AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Marco de Relaciones de Auditoría Interna con otras Funciones de Aseguramiento

GUÍA PRÁCTICA

The Institute of Internal Auditors

Instituto de Auditores Internos de España

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Marco de Relaciones de Auditoría Interna con otras Funciones de Aseguramiento

GUÍA PRÁCTICA

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN: **Óscar del Olmo, CIA, CRMA, CFE.** IBERDROLA

Paz Argamentería, CRMA. INVERSIS

Francisco José Narváez. GRUPO FUERTES

Yolanda Cortés, CIA, CRMA. VOCENTO

Lucila Carnicero. DELOITTE

Eduardo Cuesta, CISA, CISM. MAPFRE

Angel Juárez. BDO

José Ignacio Domínguez, CRMA, ROAC

José Luis Solís, ROAC, CRMA, TEC. EY

Rafael Muriel. LIBERBANK

Mónica Albadalejo, CIA, CRMA. BANCO ESPIRITO SANTO

FUNDACIÓNMAPFRE

Instituto de Auditores Internos de España

Desde 1975, FUNDACIÓN MAPFRE desarrolla actividades de interés general para la sociedad en distintos ámbitos profesionales y culturales, así como acciones destinadas a la mejora de las condiciones económicas y sociales de las personas y los sectores menos favorecidos de la sociedad.

En este marco, el Instituto de Ciencias del Seguro de FUNDACIÓN MAPFRE promueve y desarrolla actividades educativas y de investigación en los campos del seguro y de la gerencia de riesgos. Entre otras actividades, el Instituto promueve y elabora informes periódicos y publica libros sobre el seguro y la gerencia de riesgos, con objeto de contribuir a un mejor conocimiento de dichas materias.

En algunos casos estas obras sirven como referencia para quienes se inician en el estudio o la práctica del seguro, y en otros, como fuentes de información para profundizar en materias específicas. Dentro de esta actividad se encuadra el apoyo a la publicación de esta Guía Práctica "Marco de Relaciones de Auditoría Interna con otras Funciones de Aseguramiento", producción de LA FÁBRICA DE PENSAMIENTO, el *think tank* del Instituto de Auditores Internos de España.

El Instituto de Ciencias del Seguro de FUNDACIÓN MAPFRE, en el área educativa, abarca la formación académica de posgrado y especialización, desarrollada en colaboración con la Universidad Pontificia de Salamanca, así como cursos y seminarios para profesionales, impartidos en España e Iberoamérica. Estas tareas se extienden a otros ámbitos geográficos mediante la colaboración con instituciones españolas e internacionales, así como a través de un programa de formación en Internet. El Instituto promueve ayudas a la investigación en las áreas científicas del riesgo y del seguro y mantiene un Centro de Documentación especializado en seguros y gerencia de riesgos, que da soporte a sus actividades.

Desde hace unos años, Internet es el medio por el que se desarrollan mayoritariamente nuestras actividades, ofreciendo a los usuarios de todo el mundo la posibilidad de acceder a ellas de una manera rápida y eficaz mediante soportes web de última generación a través de: www.fundacionmapfre.org\cienciasdelseguro.

La FÁBRICA DE PENSAMIENTO del Instituto de Auditores Internos de España ha producido esta Guía Práctica "Marco de Relaciones de Auditoría Interna con otras funciones de Aseguramiento" para aportar luz y satisfacer las expectativas de los auditores internos y de aquellos lectores que, con independencia de su posición jerárquica en la organización, estén interesados en obtener una visión clara sobre las distintas fuentes de aseguramiento en la empresa.

Esta Guía evidencia que la existencia de mapas de aseguramiento optimiza la coordinación de las distintas líneas de aseguramiento, consigue un eficiente consumo de recursos para la organización y aporta un nivel de aseguramiento adecuado a la Dirección y al Consejo.

Este documento complementa y refuerza el modelo de "Las 3 líneas de defensa", definiendo la función de Auditoría Interna tanto como evaluador de la eficacia de la segunda línea, como coordinador de todos estos proveedores de aseguramiento interno en la imprescindible búsqueda de eficiencia.

Felicito a los autores de este trabajo, miembros de la Comisión Técnica, por mantener el nivel de excelencia al que las producciones de LA FÁBRICA DE PENSAMIENTO nos está acostumbrando en cada documento.

Desde el Instituto de Auditores Internos de España agradecemos sinceramente a FUNDACIÓN MAPFRE el patrocinio de la edición de este Guía Práctica.

José Manuel Muries
Presidente del Instituto de Auditores Internos de España

Índice

Introducción

Auditoría Interna no es una excepción, debe optimizar el uso de sus recursos manteniendo el nivel adecuado de aseguramiento.

En el Instituto de Auditores Internos de España, hemos creado una serie de Comisiones Técnicas para desarrollar documentos de posicionamiento que ayuden a los auditores internos a fijar sus posiciones, despejar incertidumbres y analizar áreas estratégicas de futuro. Esta guía práctica se enmarca en ese contexto.

Con la crisis, se ha acentuado la necesidad de mejorar la eficiencia de los recursos de que dispone cualquier actividad. Auditoría Interna no es una excepción, debe optimizar el uso de sus recursos manteniendo el nivel adecuado de aseguramiento. Para lograrlo, tiene que coordinar su actividad con las otras funciones de aseguramiento de la organización y aprovechar el trabajo de otros.

Esta guía presenta, en un solo documento, la síntesis de las distintas publicaciones sobre este asunto y recoge la experiencia de los miembros de la Comisión Técnica.

Las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna,* establecen, en su Norma 2050 – Coordinación, que: "El Director de Auditoría interna debería compartir información y coordinar actividades con otros proveedores internos y externos de servicios de aseguramiento y consultoría para asegurar una cobertura adecuada y minimizar la duplicación de esfuerzos".

