios de salvaguarda de los activos y, si procede, verificar su existencia.
- Valorar la economía y eficacia con que son utilizados los recursos.
- Revisar las operaciones o programas para verificar si los resultados están alineados con los objetivos y metas establecidos, y si las operaciones o programas se llevan a cabo en la forma prevista.

Responsabilidad y Autoridad

El departamento de auditoría interna es una parte integral de la organización y funciona sometido a las políticas establecidas por la alta dirección y el Consejo. El objeto, autoridad y responsabilidad del departamento de auditoría interna deben estar definidos en un documento formal escrito (estatuto). El Director de Auditoría Interna debería buscar la aprobación del estatuto por la alta dirección, así como también su aceptación por el Consejo. El estatuto debería señalar claramente el objeto del departamento de auditoría interna, especificando que no existen restricciones en el ámbito de su trabajo, y declarar que los auditores internos no tienen autoridad o responsabilidad sobre las actividades que auditen.

1. La Declaración de Responsabilidades de la Auditoría Interna fue originalmente publicada por el IIA en 1947. El Marco Internacional para la Práctica Profesional de la Auditoría Interna instituye y amplía este documento, que publicamos para conocimiento de los nuevos auditores internos y por la importancia que tuvo hasta la definición renovada de Auditoría Interna que se efectuó en 1999.

En todo el mundo la auditoría interna es realizada en diversos entornos y dentro de organizaciones que varían en finalidad, tamaño y estructura. Además, las leyes y costumbres dentro de los distintos países difieren de uno a otro. Estas diferencias pueden afectar a la práctica de la auditoría interna en cada entorno. El cumplimiento de las Normas, por tanto, estará influido por el entorno en el que el departamento de auditoría interna realiza sus responsabilidades asignadas. Es imprescindible seguir las Normas, antes que sus responsabilidades se realicen. Como declaró el Código de Ética, los miembros del Instituto de Auditores Internos y los *Certified Internal Auditors* adoptarán los medios adecuados para cumplir con las Normas Internacionales para la Práctica Profesional de la Auditoría Interna.

Independencia

Los auditores internos deben ser independientes de las actividades que auditen. Los auditores internos son independientes cuando pueden realizar su trabajo libre y objetivamente. La independencia permite a los auditores internos emitir juicios imparciales y sin prejuicios, lo que es esencial para la adecuada realización de las auditorías. Esto se consigue mediante un adecuado nivel en la organización y con objetividad.

El nivel organizativo del departamento de auditoría interna debe ser suficiente para permitir el cumplimiento de sus responsabilidades. El director del departamento debe ser responsable ante una persona de la organización, con suficiente autoridad para promover la independencia y asegurar una amplia cobertura de auditoría, adecuada consideración de sus informes y apropiada acción sobre sus recomendaciones.

La objetividad es una actitud mental independiente que los auditores internos deberían mantener en la realización de auditorías. Los auditores internos en ningún caso deben subordinar sus juicios en materia de auditoría a los de otros. Diseñar, instalar y manejar sistemas no son funciones de auditoría. Tampoco el diseño de procedimientos para sistemas es una función de auditoría. La realización de tales actividades supone un perjuicio para la objetividad de la auditoría.

Anexo 3 · Código de Ética

Introducción

El propósito del *Código de Ética* del Instituto es promover una cultura ética en la profesión de Auditoría Interna.

La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Es necesario y apropiado contar con un código de ética para la profesión de Auditoría Interna, ya que ésta se basa en la confianza que se imparte a su aseguramiento objetivo sobre la gestión de riesgos, control y dirección. El *Código de Ética* del Instituto abarca mucho más que la definición de Auditoría Interna, llegando a incluir dos componentes esenciales:

1. Principios que son relevantes para la profesión y práctica de la Auditoría Interna.
2. Reglas de Conducta que describen las normas de comportamiento que se espera sean observadas por los auditores internos. Estas reglas son una ayuda para interpretar los Principios en aplicaciones prácticas. Su intención es guiar la conducta ética de los auditores internos.

El *Código de Ética,* junto al *Marco Internacional para la Práctica Profesional de la Auditoría Interna* y otros pronunciamientos emitidos por el Instituto, proporcionan orientación a los auditores internos para servir a los demás. La mención a los "auditores internos" se refiere a los socios del Instituto, a quienes han recibido –o son candidatos a recibir– certificaciones profesionales del Instituto, y a aquéllos que proveen servicios de Auditoría Interna.

Aplicación y cumplimiento

Este *Código de Ética* se aplica tanto a los individuos como a las entidades que proveen servicios de Auditoría Interna.

En el caso de los socios del Instituto y de aquéllos que han recibido o son candidatos a recibir certificaciones profesionales del Instituto, el incumplimiento del *Código de Ética* será evaluado y administrado de conformidad con los Estatutos y Reglamentos Administrativos del Instituto. El hecho de que una conducta particular no se halle contenida en las Reglas de Conducta no impide que ésta sea considerada inaceptable o como un descrédito, y en consecuencia, puede hacer que se someta a acción disciplinaria al socio, poseedor de una certificación o candidato a la misma.

Principios

Se espera que los auditores internos apliquen y cumplan los siguientes principios:

INTEGRIDAD

La integridad de los auditores internos establece confianza y, consiguientemente, provee la base para confiar en su juicio.

OBJETIVIDAD

Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación

equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por otras personas.

CONFIDENCIALIDAD

Los auditores internos respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización a menos que exista una obligación legal o profesional para hacerlo.

COMPETENCIA

Los auditores internos aplican el conocimiento, aptitudes y experiencia necesarios al desempeñar los servicios de Auditoría Interna.

Reglas de conducta

INTEGRIDAD

Los auditores internos:

- Desempeñarán su trabajo con honestidad, diligencia y responsabilidad.
- Respetarán las leyes y divulgarán lo que corresponda de acuerdo con la ley y la profesión.
- No participarán a sabiendas en una actividad ilegal o de actos que vayan en detrimento de la profesión de Auditoría Interna o de la organización.
- Respetarán y contribuirán a los objetivos legítimos y éticos de la organización.

OBJETIVIDAD

Los auditores internos:

- No participarán en ninguna actividad o relación que pueda perjudicar o aparente perjudicar su evaluación imparcial. Esta participación incluye aquellas actividades o relaciones que puedan estar en conflicto con los intereses de la organización.
- No aceptarán nada que pueda perjudicar o aparente perjudicar su juicio profesional.
- Divulgarán todos los hechos materiales que conozcan y que, de no ser divulgados, pudieran distorsionar el informe de las actividades sometidas a revisión.

CONFIDENCIALIDAD

Los auditores internos:

- Serán prudentes en el uso y protección de la información adquirida en el transcurso de su trabajo.
- No utilizarán información para lucro personal o que de alguna manera fuera contraria a la ley o en detrimento de los objetivos legítimos y éticos de la organización.

COMPETENCIA

Los auditores internos:

- Participarán sólo en aquellos servicios para los cuales tengan los suficientes conocimientos, aptitudes y experiencia.
- Desempeñarán todos los servicios de Auditoría Interna de acuerdo con las Normas Internaciponales para la Práctica Profesional de Auditoría Interna.
- Mejorarán continuamente sus habilidades y la efectividad y calidad de sus servicios.

Anexo 4 · Cuestionario de Control Interno

Una revisión-evaluación sencilla y rápida del sistema de Control Interno de una organización[2]

OBJETIVOS

- ¿Existen?
- ¿Se conocen?
- ¿Se discuten?
- ¿Están escritos?
- ¿Se cumplen?
- ¿Se controlan?

SISTEMAS DE INFORMACIÓN

- ¿Hay un sistema informatizado de información corporativa?
- ¿Hay canales de información y comunicación ascendentes y descendentes?
- ¿La información la acaparan unos pocos?
- ¿Es fiable?

ASIGNACIÓN CLARA DE FUNCIONES Y RESPONSABILIDADES

- ¿Existe un organigrama actualizado, real?
- ¿Saben los empleados cuáles son sus tareas, de qué son responsables, cómo han de hacer su trabajo y qué ocurre si no lo hacen correcta y responsablemente?

COBERTURA DE BIENES Y PERSONAS

- ¿Hay una política de seguros para los bienes (activos) y para las personas?
- ¿Los activos están convenientemente registrados como propiedad de la organización?
- ¿Se producen con frecuencia accidentes, robos, fraudes?

PLANIFICACIÓN Y COORDINACIÓN

- ¿Se planifica a largo plazo?
- ¿A medio?
- ¿A corto?
- ¿Hay una actuación coordinada?
- ¿Se trabaja como un equipo?
- ¿Existen compartimentos estancos?
- ¿Existen departamentos o servicios especializados para aprovisionamientos, producción, comercial, etc., con claras y delimitadas responsabilidades?

2. Como se trata de un ejemplo, las preguntas son indicativas y no agotan otras que pueden y deben incluirse.

CONTROL DE GESTIÓN

- ¿Se asigna a una unidad concreta (Director de Control, Presupuestos, etc.)?
- ¿Qué política presupuestaria se sigue?
- ¿Cómo se elabora el presupuesto, cómo se sigue, etc.?
- ¿Se revisan los Estados Financieros por auditores externos?
- ¿Hay Auditoría Interna?
- ¿Está bien concebida?
- ¿Dispone de medios suficientes?
- ¿Es independiente?
- ¿Está profesionalizada?
- ¿Hay Comisión de Auditoría?

CONSEJO DE ADMINISTRACIÓN

- ¿Se preocupa de supervisar realmente a la dirección ejecutiva?
- ¿Existen Comités o Comisiones delegadas?
- ¿Se responsabiliza del control interno?

POLÍTICA DE PERSONAL Y RECURSOS HUMANOS

- Selección.
- Reclutamiento.
- Líneas de carrera.
- Promoción.
- Integración.
- Participación.
- Reconocimiento al mérito y a la profesionalidad.

PREVENCIÓN DE FRAUDE E IRREGULARIDADES

- ¿Existe una política de prevención?
- ¿Se informa en casos de fraude al personal?
- ¿Se castiga?
- ¿Hay un código de conducta?
- ¿Se preocupa el Consejo de la ética de la empresa?

Anexo 5 · Un ejemplo de cuestionario de Control Interno según la concepción COSO

El Consejo y el Control Interno

EXISTE COMISIÓN DE AUDITORÍA

- ¿Participa o la preside algún consejero?
- ¿Qué funciones tiene la Comisión?
- ¿Cuál es su composición?
- ¿Cuántas veces se reúne al año?
- ¿Qué temas se han tratado?
- ¿Efectúa el seguimiento de las recomendaciones?
- ¿Informa la Comisión al Consejo sobre las recomendaciones de auditoría?
- ¿Contrata la Comisión a los auditores externos?
- Si es así, ¿participa en la contratación Auditoría Interna?
- ¿El informe de los auditores externos es examinado por la Comisión antes de su entrega a la Dirección y al Consejo?
- ¿La Comisión elabora un informe sobre el control interno para el Consejo?

NO EXISTE COMISIÓN DE AUDITORÍA

- ¿Qué atención dedica el Consejo al control interno?:
  - Fiabilidad de la información.
  - Eficiencia operativa.
  - Cumplimiento de leyes, regulaciones y normas.
- ¿Qué relación directa tiene, o puede tener, la auditoría interna en el Consejo?
- ¿Recibe el Consejo sus informes?
- ¿Se preocupa del cumplimiento de sus recomendaciones?

Alta Dirección (Director General, Consejero Delegado, Director Ejecutivo, Secretario General)

- ¿Hay una clara delimitación entre el Consejo y la Dirección Ejecutiva?
- ¿De quién depende la auditoría interna?
- ¿Quién contrata a los auditores externos?
- ¿Cuál es la actitud de la alta dirección respecto a la auditoría interna?

La Alta Dirección y el Control Interno

- ¿Qué interés y atención dedican o muestran la alta dirección y directivos al control interno?
- ¿Tienen un conocimiento claro y actual de la función de auditoría?

- ¿Participan en los trabajos y discusión de los informes de auditoría interna?
- ¿Cumplen en plazo y forma las recomendaciones?
- ¿Pertenecen o presiden la Comisión de Auditoría?

Eficiencia de las operaciones (Eficiencia significa eficacia y coste óptimo)

- ¿Están convenientemente asignadas funciones, atribuciones y responsabilidades en todos los niveles organizativos?
- ¿Los procedimientos son racionales?
- ¿Hay funciones especializadas suficientes?

CONTRATACIÓN

- ¿Quién puede contratar en nombre de la organización?
- ¿Qué requisitos se exigen en los contratos?
- ¿Se cumplen?
- ¿Cómo se verifica el cumplimiento?
- ¿Se fijan penalidades por incumplimiento?
- ¿Se ejecutan?

COMPRAS

- ¿Existe un registro de proveedores homologados?
- ¿Hay un departamento especializado?
- ¿Cuál es el proceso de compras? Análisis de este.
- ¿Es racional y adecuado a las características de la organización?
  - ¿Quién puede comprar?
  - Tiempo entre petición de compra y recepción.
  - ¿Quién recepciona las compras?
  - ¿Quién comprueba las condiciones de compra al recibo de las facturaciones?
  - ¿Existen condiciones generales de compra?
  - ¿Se cumplen?

VENTAS

- ¿Hay un departamento especializado?
- ¿Existe una política de marketing?
  - Estudio de mercados.
  - Conocimiento de los clientes y sus preferencias.
  - Conocimiento de la competencia.
  - ¿Cómo se fijan los precios y descuentos?
  - Condiciones de venta.
  - Envases y embalajes.
  - Atenciones a los clientes y reclamaciones.

  - Garantías de calidad de los productos o servicios.
  - Publicidad y relaciones públicas.
- Analizar el proceso de ventas: recepción y cumplimiento de pedidos, autorización de precios, facturación y cobro, impagados, etc.

