AUDITOOL®
Red Global de Conocimientos en Auditoría y Control Interno

MANUAL PARA LA DETERMINACIÓN DEL PLAN ANUAL DE AUDITORÍA BASADO EN RIESGOS

A. INTRODUCCIÓN

En el presente manual se profundizará en detalle sobre cómo desarrollar un Plan de Auditoría Interna basado en Riesgos que incida en la organización, centrándose en las mejores prácticas conocidas, empezando por señalar que:

- El Sistema de Gestión de Riesgos es el conjunto de procesos y actividades que determinan, en forma integral, cómo se contemplan y se administran los riesgos en la organización, empezando en el desarrollo e implantación de la estrategia hasta sus actividades cotidianas.

- Refleja los valores de la empresa, influyendo en su cultura y estilo operativo, y afecta en cómo se aplican los componentes de dicha gestión, incluyendo la identificación de riesgos, los tipos de riesgos aceptados y cómo son estos gestionados.

B. METODOLOGÍA. ÁMBITO CONCEPTUAL

Sobre la base de una visión integradora de la Gestión de Riesgos, se ha optado por un enfoque metodológico basado en el "*Enterprise Risk Management*", también conocido como COSO II, el cual permite aportar valor añadido a todas las partes interesadas, a la vez que permite identificar, crear, captar y sostener el valor de la Gestión del Riesgo empresarial. Sirviendo también de soporte a la Unidad de Auditoría Interna en la definición del contenido de los planes de trabajo a proponer a la alta dirección y a aprobación de la Comisión de Auditoría.

Si bien, respecto de esta elección, se debe señalar que este protocolo ha sido recientemente renovado por el denominado ***"Marco de Gestión de Riesgos Empresariales – integrado con estrategia y desempeño (COSO 2017)",*** el cual aclara la importancia de la gestión de riesgos empresariales en la planificación estratégica y la incorpora a toda la organización, ya que el riesgo influye en el desarrollo de la estrategia y en el desempeño en todas las áreas, departamentos y funciones. En resumen, lo que se focaliza este nuevo protocolo es en la consideración de los riesgos de forma previa a la determinación del posicionamiento estratégico que sea oportuno establecer, pero también la de considerar los riesgos que puedan incidir en la ejecución de la estrategia elegida, ya que de ellos dependerá los resultados reales a alcanzar.

Por tanto, una vez definida la misión, la visión y los valores fundamentales de la organización, se deberá:

1. Definir la estrategia de acuerdo con los riesgos identificados.

2. Posibilidad de que la estrategia no esté alineada con la misión, visión y valores fundamentales de la organización.

3. Implicaciones de la estrategia seleccionada.

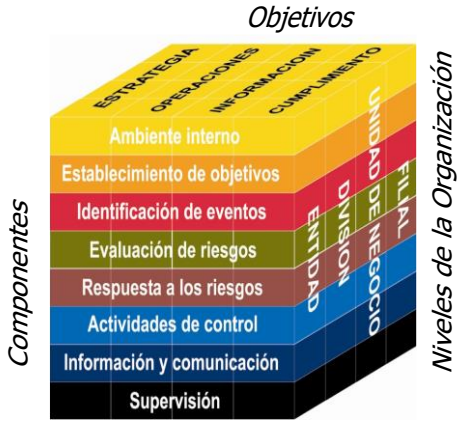
Correspondiendo a la función de Auditoría Interna incidir en la verificación de los puntos 2º y 3 anteriores, debiendo incluir estos entes auditables en el Plan Anual de Auditoría.

Pero también revisar el posible impacto de los riesgos existentes en la estrategia ya definida, para lo cual nos basaremos en el protocolo COSO II.

B.1. Metodología COSO II

La metodología COSO II se basa en un enfoque de tres dimensiones:

Dimensiones en la Gestión de Riesgos



Fuente: Metodología COSO II.

- Los **OBJETIVOS** que la organización trata de alcanzar, los cuales pueden ser analizados en cuatro categorías principales: Estratégicos, Operacionales, Informativos y Cumplimiento.

- Los **COMPONENTES** necesarios para gestionar los riesgos que pueden impedir la consecución de esos objetivos.

  Estos componentes están interrelacionados unos con otros: Ambiente de Control, Establecimiento de Objetivos, Identificación de Eventos, Evaluación de Riesgos, Respuesta a los Riesgos, Actividades de Control, Información y Comunicación, y Monitoreo o Supervisión.

- Los **NIVELES DE LA ORGANIZACIÓN** en los que pueden materializarse los Riesgos y, por tanto, sobre los que se debe trabajar para implantar el Modelo de Gestión de Riesgos. En definitiva, las actividades clave de los diferentes niveles de la organización.