El Marco Internacional para la Práctica Profesional de la Auditoría Interna de The Institute of Internal Auditors, ha emitido un conjunto de normativa (consejos para la práctica, guías prácticas y documentos de posicionamiento) que desarrollan y facilitan la implantación de la Norma 2050. El Consejo para la Práctica 2050-3 establece que "el estatuto de Auditoría Interna debería especificar que la Función de Auditoría Interna tiene acceso al trabajo de otros proveedores internos y externos de servicios de aseguramiento".

Otros documentos relevantes emitidos por The Institute of Internal Auditors son:

- Consejos para la práctica: 2050-1 *Coordinación;* 2050-2 *Mapas de Aseguramiento*; 2050-3 *Confiar en el trabajo de otros proveedores de servicios de aseguramiento.*
- Guía práctica: *Reliance by Internal Audit on Other Assurances providers.* Diciembre-2011.
- Guía práctica: *Coordinating risk management and assurance.* Marzo-2012.
- Documento de posicionamiento: *The three lines of defense in effective risks management and control.* Enero-2013. A efectos de posicionamiento de Auditoría Interna en la organización, la presente guía toma como referencia el modelo de tres líneas de defensa propuesto y desarrollado por el IIA.

DEFINICIÓN DE SERVICIO DE ASEGURAMIENTO

Las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna* definen como servicio de aseguramiento el "examen objetivo de evidencias, con el propósito de proveer una evaluación independiente de los procesos de gobierno, gestión de riesgos y control de una organización".

El documento de posicionamiento: *The three lines of defense in effective risks management and control* establece que el objetivo de las "otras funciones de aseguramiento" que componen la segunda línea es precisamente asegurar que la primera línea de defensa está diseñada y opera de manera efectiva. Es decir, cada una de las funciones de la segunda línea de defensa dispone de cierto nivel de independencia respecto de la primera línea; aunque por su naturaleza están asociadas a la gestión. Con este modelo, las defensas de la segunda línea pueden intervenir directamente sobre el desarrollo de los sistemas de gestión de riesgos y control interno. Pero, en ningún caso, estas funciones de la segunda línea pueden ofrecer a los órganos de gobierno un verdadero aseguramiento independiente de los sistemas de gestión de riesgos y control interno. El aseguramiento independiente depende de la tercera línea de defensa, la Auditoría Interna.

CLASIFICACIÓN DE PROVEEDORES DE SERVICIO DE ASEGURAMIENTO

Cualquier servicio de aseguramiento tiene siempre tres partes implicadas:

- Las personas que realizan las operaciones, ejecutan el proceso, operan el sistema, etc. y las que supervisan: gestión de riesgos, cumplimiento, etc.
- La persona que evalúa: el proveedor del servicio de aseguramiento.
- El usuario de la evaluación: internos (Alta Dirección o Consejo) y externos.

Y existen tres clases de proveedores de servicios de aseguramiento, en función del tercero

al que dan servicio, de su nivel de independencia sobre las actividades que aseguran y de la solidez de su aseguramiento:

a) **Proveedores internos de aseguramiento que informan a la Alta Dirección** y/o son parte de la dirección: auto-evaluadores de control, auditores de calidad, medio ambiente, seguridad e higiene, gestión de riesgos, desempeño de gobierno corporativo, información financiera, cumplimiento, etc.

b) **Proveedores de aseguramiento que informan al Consejo,** entre los que se incluye Auditoría Interna.

c) **Proveedores de aseguramiento que informan a personas interesadas externas** como es el auditor externo, que informa a los accionistas de las sociedades.

El correcto funcionamiento y coordinación de actividades entre Auditoría Interna y otras funciones de aseguramiento propicia beneficios.

CONFIANZA EN LA INFORMACIÓN DE TERCEROS

La decisión de confiar en el trabajo de otros proveedores de servicios obedece a varias razones:

- Para abarcar áreas que no son competencia de la Auditoría Interna.
- Para obtener la transferencia de conocimientos.
- Para ampliar la cobertura de riesgo más allá del plan de Auditoría Interna.
- Para evitar duplicidades y obtener sinergias en términos de utilización y optimización de recursos.

El correcto funcionamiento y coordinación de actividades entre Auditoría Interna y otras funciones de aseguramiento propicia **beneficios** como:

- Ampliación de la cobertura de riesgos, sin incrementar las horas de Auditoría Interna.
- Reducción de tiempos de acción en la gestión del riesgo.
- Mejor aseguramiento, por conocimiento más especializado.
- Intentar evitar el efecto "fatiga de Auditoría" dentro la organización.
- Aumento de la eficiencia, al eliminar la duplicidad de funciones.
- Aumento de calidad de cumplimiento, por el esfuerzo conjunto.

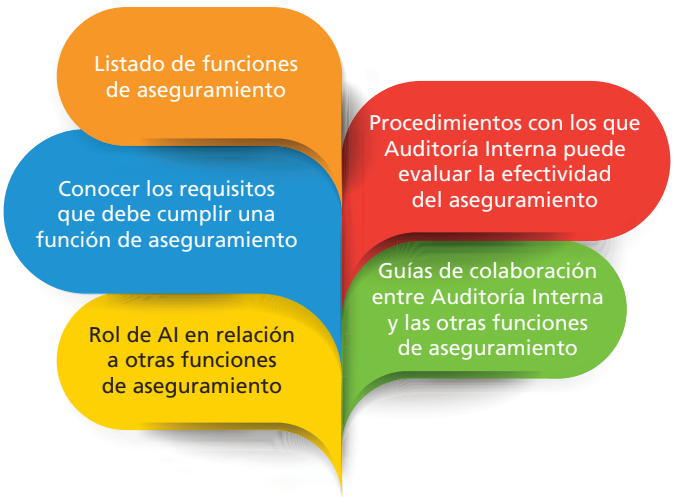
Si bien, confiar en otros proveedores también entraña **riesgos,** como:

- Deficiencias de control, por problema de cobertura del proveedor.
- No identificar problemas, por falta de independencia del proveedor.
- Aumentar, o situar fuera de contexto, riesgos evaluados, no considerados significativos por Auditoría Interna.