PERSONAL Y RECURSOS HUMANOS

- ¿Existe una política de personal para selección, reclutamiento, promoción, despido y jubilaciones?
- ¿Cuál es el grado de participación-integración del personal?
- ¿Se preocupa la organización de la formación-capacitación?

PRODUCCIÓN

- ¿Existen políticas establecidas?
  - Mantenimiento.
  - Calidad total.
  - Homologación de productos.
- ¿Cómo se controla la producción?
- ¿Se trabaja sobre pedido o para almacén?
- ¿Hay un control adecuado de los almacenes?
- ¿Existen paradas o tiempos muertos?
- ¿Cuál es el aspecto de los talleres en cuanto a?
  - Orden.
  - Limpieza.
  - Condiciones de trabajo.
  - Seguridad e higiene:
    - Accidentes.
    - Lesiones.
    - Heridas.
- ¿Cómo se controlan las entradas y salidas del personal?
- ¿Hay instalaciones infrautilizadas?
  - Capacidad de producción teórica.
  - Producción real.
  - Personal empleado.
- ¿Absentismo del personal?
  - Faltas no justificadas.
  - Enfermedad.
  - Permisos, etc.
- ¿La plantilla es adecuada? ¿Exceso o defecto?
- ¿Cómo se controla esto?
  - Por simple observación del ritmo de trabajo y movimientos del personal.
  - Por comparación con estándares establecidos para actividades similares.
  - Comparando las cifras de producción con la plantilla media y el coeficiente de absentismo.
  - Entrevistando a los responsables y a los empleados.

PREVENCIÓN Y LUCHA CONTRA EL FRAUDE

- Datos históricos de un determinado período inmediatamente anterior (cinco años).
- ¿Dónde pueden producirse actualmente?
- ¿Existe un código de conducta?
- ¿Hay normas claras de la dirección en caso de fraude y para su prevención?
- ¿Están escritas y distribuidas al personal?

Fiabilidad de la información

- Análisis del sistema de información corporativo comprobando:
  - Confiabilidad de los datos de base.
  - Racionalidad de los procesos para su obtención.
  - Confidencialidad.
  - Seguridad y custodia.
- Comprobar:
  - Hardware.
  - ¿La información es la que se necesita?
  - ¿Se recibe en tiempo y forma?
  - ¿Puede suprimirse parte de la información?
  - ¿Debe aumentarse?
  - ¿Quién recibe la información y cómo la recibe?
  - ¿El Centro de Proceso de Datos está correctamente organizado?
    - Localización.
    - Medios técnicos y humanos.
    - Seguridad.
    - Software.
    - Informática descentralizada.
  - ¿La informática sirve al usuario?
  - ¿Cómo se llevan a cabo los sistemas en desarrollo?
    - Establecimiento.
    - Desarrollo.
    - Recepción, etc.
  - ¿Qué información se recibe del exterior?
  - ¿Qué información se hace pública?
  - ¿Cómo se establece el presupuesto?
    - Objetivos.
    - Aceptación-participación.
    - Orientación-información.
    - Vigilancia.
    - Control desviaciones.

Cumplimiento de Leyes y Normas internas y externas

- ¿Qué leyes afectan a la organización?
  - Contables.
  - Fiscales.
  - Seguridad y medicina del trabajo.
  - Ecológicas y ambientales.
  - Sanitarias.
  - Laborales.
  - Protección de datos.
  - Otras.
- ¿Cuál es la política de la organización sobre cumplimientos de leyes y disposiciones administrativas?
- ¿La organización ha sido sancionada?
- ¿Por qué, cuántas veces, responsabilidades?
- ¿Hay una información suficiente sobre las regulaciones y leyes que afectan a la organización?
- ¿Existen normas internas?
- ¿Quién y cómo se elaboran?
- ¿Hay información suficiente sobre ellas?
- ¿Qué pasa si se incumplen?
- ¿Son necesarias, faltan, se revisan periódicamente?

Observaciones

Este cuestionario es un modelo orientativo que debe adaptarse a las características de la organización, ampliándolo, reduciéndolo o modificándolo según proceda y se estime necesario. Se recomienda su elaboración a los auditores internos para que tengan una visión general de cuál es la situación en la que se encuentra su organización en lo que res-pecta al control interno o control general de gestión de esta.

Anexo 6 · Modelo de Estatuto de la Actividad de Auditoría Interna

Propósito y Misión

El propósito del [departamento/actividad] de Auditoría Interna de [nombre de la organización] es proporcionar servicios independientes y objetivos de aseguramiento y consultoría, concebidos para agregar valor y mejorar las operaciones de [nombre de la organización]. La misión de la auditoría interna es mejorar y proteger el valor de la organización proporcionando aseguramiento, asesoría y análisis en base a riesgos. El [departamento/actividad] de Auditoría Interna ayuda a [nombre de la organización] a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gobierno, gestión de riesgos y control.

Normas para la Práctica Profesional de la Auditoría Interna

El [departamento/actividad] de Auditoría Interna se adhiere a los elementos de cumplimiento obligatorio del *Marco Internacional para la Práctica Profesional* del Instituto de Auditores Internos, incluidos los *Principios Fundamentales para la Práctica Profesional de la Auditoría Interna, el Código de Ética, las Normas,* y la *Definición de Auditoría Interna*. El Director de Auditoría Interna informará periódicamente a la alta dirección y al [Consejo / comisión de auditoría / comité de supervisión] respecto a la conformidad del [departamento / actividad] de Auditoría Interna con el Código de Ética y las Normas.

Autoridad

El Director de Auditoría Interna reportará funcionalmente al [Consejo / comisión de auditoría / comité de supervisión] y administrativamente (es decir, operaciones cotidianas) al [director ejecutivo/gerente general]. Para establecer, mantener y asegurar que el [departamento / actividad] de Auditoría Interna de [nombre de la organización] tiene la autoridad suficiente para cumplir completamente con sus obligaciones, el [Consejo / comisión de auditoría / comité de supervisión] deberá:

- Aprobar el estatuto del [departamento / actividad] de Auditoría Interna.
- Aprobar el plan de auditoría interna basado en riesgos.
- Aprobar el presupuesto y el plan de recursos del [departamento / actividad] de Auditoría Interna.
- Recibir comunicaciones del Director de Auditoría Interna sobre el desarrollo del plan de auditoría interna del [departamento / actividad] y otros asuntos.
- Aprobar las decisiones referentes al nombramiento y cese del Director de Auditoría Interna.
- Aprobar la remuneración del Director de Auditoría Interna.
- Formular las preguntas adecuadas a la Dirección y al Director de Auditoría Interna para determinar si existen alcances inadecuados o limitaciones de recursos.

El Director de Auditoría Interna tendrá acceso irrestricto, y se comunicará e interactuará directamente con el [Consejo / comisión de auditoría / comité de supervisión], incluso en reuniones privadas sin la presencia de la administración.

El [Consejo / comisión de auditoría / comité de supervisión] autoriza al [departamento / actividad] de Auditoría Interna a:

- Tener acceso completo, libre y sin restricciones a todas las funciones, registros, propiedad y personal pertinentes, para llevar a cabo cualquiera de sus compromisos, sujeto a su responsabilidad de confidencialidad y salvaguarda de los registros e información.
- Asignar recursos, establecer frecuencias, seleccionar temas, determinar alcances de trabajo, aplicar las técnicas necesarias para cumplir con los objetivos de la auditoría y emisión de informes.
- Obtener asistencia del personal necesario de [nombre de la organización], así como de otros servicios especializados dentro o fuera de [nombre de la organización], a fin de completar el compromiso.

Independencia y objetividad

El Director de Auditoría Interna se asegurará que [departamento / actividad] de Auditoría Interna permanezca libre de todas las condiciones que amenacen la capacidad de los auditores internos para cumplir sus responsabilidades de manera imparcial, incluyendo asuntos de selección, alcance, procedimientos, frecuencia, oportunidad y contenido del informe de auditoría. Si el Director de Auditoría Interna determina que la independencia u objetividad se viese comprometida de hecho o en apariencia, los detalles del impedimento deben darse a conocer a las partes correspondientes.

Los auditores internos mantendrán una actitud mental imparcial que les permita realizar sus compromisos objetivamente y de tal manera que se confíe en el producto de su trabajo, no se comprometa la calidad y no subordinen su juicio a otros, sobre asuntos de la auditoría.

Los auditores internos no tendrán responsabilidad operacional directa o autoridad sobre ninguna de las actividades auditadas. En consecuencia, los auditores internos no implementarán controles internos, desarrollarán procedimientos, instalarán sistemas, prepararán registros o participarán en cualquier otra actividad que pueda perjudicar su juicio, incluyendo:

- Evaluar las operaciones específicas de las cuales hayan sido responsables en el año anterior.
- Realizar cualquier tarea operacional para [nombre de la organización] o sus afiliadas.
- Iniciar o aprobar operaciones externas a los procesos de la [actividad / departamento] de Auditoría Interna.
- Dirigir las actividades de cualquier empleado de [nombre de la organización] que no esté contratado por el [departamento / actividad] de Auditoría Interna excepto en la medida que dichos empleados hayan sido apropiadamente asignados a los equipos de auditoría o para ayudar a auditores internos.

Cuando el Director de Auditoría Interna tiene o se espera que tenga funciones y/o responsabilidades más allá de auditoría interna, se establecerán salvaguardas para limitar los impedimentos a la independencia u objetividad.

Los auditores internos deberán:

- Declarar cualquier impedimento de independencia u objetividad, de hecho o apariencia, a las partes apropiadas.
- Demostrar objetividad profesional en la recolección, evaluación y comunicación de información sobre la actividad o proceso que se está examinando.
- Hacer evaluaciones equilibradas de todos los hechos y circunstancias disponibles y relevantes.

- Tomar las precauciones necesarias para evitar ser influenciados indebidamente por sus propios intereses o por otros, en la formación de los juicios.

El Director de Auditoría Interna confirmará al [Consejo / comisión de auditoría / comité de supervisión], al menos una vez al año, la independencia organizacional del [departamento / actividad] de Auditoría Interna.

El Director de Auditoría Interna comunicará al [Consejo / comisión de auditoría / comité de supervisión] cualquier interferencia e implicaciones relacionadas en la determinación del alcance, desarrollo del trabajo y / o la comunicación de los resultados de la auditoría interna.

Alcance de las actividades de Auditoría Interna

El alcance de las actividades de Auditoría Interna abarca, pero no se limita a, exámenes objetivos de evidencia con el propósito de proporcionar evaluaciones independientes al [Consejo / comisión de auditoría / comité de supervisión], a la administración y a terceros sobre la adecuación y eficacia de los procesos de Gobierno, Gestión de Riesgos y Control de [nombre de la organización]. Las evaluaciones de Auditoría Interna incluyen verificar si:

- Los riesgos relacionados con el logro de los objetivos estratégicos de [nombre de la organización] están adecuadamente identificados y gestionados.
- Las acciones de los oficiales, directores, empleados y contratistas de [nombre de la organización] cumplen con las políticas, procedimientos y leyes aplicables, regulaciones y normas de gobierno de [nombre de la organización].
- Los resultados de las operaciones o programas son consistentes con las metas y objetivos establecidos.
- Las operaciones o programas se están llevando a cabo de manera efectiva y eficiente.
- Los procesos y sistemas establecidos permiten el cumplimiento de las políticas, procedimientos, leyes y reglamentos que podrían afectar significativamente a [nombre de la organización].
- La información y los medios utilizados para identificar, medir, analizar, clasificar y reportar dicha información, son confiables y tienen integridad.
- Los recursos y activos se adquieren económicamente, se utilizan eficientemente y se protegen adecuadamente.

El Director de Auditoría Interna informará periódicamente a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión], con respecto a:

- El propósito, autoridad y la responsabilidad del [departamento / actividad] de Auditoría Interna.
- El plan y el desarrollo del plan del [departamento / actividad] de la Auditoría Interna.
- El cumplimiento del [departamento / actividad] de Auditoría Interna con el Código de Ética y Normas del IAI, y de los planes de acción para abordar cualquier desviación de incumplimiento significativa.
- Exposiciones significativas a riesgos y asuntos de control, incluidos riesgos de fraude, cuestiones de gobernanza y otros asuntos que requieren la atención del [Consejo / comisión de auditoría / comité de supervisión].
- Resultados de los trabajos de auditoría u otras actividades.
- Requerimientos de recursos.

- Cualquier respuesta al riesgo de la administración que pueda ser inaceptable para [nombre de la organización].

El Director de Auditoría Interna también coordina las actividades, cuando es posible, y considera confiar en el trabajo de otros proveedores de servicios de aseguramiento y consultoría internos y externos, según sea necesario. El [departamento / actividad] de auditoría interna puede realizar asesoría y otros servicios relacionados a las actividades de clientes, cuya naturaleza y alcance se acordarán con ellos, siempre y cuando [departamento / actividad] de auditoría interna no asuma responsabilidad administrativa.

Oportunidades para mejorar la eficiencia de los procesos de gobierno, gestión de riesgos y control pueden ser identificadas durante los compromisos. Estas oportunidades se comunicarán al nivel adecuado de la administración.