Basándonos en COSO II, se adoptan las siguientes definiciones de los términos clave en relación con la Gestión de Riesgos:

- **Evento**: Incidente o acontecimiento derivado de fuentes internas o externas a la organización, que podría afectar a la implantación de la Estrategia o la consecución de los objetivos del negocio. Según se trate de acontecimientos que favorezcan, o dificulten la consecución de los objetivos, nos encontraremos con:

- **Riesgo**: Cualquier evento potencial que pueda impedir que la organización alcance sus objetivos.

- **Oportunidad**: Posibilidad de que un evento ocurra y afecte de forma positiva a la consecución de los objetivos de negocio.

B.2. Fundamentos

El Modelo de Gestión de Riesgos a aplicar se basa en tres grandes pilares:

- **Objetivos de la Dirección en materia de Gestión de Riesgos**: Determina el Modelo Organizativo finalmente adoptado y el ámbito de actuación del mismo.

- **Procesos de Gestión de Riesgos**: Definición de los procesos de Gestión de Riesgos, las prácticas, los procedimientos y las herramientas facilitadas para el correcto desarrollo del modelo implantado. Se han de determinar cinco fases fundamentales: identificación del riesgo, evaluación, respuesta, seguimiento o monitorización, y reporting.

- **Estructura de la Función de Gestión de Riesgos:** Definición de estructuras, herramientas técnicas, responsabilidades y acciones en la organización como soporte al modelo implantado, con el objetivo de colaborar a reforzar la cultura de riesgo dentro de la organización.

El empleo de este procedimiento debe generar un elevado entendimiento de los objetivos a nivel operativo de cada Dirección, así como una adecuada comunicación de la información pertinente en tiempo y forma, que facilite a la Dirección la toma de decisiones y las operaciones en el día a día.

C. PROCESO GESTIÓN DE RIESGOS: FASES Y ACTIVIDADES CLAVE

C.1. Introducción

El enfoque adoptado se basa en cuatro aspectos y su adecuada alineación a través del proceso de Gestión de Riesgos:

- **Objetivos de negocio**: Metas estratégicas y operativas de la organización.

- **Riesgos**: Cualquier evento potencial que pueda impedir que la organización alcance sus objetivos estratégicos.

- **Controles**: Respuestas de la Dirección a los riesgos.

- **Alineación de los objetivos de negocio:** riesgos y controles con base en la tolerancia y el Apetito al Riesgo de la empresa.

  El Apetito al Riesgo quedará definido como el nivel de riesgo que la organización está dispuesta a aceptar al entenderlo compatible con la consecución de las metas estratégicas establecidas. Es consensuado entre la Alta Dirección y el Consejo de Administración, y adecuadamente comunicado al Gestor de Riesgos y demás partes interesadas.

  En tanto que la **Tolerancia al Riesgo** queda definida como el nivel de variación que la empresa acepta como asumible en la consecución de un determinado objetivo. Es, por tanto, el umbral aceptable para cada Riesgo y objetivo. La tolerancia al Riesgo queda definida por el Apetito, y debe ser actualizada de forma periódica por cada Gestor de Riesgos.

C.2. Fases

El proceso de Gestión de Riesgos es un ciclo continúo sustentado en cuatro fases clave. En cada fase, una comunicación coherente y periódica es esencial para lograr buenos resultados. Al tratarse de un ciclo continuo, es necesario el *feedback* permanente con el objetivo de mejorar continuamente la Gestión de Riesgos.

C.2.1. Identificación

Para cada objetivo del negocio es necesaria la identificación de los riesgos clave que puedan impedir su consecución. La identificación de riesgos está instituida como elemento necesario en todos los procesos de negocio clave y en las operaciones del día a día. Por ejemplo, en la toma de decisiones relevantes para la organización (a nivel de Dirección, en cada proceso de negocio, en nuevas inversiones, etc.), en los cambios organizativos, en los procesos o los sistemas, etc.

El proceso de identificación de riesgos consiste en la búsqueda de aquellos eventos, asociados a factores internos o externos, que pueden dar lugar a amenazas u oportunidades con incidencia en la consecución de los objetivos buscados. Todo ello en el contexto del ámbito global de la empresa, identificando, asimismo, los objetivos de negocio que se puedan ver afectados, bien favorable como desfavorablemente.

A tal fin debe establecerse un **Catálogo de los Riesgos**, con el que se procederá a la identificación de los que puedan manifestarse en los procesos de la organización, con el fin de identificarlos y actualizar de forma periódica el Catálogo observando posibles riesgos a los adicionalmente considerados.