Objetivo y Alcance del Trabajo de la Comisión

En este documento hemos elaborado una guía práctica de la relación de Auditoría Interna con las otras funciones de aseguramiento interno, que nos facilita:

- **Un listado de funciones de aseguramiento** (no exhaustivo).
- **Conocer los requisitos que debe cumplir una función de aseguramiento** para que aseguramiento sea efectivo.
- **Procedimientos con los que Auditoría Interna puede evaluar la efectividad del aseguramiento** que proporcionan otras funciones de aseguramiento.
- **Definir el rol que puede desempeñar Auditoría Interna en relación a otras funciones de aseguramiento** y las líneas rojas que no debe traspasar. Así mismo, identificar aquellas actividades que son "patrimonio" de Auditoría Interna y no deben ser desempeñadas por terceros.
- **Establecer guías de colaboración entre Auditoría Interna y las otras funciones de aseguramiento,** que facilitan mayores estándares de aseguramiento, mayor eficiencia y evitan duplicidades.



Listado de Funciones de Aseguramiento

Tratamos exclusivamente de las relaciones de Auditoría Interna con otros proveedores internos de aseguramiento que informan a la Alta Dirección o al Consejo, y son parte de la Dirección de la sociedad.

Es muy complejo establecer un modelo único organizativo respecto a las "organizaciones internas" o "funciones" que, en una sociedad, deben prestar los servicios de aseguramiento. Depende de su grado de madurez, del sector y de las circunstancias. No obstante, consideramos que, con independencia de quién es el responsable de determinadas actividades de aseguramiento, sí deben existir un conjunto de actividades que, conforme a las particularidades del sector, regulación, etc., deben realizarse y por tanto estar reconocidas de alguna forma en las "organizaciones o funciones internas".

En particular, identificamos las siguientes actividades/funciones de aseguramiento, en relación a los siguientes ámbitos:

1. **Control Interno:** aseguramiento del control interno de la compañía. Su alcance son los procesos operativos, administrativos y de tecnologías de la información de la misma.
2. **Control Interno sobre la Información Financiera:** aseguramiento del sistema de control interno en los procesos de elaboración de la información financiera (SCIIF).
3. **Seguridad de la Información:** aseguramiento de la infraestructura tecnológica y garantiza la confidencialidad, integridad y disponibilidad de la información.
4. **Seguridad física de activos y personas:** aseguramiento de la integridad de los activos y de las personas, y garantiza la continuidad de las actividades[1].
5. **Cumplimiento Normativo:** aseguramiento del cumplimiento de la Ley Orgánica de Protección de Datos (LOPD), Prevención de Blanqueo de Capitales y Financiación del Terrorismo, Reglamento Interno de Conducta de los Mercados de Valores, Códigos Éticos, determinados aspectos respecto de la responsabilidad penal de las sociedades y normativa específica sectorial.
6. **Gestión de riesgos:** aseguramiento de la adecuada gestión de los riesgos que afectan de manera significativa a las actividades de la sociedad.

1. Las nuevas legislaciones y las tendencias en materia de seguridad apuntan hacia una gestión integral y coordinada de la seguridad, poniendo el foco, no en la protección específica de un dominio físico o lógico, sino en la protección global de un activo.

7. **Sistemas de gestión integral:** aseguramiento del cumplimiento de la normativa en materia de calidad, medio ambiente, prevención de riesgos laborales, I+D+i

8. **Responsabilidad Corporativa (RC) y Reputación Corporativa:** aseguramiento de la transparencia de las actividades de la sociedad y las relaciones con grupos de interés.

Requisitos de una Función de Aseguramiento para poder concluir respecto al Aseguramiento Efectivo de la misma

Según la Guía Práctica del IIA, *Reliance by Internal Audit on other assurance providers,* de diciembre de 2011, los principios/elementos para evaluar el trabajo de proveedores de aseguramiento interno y determinar el grado de confiabilidad, son:

1. **Propósito de los trabajos:** el propósito del trabajo de los proveedores debe estar especificado, ser claro y relevante para el alcance y objetivos de Auditoría Interna. (Establecido en documento interno, en caso de proveedores internos).

2. **Objetividad del proveedor del servicio:** los proveedores de aseguramiento han de demostrar su imparcialidad y objetividad.

3. **Competencias técnicas:** se consideran factores de este principio la experiencia aportada y demostrable. El principio de competencia se hace más importante en los casos en que se aprecia falta de independencia (departamentos internos, proveedores contratados por la dirección,…)

4. **Prácticas y metodologías:** valorar si disponen de políticas, programas y procedimientos que utilizan en la realización de los trabajos. Los trabajos están adecuadamente planificados, supervisados, documentados y revisados y están soportados por un nivel adecuado de evidencia. Disponen de adecuado acceso a la información necesaria para alcanzar conclusiones.

5. **Comunicación de resultados y acciones correctoras:** existen procedimientos de comunicación de los resultados de los trabajos de aseguramiento a la Dirección, con objeto de que se tomen las medidas correctoras y se realice seguimiento de su implantación.