Responsabilidad

El Director de Auditoría Interna tiene la responsabilidad de:

- Presentar, al menos una vez al año, a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión] el plan de auditoría interna basado en riesgos, para su revisión y aprobación.
- Comunicar a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión] el impacto de limitaciones de recursos sobre el plan de auditoría interna.
- Revisar y ajustar el plan de auditoría interna, según sea necesario, en respuesta a cambios en los negocios, riesgos, operaciones, programas, sistemas y controles de [nombre de la organización].
- Comunicar a la alta gerencia y al [Consejo / Comisión de auditoría / comité de supervisión] cualquier cambio provisional significativo al plan de auditoría interna.
- Asegurar que se ejecute cada compromiso del plan de auditoría interna, incluyendo el establecimiento de objetivos y alcance, la asignación de recursos apropiados y su supervisión, la adecuada documentación de los programas de trabajo y los resultados de las pruebas y la comunicación de los resultados del trabajo, con las conclusiones y recomendaciones aplicables a partes interesadas.
- Efectuar seguimiento a las observaciones y acciones correctivas, e informar periódicamente a la alta dirección y al [Consejo / comisión de auditoría / comité de supervisión] cualquier acción correctiva no implementada efectivamente.
- Asegurar que los principios de integridad, objetividad, confidencialidad y competencia sean aplicados y defendidos.
- Asegurar que el [departamento / actividad] de auditoría interna posee colectivamente u obtiene los conocimientos, habilidades y otras competencias necesarias para alcanzar los requerimientos del estatuto de auditoría interna.
- Asegurar que las tendencias y los problemas emergentes que puedan afectar a [nombre de la organización] se consideren y se comuniquen a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión], cuando sea apropiado.
- Asegurar que las tendencias emergentes y las prácticas exitosas están siendo consideradas en Auditoría Interna.
- Establecer y asegurar el cumplimiento de las políticas y procedimientos diseñados para guiar el [departamento / actividad] de Auditoría Interna.

- Asegurar el cumplimiento de las políticas y procedimientos relevantes de [nombre de la organización], a menos que tales políticas y procedimientos entren en conflicto con el estatuto de Auditoría Interna. Cualquier conflicto de este tipo se resolverá o se comunicará a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión].
- Asegurar la conformidad del [departamento / actividad] de Auditoría Interna con las Normas, con las siguientes reservas:
  - Si el cumplimiento de ciertas partes de las Normas del [departamento / actividad] de Auditoría Interna está prohibida por ley o regulación, el Director de Auditoría Interna asegurará la revelación apropiada de ello, así como el cumplimiento de todas las demás partes de las Normas.
  - Si las Normas se usan conjuntamente con requerimientos emitidos por [otros órganos autorizados], el Director de Auditoría Interna asegurará que [departamento / actividad] de Auditoría Interna cumpla con las Normas e incluso si [departamento / actividad] de Auditoría Interna también cumple con requisitos más restrictivos de [otras entidades autorizadas].

Programa de Aseguramiento y Mejora de la Calidad

El [departamento / actividad] de Auditoría Interna mantendrá un programa de aseguramiento y mejora de la calidad que comprenda todos los aspectos del [departamento / actividad] de Auditoría Interna. El programa incluirá una evaluación del cumplimiento del [departamento / actividad] de Auditoría Interna con las Normas y una evaluación si los auditores internos aplican el Código de Ética del IIA. El programa también evaluará la eficiencia y la eficacia del [departamento / actividad] de Auditoría Interna e identificará oportunidades de mejora.

El Director de Auditoría Interna comunicará a la alta gerencia y al [Consejo / comisión de auditoría / comité de supervisión] el programa de aseguramiento y mejora de calidad del [departamento / actividad] de Auditoría Interna, incluidos los resultados de las evaluaciones internas (continuas y periódicas) y las evaluaciones externas llevadas a cabo por lo menos una vez cada cinco años, por un evaluador o equipo de evaluación calificado e independiente de [nombre de la organización].

Aprobación / Firmas

Director de Auditoría Interna	Fecha
Presidente [Consejo / Comisión de Auditoría / Comité de Supervisión]	Fecha
[Director o Gerente General]	Fecha

Anexo 7 · Ejemplo de Procedimiento de Auditoría

Elaboración de informes de auditoría

OBJETO

Este procedimiento tiene por objeto determinar la sistemática que deberá seguir un auditor para la realización de un informe de auditoría.

ÁMBITO DE APLICACIÓN

Este procedimiento es aplicable a todo el personal de auditoría. El auditor que elabora el informe será el responsable del cumplimiento de este procedimiento y, en el caso de realizar el trabajo en equipo, lo será el auditor jefe de equipo.

DESCRIPCIÓN DEL PROCEDIMIENTO

1. Consideraciones generales

- El DAI indicará al auditor responsable el informe que deberá realizar, facilitándole toda la información que sea necesaria para precisar el alcance y objetivos de este y determinando los plazos para su realización.
- El DAI notificará verbalmente la iniciación del informe al director correspondiente y al jefe de la unidad responsable de la actividad concreta que se audita, iniciándose la actuación en el plazo de tres días, sin otro trámite formal que la presentación al citado jefe de unidad del programa o de la orden escrita del presidente –según se trate de informes normales o especiales– si le fueran requeridas tales autorizaciones.
- El auditor responsable establecerá el programa específico que determinará las diversas fases de actuación en la elaboración del informe correspondiente, paralo cual utilizará el manual interno de procedimientos y técnicas de auditoría, así como la documentación y bibliografía que considere necesarias.
- Una vez elaborado el programa, lo someterá a la aprobación del DAI.
- Aprobado el programa y obtenida la correspondiente autorización del responsable del área a auditar, procederá a la ejecución del trabajo, informando constantemente al DAI del desarrollo de este.
- Finalizado el trabajo, elaborará con el DAI el informe de auditoría, de acuerdo con la siguiente estructura:
  1. Introducción.
  2. Objetivos o programa.
  3. Alcance.
  4. Dictamen de auditoría.
  5. Recomendaciones.
  6. Resumen de excepciones.

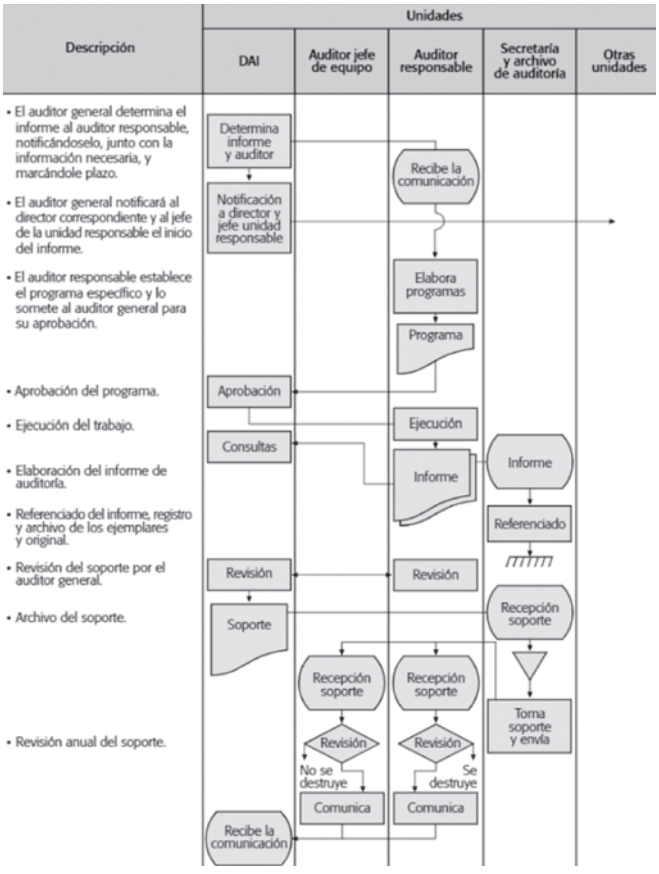
     Si fuera necesario establecer subepígrafes se recurrirá al sistema de numeración decimal, subrayando el título de cada uno, que sólo llevará la primera letra en mayúscula. Ejemplo:

     6. Resumen de excepciones:
        6.1. Archivo general.
        6.2. Tesorería.

- La referencia de los informes de auditoría comprenderá la letra A, el número del informe y las dos últimas cifras del año en que se haya elaborado. Ejemplo: A-7-XX correspondería al séptimo informe realizado por auditoría en 20XX.
- Seguidamente se procederá al registro y archivo del informe con toda la correspondencia que se produzca al respecto.
- Finalmente, los papeles de trabajo, la documentación utilizada en la elaboración del informe, el borrador de este, así como una copia del texto definitivo constituirán el denominado «soporte del informe», que será archivado adecuadamente, preferiblemente en formato electrónico.
- El soporte deberá ser presentado al DAI, o a la persona en quien ésta delegue, por el auditor responsable para su examen y verificación.
- El DAI remitirá el soporte a la persona encargada del registro y archivo de informes de auditoría, para su archivo definitivo, en caso de no disponer de una herramienta informática que ejecute el proceso de archivo de forma automática.

2. Descripción

Diagrama de funcionamiento del procedimiento y descripción de este (Tabla 1).



Remisión de Informes de Auditoría

OBJETO

Este procedimiento tiene por objeto determinar la sistemática a seguir en el envío de los informes de auditoría a los responsables de las áreas auditadas.

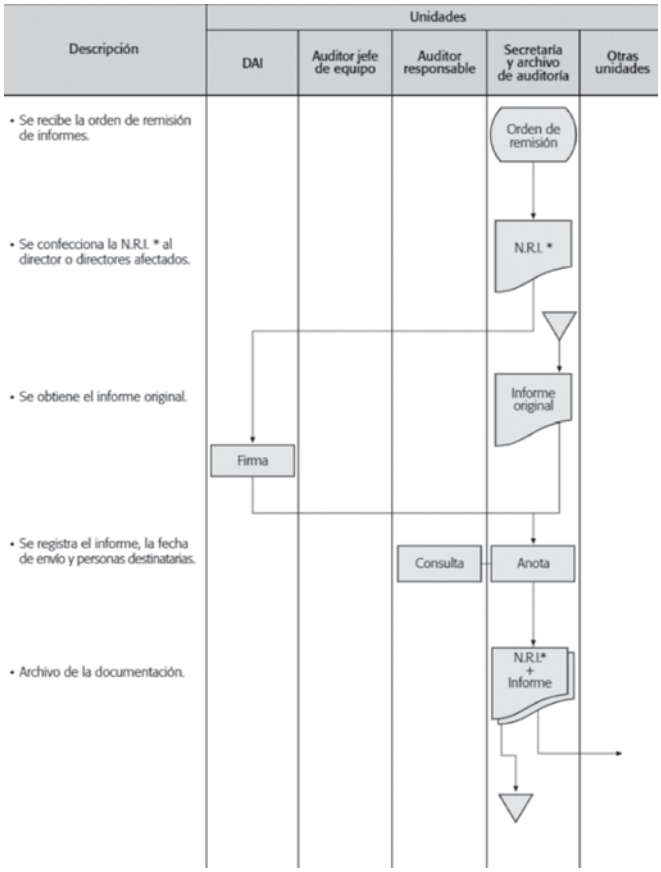
ÁMBITO DE APLICACIÓN

Este procedimiento es aplicable a todo el personal de auditoría. La responsabilidad del cumplimiento del procedimiento corresponderá al DAI.

DESCRIPCIÓN DEL PROCEDIMIENTO

1. Consideraciones generales
   - Una vez elaborado el informe (Procedimiento A-001), la persona encargada de la secretaría y archivo de auditoría solicitará del auditor responsable el número de ejemplares necesarios para su distribución.
   - Del informe se remitirán en sobre cerrado los siguientes ejemplares:
     a) Un ejemplar al presidente.
     b) Un ejemplar al consejero delegado.
     c) Dos ejemplares al director del área auditada, uno de los cuales estará destinado al responsable directo de la unidad afectada.
     d) Otros ejemplares a las personas que, en cada caso, el auditor general o el auditor que realizó el trabajo estimen conveniente.
   - La persona encargada de la secretaría y archivo de auditoría anotará la fecha de envío de estos, así como el nombre de las personas a las que se remitieron. Dicho libro registro será revisado periódicamente por el auditor jefe de equipo y los auditores.
   - Finalmente, la misma persona encargada de la secretaría y archivo de auditoría archivará toda la documentación producida convenientemente.
2. Descripción

   Diagrama de funcionamiento del presente procedimiento y descripción de este (Tabla 2).


Descripción
Unidades
DAI
Auditor jefe de equipo
Auditor responsable
Secretaría y archivo de auditoría
Otras unidades
• Se recibe la orden de remisión de informes.
Orden de remisión
• Se confecciona la N.R.I. * al director o directores afectados.
N.R.I. *
• Se obtiene el informe original.
Informe original
Firma
• Se registra el informe, la fecha de envío y personas destinatarias.
Consulta
Anota
• Archivo de la documentación.
N.R.I.* + Informe

Anexo 8 · Ejemplo de Memoria de Actividades

Introducción

Según prescribe el Estatuto de Auditoría que regula la actividad de Auditoría Interna en la organización, se confecciona la presente memoria, en la que se reflejan sus actividades durante el ejercicio de 20XX.

Dicha memoria ha de presentarse a la Comisión de Auditoría para su conocimiento y posterior distribución al primer y segundo nivel de la empresa, debiendo contener, entre otras, las siguientes informaciones:

1. Un resumen de las actividades e informes realizados en el ejercicio al que corresponde la memoria, expresando los que, estando previstos en el ejercicio, no fueron realizados.
2. Un inventario de las recomendaciones y sugerencias contenidas en los distintos informes de auditoría, haciendo constar por separado:
   a) Las aceptadas y su grado de implantación.
   b) Las expresamente rechazadas.
3. No se incluyen las cartas de recomendaciones formuladas a las empresas filiales en las que se han efectuado auditorías, ya que las mismas son responsabilidad de sus consejos de administración.

Actividades de Auditoría

El resumen de horas trabajadas para cada área es el siguiente:

Área	Horas totales
Asociaciones y agrupaciones	1.847
Comercial	127
Producción	50
Económico-financiero	435
Almacén A	303
Grupo empresas	429
Informática	1.151
Almacén B	972
Producción equipos	828
Oficinas centrales	224
Empresas participantes	1.626
Relaciones laborales	117
Centro C	286
Centro D	341
Ingeniería	589
Auditoría *	1.852
TOTAL	**11.177**

* Gestión de la unidad, programas de calidad y colaboración con otras direcciones.