Habitualmente, se reconocen las siguientes **fuentes de origen de riesgos**, con independencia de otras muchas existentes. El objetivo es identificar rápidamente la fuente de origen del riesgo para poder definir más fácilmente respuestas y responsabilidades:

- Dirección y toma de decisiones a nivel corporativo
- Influencia externa
- Recursos Humanos
- Sistemas de Información
- Regulaciones vigentes y aparición de nueva normativa
- Eventos naturales (Crecidas, cambio climático, etc.)
- Seguridad y salud en el trabajo
- Proveedores y subcontratistas
- Tecnología
- Procesos Internos (contratación, etc.)

Asimismo, cada riesgo será clasificado en función de los cuatro grandes grupos de objetivos definidos en la propia metodología COSO II:

- Estratégicos
- Operacionales
- Reporting/Información
- Cumplimiento

C.2.2. Evaluación

Se deberán valorar todos los eventos identificados desde una doble perspectiva (probabilidad de ocurrencia e impacto). Los resultados positivos y negativos de los eventos potenciales se valoran en función de esta doble perspectiva (impacto y probabilidad), distribuyéndolos en función de la categoría de riesgo a la que pertenezca (Estratégico, Operacional, Reporting y Cumplimiento).

El proceso de **Evaluación de Riesgos** recae sobre la Dirección, los responsables de los procesos de negocio y los Gestores de Riesgos, quienes tendrán que autoevaluar los riesgos identificados desde la perspectiva residual, es decir,

después de la implantación de los controles. Adoptando las medidas que se consideren precisas para reconducir los riesgos a los entornos de la tolerancia al riesgo que se haya considerado viable con las metas de la organización.

La herramienta principal para la Evaluación de Riesgos es el **Mapa de Riesgos**. El proceso de evaluación consiste en la ubicación dentro del Mapa de Riesgos de aquellos eventos que supongan una amenaza para los objetivos y/o reputación de las siguientes áreas funcionales:

- **Empresa**, en general
- **Dirección**
- **Subdirección / Departamento**

C.2.3. Gestión de Riesgo

Si el nivel de riesgo una vez considerados los controles y acciones estimadas pertinentes (Riesgo Residual) que se llevan a cabo para su mitigación, no se encuentra en la zona de confort (próximo del apetito del riesgo de la organización), se requiere una acción adicional (Plan de Acción) para bajar aún más el nivel de riesgo deseado (Riesgo Objetivo).

A continuación, se exponen las opciones de gestión con cada riesgo y algunos ejemplos relevantes para cada una de ellas:

- **Rechazar:** Decisión adoptada con el fin de evitar los hechos indeseados. Algunos ejemplos podrían ser los siguientes:

    - Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos.
    - Prescindir de una unidad de negocio, línea de producto o segmento geográfico.

- **Compartir:** Transferir el efecto de una posible pérdida a terceras partes. Algunos ejemplos podrían ser los siguientes:

    - Externalizar procesos de negocio.
    - Adoptar seguros contra pérdidas inesperadas significativas.
    - Distribuir el riesgo mediante acuerdos contractuales con clientes, proveedores u otros socios del negocio.

  - Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo.
  - Establecer acuerdos con otras empresas.

- **Mitigar:** Reducir la probabilidad de ocurrencia de un evento y/o el impacto. Algunos ejemplos podrían ser los siguientes:

  - Establecer procesos de negocio eficaces.
  - Establecer límites operativos.
  - Aumentar la implicación de la Dirección en la toma de decisiones y el seguimiento.
  - Reasignar el capital entre las unidades operativas.

- **Aceptar:** Decisión debidamente comunicada y soportada de aceptar el impacto y la probabilidad de un determinado evento. Por ejemplo:

  - Confiar en las compensaciones naturales existentes dentro de una cartera.

El diseño de las respuestas a los riesgos debe considerar un análisis coste - beneficio entre la trascendencia de la minoración del riesgo y las acciones a desarrollar para gestionarlo.

El proceso de análisis y diseño de las respuestas a los riesgos recaerá sobre las siguientes personas en la organización:

- Los **gestores/responsables de los procesos**, los cuales deben optar por proporcionar la respuesta adecuada al riesgo que lo mitigue de modo eficiente. Es necesaria una constante comunicación de estos con el Gestor de Riesgos, el cual deberá evaluar las adecuadas respuestas a cada riesgo a través de la comparación de los riesgos residuales existentes y los objetivos.

- El **Comité de Dirección**, que debe decidir acerca de la oportunidad de las respuestas que se le da a cada uno de los riesgos identificados y evaluados como críticos, tomando como base de su opinión, las informaciones del Gestor de Riesgos y del responsable de Auditoría Interna.

- El área de Auditoría Interna que supervisará todo el proceso aportando su opinión respecto del nivel de seguridad razonable que puede esperarse del mismo.