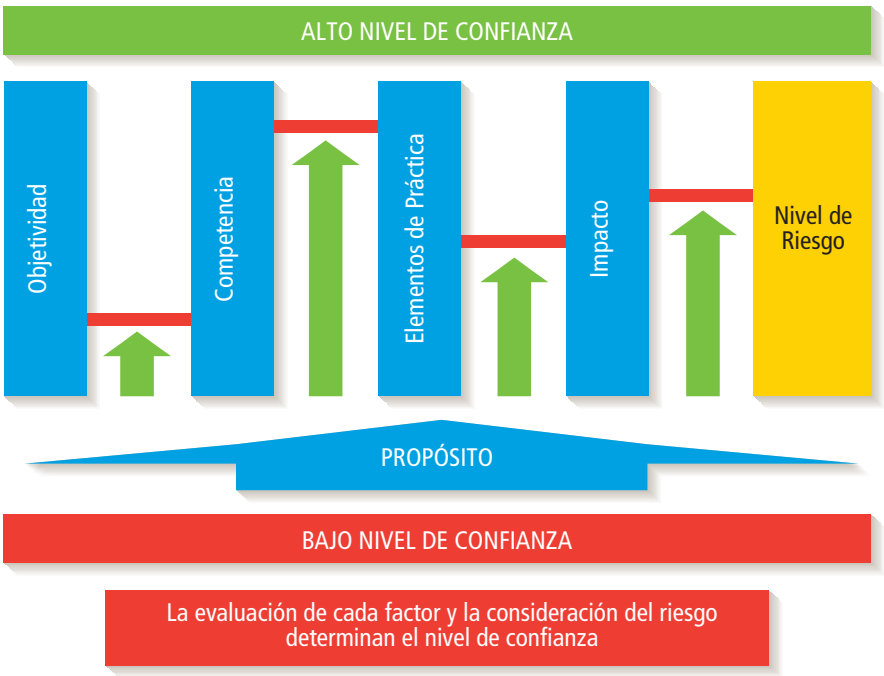
Procedimientos de Auditoría Interna para Evaluar la Efectividad del Aseguramiento proporcionado por Otras Funciones de Aseguramiento

La decisión de confiar en el trabajo de otras funciones de aseguramiento debe venir avalada por una evaluación previa de Auditoría Interna y la fiabilidad de esta decisión se basa en cuatro factores:

1. **Objetividad de la función de aseguramiento respecto al supervisado:**
   a. Línea ejecutiva y nivel jerárquico al que reporta la función de aseguramiento.
   b. Independencia en la determinación de los programas de trabajo y el alcance de las pruebas respecto de la línea ejecutiva.
   c. Políticas y prácticas que eviten el conflicto de interés como consecuencia de que determinados miembros del equipo de aseguramiento hubieran desempeñado responsabilidades operativas con anterioridad.
2. **Competencia profesional de los miembros de la función de aseguramiento:**
   a. Nivel educativo y experiencia profesional del personal de la función de aseguramiento.
   b. Obtención de certificaciones profesionales y planes de formación que aseguren una formación continuada.
3. **Existencia de políticas, procedimientos y programas escritos respecto al ejercicio de las funciones de aseguramiento.**
   a. Existencia de políticas, programas y procedimientos para el desempeño de la actividad de aseguramiento.
   b. Procedimientos internos que aseguren la calidad de los papeles de trabajo, informes y recomendaciones. Existencia de soporte documental de conclusiones basadas en evidencias y seguimiento de recomendaciones.
   c. Procedimientos de supervisión y revisión de las actividades del personal de la función. Evaluación anual del desempeño del personal.
4. **Emisión de informes de conclusiones y recomendaciones, así como seguimiento hasta su implantación.**
   a. Existencia de procedimientos de comunicación de los resultados de los trabajos de aseguramiento a la Dirección, con objeto de que se tomen las medidas correctoras.
   b. Existencia de procedimientos de seguimiento de las recomendaciones emitidas y de las medidas comprometidas para la subsanación de incidencias.

Por último, Auditoría Interna debe llevar a cabo sus propios procedimientos de análisis y revisión de estos trabajos, para disponer de evidencias sobre la calidad y rigor de las actividades de aseguramiento.

Para asegurar el desempeño y calidad de la actividad de Auditoría Interna es necesario someterse a evaluaciones periódicas, tanto internas como externas, tal y como recoge la Norma 1.300.- "Programa de aseguramiento y mejora de la calidad" en el *Marco Internacional para la Práctica Profesional de la Auditoría Interna.*



Fuente: Guía práctica del IIA, *Reliance by internal audit on other assurance providers.*

Para asegurar el desempeño y calidad de la actividad de Auditoría Interna es necesario someterse a evaluaciones periódicas, tanto internas como externas.

Alcance y Rol de AuditorÍa Interna en relación a Otras Funciones de Aseguramiento

Frecuentemente encontramos que determinadas actividades desempeñadas por otras funciones de aseguramiento son redundantes e incluso entran en ámbitos propios de Auditoría Interna, o viceversa; y puede ocurrir que se confundan los roles de Auditoría Interna con el de estas otras funciones.

Para ayudar a clarificar el alcance y rol de Auditoría Interna en relación con cada una de las otras funciones de aseguramiento, incorporamos en este documento una serie de anexos con fichas individuales para cada una de las actividades/funciones de aseguramiento identificadas. Para cada una de ellas identificamos una relación de actividades que son "patrimonio" de Auditoría Interna y no deben ser desempeñadas por terceros, y una serie de "líneas rojas" que no debe traspasar Auditoría Interna. *(Páginas 22 a 37)*

Guías de Colaboración entre Auditoría Interna y Otras Funciones de Aseguramiento. Los Mapas de Aseguramiento

Una de las responsabilidades más importantes del Consejo de Administración es asegurar que los procesos de la sociedad se llevan a cabo según los parámetros establecidos para alcanzar los objetivos. Pero para conseguirlo, el Consejo dispone múltiples recursos de aseguramiento, y aparecen así las zonas grises entre dichas funciones de aseguramiento. Por eso, hay que determinar si los procesos de gestión de riesgos funcionan de manera efectiva, y si los riesgos clave o críticos del negocio se gestionan de forma aceptable.

Una buena alternativa es elaborar un **Mapa de Aseguramiento.** Al coordinar las diferentes actividades de aseguramiento, se visualiza el esfuerzo en común y se mitigan los riesgos. Adicionalmente, los mapas de aseguramiento son una buena herramienta para coordinar la gestión de riesgos y aseguramiento entre las distintas funciones de una organización.

Proponemos que sea Auditoría Interna quien cree los mapas de aseguramiento coordinados con el resto de funciones, ya que es la responsable de entender los requisitos de aseguramiento dictados por el Consejo y definir los roles y el nivel de aseguramiento.