INFORMES REALIZADOS

Los informes realizados en las distintas áreas han sido: *Asociaciones y agrupaciones, Comercial, Económico-financiero, Centros, Grupo de empresas;* y en el ámbito de la auditoría: *Memoria anual, Planificación anual, Varios auditoría, Revisión interna Auditoría Interna, Exigencia de calidad en Auditoría Interna.*

OTRAS ACTIVIDADES

- Auditoría Interna ha pasado en el año los siguientes cargos (sin incluir el IVA) por prestación de servicios profesionales:

  TOTAL .....

- El Grupo de Calidad «Auditoría» ha celebrado en el año nueve sesiones, tratando otros tantos problemas específicos sobre el funcionamiento interno de la unidad. El número total de horas destinadas a la calidad ha sido de 150.
- Durante tres semanas hemos atendido la visita del director de auditoría de la empresa X, que se ha realizado de acuerdo con el «Convenio de colaboración» firmado con su país. El programa de trabajo se preparó, en colaboración con la dirección de asuntos internacionales, tratando de que pudiese obtener una visión global de la empresa y, con especial detenimiento, de nuestra unidad, para lo cual el guión de desarrollo del trabajo fue:

  .....

FORMACIÓN

Las horas dedicadas a Formación por el personal de Auditoría y los temas en las que se han empleado han sido:

	Horas totales
Valoración de empresas (seminario)	
Control servicios generales y administrativos (seminario)	
Imagen empresa-medios comunicación (seminario)	
Curso: Marketing de la Auditoría Interna	
Curso: Auditoría de Gestión	
Control de calidad para departamentos de auditoría	
Simpósium	
Curso: Gestores de los años XX	
Curso: Contabilidad Financiera	
Curso: Contabilidad de costes	
Auditoría fiscal (seminario)	

Cumplimiento de la Planificación

Los informes A, B, C y D, previstos en la planificación anual no han sido realizados por las razones siguientes:

- Falta de tiempo.
- Innecesarios.
- Otras prioridades.

Cumplimiento de los Objetivos

OBJETIVO 1

Alcanzar una cobertura anual de los centros productivos y empresas participadas de horas .....

El número de horas empleadas en este objetivo ha sido de .....

OBJETIVO 2

Conseguir que la implantación de las recomendaciones de auditoría se efectúe dentro de los plazos previstos, como mínimo en un 70 por 100 de los casos.

De las recomendaciones formuladas en 20XX se han implantado a 31-12-XX el 60 por 100.

OBJETIVO 3

Desarrollar en su segunda fase el *software* de auditoría informática.

El desarrollo del *software* de auditoría, o la aplicación de la informática como herramienta de la auditoría, es una labor continua que se realiza a medida que las circunstancias o trabajos de auditoría lo requieren.

Durante el pasado año se ha prestado atención especial al programa……

Inventario de Recomendaciones

Recomendaciones aceptadas e implantadas

«Auditoría de...»

Número de recomendación	Texto de la recomendación
……	……

«Auditoría de...»

Número de recomendación	Texto de la recomendación
……	……

«Auditoría de...»

Número de recomendación	Texto de la recomendación
……	……

Recomendaciones aceptadas y en proceso de implantación

……..

Situación de las recomendaciones aceptadas y en proceso de implantación correspondientes a 20XX

Continúan en esta situación las siguientes recomendaciones:

……..

Anexo 9 · Un Programa de Auditoría

Auditoría sobre el área financiera de una empresa industrial

OBJETIVOS

- Determinar si la estructura actual de las distintas unidades del área se ajusta a las necesidades reales de la empresa, con especial atención a la unidad de gestión económico-financiera.
- Evaluar el control interno existente en las diversas unidades encargadas de la gestión de los recursos y tesorería de la empresa.
- Analizar la política financiera seguida en los últimos ejercicios.
- Comprobar la adecuada contabilización de las operaciones financieras.

DESARROLLO DEL PROGRAMA

1. Estructura.
   - 1.1. Analizar el organigrama actual.
   - 1.2. Examinar la plantilla existente en la actualidad, sus distintos niveles y su adecuación a la descripción de funciones anterior.
   - 1.3. Ídem los medios materiales de que disponen las diferentes unidades.
   - 1.4. Ídem los sistemas mecanizados en funcionamiento.
2. Control interno.
   - 2.1. Describir y analizar los procedimientos vigentes en cada unidad (flujogramas).
   - 2.2. Definir los sistemas de información existentes.
   - 2.3. Analizar la información periódica elaborada por las distintas unidades, así como los canales de información utilizados.
   - 2.4. Verificar para los procedimientos aplicados por las distintas unidades que:
     - Todas las operaciones son realizadas por personas autorizadas y aprobadas por los niveles responsables.
     - Todos los documentos y registros permanentes están sometidos a eficaces controles de custodia y de protección física.
     - Todas las operaciones se registran rápida y exactamente en adecuados registros con el detalle suficiente, y se remiten los informes necesarios.
   - 2.5. Verificar que entre las distintas unidades existen la adecuada segregación defunciones y que no se producen duplicidades.
   - 2.6. Realizar las siguientes pruebas y verificaciones en áreas que a continuación se indican:

     2.6.1. Área de presupuesto de Tesorería:
     - Verificar el procedimiento de elaboración de los presupuestos mensuales y anuales, así como las previsiones periódicas de Tesorería de la empresa.
     - Analizar la concordancia entre presupuesto y realidad.

     2.6.2. Área de financiación nacional:
     - Verificar pólizas de préstamos y créditos nacionales, así como las líneas de financiación especial y pagos de las distintas contrataciones.

- Verificar la correcta aplicación de intereses, comisiones y demás cargos derivados de los anteriores conceptos, así como las amortizaciones y desembolsos realizados.
- Verificar los controles existentes sobre los pagos de cupones de obligaciones y demás títulos de renta fija emitidos por la empresa.
- Ídem sobre las emisiones de obligaciones, bonos y pagarés.
- Analizar el control existente en la gestión de títulos de renta variable.

2.6.3. Área de financiación internacional:

- Verificar los contratos y pólizas de créditos extranjeros.
- Verificar la correcta aplicación de los cargos y abonos bancarios por operaciones en divisas, con especial atención a las valoraciones de cambio y a las diferencias de cambio en moneda extranjera.
- Verificar la correcta disposición de los créditos específicos, conciliándola con la ejecución de los presupuestos de inversiones.
- Verificar que se cumplan las condiciones contractuales en lo que se refiere a amortizaciones y desembolsos de los créditos.

3. Política financiera.

3.1. Criterio seguido para determinar el saldo mínimo necesario de liquidez.

3.2. Analizar o calcular, en su defecto, los ratios característicos determinantes dela estructura financiera.

3.3. Analizar la política de financiación por la línea de grandes bienes de equipo.

3.4. Análisis de las condiciones generales de financiación de las compras.

3.5. Realizar el estudio de comparación entre la rentabilidad de los recursos propios y los ajenos (incluyendo en éstos las diferencias de cambio).

3.6. Analizar la gestión en la financiación de nuevos proyectos de inversión.

3.7. Analizar la política seguida en la colocación de recursos propios en las entidades financieras.

3.8. Evaluar el riesgo del negocio bancario existentes con las mismas.

3.9. Criterios seguidos a la hora de elegir el tipo de moneda en los créditos extranjeros.

3.10. Realizar el estudio de comparación entre el coste de los recursos obtenidos con financiación nacional y con financiación extranjera, incluyendo en esta última el coste producido por las diferencias de cambio.

3.11. Analizar la información existente sobre los distintos mercados en los que se puede captar dinero.

3.12. Evaluar la imagen financiera de la empresa.

3.13. Cumplimiento de leyes y normas.

4. Contabilización.

4.1. Verificar que todo el movimiento financiero tiene su adecuado reflejo en la contabilidad, con especial atención al principio del devengo.

4.2. Especial atención al cumplimiento y seguimiento del Plan Contable del Sector.

Anexo 10 · Modelo de desarrollo de una Auditoría

DELIMITACIÓN DEL ÁREA AUDITADA

Auditoría de los Servicios Comerciales (Ventas).

OBJETIVOS

- Conocer la organización actual de los servicios.
- Analizar políticas, normas internas y externas, instrucciones y verificar su cumplimiento y adecuación.
- Procedimientos y sistemas de trabajo empleado.
- Determinar áreas de riesgo y examinar controles establecidos.
- Analizar relaciones con clientes.

INFORMACIÓN PREVIA

- Conocer el mercado de nuestros productos y problemas actuales y futuros.
- Qué información existe en la empresa sobre el particular.
- Qué lugar ocupa la empresa en ese mercado.
- Quiénes son nuestros competidores.
- Cómo actúan y cuál es su organización.
- Cuál es la organización de nuestros servicios comerciales y quiénes son sus hombres-clave.
- Qué informes emiten a la Dirección y a otros servicios.
- Cuál es su presupuesto y desviaciones.
- Etc.

ALCANCE

En esta primera auditoría no analizamos los resultados de los servicios de venta ni la rentabilidad de estos, así como tampoco el grado de penetración en los mercados de nuestros productos. Igualmente, hacemos abstracción de su presentación, envase, embalajes, etc.

PLANIFICACIÓN DE LA AUDITORÍA

- Medios humanos.
- Tiempo de realización.
- Centros u oficinas por visitar.
- Entrevistas a realizar.
- Programa.

  El Programa se desarrolla seguidamente por objetivos:

  Objetivo 1
  - Comprobar si existe Manual de Organización.
  - Verificar su adecuación a la realidad.
  - Si no existe, establecer la organización formal.
  - Determinar la organización informal (quién es quién realmente).

- Canales de comunicación interna y externa.
- Conocer la cultura del servicio:
  - Integración-participación.
  - Creatividad.
  - Gusto por el riesgo.
  - Delegación.
  - Etc.

Síntesis de la información recogida, conclusiones y recomendaciones.

Objetivo 2
- ¿Existen políticas, normas e instrucciones escritas?
- ¿Se conocen por todos?
- ¿Se cumplen?
- ¿Son adecuadas?
- Si no existen, ¿cómo se funciona en la práctica?

Síntesis de la información recogida, conclusiones y recomendaciones.

Objetivo 3
- ¿Hay Manual de Procedimientos?
- ¿Se cumple?
- Si no, ¿por qué razones?
- Si no existe Manual, establecer diagramas funcionales de los principales procedimientos.
- Sistema de ventas, facturación, cobros, reclamaciones, etc.

Síntesis de la información recogida, conclusiones y recomendaciones.

Objetivo 4
- Determinar áreas de riesgo potenciales y reales.
- Puntos de fraude; evaluación de posibles fraudes; fraudes habidos, etcétera.
- Verificar si existen controles y comprobar su funcionamiento.
- Necesidad de otros controles no establecidos.
- Evaluación de áreas de riesgo.

Síntesis de la información recogida, conclusiones y recomendaciones.

Objetivo 5
- ¿Cómo son estas relaciones?:
  - Buenas.
  - Malas.
  - Normales.
- ¿Hay planes de visita y atenciones a clientes?
  Marketing: publicidad, campañas, etc.
- Reclamaciones y deficiencias.
- Cumplimiento de pedidos.
- Precios y condiciones de venta.
- ¿Conocemos a nuestros clientes y ellos a nosotros?

Síntesis de la información recogida, conclusiones y recomendaciones.

SíNTESIS GLOBAL.

DETERMINAR FALLOS Y DEFICIENCIAS.

VERIFICACIÓN Y DISCUSIÓN CON AFECTADOS PARA CONFIRMAR LA CONSISTENCIA DE NUESTRO ANÁLISIS.

REDACCIÓN/INFORME-BORRADOR PARA DISCUSIÓN CON LOS RESPONSABLES DEL ÁREA AUDITADA.

ESTABLECIMIENTO DEL ACTA CON RECOMENDACIONES ACEPTADAS Y PLAZO DE IMPLANTACIÓN, INDICANDO RESPONSABLE Y, EN SU CASO, EXPRESIÓN DE LAS RECHAZADAS CON INDICACIÓN DE LAS RAZONES POR LAS QUE SE RECHAZAN.

ENVÍO DEL INFORME Y ACTA A DIRECCIÓN.

SEGUIMIENTO DE LAS RECOMENDACIONES.

Cómo debe redactarse un informe de auditoría

INTRODUCCIÓN

Este informe ha sido realizado de conformidad con el/la Programa/Planificación Anual de Auditoría 20XX... aprobado por la Comisión de Auditoría/Dirección. El retraso o adelanto con las fechas previstas se ha debido a……

OPINIÓN O DICTAMEN DE AUDITORÍA

Objetivo 1
La organización actual de los Servicios de Ventas no se corresponde con las necesidades de nuestros productos, ni con las características de la organización. Hemos comprobado que las compañías similares del sector operan con una estructura orgánica diferente, lo que está suponiendo unas pérdidas en el ejercicio X que estimamos en XXX euros.

Recomendación
La Dirección Comercial debe estructurar los Servicios de Ventas y de Marketing definiendo claramente sus funciones y atribuciones, y considerar si ambos Servicios no debieran integrarse en uno solo. La Dirección Comercial debe mejorar los canales de información y comunicación.

Objetivo 2
No existe ningún tipo de Norma o Instrucción escrita firmada por la Dirección para regular determinadas operaciones repetitivas. Tampoco hemos observado que se fijen objetivos de venta, anuales o periódicos, ni globales ni parciales.

Recomendación
La Dirección debería establecer la política comercial de la empresa por escrito, para conocimiento de todo el personal. La Dirección de Organización y Servicios debe proponer una Norma de Viajes en Comisión de Servicio. La Dirección de Organización, junto con la Dirección Comercial, deben establecer y concretar objetivos de venta por producto y zona comercial.