C.2.4. Seguimiento o Monitorización

Consiste en la supervisión del proceso seguido de forma que permita, con una seguridad razonable, concluir si las respuestas dadas a los riesgos son viables y eficientes. Es la fase en la que la Unidad de Auditoría Interna se manifiesta como una actuación preferente.

Se trata de un proceso continuado. Los objetivos de esta revisión, que se realizará como mínimo una vez al año, son los siguientes:

- Asegurar que los riesgos, en especial los más significativos, están identificados y están siendo gestionados de la forma prevista por la Dirección.

- Evaluar si los planes de respuesta siguen siendo eficientes, proveer de feedback a los responsables de los mismos e iniciar los pertinentes planes de acción en caso de que sea necesario.

- Determinar si el Catálogo de Riesgos contiene todas las amenazas que puedan producir cambios en las circunstancias en las que se desarrolla el negocio, o que puedan conducir a unas nuevas condiciones económicas.

La monitorización de los riesgos será una combinación de comunicación regular entre los distintos implicados en la Gestión de Riesgos, revisiones o auditorías periódicas de los componentes del Modelo y evaluaciones por Directivos independientes a un nivel adecuado dentro de la organización. Entre las técnicas más destacadas se incluyen:

- Pruebas periódicas sobre una muestra de Controles, Riesgos y Ámbito de Control interno.

- Revisiones de calidad del Sistema de Gestión de Riesgos.

- Revisiones después de implementaciones o cambios significativos en el Modelo.

- Auditorías sobre la eficiencia de la Gestión.

D. ENFOQUE DE AUDITORÍA BASADASEN RIESGOS Y METODOLOGÍA APLICADA

D.1 Determinación del Plan de Auditoría

Partiendo del principio básico de que la función de auditoría interna debe garantizar la eficacia y la eficiencia de la actividad de la organización, también la suya propia, el Plan Anual de Auditoría ha de configurarse con los entes auditables prioritarios identificados, centrando la actuación de la Unidad de Auditoría Interna en ellos.

El Plan de Auditoría debe incluir información de todos los aspectos a atender/desarrollar durante el período considerado, tal como se indica a continuación:

- Objetivos a cubrir:
  - Actividad auditora
  - Formación a cubrir
  - Seguimiento de recomendaciones
  - Colaboraciones o consultorías
  - Trabajos especiales.
- Presupuesto preciso para desarrollar la actividad
- Plantilla requerida para el desarrollo de las acciones con las que cumplir los objetivos marcados.

Para ello, se hace preciso establecer la política y los procedimientos a aplicar.

Política:

La concreción del Plan de Auditoría Interna y su posterior desarrollo es responsabilidad del Director de Auditoría Interna (DAI), y debe ser consistente con las metas y objetivos estratégicos de la empresa. Corresponde también al DAI la presentación de los Planes de Auditoría previstos realizar a la alta dirección y al Consejo/Comité de Auditoría para la adecuada revisión y aprobación, respectivamente.

Procedimientos:

Los objetivos que conformen definitivamente los Planes de Auditoría Interna deben ser atendidos sobre la base de un procedimiento previamente establecido. Dichos objetivos pueden ser obtenidos de distintas vías, tal como se describe a continuación:

1. Comité de Auditoría

Las directrices/requerimientos recibidos deberán ser incluidas como objetivos en el Plan de Auditoría Interna.

2. Organismos regulatorios

Se corresponde con los trabajos requeridos por los **órganos de supervisión** respecto de las exigencias que entiendan necesario para la verificación del cumplimiento de las normas internas y externas (leyes, reglamentos, políticas corporativas, normativas específicas, etc.).

3. Dirección ejecutiva

Para que el Plan de Auditoría Interna sea efectivo y la UAI aporte un servicio de valor agregado real en las distintas entidades de la entidad, es necesario que el Plan recoja las inquietudes y requerimientos de los Directivos de las distintas Unidades de Negocio. En tal sentido, el Director de la UAI deberá reunirse con las gerencias operativas, con la finalidad de determinar lo siguiente:

3.1. Obtener un entendimiento de los cambios significativos y/o pendientes de cada unidad de negocio.

3.2. Comentar y entender los mayores riesgos de cada área o unidad, incluyendo los riesgos emergentes para los próximos doce meses. El análisis de los riesgos deberá basarse en el Modelo COSO-ERM citado:

Riesgos estratégicos: Riesgos que afectan los objetivos de alto nivel, alineados con la misión de la entidad y dándole apoyo.

Riesgos operacionales: Riesgos que afectan a los objetivos vinculados al uso eficaz y eficiente de los recursos de la entidad.

Riesgos de reporte: Riesgos que afectan los objetivos de fiabilidad de la información suministrada.

Riesgos de cumplimiento: Riesgos relativos al cumplimiento de leyes y normas aplicables.