El propósito último de un Mapa de Aseguramiento es facilitar al Consejo y a la Alta Dirección, primero, la situación, a una fecha determinada, del nivel de aseguramiento global en relación a los principales riesgos que pueden impactar en la compañía; segundo, identificar la función que proporciona el aseguramiento; y, tercero, evaluar los riesgos por categorías en función del grado de aseguramiento proporcionado.

Esta información puede ser la base sobre la que Auditoría Interna orienta sus actuaciones incluidas en su Plan Anual de Actividades, para enfocarlas hacia aquellos riesgos relevantes cuyo nivel de aseguramiento no considere adecuado.

Proceso elaboración de los mapas de aseguramiento

La elaboración de mapas de aseguramiento se estructura en tres fases:

- **Fase 1: Identificamos los procesos o actividades relevantes de la sociedad,** para garantizar la integridad del mapa de aseguramiento. Elaboramos un **"mapa de procesos"** e identificamos para cada uno de

En función del Mapa de Aseguramiento resultante Auditoría Interna determina las actividades poniendo el foco en los riesgos que presentan déficits de supervisión.

ellos el responsable de la actividad, y la función de aseguramiento que ejerce el segundo nivel de control en cada una de ellas.

- **Fase 2. Asignamos a los procesos o actividades anteriores uno o varios riesgos.** El objetivo es asociar los principales riesgos a los que se enfrenta la sociedad, ya identificados en el modelo de riesgos, a sus correspondientes procesos.

  En esta fase incorporamos métricas (límites o indicadores) que midan los riesgos en relación al valor deseable. Las medidas se determinan en función del Apetito y Tolerancia al riesgo definido y determinado por el Consejo de Administración (*ver documento de LA FÁBRICA DE PENSAMIENTO: Definición e implantación de Apetito de Riesgo)*

- **Fase 3. Identificamos las funciones que aseguran cada uno de los riesgos; evaluamos el nivel de aseguramiento de cada función en relación a cada riesgo bajo su supervisión. Todo ello conforma el "mapa de aseguramiento".**

En función del Mapa de Aseguramiento resultante, Auditoría Interna determina las actividades. El foco se coloca en los riesgos que presentan déficits de supervisión, ya sea por su ausencia o porque que es insuficiente.

EJEMPLO MAPA DE ASEGURAMIENTO

Categoría de Riesgos	RIESGO		2ª LÍNEA DE DEFENSA								3ª LÍNEA DE DEFENSA
	Nombre	Descripción	Control Interno	Control Información Financiera	Seguridad de la Información	Seguridad física de activos	Cumplimiento Normativo	Gestión de riesgos	Sistema integral de gestión	RSC y reputación corporativa	Auditoría Interna
Estratégicos											
Operacionales											
Cumplimiento y regulatorios											
Información financiera y mercados											

Con diferentes colores, se marcaría en la celda que cruza riesgo con función que realiza el aseguramiento, el nivel de aseguramiento proporcionado, indicando asimismo cuál es la actividad que proporciona ese aseguramiento

Glosario

AEB
Asociación Española de Banca

CAAT
Computer Assisted Auditing Techniques (Técnicas y Programas desarrollados para los Procesos de Auditoría)

CNMV
Comisión Nacional del Mercado de Valores

COBIT
Control Objectives for Information and Related Technology (Objetivos de Control para Información y Tecnologías Relacionadas)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

DGSFP
Dirección General de Seguros y Fondos de Pensiones

EBA
European Banking Association (Asociación de Banca Europea)

EFQM
European Foundation for Quality Management (Fundación Europea para la Gestión de Calidad)

EIOPA
European Insurance and Occupational Pensions Authority (Autoridad Europea de Seguros y Pensiones)

ESMA
European Supervision Market Authority

IAGC
Informe Anual de Gobierno Corporativo

IDS
Intrusion Detection System (Sistemas de Detección de Intrusiones)

IEC
Comisión Electrotécnica Internacional

IIA
Institute of Internal Auditors

ISO
Organización Internacional de Normalización, cuyo nombre no proviene de las siglas en inglés, sino del griego "isos" ("igual")

LISI
Ley del Impulso de la Sociedad de la Información

LOPD
Ley Orgánica de Protección de Datos

LSSI
Ley de Servicios de la Sociedad de la Información

MIFID
Markets in Financial Instruments Directive (Directiva sobre los Mercados Financieros)

NIIF
Normas Internacionales de Información Financiera

OHSAS
Occupational Health and Safety Assessment Series (Sistemas de Gestión de Salud y Seguridad Laboral)

PBC y FT
Prevención de Blanqueo de Capitales y Financiación del Terrorismo

PCI-DSS
Payment Card Industry - Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)

RC
Responsabilidad Corporativa

SCIIF
Sistema de Control Interno de la Información Financiera

SEPBLAC
Servicio Ejecutivo de Prevención de Blanqueo de Capitales

SGIIC
Sociedad Gestora de Instituciones de Inversión Colectiva

Solvencia II
Directiva sobre las normas europeas del Seguro

SOX
Ley Sarbanes-Oxley

TI
Tecnología de la Información

UNE
Conjunto de normas tecnológicas en España

UNEP
United Nations Environment Programme (Programa de las Naciones Unidas para el Medio Ambiente)

Anexo 1 · Control Interno

MISIÓN Y OBJETIVOS

La misión y objetivos de la Función de Control Interno es dar soporte a la compañía en la difusión de la cultura de control en la organización, así como diseñar, implantar y gestionar un sistema de control interno que proporcione a la Dirección y al Comité de Auditoría, seguridad razonable sobre la fiabilidad de los controles establecidos en los procesos de negocio y soporte (destacando el papel principal de los procesos de TI como soporte del negocio) con el objetivo de minimizar riesgos y conseguir los objetivos estratégicos de la compañía.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Soporte a la Alta Dirección en la difusión de la cultura de control interno e incremento del ambiente de control.
- Coordinación en la homogenización de las políticas, procedimientos y controles internos.
- Seguimiento del cumplimiento de los sistemas de control interno en la organización para garantizar una adecuada cobertura de los riesgos y una protección de la reputación de la organización.