Objetivo 3
Los procedimientos son repetitivos y en muchos casos excesivamente farragosos, lo que burocratiza en exceso la operatividad del pedido y un rápido servicio. En este sentido hemos comprobado que algunos clientes han dejado de serlo por la tardanza en recibir pedidos, lo que ha supuesto unas pérdidas de XXX euros/año.

Recomendación
La Dirección de Organización debe analizar los procedimientos actuales, simplificándolos al máximo y eliminando los que sean innecesarios, de acuerdo con la Dirección Comercial.

Objetivo 4
El Control Interno es deficiente: no están definidas atribuciones y responsabilidades de cada Sección y faltan controles para paliar o evitar determinados riesgos (incobrables, fraudes, duplicidad de pedidos), que evaluamos en XXX euros/año.

Recomendación
La Dirección de Control y la Comercial deberán establecer controles para asegurar que no se producen incobrables, creando un mecanismo sistemático de análisis de clientes. Asimismo, conviene publicar un Código de Conducta para el personal comercial, recogiendo la política de la empresa al respecto. Finalmente, la Dirección Comercial debe establecer un procedimiento recogiendo a quien corresponde en cada caso la responsabilidad de admitir un pedido, según la cuantía e importancia de este, señalando plazos para su cumplimentación y entrega.

Objetivo 5
El contacto con los clientes es impersonal y burocrático. No existe una mentalidad de servicio al cliente y los vendedores desconocen los métodos y prácticas que la competencia utiliza y los que teóricamente deben emplearse. Hemos comprobado que existen quejas y reclamaciones varias que no han sido contestadas y, lo que es peor, ni siquiera estudiadas y comprobadas.

Recomendación
Sugerimos que la Dirección Comercial forme convenientemente a sus vendedores, bien por sí mismo, ya recurriendo a compañías de formación y cualificación. Asimismo, debe establecer el procedimiento de estudio y resolución de quejas y reclamaciones, de acuerdo con la política comercial de la empresa.

Anexo 11 · Un Programa de Auditoría de Gestión

Auditorías sobre la gestión de los administradores de una compañía mercantil*

OBJETIVOS

1. Analizar la estructura, composición y funciones del Consejo de Administración.
2. Determinar el coste de su existencia y funcionamiento.
3. Conocer las responsabilidades efectivas de sus miembros y evaluar cómo se han asumido.
4. Determinar si los administradores establecen las políticas, programas y objetivos de la compañía.
5. Comprobar el cumplimiento de leyes y disposiciones administrativas, así como el de normas y procedimientos internos.

DESARROLLO DEL PROGRAMA

1. **Analizar la estructura, composición y funciones del Consejo de Administración.**
   - 1.1 ¿Existen Comisiones específicas dentro del Consejo?
     ¿Comisión ejecutiva?
     ¿Comisión de Auditoría?
     ¿Comisión de control?
     Etc.
   - 1.2 ¿Quiénes son los componentes del Consejo y cuál es su experiencia en gestión y administración de sociedades?
     ¿A quién representan y por qué ostentan tal representación?
     ¿Son a la vez consejeros de otras sociedades?
     ¿Qué participación accionarial tienen en ellas?
   - 1.3 ¿Qué funciones tiene atribuidas el Consejo por leyes o regulaciones reglamentarias?
     ¿Cuáles son en realidad las que efectivamente ejerce?
     ¿Están definidas por escrito las funciones de cada Comisión?
     ¿Cuál es la composición y quién lo preside?
     ¿Constan en las correspondientes actas de las sesiones del Consejo su estructura y las responsabilidades asignadas a las Comisiones?
     ¿Qué funciones realiza la secretaría del Consejo?
2. **Conocer su funcionamiento y el coste de su existencia.**
   - 2.1 ¿Cómo funcionan el Consejo y sus Comisiones?
     ¿Cuántas reuniones se celebran y dónde en cada ejercicio?
     ¿Se levantan actas de todas ellas?

* A los fines de este trabajo de auditoría, se entenderá por administradores a los componentes del Consejo de Administración, incluido su presidente, siendo la compañía en cuestión una sociedad anónima. Esta auditoría únicamente podrá ser realizada por el servicio de auditoría interna de la compañía, a petición expresa del propio Consejo a través de la Comisión de Auditoría, o del presidente del Consejo.

¿La contabilidad de la compañía recoge correctamente los gastos y remuneraciones de los consejeros en concepto de?:
- Contratos de prestación de trabajo.
- Remuneraciones.
- Dietas y gastos de viaje.
- Gastos de representación.
- Pagos en especie:
  · Automóvil.
  · Casas.
  · Vacaciones.
  · Etc.
- Otros gastos:
  · Tarjetas de crédito.
  · Utilización de servicios de la compañía.

¿Cómo funciona la secretaría del Consejo?

¿Existe un secretario no consejero?

¿Hay otros empleados de la compañía al servicio exclusivo del Consejo?

¿Qué servicios utiliza de la compañía?

¿Cuál es el coste de la secretaría del Consejo?

3. Conocer las responsabilidades efectivas de sus miembros y evaluar su desempeño.

3.1 ¿Están definidas por escrito las responsabilidades asignadas a cada miembro del Consejo?

Si lo están, ¿cómo han sido asumidas a lo largo del ejercicio?

Si no lo están, ¿quién asume toda la responsabilidad?:
a) Seguir la Ley de Sociedades Anónimas.
b) Seguir el Código Penal.
c) Otras legislaciones.

3.2 Determinar, a través de la lectura de las actas de las sesiones del Consejo y de sus órganos, quién toma las decisiones y hasta qué punto hay una administración colegiada.
Efectuar las entrevistas y consultar a los miembros del Consejo y a la secretaría, que se consideren necesarias.

4. Determinar si los administradores establecen las políticas, programas y objetivos de la compañía.

4.1 Comprobar si hay políticas, programas y objetivos establecidos formalmente por escrito.

4.2 Conocer quién los establece y cómo se implantan tales políticas, programas y objetivos, y en qué participa, o las determina, el Consejo de Administración.

4.3 Analizar la información que recibe y la que emite el Consejo de Administración, a través de las Actas del Consejo y de la información que se envía a los consejeros.

4.3.1 Si existen Comisión Permanente, Ejecutiva, etc., del Consejo, el auditor debe examinar y analizarlas todas ellas separadamente.

4.3.2 Hacer un inventario de la información ascendente señalando quién y cómo se produce y se remite al Consejo.

4.3.3 Ídem de la información descendente indicando los receptores de esta.

5. **Comprobar el cumplimiento de la legalidad vigente por los administradores, así como el de las normas y procedimientos internos.**

   5.1 Investigar y elaborar la historia de fraudes e irregularidades de la compañía, evaluando su importancia y repercusión en la ética del personal. Esta investigación puede efectuarse tomando el período de los cinco años anteriores al que se realiza esta auditoría, por ejemplo.

   5.1.1 Quién los cometió, dónde y cuánto.

   5.1.2 Por qué ocurrieron (control interno).

   5.1.3 Qué decidió la Dirección.

   5.1.4. ¿Hubo implicación de algún consejero?

   5.2 Determinar si los administradores-consejeros han asumido algún tipo de responsabilidad, según la Ley de Sociedades Anónimas, Texto Refundido de1989.

   5.2.1 Responsabilidad jurídico-societaria.

   5.2.2 Responsabilidad penal.

   5.2.3 Responsabilidad administrativa (Derecho administrativo).

   5.2.4 Responsabilidad fiscal.

   5.2.5 Responsabilidad financiera.

   5.2.6 Responsabilidad medioambiental.

   5.2.7 Responsabilidad laboral.

   5.3 Comprobar si existe un Código de Conducta y analizar sus disposiciones, determinando su observancia o incumplimiento por los afectados, si no es de carácter general para todo el personal de la compañía.

   5.3.1 ¿Hay un órgano, comisión o consejero responsable de su cumplimiento? ¿Qué medidas se han adoptado cuando un consejero lo ha incumplido?

   5.4 Verificar el cumplimiento por los administradores consejeros de las normas de régimen interior y de los procedimientos de la compañía.

   5.4.1 Viajes y desplazamientos.

   5.4.2 Utilización de medios de la compañía.

   5.4.3 Tesorería (anticipos, préstamos, etc.).

   5.4.4 Compras, etc.

Anexo 12 · Un ejemplo de un Programa de formación interna

Plan de formación para personal de un organismo autónomo de la administración que ingresa en la auditoría

1. Deben haber sido convenientemente seleccionados.
2. Supuesto que reúnen los requisitos básicos. ¿Cómo debiera ser un proceso de formación?

   Se supone que conocen la Administración Pública y concretamente el organismo. Si no es así, tendrán que empezar por conocer:

   - Organización del organismo.
   - Funciones.
   - Cultura.
   - Normas.
   - Organización de la unidad de auditoría.
   - Actividades que hace.
   - Información general de interés:
     · Cómo se trabaja.
     · Reglamentos.
     · Vacaciones.
     · Memoria.
     · Informes de otras unidades.
     · Etc.

FORMACIÓN TEÓRICA

- Organización y administración de empresas. Principios.
- Contabilidad general y de costes:
  · Mercado.
  · Precios.
- Teoría económica:
  · Empresa.
  · Demanda, oferta.
  · Etc.
- Relaciones humanas/Habilidades directivas.
- Técnicas de reuniones.
- Redacción de informes.
- Comunicación.

FORMACIÓN EN AUDITORÍA

- Teoría:
  · Qué es la auditoría interna.
  · Qué es la auditoría externa.

  - Funciones.
  - Objetivos.
- Auditoría financiera.
- Auditoría de gestión.
- Manual de auditoría.

FORMACIÓN PRÁCTICA

- Análisis funcional:
  - Flujogramas.
  - Papeles de Trabajo (PP.TT.).
  - Programas de auditoría (elaboración).
- Redacción de informes.
- Reuniones de discusión de informes.
- Técnica de entrevistas.

Este plan puede ampliarse o reducirse según los casos y características de cada organización, y es tan sólo un sencillo ejemplo.

Anexo 13 · Marco de Competencias de Auditoría Interna

PROFESIONALISMO · Competencias requeridas para demostrar la autoridad, credibilidad y conducta ética esencial para una Auditoría Interna valiosa

ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA: CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
Misión de Auditoría Interna	Describir el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna; distinguir entre servicios de aseguramiento y de consultoría.	Demostrar la capacidad de llevar a cabo trabajos tanto de aseguramiento como de consultoría en conformidad con las *Normas.*	Examinar la capacidad de la actividad de auditoría interna de llevar a cabo trabajos tanto de aseguramiento como de consultoría para agregar valor y mejorar las operaciones de la organización.
Estatuto de Auditoría Interna	Describir el propósito de un estatuto de auditoría interna; identificar los elementos requeridos de un estatuto de auditoría interna de acuerdo con las *Normas.*	Preparar un estatuto de auditoría interna en conformidad con las *Normas* y recibir su aprobación por parte del Consejo.	Evaluar y revisar un estatuto de auditoría interna para lograr conformidad con las *Normas* y promover un desempeño de primer nivel.
Independencia dentro de la organización	Describir la importancia de que la actividad de auditoría interna tenga independencia dentro de la organización; identificar injerencias que afectan la independencia.	Detectar cualquier impedimento potencial a la independencia de la auditoría interna y su impacto.	Abordar cualquier impedimento potencial para la independencia de la auditoría interna para alcanzar conformidad con las *Normas;* comunicar el impacto de cualquier impedimento restante.
Objetividad individual	Describir la importancia de la objetividad en auditoría interna; identificar factores que pueden o aparenten ser un impedimiento a la objetiviad.	Detectar y gestionar cualquier impedimiento real o percibido a la objetividad individual del auditor interno; evaluar y mantener la objetividad de auditoría interna.	Desarrollar y mantener políticas internas que rijan la objetividad; recomendar estrategias para promover la objetividad.
Compromiso ético	Describir la importancia de un código de ética para auditores internos; identificar los principios del Código de Ética del IIA.	Demostrar cumplmimiento individual con el Código de Ética del IIA.	Evaluar la conformidad de la actividad de auditoría interna con el Código de Ética del IIA; recomendar estrategias para mantener y promover los más altos estándares éticos para auditores internos y la actividad de auditoría interna.
Debido cuidado profesional	Describir el debido cuidado profesional.	Demostrar el debido cuidado profesional.	Evaluar y concluir sobre la aplicación del debido cuidado profesional.
Desarrollo profesional	Reconocer los conocimientos, las habilidades y las competencias necesarias para cumplir las responsabilidades de la actividad de auditoría interna y la necesidad de desarrollo profesional continuo.	Demostrar competencia de auditoría interna a través de desarrollo profesional continuo.	Evaluar las competencias requeridas para cumplir con las responsabilidades de la actividad de auditoría interna; promover el desarrollo profesional.