3.3. Reunir información sobre los principales apoyos a solicitar de la Dirección sobre la Unidad de Auditoría Interna.

3.4. Promover buenas relaciones entre la UAI y la Alta Dirección.

4. EL PROPIO ANÁLISIS EFECTUADO POR LA UAI

El análisis efectuado por la UAI deberá basarse en una evaluación de riesgos, el cual deberá considerar diversas fuentes, tomando en cuenta los requerimientos de la Dirección y la experiencia del auditor, de acuerdo con los siguientes aspectos.

4.1. Universo de Auditoría Interna. El Universo es crítico en la creación del Plan de Auditoría Interna, ya que representa todos los posibles puntos auditables en la entidad. El Universo no puede ser estático y debe ser visto como un proceso dinámico que cambia con el tiempo. El Universo considera numerosos aportes, incluyendo los que provienen del auditor y de la Dirección.

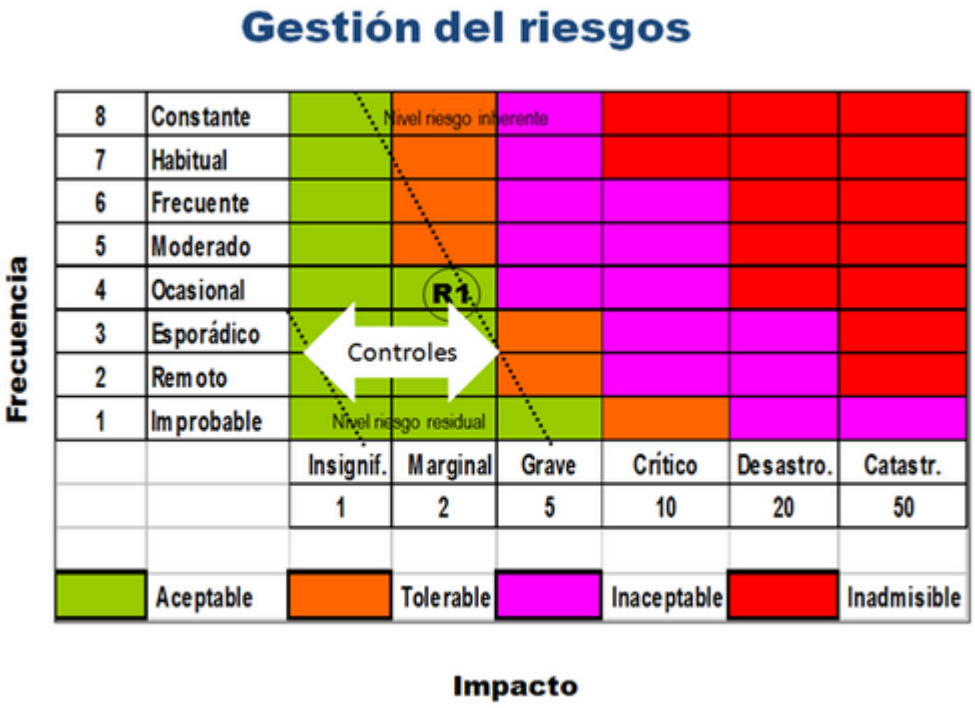
El auditor debe tener un conocimiento permanente de la entidad a auditar, de modo tal que, cualquier cambio en la entidad debe redireccionarse en el Universo para reflejar el ambiente actual

4.2. Resultados de la evaluación corporativa de la Gestión de Riesgos

La coordinación entre el Gestor de Riesgos y el Director de Auditoría Interna debe ser plena, ya que al desarrollar ambas actividades complementarias, su interacción debe ser permanente. Teniendo presente que a la Auditoría le corresponde verificar la bondad de las estimaciones y decisiones efectuadas por la empresa en la gestión de riesgos con las que administrarles adecuadamente.

En este sentido, si el mapa de riesgos residuales recogiera determinadas amenazas no situadas aún en el entorno de la tolerancia al riesgo que se hubiese considerado adecuada, Auditoría debe solicitar los planes de acción que se hayan elaborado para reconducir la situación, valorando la oportunidad de los mismos, siendo estas revisiones de los planes de actuación los entes auditables a incluir el Plan de Auditoría.

De no existir definidas las actuaciones con las que administrar los riesgos en cuestión, Auditoría deberá sugerir al Gestor de Riesgos que actúe adecuadamente para disponer de ellos, para proceder a su posterior verificación.



Por el contrario, sí serán susceptibles de ser considerados entes auditables en el Plan de Auditoría que se esté preparando, aquellos procesos cuyos riesgos residuales estén situados en el Mapa de Riesgos en los espacios próximos a los apetitos al riesgo que se consideren factibles con los objetivos de la organización, ya que una inadecuada evaluación pondría en cuestión los objetivos empresariales. Motivo por el que se hace necesaria para ellos la evaluación objetiva e independiente de Auditoría Interna. Actuando con este colectivo de forma selectiva, pues los recursos disponibles no son ilimitados.