Entregables:

- Informe sobre control interno a la Alta Dirección.
- Mapa de riesgos.
- Propuesta de información a incluir en el IAGC.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comités de Control Interno.
- Modeladores de procesos y herramientas de gestión de riesgos y de tratamiento masivo de datos CAAT.
- Indicadores para la descripción del ambiente del control interno.
- Mapas de procesos y matrices de riesgos y controles. Manuales de procedimientos.
- Informes de revisión periódicos.

Anexo 1 · Control Interno

REGULACIÓN y MARCOS DE REFERENCIA

Externa:

- Disposiciones de organismos reguladores sectoriales, principalmente actividades financieras y aseguradoras (Guía 44 EBA sobre Control Interno).
- Normativa contable aplicable (Plan General Contable, NIIF, …)
- Ley del Mercado de Valores y Normativa CNMV.
- Ley de Auditoría de Cuentas y Ley de Economía Sostenible.
- Código de Buen Gobierno.
- Recomendable: COSO, COBIT.

Interna:

- Principios de actuación de la Función.
- Políticas y manuales de procedimientos internos de la Función.
- Planes estratégicos y anuales de la Función.
- Código de Buen Gobierno; Código ético y de conducta; Política y manuales de Control Interno, etc.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Revisión y evaluación del Marco de Control Interno y de la función de aseguramiento.
- Revisión de la eficacia de dichos controles y de la correcta evaluación y gestión de riesgos.
- Seguimiento de los planes de acción relacionados con la implementación de los controles recomendados.
- Proporcionar aseguramiento respecto a los procesos de evaluación del control interno.
- Reporte periódico de las observaciones de Auditoría sobre el control interno y planes de acción para su ejecución.
- Asistencia a Comités de Control Interno, en su caso.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Colaborar en la elaboración de políticas y procedimientos internos y el traslado de conocimiento sobre el ambiente de control interno.
- Reuniones periódicas de coordinación y divulgación de actividades de ambas funciones de aseguramiento para establecer nexos de unión y colaboración.
- Apoyo en la identificación de ausencias de control en los procesos de TI y negocio.
- Asesorar a la Dirección en el establecimiento de prioridades para la ejecución de los planes de acción.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Definición e implantación del Marco de Control Interno en la compañía: políticas y procedimientos internos.
- Asumir la responsabilidad en el diseño, implantación y mantenimiento de los controles internos.

Anexo 2 · Control Interno sobre la Información Financiera

MISIÓN Y OBJETIVOS

La misión y objetivos del Sistema de Control Interno de la Información Financiera es proporcionar a la Dirección y al Comité de Auditoría, seguridad razonable sobre la fiabilidad de la información financiera que presentan para su aprobación al Consejo de Administración y que se hace pública periódicamente a los reguladores y al mercado.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Diseño e implantación del sistema de control interno para la elaboración de la información financiera fundamentado en la evaluación de los riesgos.
- Gestión de los componentes de control interno, de acuerdo con el marco de referencia escogido.
- Seguimiento del grado de cumplimiento del sistema de control interno en la organización y reporte a la dirección.

Entregables:

- Mapa de riesgos de los procesos de elaboración de la información financiera.
- Informe Anual de Gobierno Corporativo (en el que se describe el SCIIF).
- Normativa interna sobre SCIIF.
- Informe sobre cumplimiento de SCIIF a la Alta Dirección.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comité de control.
- Sistemas informáticos de elaboración de la información financiera.
- Sistemas informáticos de gestión de SCIIF.
- Mapas de riesgos de los procesos de elaboración de la información financiera.

Anexo 2 · Control Interno sobre la Información Financiera

REGULACIÓN y MARCOS DE REFERENCIA

Externa:

- Normativa contable aplicable (Plan General Contable, NIIF, …)
- Ley del Mercado de Valores, Normativa CNMV y/o SOX.
- Ley de Auditoría de Cuentas y Ley de Economía Sostenible.
- Recomendadas: COSO, COBIT.

Interna:

- Principios de actuación de la Función.
- Políticas y manuales de procedimientos internos de la Función.
- Planes estratégicos y anuales de la Función.
- Código interno de conducta en el Mercado de Valores.
- Normativas y políticas contables, de cierre contable y reporte de la información, de seguridad de la información, de actividades subcontratadas, y otras realidades que afecten de forma significativa a los procesos de elaboración de la Información Financiera.

ROL DE AUDITORíA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Evaluación anual del funcionamiento y efectividad global del SCIIF (analizar si el sistema es capaz de detectar o prevenir riesgos con impacto significativo en la fiabilidad de la información financiera).
- Revisión periódica de efectividad de controles sobre el SCIIF.
- Reporte al Comité de Auditoría.
- Seguimiento de recomendaciones.
- Revisión del apartado del Informe Anual de Gobierno Corporativo relativo al SCIIF.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Apoyo metodológico respecto a la identificación y evaluación de riesgos del proceso de información financiera.
- Apoyo en la identificación de controles o diseño de los mismos.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Asumir funciones ejecutivas en la gestión del SCIIF.
- Ejecución de actividades de control.

Anexo 3 · Seguridad de la Información

MISIÓN Y OBJETIVOS

La misión y objetivos de la Función de Seguridad de la Información es definir y establecer mecanismos, estrategias, soluciones organizacionales y de sistemas tecnológicos que permitan alcanzar, resguardar, proteger y garantizar las principales características de la seguridad de los activos de información (confidencialidad, integridad y disponibilidad).

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Establecimiento de una estructura de gobierno de la seguridad de la información en la compañía y definición de un marco normativo en materia de seguridad de la información.
- Establecimiento de los controles y mecanismos para garantizar las medidas necesarias en materia de seguridad de la información, así como establecimiento de revisiones tecnológicas de seguridad con objeto de detectar vulnerabilidades en los sistemas.
- Apoyo a la informática forense en la detección y prevención de fraudes.