DESEMPEÑO · Competencias requeridas para planear y realizar trabajos de auditoría interna de conformidad con las *Normas*.			
ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
Gobernanza en la organización	Describir el concepto de gobernanza en la organización.	Detectar riesgos relacionados a las políticas, los procesos y las estructuras de gobernanza en la organización.	Recomendar mejoras a las políticas, los procesos y las estructuras de gobernanza en la organización.
Fraude	Reconocer tipos de fraude, riesgos de fraude y alertas o señales de fraude.	Evaluar el potencial de fraude y cómo la organización detecta y gestiona los riesgos de fraude; recomendar controles para prevenir y detectar fraude; educar para enriquecer la concienciación de fraude en la organización.	Aplicar técnicas de auditoría forense en prevención, disuasión e investigación de fraude.
Gestión de riesgos	Describir conceptos fundamentales de riesgo y gestión de riesgo; describir marcos de gestión de riesgo.	Utilizar un marco de gestión de riesgos para identificar amenazas potenciales; examinar la efectividad de la gestión de riesgos dentro de procesos y funciones.	Evaluar los métodos usados para evaluar la efectividad de la identificación y gestión de riesgos.
Control interno	Identificar tipos de controles.	Usar un marco de control interno para examinar la eficacia y eficiencia de controles internos.	Evaluar y recomendar mejoras al marco de control interno de la organización; evaluar la implementación de la organización sobre su marco de control interno.
Planificación del trabajo · Objetivos y alcance · Evaluación de riesgos · Programa de trabajo · Recursos	Describir roles y actividades clave para establecer los objetivos, criterios de evaluación y alcance de un trabajo.	Determinar los objetivos, criterios de evaluación y alcance de un trabajo.	Evaluar los objetivos y el alcance del trabajo de auditoría para asegurar la calidad del trabajo.
	Describir el propósito y los pasos involucrados de realizar una evaluación de riesgo durante la planificación del trabajo.	Completar una evaluación de riesgo detallada, que incluya priorizar riesgos y controles clave.	Evaluar el proceso de evaluación de riesgos durante el trabajo de auditoría.
	Describir el propósito y componentes clave de un programa de trabajo de auditoría	Preparar un programa de trabajo de auditoría.	Evaluar el programa de trabajo de auditoría.
	Describir los factores que influyen en la planificación de personal y recursos para un trabajo.	Determinar personal y recursos para un trabajo.	Evaluar personal y recursos para un trabajo.

DESEMPEÑO · Competencias requeridas para planear y realizar trabajos de auditoría interna de conformidad con las *Normas*.

ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA: CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
	Describir el propósito de encuestas preliminares del área de trabajo, listas de verificación y cuestionarios de riesgo y control.	Elaborar una encuesta preliminar del área del trabajo; desarrollar listas de verificación y cuestionarios de riesgo y control; examinar información relevante durante un trabajo de auditoría interna.	Evaluar actividades para la recopilación de información.
	Describir las diversas técnicas de muestreo, así como las ventajas y desventajas de cada una.	Aplicar técnicas de muestreo apropiadas.	Evaluar técnicas de muestreo utilizadas en el trabajo de auditoría interna.
Trabajo de campo · Recopilación de información · Muestreo · Herramientas y técnicas de auditoría asistida por computación · Analítica de datos · Evidencia · Mapeo de procesos · Revisión analítica · Documentación	Describir el propósito, ventajas y desventajas de usar herramientas y técnicas de auditoría asistida por computación.	Usar herramientas y técnicas de auditoría asistida por computación.	Evaluar el uso de herramientas y técnicas de auditoría asistida por computación durante los procedimientos del trabajo de auditoría.
	Describir qué es analítica de datos, el proceso de analítica de datos y la aplicación de métodos de analítica de datos en auditoría interna.	Aplicar métodos de analítica de datos.	Evaluar el uso de analítica de datosen auditoría interna.
	Reconocer fuentes potenciales de evidencia.	Evaluar la relevancia, suficiencia y confiabilidad de fuentes potenciales de evidencia.	Desarrollar pautas para asegurar que la evidencia sea relevante, suficiente y confiable.
	Describir el propósito, las ventajas y desventajas de diversas técnicas de mapeo de procesos.	Aplicar enfoques analíticos apropiados y técnicas de mapeo de procesos.	Evaluar el mapeo de procesos del trabajo de auditoría.
	Describir el propósito, ventajas y desventajas de diversas técnicas de revisión analítica.	Determinar y aplicar técnicas de revisión analítica.	Evaluar técnicas de revisión analítica implementadas durante el trabajo de auditoría.
	Describir requisitos de papeles de trabajo y documentación.	Preparar papeles de trabajo y documentación.	Evaluar documentación del trabajo de auditoría.

DESEMPEÑO · Competencias requeridas para planear y realizar trabajos de auditoría interna de conformidad con las *Normas*.

ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
Resultados del trabajo · Calidad de las comunicaciones · Conclusiones · Recomendaciones · Informes · Riesgo residual y aceptación de riesgos · Plan de acción de la dirección · Seguimiento de resultados	Describir los elementos de calidad en las comunicaciones del trabajo.	Demostrar calidad en las comunicaciones del trabajo, incluyendo la comunicación con los clientes del trabajo en la etapa preliminar.	Evaluar las comunicaciones del trabajo de auditoría.
	Reconocer los elementos de una conclusión apropiada del trabajo.	Resumir y desarrollar las conclusiones del trabajo.	Evaluar las conclusiones del trabajo de auditoría.
	Reconocer la importancia de brindar recomendaciones.	Formular recomendaciones para mejorar y proteger el valor de la organización.	Evaluar recomendaciones del trabajo de auditoría.
	Describir el proceso de comunicación e informe de resultados, que incluye informes interinos, la reunión de cierre, obtener la respuesta de la gerencia, el proceso de aprobación del informe y la distribución del mismo.	Preparar un informe interino; preparar un informe de auditoría final, buscar aprobación y distribuir a las partes correspondientes.	Revisar y aprobar informes del trabajo, recomendar distribución del informe a las partes correspondientes.
	Describir la responsabilidad del Director de Auditoría Interna (DAI) sobre la identificación y evaluación de riesgo residual y el proceso de comunicar la aceptación de riesgo por parte de la gerencia.	Identificar el riesgo residual.	Revisar y aprobar informes deltrabajo, recomendar distribución del informe a las partes correspondientes.
	Describir los resultados del trabajo; describir el propósito de un plan de acción por parte de la gerencia.	Evaluar los resultados del trabajo; incluso el plan de acción de la gerencia.	Evaluar los resultados colectivos de trabajos realizados por la actividad de auditoría interna.
	Reconocer la importancia de la supervisión y el seguimiento de la disposición de los resultados del trabajo de auditoría comunicados a la gerencia y al Consejo.	Dirigir la supervisión y el seguimiento de la disposición de los resultados del trabajo de auditoría comunicados a la gerencia y al Consejo.	Evaluar la supervisión y seguimiento realizado por la actividad de auditoría interna.

AMBIENTE · Competencias requeridas para identificar y abordar los riesgos específicos de la industria y el ambiente en el que opera la organización.			
ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
Planificación y gestión estratégica de la organización · Estructura · Medidas de desempeño · Comportamiento organizacional · Liderazgo	Identificar las implicaciones de distintas estructuras organizacionales sobre riesgo y control.	Evaluar la estructura de gobierno corporativo de la organización y el impacto de la estructura, así como la cultura organizacional en el entorno general de control y la estrategia de gestión de riesgos.	Recomendar mejoras a la estrategia general de gestión de riesgos y el entorno de control.
	Describir la planificación estratégica de la organización.	Analizar el proceso de planificación estratégica de la organización.	Recomendar mejoras para el proceso de planificación estratégica de la organización.
	Describir parámetros comunes para medidas de desempeño.	Examinar medidas de desempeño usadas por la organización.	Seleccionar medidas de desempeño apropiadas.
	Explicar técnicas de gestión del comportamiento y desempeño organizacional.	Examinar técnicas existentes de gestión del comportamiento y desempeño organizacional.	Recomendar técnicas apropiadas de gestión del comportamiento y desempeño organizacional.
	Describir la efectividad de la gerencia para liderar y construir compromiso organizacional.	Examinar la eficacia de la gerencia para liderar y construir compromiso organizacional.	Recomendar acciones para mejorar el enfoque de la gerencia para liderar y desarrollar el compromiso organizacional.
Procesos empresariales comunes	Describir las implicaciones de riesgo y control de procesos institucionales comunes (recursos humanos, compras y contratación, desarrollo de productos, gestión de proyectos, ventas, mercadotecnia, logística, administración de procesos tercerizados, etc.)	Examinar los riesgos y controles relacionados con los procesos institucionales.	Recomendar acciones para abordar riesgos relativos a los procesos institucionales.
Responsabilidad social	Describir la responsabilidad social de las empresas y la sostenibilidad.	Examinar el enfoque de la organización respecto a la responsabilidad social y a la sostenibilidad.	Recomendar acciones para mejorar enfoque de la organización respecto a la responsabilidad social y a la sostenibilidad.
Tecnología de información · Análisis de datos · Seguridad y privacidad · Marcos de control de TI	Describir los conceptos básicos de TI y análisis de datos.	Utilizar análisis de datos y TI en auditoría.	Evaluar el uso de análisis de datos y TI en auditoría.
	Describir los diversos riesgos relacionados con TI, seguridad de información y privacidad de datos.	Identificar y evaluar los diversos riesgos relacionados con TI, seguridad de información y privacidad de datos.	Recomendar acciones para abordar riesgos de TI, seguridad de información y privacidad de datos.
	Reconocer el propósito y las aplicaciones de marcos de control de TI y los controles básicos de TI.	Aplicar marcos de control de TI.	Evaluar el uso de marcos de control de TI.
Contabilidad y finanzas	Identificar diversos conceptos de contabilidad general y financiera y los principios subyacentes.	Realizar análisis financieros; examinar e interpretar estados contables.	Evaluar la fiabilidad de los estados financieros y proporcionar aseguramiento.

LIDERAZGO Y COMUNICACIÓN · Competencias requeridas para dar dirección estratégica, comunicar con eficacia, mantener relaciones y administrar el personal y los procesos de auditoría interna.			
ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
Planificación estratégica y gestión de auditoría interna	Reconocer la importancia de alinear el plan estratégico de auditoría interna con la estrategia de la organización.	Crear el plan estratégico de auditoría interna alineado con la estrategia, el perfil de riesgo y la estrategia de gestión de riesgos de la organización; crear un presupuesto eficaz y eficiente para la actividad de auditoría interna.	Evaluar el plan estratégico de auditoría interna; evaluar y recomendar mejoras al presupuesto de la actividad de auditoría interna.
	Diferenciar diversos roles de auditoría interna, incluido el del supervisor del trabajo y del DAI.	Administrar el personal de auditoría interna (incluye reclutamiento,desarrollo, motivación, gestión de conflictos, creación de equipos y plan de sucesión); crear políticas y procedimientos para dirigir operaciones de auditoría interna.	Evaluar esfuerzos de administración de talento de la actividad de auditoría interna; evaluar políticas, procedimientos y actividades administrativas de la actividad de auditoría interna.
	Identificar actividades clave en la supervisión de trabajos.	Supervisar trabajos.	Evaluar actividades de supervisión de trabajos para asegurar la calidad de la actividad de auditoría interna.
Plan de auditoría y coordinación de esfuerzos de aseguramiento	Identificar fuentes de potenciales trabajos de auditoría que incluyan tendencias de industria y riesgos emergentes.	Realizar una evaluación de riesgos, priorizar trabajos, desarrollar un plan de auditoría basado en riesgos y obtener aprobación del Consejo.	Evaluar y revisar un plan de auditoría interna basado en riesgos para satisfacer las necesidades cambiantes de la organización.
	Describir la coordinación de esfuerzos de auditoría interna con el auditor externo, órganos de supervisión regulatoria y otras funciones internas de aseguramiento y posible dependencia con otros proveedores de aseguramiento.	Preparar un mapa de aseguramiento de riesgos.	Coordinar esfuerzos de aseguramiento con otros proveedores para garantizar una cobertura adecuada y minimizar la duplicación de esfuerzos.
Programa de Aseguramiento y Mejora de la Calidad	Describir requisitos del Programa de Aseguramiento y Mejora de la Calidad.	Programar y completar evaluaciones de calidad internas y externas para cumplir requisitos e informar resultados.	Evaluar las prácticas de aseguramiento y mejora de la calidad de la actividad de auditoría interna y evaluar su conformidad con las *Normas*.
	Identificar la divulgación apropiada de conformidad versus no conformidad con las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna* del IIA.	Formular divulgaciones apropiadas de conformidad versus no conformidad con las *Normas*.	Evaluar las divulgaciones de la actividad de auditoría interna sobre conformidad versus no conformidad con las *Normas*.

LIDERAZGO Y COMUNICACIÓN · Competencias requeridas para dar dirección estratégica, comunicar con eficacia, mantener relaciones y administrar el personal y los procesos de auditoría interna.

ÁREA DE CONOCIMIENTO	NIVEL DE COMPETENCIA: CONOCIMIENTO GENERAL	CONOCIMIENTO APLICADO	EXPERTO
	Reconocer el valor de fomentar y promocionar y la importancia de mantener relaciones con las partes interesadas (por ejemplo, Consejo, alta dirección, clientes de auditoría, otros proveedores de aseguramiento o terceros).	Administrar la reputación de la actividad de auditoría y expectativas de las partes interesadas; demostrar sinceridad, honestidad y empatía en comunicaciones con las partes interesadas para construir confianza y mantener relaciones.	Evaluar relaciones con las partes interesadas y recomendar acciones para lograr mejoras; evaluar esfuerzos de defensa y promoción de la actividad de auditoría interna.
Comunicación · Fomentación y promoción · Relaciones · Informes · Habilidades interpersonales · Innovación	Describir comunicaciones apropiadas entre auditores internos y partes interesadas, que incluyen indicadores clave de desempeño; reconocer que el DAI informa sobre la efectividad general de los procesos de control interno y gestión de riesgos de la organización a la alta dirección y al Consejo.	Preparar comunicaciones relevantes y apropiadas para las partes interesadas, incluso informes a la alta dirección y al Consejo (por ejemplo, perfil de riesgos significativos e indicadores clave del desempeño)	Evaluar las comunicaciones de auditoría interna con las partes interesadas, incluyendo indicadores clave de desempeño para evaluar el éxito de la actividad de auditoría interna y recomendar mejoras.
	Reconocer la importancia de habilidades de comunicación escrita y oral, incluso habilidades interpersonales tales como gestión de conflictos, influencia y persuasión.	Demostrar habilidades interpersonales (gestión de conflictos, influencia y persuasión); proporcionar consultoría perspicaz para contribuir a la efectividad de la organización; detectar oportunidades de cambio y facilitar el mismo.	Evaluar las habilidades de comunicación escrita y oral de la actividad de auditoría interna, sus habilidades interpersonales e innovación; recomendar mejoras.