4.3. Priorización de los entes auditables por Auditoría Interna. A fin de seleccionar las actuaciones supervisoras que vayamos a incluir en el Plan de Auditoría, se hace imprescindible establecer un ranking de prioridades de los entes auditables, a través de una ponderación de las circunstancias que afecten a cada elemento en el Universo de Auditoría, para ello los procesos existentes pueden perfectamente identificarse con los entes auditables. Los aspectos con los que ponderar deberán ser cuantitativos y cualitativos.

4.3.1. Los factores cuantitativos dependen del juicio del auditor, pero pueden incluir otros elementos como: (1) impacto monetario de dichos procesos en los estados financieros, y/o (2) volumen de las transacciones procesadas.

4.3.2. El análisis cualitativo incluye factores tales como: (1) madurez del proceso, (2) nivel de automatización, (3) nivel de subjetividad en la toma de decisiones, (4) tiempo transcurrido desde la última auditoría realizada, (5) nivel de centralización o descentralización, y (6) complejidad del proceso.

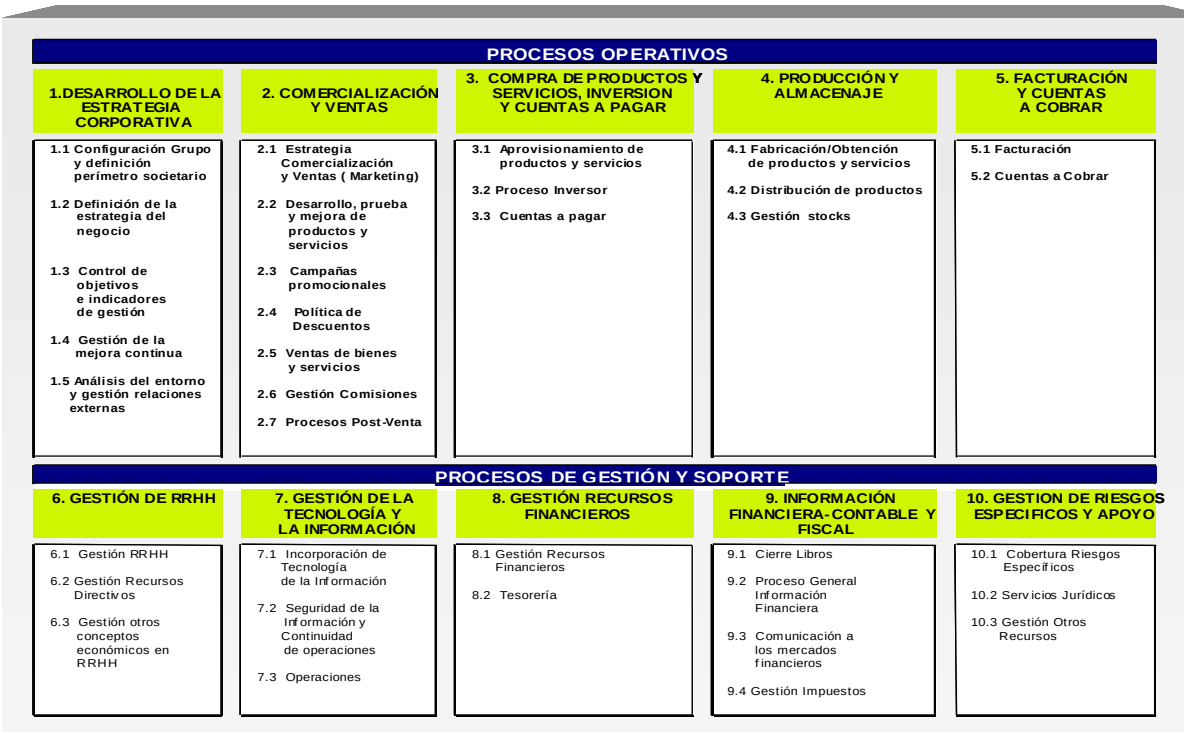
Una vez que la UAI haya analizado tanto los factores cuantitativos, como los cualitativos, se podrá determinar la prioridad de cada elemento en particular. Esta determinación está basada en todo el análisis cuantitativo y cualitativo efectuado, y deberá ser adecuadamente documentado para cada uno de los procesos identificados.