Entregables:

- Plan director de seguridad.
- Mapas de riesgo de seguridad de la información.
- Políticas, normas y procedimientos en materia de seguridad de la información.
- Informes sobre revisiones tecnológicas de seguridad, tanto internas (caja blanca) como externas (caja negra).

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comités de Seguridad.
- Herramientas informáticas de cifrado de los sistemas, controles y monitorización de eventos de seguridad.
- Sistemas de prevención (antivirus y firewalls) y de detección de intrusiones (IDS).
- Sistemas de control de accesos a los sistemas. Matrices de autorizaciones y tipos de accesos a los sistemas.
- Protocolos seguros de comunicación.

Anexo 3 · Seguridad de la Información

REGULACIÓN y MARCOS DE REFERENCIA

Externa:

- Legislación en materia de Protección de Datos de Carácter Personal (LOPD y Reglamento de Medidas de Seguridad).
- Ley de Servicios de la Sociedad de la Información y Ley del Impulso de la Sociedad de la Información (LSSI y LISI).
- Legislación en materia de infraestructuras Criticas: Ley 8/2011, de 28 de abril y RD 704/2011 de 20 de mayo.
- Ley de Firma Electrónica.
- Dinero electrónico (PCI-DSS y Ley 21/2011).
- Recomendable: COSO, COBIT, ISO/IEC 27000 Series.

Interna:

- Políticas y manuales de procedimientos internos de la función.
- Planes estratégicos y anuales de los sistemas de información.
- Política de seguridad de la información.
- Política de continuidad de negocio. Cuerpo Normativo en materia de seguridad de la información.
- Código ético y de conducta.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Revisión y evaluación de la función de seguridad de la información dentro de la compañía en cada una de sus áreas de responsabilidad.
- Seguimiento de planes de acción relacionados con seguridad de la información, fruto de auditorías previas.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Elaboración del Plan Anual de Auditoría de TI. Factor adicional para determinar posibles trabajos de auditoría.
- Apoyo en la identificación de debilidades en materia de seguridad de la información.
- Reuniones periódicas de coordinación y divulgación de actividades de ambas funciones de aseguramiento para establecer nexos de unión y colaboración.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Definición e implantación del cuerpo normativo en materia de seguridad de la información.
- Definición de los controles y acciones relativos a esta materia.

Anexo 4 · Seguridad Física de Activos y Personas

MISIÓN Y OBJETIVOS

La misión y objetivos de la función de seguridad física de activos y personas es salvaguardar los activos físicos de la compañía, así como la seguridad física de los empleados y directivos de la organización, gestionar los riesgos externalizables con las pólizas de seguros más adecuadas, así como, en el caso de organizaciones sujetas a normativa de infraestructuras críticas en particular, minimizar los riesgos generados por el terrorismo internacional, la proliferación de armas de destrucción masiva y el crimen organizado.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Definición e implantación de la política de seguridad de la organización, en cuanto a activos críticos y personal.
- Gestión, coordinación y supervisión del funcionamiento de los servicios de seguridad internos y externos.
- Planificación y ejecución de los planes de formación en materia de seguridad, asesorando a las distintas áreas de la organización cuando sean requeridos.

Entregables:

- Mapas de riesgos de seguridad física y de personas.
- Plan estratégico de seguridad, políticas y procedimientos de actuación interna y externa.
- Informes periódicos de capitales asegurados por activos y riesgos personales.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comités de riesgos.
- Políticas de gestión de seguros de la organización
- Herramientas informáticas de análisis actuarial de riesgos asegurables.
- Herramientas Informáticas de gestión y control de los riesgos. Modelos estocásticos y estadísticos.
- Manuales de procedimientos internos de seguridad física de activos y empleados.

Anexo 4 · Seguridad Física de Activos y Personas

REGULACIÓN Y MARCOS DE REFERENCIA

Externa:

- Ley 23/1992 de Seguridad Privada y RD 2364/1994.
- Legislación en materia de infraestructuras críticas: Ley 8/2011 de 28 de abril y RD 704/2011 de 20 de mayo.
- Recomendable: ISO/IEC 27000 Series.

Interna:

- Políticas y manuales de procedimientos internos de la función, comunicación de siniestros, seguridad y control de accesos, etc.
- Planes estratégicos y anuales de la función.
- Políticas generales de contratación de seguros.
- Manuales de seguridad para empleados en países con especiales riesgos.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Proporcionar aseguramiento respecto a los procesos de gestión de estos riesgos.
- Evaluar los procesos de gestión de riesgos en relación con seguridad física de activos y personas.
- Evaluar la elaboración de informes sobre estos riesgos críticos y revisar la gestión de los mismos.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Colaborar en la elaboración de los mapas de riesgos: identificación y evaluación de los principales riesgos.
- Asesorar a la dirección en la respuesta a los riesgos identificados en relación a este área.
- Colaborar en la implantación y mantenimiento del marco de la gestión de estos riesgos y su política, como soporte para el Consejo a través de la Comisión de Auditoría.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Definición de cuáles son riesgos externalizables o no.
- Imponer procesos de gestión de riesgos de seguridad física de activos y personas.
- Asumir funciones ejecutivas en el aseguramiento de estos riesgos o la respuesta a los mismos.
- Asumir responsabilidades sobre la gestión propia de estos riesgos.

Anexo 5 · Cumplimiento Normativo

MISIÓN Y OBJETIVOS

La misión y objetivos de la función de cumplimiento normativo es identificar los requisitos normativos derivados de leyes, regulaciones y requerimientos administrativos, supervisar el grado de cumplimiento de los requisitos normativos e identificar las deficiencias y responsables, coordinar con las áreas implicadas el diseño y lanzamiento de planes de subsanación, evaluar el posible impacto de cambios en el entorno regulatorio sobre las operaciones de la empresa en materias de su competencia, y establecer y definir el programa de cumplimiento sobre la base del inventario de hechos regulatorios.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Identificación de requisitos normativos derivados de leyes, regulaciones y requerimientos administrativos del sector así como evaluación del impacto de cambios regulatorios sobre las operaciones de la empresa.
- Establecimiento y definición del programa de cumplimiento sobre la base del inventario de hechos regulatorios
- Seguimiento del grado de cumplimiento de los requisitos normativos, identificación de deficiencias y responsables así como coordinación con las áreas implicadas en el diseño y lanzamiento de planes de subsanación.