NOTA: Se asume que un auditor interno en el nivel de competencia "Conocimiento Aplicado" en determinada área también tendría un nivel de "Conocimiento General" en ésta misma área. Del mismo modo, un auditor interno en el nivel de competencia "Experto" a su vez también tendría un nivel de "Conocimiento Aplicado" en la misma área de conocimiento.

Fuente: FLAI

Anexo 14 · Ejemplo de un Código de Conducta

Es un documento en el que se determinan las obligaciones que los empleados de una organización o empresa tienen para con ésta, con independencia de cualquier otro compromiso social, político o económico.

La infracción u olvido de las disposiciones del Código debe considerarse falta grave, y puede comportar de forma automática la expulsión del empleado que incurre en falta, de la organización o empresa.

Dicho Código debe redactarse y establecerse de acuerdo con las leyes y reglamentos de cada país y negociado con los Sindicatos, si procede, para que su aplicación sea realmente efectiva.

A modo de ejemplo, damos las líneas generales de lo que pudiera ser un Código de Conducta de una empresa:

«La ética de esta organización se basa fundamentalmente en los siguientes principios, que deben prevalecer sobre cualquier otra consideración:

- El respeto a los compromisos adquiridos.
- El cumplimiento estricto de los contratos, convenios, pactos, etc.
- El sometimiento a las leyes y disposiciones vigentes.
- Dar a nuestros clientes las mejores calidades en productos o servicios y según las condiciones de los mercados y sin precios abusivos.
- No cometer fraudes, realizar sobornos, ofrecer comisiones o aceptar prebendas que perjudiquen a terceros u otras empresas.

Las exigencias anteriores, que la organización se impone a sí misma, dan fuerza moral a la Dirección para establecer las siguientes normas al personal empleado, cualquiera que sea su categoría, actividad, funciones y responsabilidades en la empresa:

- La conducta desleal con la empresa será objeto de sanción o despido automático, una vez debidamente demostrada. En cualquier caso, la simple sospecha de tal comportamiento permitirá a la Dirección ordenar el cese provisional del personal afectado, en su actividad y puesto habituales. Corresponderá a la Auditoría Interna efectuar las investigaciones correspondientes, proponiendo a la Dirección la suspensión temporal del personal afectado.
- El incumplimiento de las normas y procedimientos establecidos es conducta desleal.
- Ningún empleado aceptará comisiones, obsequios, sobornos, ventajas o condiciones especiales para su persona o familia, de personal, empresas u organizaciones que tengan relación comercial o contractual con la empresa. La conducta que exige la empresa es devolver incluso lo que se haya recibido, exponiendo las razones de tal devolución o rechazo.
- La transmisión o facilitación de información confidencial a terceros, e incluso a miembros de la propia organización, está prohibida. Es información confidencial la que circule con tal carácter, y la que sin recibir esta denominación coloca a terceros en posición ventajosa para contratar o comerciar con la empresa, o infringe el espíritu de las normas, políticas e instrucciones establecidos dentro de la organización.
- Ningún empleado de la empresa podrá trabajar en otra empresa o institución, sin la autorización de la Dirección. Asimismo, las Direcciones deberán ser informadas del ejercicio de cargos políticos o representativos.

- Los fraudes, robos y sustracciones de cualquier herramienta, material, equipo, prendas, etc., de la empresa serán objeto de despido automático, salvo cuando el material sea de pequeño valor, en cuyo caso será amonestado o, en su caso, sancionado.
- Ningún empleado facilitará información sobre sistemas, métodos, patentes, procedimientos, etc., a empresas de la competencia o a cualquier otra organización.»

Como se desprende de la lectura de las anteriores disposiciones, éstas pueden ampliarse o pormenorizarse mucho más, según lo exijan las características de la empresa, su actividad o los criterios de la Dirección.

La finalidad de un Código de Conducta es señalar claramente las reglas de comportamiento que la Dirección espera y exige de todo el personal de una organización. Y cuando escribimos todo se entiende que compromete tanto a los más altos cargos y niveles de la organización, como a los más bajos. Ha de ser redactado de manera que pueda entenderse fácilmente su contenido, sin terminología legal o complicada y refiriéndose concreta y claramente a cada situación. Como se recoge en la publicación de la serie de monografías del Institute of Internal Auditors (IIA), ***Cómo desarrollar un Código de Conducta,*** *"un Código de Conducta debe ser informativo, fácil de leer y entender; debe ser escrito para que sea aplicable a todos los empleados y debe dirigirse a situaciones prácticas que involucren a todo el personal, desde el obrero de planta hasta el director general.*

La mayoría de las organizaciones tienen decenas de políticas, procedimientos, requerimientos, que regulan cómo los empleados deben realizar su trabajo. El Código de Conducta no es el lugar para reproducirlos todos; al contrario, un resumen de áreas de ética importantes que se comprenden en estos otros documentos es suficiente".

Las ventajas de un Código de Conducta son, entre otras menos significativas, las que enumeramos seguidamente:

- Mejora la imagen de la organización y aumenta la confianza de los inversores y clientes.
- Contribuye a fortalecer la moral y ética de los empleados, posibilitan la cooperación y el trabajo en equipo.
- Posibilita la formación del personal en materia de lucha contra el fraude y las irregularidades.
- Contribuye a la total transparencia y claridad de las actividades de la organización.
- Predispone a la Administración Pública favorablemente respecto a la organización, en sus requerimientos legales y administrativos.

Anexo 15 · Revisión Interna de la Auditoría (Autoevaluación de la auditoría) Ejemplo

OBJETIVOS

1. Evaluar el grado de credibilidad, conocimiento y confianza de la Auditoría en la Empresa y fuera de ella.
2. Evaluar la profesionalidad del trabajo de Auditoría.
3. Determinar la adecuación de la estructura y funciones de la Unidad a las necesidades reales y al entorno actual.
4. Determinar los costes y su incidencia en los resultados de la Empresa.
5. Examinar y evaluar el nivel de supervisión de los trabajos de Auditoría.
6. Analizar la entidad de las recomendaciones, su seguimiento y el grado de implantación.
7. Analizar la política de formación del personal de la Unidad.
8. Analizar otras actividades que se realicen en la Auditoría, si las hubiese.

PROGRAMA

1. **Evaluar el grado de credibilidad, conocimiento y confianza de la Auditoría en la Empresa y fuera de ella.**

   1.1 Evaluación del conocimiento de la Auditoría dentro de la empresa.
   - Inventariar la información periódica que se emite y a quien se envía.
   - Relacionar las áreas de la Empresa que históricamente han tenido poco o ningún contacto con Auditoría.
   - Determinar si deben ser auditadas y por qué no lo han sido hasta la fecha.
   - Evaluar y ponderar el conocimiento y la receptividad que tienen las distintas áreas de la Empresa respecto a la Auditoría.
   - Determinar los niveles jerárquicos y estructurales a los que llega este conocimiento.
   - Cultura de Auditoría en la Empresa.

   1.2 Evaluación de la credibilidad y confianza que tiene la Auditoría en la Empresa.
   - Determinar la proyección de la imagen de Auditoría a la Dirección y al resto de las áreas de la Empresa, de acuerdo con la evaluación de las siguientes variables:
     · Actitud del Director de Auditoría.
     · Actitud del resto del personal de Auditoría.
     · Funcionamiento de Auditoría.
     · Informes encargados por la Dirección.
   - Confianza en la Auditoría:
     · De la Dirección.
     · De los ejecutivos y mandos.
     · De los auditores externos.

   1.3 Evaluación del conocimiento y credibilidad de Auditoría fuera de la Empresa.
   - Inventariar las empresas, organismos y entidades con las que tiene o ha tenido alguna relación Auditoría.

- Señalar el tipo de relación existente y según el mismo ponderar el conocimiento y la credibilidad.
- Publicaciones, intervenciones públicas de alguno de sus miembros, seminarios, etc.
- Liderazgo del Departamento en la profesión.

2. Evaluar la profesionalidad del trabajo de Auditoría.

2.1 Métodos y técnicas empleadas.
- Planificación estratégica y Programa Anual. Análisis.
- Determinar la suficiencia o insuficiencia de la dotación de medios materiales.
- Sometimiento a las Normas incluidas en el *Marco Internacional para la Práctica Profesional de la Auditoría Interna.*
- Analizar si son empleadas correcta y unificadamente las técnicas y métodos más usuales en Auditoría.
- Estudiar si el archivo está suficientemente organizado para garantizar el adecuado funcionamiento de la Unidad.
- Cumplimiento del Código de Ética.

2.2 Informes.
- Inventariar los informes realizados en los últimos tres años, ponderando el grado de importancia de estos en función de la entidad de las áreas auditadas y del riesgo cubierto, cuantificado el mismo en la medida de lo posible.
- Analizar si la estructura actual de los informes es la más adecuada.
- Procedimientos de elaboración y discusión de los informes.

2.3 Memoria Anual.
- Analizar si la estructura actual es la más adecuada.
- Analizar el proceso de distribución.

3. Determinar la adecuación de la estructura y funciones de la Unidad a las necesidades reales y al entorno actual.

- Analizar el actual Manual de Organización comprobando:
  · Si el organigrama se ajusta a la estructura real de la Unidad.
  · Si las funciones son las más adecuadas en razón de la formación, conocimiento y categoría de las personas que componen la Unidad.
  · Si la organización actual está dentro de las exigencias de la Empresa.
- Proponer la organización más adecuada.

4. Analizar los costes y su incidencia en los resultados de la Empresa.

- Actualizar los datos sobre costes de la Unidad partiendo del último trabajo realizado en el año 20XX.
- A la vista de los datos, obtener ratios relativos a:
  · Coste por informe.
  · Coste por recomendación.
  · Coste por hora.
  · Etc.
- Cuantificar, en la medida de lo posible, el beneficio que supone para la Empresa el trabajo de Auditoría: por facturación de servicios o por ahorro indirecto.

- Evaluar, en función de los anteriores datos, y en relación con las conclusiones del epígrafe 2.2 («Calidad de los informes»), la aportación y significación de Auditoría Interna para la Empresa.

5. Examinar y evaluar el nivel de supervisión de los trabajos de Auditoría.
   - Determinar el nivel de supervisión existente mediante la evaluación de los siguientes puntos de control:
     · Adecuada planificación a las necesidades y riesgos potenciales.
     · Concreción y claridad en las instrucciones para realizar los trabajos a los auditores.
     · Programas detallados del trabajo para cada área.
     · Revisión de papeles de trabajo, soportes, etc.
     · Control de informes.
     · Control de recomendaciones.
     · Controles de tiempo de trabajo.
     · Controles de gastos.
     · Controles de eficacia de los auditores en la realización de sus trabajos.
     · Memorias periódicas.
   - Analizar la supervisión ejercida sobre la Unidad por la Dirección y la Comisión de Auditoría.

6. Analizar la entidad de las recomendaciones. Su nivel de seguimiento y el grado de implantación.
   - Efectuar un inventario de las recomendaciones formuladas en los últimos tres años, ponderando su entidad.
   - Revisar el procedimiento actualmente establecido en el MOPE de discusión de informes y seguimiento de recomendaciones.
   - Determinar si el seguimiento que actualmente se realiza es suficiente para asegurar la fiabilidad de este.
   - En el inventario descrito en el primer punto determinar el grado de implantación reflejado en las Memorias.
   - Analizar las desviaciones producidas respecto a lo reflejado en la Memoria respecto a la realidad.
   - Determinar el cumplimiento de los plazos de implantación según lo estipulado en las Actas de discusión de los informes.
   - Revisar, si existe, el procedimiento de seguimiento de la implantación.

7. Analizar la política de formación del personal de la Unidad.
   - Examinar el Programa de Formación.
   - Inventariar los cursos y los asistentes de los tres últimos años.
   - Evaluar la utilidad y aprovechamiento reportadas para el asistente a través de un cuestionario a aplicar al respecto.
   - Evaluar el aprovechamiento del curso por el resto del personal de Auditoría.
   - Analizar el aspecto cuantitativo y cualitativo de la formación en Auditoría.

8. Analizar otras actividades que se realizan en Auditoría.
   8.1. Participación en Comités, Grupos de Trabajo, etc.
   8.2. Participación en actos externos.
   8.3. Representación en organismos externos (organizaciones y colegios profesionales, etc.)
   8.4. Otras actividades.

Anexo 16 · La Auditoría Interna y las Empresas Pequeñas

Cuando escribimos *empresas pequeñas* queremos englobar con esta expresión a todas las que pueden catalogarse por su condición de tales, es decir, lo pequeño las caracteriza, por su tamaño físico, número de empleados, volumen de negocio, capacidad de influir en su mercado, etc. No nos interesa entrar en precisar una definición, ni hablar de pequeñas y medianas empresas, sino tan sólo considerar que sean realmente empresas y, partiendo de este planteamiento, tratar de llegar a algunas conclusiones referidas a en qué medida y de qué forma es posible utilizar en ellas la función de Auditoría Interna.

Por tanto, estamos hablando de estructuras empresariales, no de negocios o actividades lucrativas, puesto que éstos se pueden manejar sin organización, o con una mínima gestión informal; pero una empresa, cualquiera que sea su tamaño, exige un sistema de dirección que actúe sobre el soporte de ese sistema, que es justamente su organización.