4.3.3. Para efectos de la evaluación, deberá utilizarse como herramienta una matriz en Excel, que deberá contener todos los procesos definidos y, sobre la cual, se solicitará información (variables) que concurran en cada proceso, debiendo ser consideradas las variables que se estimen convenientes aplicar, como por ejemplo las que se detallan a continuación. Las cuales podrán ser modificadas, tanto cuantitativa, como cualitativa que el DAI estime pertinentes:

1ª Variable (Peso 35 puntos). Interacción riesgos y procesos.

Procesos: El modelo que estamos describiendo consta de 10 actividades a un primer nivel: (1) Desarrollo de la estrategia corporativa, (2) Comercialización y ventas, (3) Compras de productos y servicios - Inversiones y Cuentas a pagar-, (4) Producción y almacenaje, (5) Facturación y cuentas a cobrar, (6) Gestión de Recursos Humanos, (7) Gestión de la Tecnología y la Información, (8) Gestión Recursos Financieros, (9) Información Financiera - Contable y Fiscal, (10) Gestión Riesgos específicos y apoyo.

En tanto que se desglosan en 35 subprocesos a dos niveles. Según se desprende del cuadro que aparece a continuación.



En cuanto a los riesgos, el modelo empleado consta de 52 tipos de riesgo:

- ✓ Satisfacción del cliente
- ✓ Duración proceso productivo
- ✓ Desarrollo de productos y servicios
- ✓ Proveedores - Recursos externos
- ✓ Obsolescencia - gestión inventarios
- ✓ Incumplimiento de compromisos

- ✓ Facturación / Pérdida de ingresos
- ✓ Comunicación interna
- ✓ Eficiencia
- ✓ Capacidad
- ✓ Diferenciación
- ✓ Interrupción del negocio
- ✓ Medio Ambiente
- ✓ Salud y seguridad
- ✓ Imagen
- ✓ Subcontratación
- ✓ Fraude interno
- ✓ Fraude externo
- ✓ Recursos Humanos
- ✓ Incentivos
- ✓ Límites
- ✓ Autoridad - Segregación
- ✓ Funciones
- ✓ Liderazgo
- ✓ Flexibilidad al cambio
- ✓ Acceso
- ✓ Integridad
- ✓ Relevancia/Disponibilidad
- ✓ Evolución mercados financieros
- ✓ Liquidez
- ✓ Crédito a clientes
- ✓ Garantía
- ✓ Fijación de precios
- ✓ Compromisos adquiridos
- ✓ Medición del desempeño
- ✓ Alineación con la estrategia
- ✓ Diversificación del negocio
- ✓ Valor del negocio
- ✓ Planificación estratégica
- ✓ Normativa
- ✓ Ciclo de vida
- ✓ Planificación y presupuestación
- ✓ Información financiero - contable y fiscal
- ✓ Evaluación de la información financiera
- ✓ Evaluación de inversiones

- ✓ Disponibilidad recursos financieros
- ✓ Competencia
- ✓ Relaciones con accionistas
- ✓ Cambios en la industria
- ✓ Entorno Legal y Fiscal
- ✓ Regulación
- ✓ Entorno Político y Económico

El universo de auditoría, en consecuencia, estará compuesto como máximo por 52 riesgos x 35 subprocesos, es decir, un total de 1820 entes auditables, a los que habrá que ordenarles según su incidencia en la consecución de los objetivos empresariales y la importancia ponderada de todos los riesgos que afecten a dichos procesos.

Para ello, lo primero que habrá que ordenar es el nivel de transcendencia de los 35 subprocesos de acuerdo con su vinculación con los objetivos estratégicos y operacionales de la compañía, asignándoles un factor de trascendencia (T) valor 1, 1/2, 1/3, 1/4 y 0 según nivel de aportación y participación en las metas de la empresa. Factor de trascendencia que afectará al nivel de riesgo global que se asigne a los riesgos que estén afectando a dichos procesos (R):

- Riesgo alto, peso 35
- Riesgo medio, peso 25
- Riesgo bajo, peso 10

La combinación “trascendencia” y “riesgo global” determinará el peso de la variable, de acuerdo con la siguiente fórmula. **Peso 1ª variable = T x R.**

Adicionalmente, y dado que los entes auditables se determinan, en principio, por la combinación riesgo/proceso, la confluencia de más de un riesgo en un mismo proceso determinará el alcance de la auditoría, siempre que el acumulado de puntos supere el umbral de revisión que finalmente se establezca.

Variable 2 (Peso 10 puntos)

Esta variable se refiere al tiempo transcurrido desde la última auditoría realizada. La finalidad es evaluar el mayor riesgo que representa el retraso de la supervisión/análisis de un proceso, para lo cual se utilizarán los siguientes pesos:

- Auditado en el presente año y el anterior: 0
- Auditado hace 2 años: 5
- Nunca auditado o auditado hace 3 o más años: 10.