En nuestra opinión, las siguientes características, todas o la mayor parte de ellas, indican la existencia de una estructura empresarial:

- Hay un nivel de organización, más o menos desarrollado, al servicio de una intención creadora de riqueza.
- Existe una dirección que gestiona los medios humanos y materiales de esa organización.
- Cuenta con personal asalariado externo y no tan sólo con empleados familiares.
- Tiene necesidades financieras que satisface a través del sistema bancario y crediticio.
- Cumple sus obligaciones cívicas y sociales con la Administración, con sus empleados, con sus clientes (proveedores, accionistas, bancos, solicitantes de información, etc.).
- Se ha creado mediante la aportación de un propietario o de varios, tanto en capital como en trabajo, y supone un riesgo frente a la incertidumbre del mercado.
- Sus actividades están ordenadas a la consecución de fines determinados.
- Nace con vocación de continuidad o permanencia.

¿Es necesaria la Auditoría Interna en las PYME?

Con la estructura que acabamos de señalar es indudable que existen en España y en todo el mundo una multitud de empresas pequeñas, que en sectores diversos producen, distribuyen, comercializan, venden servicios, etc., y es asimismo cierto que en todas ellas la función de control interno, es decir, el que tendría que ejercer su propia dirección es vital, o sea, es necesario para asegurar su permanencia. La pregunta entonces sería, ¿puede darse un buen sistema de control interno sin utilizar la función de Auditoría Interna? Creemos que no; en consecuencia, esta función auditora, como un instrumento más de los que utilizan los gestores modernos, puede ser implantada en todas las organizaciones con independencia de su tamaño.

En este sentido, hemos venido proclamando desde los tiempos en que desarrollamos la primera organización empresarial española de la pequeña y mediana empresa, que no es razón suficiente escudarse en la dimensión para decir, esta técnica, estos métodos y sistemas que emplean las grandes empresas no son adecuados para las pequeñas. Por el contrario, creemos que pueden y deben aplicarse también en las de pequeño tamaño, a condición de que sean adaptados a sus necesidades y características con criterios eminentemente prácticos, económicos y de fácil implantación.

Es lo que con estos comentarios quisiéramos explicitar: cómo los propietarios de empresas pequeñas podrían usar los servicios de auditoría interna y cómo adaptar la función a las necesidades y características de empresas de esta naturaleza.

Cómo puede utilizarse

La función de Auditoría Interna en este tipo de empresas puede utilizarse externalizándola, recurriendo a la contratación temporal de auditores internos independientes, lo cual es de por sí un problema porque no estamos pensando en las grandes compañías de auditoría y consultoría, sino en profesionales de probada experiencia en auditoría interna que, en la actualidad, estén dispuestos a prestar estos servicios porque disponen de tiempo y libertad para ello y están actuando como profesores en seminarios o escuelas de formación posuniversitarias o tienen su propia pequeña compañía de asistencia, o son prejubilados o jubilados, que han pertenecido a importantes departamentos de Auditoría Interna y, en definitiva, están «en forma» y actualizados profesionalmente, entre otras cosas porque son miembros del IAI, participan en sus actos y actividades y, además, son poseedores de diplomas y certificaciones que les acreditan como especialistas en auditoría interna.

El IAI conoce algunos de estos profesionales, cuyos honorarios serán, tienen que serlo, infinitamente más reducidos y al alcance de las posibilidades de estas empresas de pequeña dimensión, que las facturaciones de las grandes consultoras, en el supuesto poco probable de que éstas dispongan de verdaderos auditores internos habituados a trabajar en pequeñas unidades como las que son objeto de estos comentarios.

Además, la prestación de servicios de consulta a las empresas pequeñas, ha de serlo a bajo coste de facturación, con disposición total del tiempo del auditor, pago del servicio a tanto alzado y no por horas, dentro de cierta flexibilidad, y máxima transparencia en la información y comunicación del auditor con la propiedad de la empresa, que será quien haya decidido la contratación de tales servicios, ya que un gerente o director creemos que no será partidario de que alguien ajeno a la empresa la audite, máxime cuando ésta no está obligada legalmente a la revisión de sus estados financieros por auditores de cuentas externos.

Otra forma de recurrir a los servicios de Auditoría Interna, que es la que la doctrina recomienda para las grandes corporaciones y cómo éstas la utilizan, es la implantación de la función de forma permanente, realizada por personal de la empresa, que se dedica única y con exclusión de cualesquiera otras responsabilidades, al ejercicio de las amplias y diversas competencias que abarca el marco conceptual moderno de la Auditoría Interna. En el supuesto de las empresas pequeñas no es fácil encontrar las que puedan disponer de un servicio, o de una persona, cuyo trabajo consista en la práctica de la auditoría, sin ningún otro cometido dentro de la gestión de la compañía.

Tengamos en cuenta que, por lo general, como hemos dicho, no se lleva a cabo ninguna auditoría externa para la revisión de sus cuentas, salvo por exigencias bancarias a la hora de solicitar apoyos financieros y, en consecuencia, la palabra auditoría, tanto interna como externa, no les dice gran cosa, lo que significa que la función les suena a música celestial.

Desde este planteamiento no es aventurado suponer que sería prioritario para implantar la auditoría interna o utilizarla en estas empresas explicar lo que es, cómo se practica y qué puede aportar a sus resultados y a su supervivencia, lo que comportaría la designación de un responsable, y así suele ocurrir según mi propia experiencia. Es práctica habitual –cosa lógica dada la reducción de sus plantillas– asignar varias funciones a una misma persona o unidad, lo que probablemente originará debilidades de control

por carencia de la necesaria segregación de estas, una razón más, entre otras, que podrían aducirse para justificar la utilización de la auditoría interna en estas empresas. Así, por ejemplo, el concepto de control interno actualmente aceptado en todo el mundo es igualmente válido para ellas porque, grandes o pequeñas, sus direcciones deben trabajar y tomar decisiones sobre la base de una información fiable, con una gestión eficiente y cumpliendo las regulaciones de control externo que les afecten. Éste es justamente el contenido del aseguramiento, que junto con la evaluación de riesgos y la consultoría son funciones de la Auditoría Interna.

Quién y cómo implantarla

Entramos en el meollo de la cuestión que debatimos, es decir: ¿quién podría asumir el compromiso de implantar la Auditoría Interna en la organización, utilizando sus métodos y desde la independencia y objetividad?

Creemos que el propietario, o un accionista, capacitados para ello y con ganas de hacerlo porque ser empresario es un trabajo bien difícil y un buen empresario, en principio, podría hacer de auditor, que en el supuesto que nos ocupa sería, pues, que conoce la empresa, su negocio y su personal, una apuesta que, a buen seguro, ganaría. Estamos pensando en situaciones límite, puesto que, en la medida en que las plantillas se van ampliando, no será difícil designar una persona que, entre sus funciones, tenga la de realizar auditorías esporádicamente, una vez que se informe y se prepare para ello.

La información sobre el particular, gracias a Dios, está hoy al alcance de quien la busque con sólo acercarse al IAI; después asistir a un seminario sacando el máximo provecho, participando activamente, preguntando, recogiendo documentación y dejando abierta una posible conexión con el profesor o ponente por si precisara consultas que evacuar a la hora de poner en práctica los conocimientos adquiridos.

Un segundo paso, dentro del proceso que estamos describiendo, sería producir información para los responsables de las áreas básicas de la gestión de su organización –lo que es y en qué consiste la función de Auditoría Interna– que en estas empresas suelen ser el jefe de administración, el de contabilidad y finanzas, el comercial y el de producción, quienes, junto con el gerente, debieran ser convenientemente informados sobre el particular, así como los propietarios, que tendrían que constituir el motor y apoyo de esta iniciativa.

Se trataría de elaborar un pequeño y sencillo folleto, presentándolo en una reunión a la que podría asistir algún auditor profesional, tal vez el ponente del seminario al que hemos aludido; a partir de aquí, trasladar una sencilla divulgación al resto del personal y determinar las atribuciones del auditor interno cuando trabaje como tal, que será siempre una tarea más de las que tuviera ya asignadas.

La cuestión que se plantea ahora es, más que indicar qué auditorías habría que llevar a cabo a partir del momento en que se ha decidido utilizar esta función en la empresa, cómo deberían empezar a trabajar en ellas los auditores internos, por lo que atañe al auditor que no pertenece a la misma, que es al que nos estamos refiriendo.

Lo más adecuado y conveniente es presentarse preferentemente ante el propietario o propietarios o el Consejo de Administración y, en su defecto, el máximo responsable de la organización, que serán las instancias ante las que el auditor interno tendría que leer y comentar el informe de la auditoría que se haya convenido. Se trata de recabar la colaboración y apoyo total de los mismos, y de informarles de lo que va a hacer y cómo.

Conviene designar una persona, si nadie ha asistido a un seminario de iniciación, en cuyo caso ésta sería quien hubiera asistido, para que actúe como facilitador entre el auditor interno y los empleados, y para que vaya conociendo los métodos y técnicas de trabajo de la auditoría interna, que debería ser capaz de utilizar él mismo en lo sucesivo, bien solo, ya con mínimas asistencias del exterior.

Al iniciar la auditoría hay que dejar muy claro a las instancias de poder y dirección, que el auditor sólo les informará al concluir el informe de auditoría, que deberá comentar con los «auditados» antes de celebrar con dichas instancias la reunión de cierre del informe; que entiendan que no deben solicitar del auditor más que esta información y en su momento.

Es importante, es fundamental, que a lo largo de la auditoría no surjan problemas, discusiones, quejas, incomprensiones, etc., lo cual vale tanto como decir que el auditor interno ha de mantener un comportamiento impecable, mucha humildad y sencillez, seriedad y, al mismo tiempo, carácter, seguridad y confianza en lo que hace y en los positivos resultados que con ello alcanzará la empresa.

En todo momento el auditor interno ha de procurar molestar o distraer al personal lo menos posible haciendo, por sí mismo, el máximo trabajo posible.

Cuestionario de información

Dicho lo anterior, exponemos a continuación un sencillo cuestionario de información que le permitirá al auditor interno obtener un conocimiento global de la empresa y de su nivel de control y organización, de su cultura, pues podría darse el caso de que el auditor perciba, que más que auditorías lo que se necesita es proceder a una reorganización y saneamiento financiero de la misma. Y que la disposición para el cambio, colaborar y aceptar recomendaciones sea claramente negativa, algo que no es aventurado considerar, y de hecho lo hemos vivido, durante nuestra experiencia de consultores.

Las preguntas que se relacionan son indicativas y pueden ampliarse, reducirse o cambiarse, porque no pretenden otra cosa que señalar el posible proceso de actuación de los auditores internos en las empresas pequeñas.

Naturalmente que esta fuente de información «primaria» tendrá que ser verificada con las investigaciones propias del auditor interno, pero suele ser una forma de tomar contacto, con independencia del que se haya realizado con la dirección o la propiedad de la empresa, que permite adentrarse en una organización que el auditor interno desconoce por completo.

Todo esto no significa abandonar las técnicas y métodos de la auditoría interna, ni mucho menos, pero la primera preocupación del auditor tendría que ser hacer un análisis de la situación en la que está la empresa, sea cual sea la auditoría concreta que le hayan solicitado. Se trata de tener una rápida visión del nivel de organización y control de la empresa, porque otra de las exigencias de las empresas pequeñas es la brevedad del tiempo de permanencia de los consultores en ellas. Si son pequeñas todo en ellas ha de ser pequeño, excepto la calidad del servicio que se les preste.

Ofrecemos seguidamente un sencillo cuestionario de información aplicable y pensado para estas empresas:

- ¿Existe un organigrama y una clara asignación de atribuciones y responsabilidades?
- ¿Se establece un presupuesto anual y se controla adecuadamente?
- ¿Se conocen con precisión los costes reales?

- ¿Los beneficios aseguran la continuidad de la compañía?
- ¿Está la empresa en un sector que se corresponde con sus características?
- ¿Cómo se gestiona la Tesorería?
- ¿Se hace un seguimiento adecuado sobre las cuentas a cobrar vencidas?
- ¿Hay límites de crédito establecidos y se cumplen?
- ¿Existe un plan contable?
- ¿Qué información financiera recibe la dirección?
- ¿Se consideran las ventajas que pudiera tener el alquiler de activos en vez de comprarlos?
- ¿La política de amortización es consecuente con la vida de los activos?
- ¿Se están cumpliendo las leyes y regulaciones fiscales?
- ¿Hay una adecuada planificación fiscal para conseguir las mejores condiciones en el pago de los impuestos?
- ¿La cobertura de seguros y la política que se sigue es correcta?
- ¿Cuáles son los riesgos más importantes a tener en cuenta?
- ¿Cómo se gestionan?
- ¿Cómo se gestionan los RR.HH.?
- ¿Cuáles son las políticas comerciales y de ventas?
- ¿Cuál es el nivel de competencia en el mercado?
- ¿Está la empresa operando en mercados exteriores?
- ¿Cuál es la red de distribución de los productos o servicios?
- ¿Cómo se seleccionan los proveedores?
- ¿Se obtienen ofertas diferentes regularmente?
- ¿Qué ocurre con los almacenes?
- ¿Se controlan los niveles de existencias, las partidas con poco movimiento?
- ¿Hay un presupuesto de publicidad y promoción?
- ¿Qué porcentaje de los gastos se dedican a publicidad?
- ¿Cómo funcionan nuestros competidores de similar categoría?

En este tipo de empresas, cualquiera que fuere la auditoría concreta que se realice, el auditor del exterior ha de conocer con mentalidad analítica y sintética en qué situación se encuentra la empresa en cuestión.

Comentario final

No debería existir ninguna empresa, sea cual sea su tamaño y dimensión, en la que no se conozca y de forma permanente o periódica, la función de auditoría interna no se utilizase para asegurar el control y eficiencia de la organización.

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

ISBN: 978-84-124893-1-6
Depósito legal: M-3022-2022

Diseño y maquetación: desdecero, estudio gráfico

Instituto de Auditores Internos de España