Variable 3 (Peso 10 puntos)

En caso de existir auditorías previas, se debe identificar la valoración otorgada al informe:

- Buena: 0
- Buena con excepciones: 3
- Mejorable: 6
- Deficiente: 10
- No existencia de auditoría previa: 5.

Variable 4 (Peso 10 puntos)

Esta variable otorga un peso a la legislación existente. La ausencia de regulación implicaría un riesgo mayor:

- Con Legislación existente: 0
- No existe legislación que le afecte: 10

Variable 5 (Peso 10 puntos)

Esta variable otorga peso a la situación y grado de cumplimiento de las recomendaciones formuladas por los auditores internos y externos como resultado de sus respectivas auditorías y/o por el organismo supervisor durante sus visitas de inspección.

- Recomendaciones atendidas: 0
- Recomendaciones en vías de implementación: 5
- Recomendaciones pospuestas o rechazadas: 10

Variable 6 (Peso 25 puntos)

Esta variable otorga peso basado en la opinión profesional del auditor. Esta evaluación puede basarse en el conocimiento de fraudes, resultados financieros, riesgo inherente, etc. Los pesos asignados son un máximo de 25.

Después de completar todas las variables, tomando como referencia la columna "Suma de valores", preliminarmente serán considerados como "auditables" todos aquellos valores que sean iguales o superiores a un determinado valor, el que se considere determinar la frontera entre entes auditables y entes a los que no es preciso auditar, por ejemplo, los 70 puntos.

Solicitudes expresas de las partes interesadas:

Posteriormente, y con base a los otros criterios de selección complementaria al análisis de riesgos, se identificarán los procesos dentro de la siguiente clasificación:

1. Auditorías a realizar por los requisitos legales y de cumplimiento.
2. Auditorías solicitadas por el Comité de Auditoría.
3. Auditorías solicitadas por la Dirección.

Con base en esta nueva clasificación, se determinan los procesos auditables bajo "otros criterios", a los que habrá que añadir los planes de formación, supervisión de los planes de remediación y las consultorías que se consideren conveniente atender.

Como resultado de los apartados anteriores, se determinan las actividades/procesos que serían "auditables".

Finalmente, basados en todos los niveles de aporte, y la ponderación de los riesgos efectuados para cada elemento del Universo, el Director de la UAI determinará los elementos que deberán ser incluidos en el Plan de Auditoría Interna; pero antes de darlos por definitivos, se comprobará si alguno de estos entes auditables están previstos ser supervisados por algún otro proveedor de aseguramiento, coordinando las actuaciones y evitando duplicidades. Aspecto que deberá estar especificado en la información trasladada a los responsables de la aprobación del Plan.

Si por razones de capacidad y/o recursos disponibles, algún objetivo "auditable" no se pudiese desarrollar, la UAI deberá hacer un análisis final para seleccionar los que pueden llevarse a cabo, lo que justificaría la exclusión y la documentación de sustento respectiva. En otras palabras, este análisis servirá de base para la determinación de las horas disponibles para cada una de las auditorías y que será incluida en el Plan Anual de Auditoría, para lo cual se debe incluir una columna con los tiempos estimados para llevar a cabo dichas auditorías.

Dado que la responsabilidad final del Plan es del Consejo/Comité de Auditoría, en el supuesto que por razones de limitación de recursos hubiese que excluir algún trabajo del Plan, esta circunstancia debería quedar explícitamente recogida en la información a aportar a la alta dirección y al Comité de Auditoría, ya que lo que finalmente se incluya en el Plan, comporta una responsabilidad compartida de todos los que en su determinación intervienen (DAI, Alta Dirección y Comité de Auditoría).

Contenido del Plan Anual de Auditoría Interna

El contenido del Plan Anual de Auditoría deberá considerar, como mínimo, los siguientes aspectos:

Objetivos de Auditoría Interna para el ejercicio planificado.

1. Auditorías a realizar durante del año.
2. Colaboración con los otros proveedores de aseguramiento.
3. Otras actividades a ser realizadas por la Unidad: participación en Comités u otros trabajos administrativos propios de la función de Auditoría Interna.
4. Seguimiento de las recomendaciones de Auditoría Interna, Externa, y Organismos Reguladores.
5. Formación: indicar las horas que esté previsto dedicar a la capacitación
6. Programa de Aseguramiento y Mejora de la Calidad.

Después de este detallado trabajo de planificación, el resultado se debe plasmar en una hoja resumen, en la que aparezca la tipificación de los entes auditables, su ponderación y motivo por el que se incluye o no en el Plan de Auditoría. La discriminación entre auditables o no auditables, en función del riesgo, dependerá del peso mínimo que se haya estimado para ser considerado ente a auditar. En el caso descrito, el peso mínimo es de 70 puntos.