Entregables:

- Mapa de riesgos regulatorios.
- Actas del Comité de Cumplimiento Normativo y del Comité de Prevención de Blanqueo de Capitales.
- Informe periódico sobre cumplimiento normativo a la Alta Dirección.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Código de conducta.
- Herramientas de alertas.
- Procedimientos internos y manuales de funciones.
- Inventario de hechos regulatorios.

REGULACIÓN Y MARCOS DE REFERENCIA

Externa:

- Disposiciones de organismos reguladores sectoriales, principalmente actividades financieras y aseguradoras (Comité de Supervisión Bancaria de Basilea, Banco Central Europeo, EBA, ESMA, Banco de España, CNMV, SEPBLAC), entre otras, por su relevancia:
  - Directiva MIFID 2004/39/CE y su transposición 2008/10/CE, Ley de Transparencia Bancaria 7/2012, Ley del Mercado de Valores 24/1988, Circular 6/2009 sobre Control Interno de SGIIC, Ley 10/2010 de 28 de abril sobre PBCyFT.
  - Ley de Mediación de Seguros, Reglamento de Ordenación y Supervisión de los Seguros Privados, Directiva de Solvencia II, Normativa de la DGSFP, Normativa EIOPA.

Anexo 5 · Cumplimiento Normativo

REGULACIÓN Y MARCOS DE REFERENCIA

- Legislación en materia de Protección de Datos de Carácter Personal (LOPD, Ley 15/1999 y RD 1720/2007).
- Ley 5/2010 de Reforma del Código Penal.
- Recomendadas: AEB, EIOPA, COSO.

Interna:

- Principios de actuación de la función.
- Políticas y manuales de procedimientos internos de la función.
- Planes estratégicos y anuales de la función.
- Manuales y políticas internas: Prevención de riesgos penales, Prevención de blanqueo de capitales, Normativa MIFID, Ley de protección de datos, Código ético y de conducta, Canales de denuncias, etc.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Evaluar periódicamente y de forma independiente la efectividad en el cumplimiento de las actividades asignadas a la función de cumplimiento normativo.
- Analizar la claridad y transparencia respecto a las actividades asignadas a la función.
- Mantener informada a la función de cumplimiento de cualquier circunstancia hallada dentro de la Función de Auditoría Interna y que tenga implicaciones normativas.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Relación con supervisores y reguladores.
- Colaborar en la elaboración de los mapas de riesgos: identificación y evaluación de los principales riesgos.
- Colaborar en la coordinación de la gestión de riesgos de cumplimiento normativo.
- Colaborar en el mantenimiento del marco de la gestión de riesgos y su estrategia como soporte del Consejo.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Imponer procesos de gestión de riesgo de cumplimiento.
- Definir niveles de apetito de riesgo de cumplimiento.
- Mantener responsabilidades en la gestión del riesgo de cumplimiento normativo, en particular, tomando decisiones de respuesta a situaciones de riesgo o ejecutando controles primarios.

Anexo 6 · Gestión de Riesgos

MISIÓN Y OBJETIVOS

La misión y objetivos de la función de gestión de riesgos es adoptar, aplicar y mantener procedimientos y políticas de gestión del riesgo que permitan suministrar información relevante sobre la situación de los riesgos de la organización, a la Alta Dirección y los Órganos de Gobierno, para conocer su impacto en la consecución de los objetivos de dicha organización.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Coordinación de los procesos de identificación y evaluación de los riesgos mediante la elaboración y actualización de los mapas de riesgos, atendiendo a su potencial amenaza en la consecución de los objetivos de la organización.
- Coordinación de los procesos de medición de los riesgos, así como los controles y procedimientos necesarios para mitigarlos, contribuyendo a conseguir el nivel de apetito y la tolerancia al riesgo definido por el Consejo de Administración.
- Establecimiento de los mecanismos de comunicación periódica de la evolución y el seguimiento de los riesgos, especialmente de aquellos más críticos o que se hayan materializado, informando sobre las consecuencias y el impacto económico de los mismos.

Entregables:

- Mapas de riesgos de la organización.
- Informes de seguimiento de riesgos, de materialización de riesgos y planes de acción.
- Información sobre gestión de riesgos en el IAGC.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comités de riesgos.
- Políticas de gestión de riesgos y manuales de procedimientos.
- Herramientas informáticas de gestión y control de los riesgos.
- Mapas de riesgos y de procesos.

Anexo 6 · Gestión de Riesgos

REGULACIÓN Y MARCOS DE REFERENCIA

Externa:

- Ley del Mercado de Valores y normativa CNMV.
- Ley de Auditoría de Cuentas y Ley de Economía Sostenible.
- Ley de Transparencia Bancaria 7/2012.
- Código de Buen Gobierno.
- Recomendable: COSO, COBIT, Norma ISO 31000.

Interna:

- Principios de actuación de la función.
- Políticas de gestión de riesgos y Reglamentos de la Comisión de Auditoría y Consejo de Administración en relación a las funciones de supervisión de los sistemas de gestión de riesgos.
- Planes estratégicos y anuales de la función.
- Código ético-Código de conducta.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Proporcionar aseguramiento respecto a los procesos de gestión de riesgos y la correcta evaluación de los mismos.
- Evaluar los procesos de gestión de riesgos, incluyendo la supervisión de controles y procedimientos.
- Evaluar y revisar la elaboración de informes sobre riesgos clave y revisar la gestión de los mismos.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Colaborar en la identificación y evaluación de los principales riesgos.
- Asesorar a la dirección en la respuesta a los riesgos identificados.
- Colaborar en la coordinación de la gestión de riesgos.
- Colaborar en la implantación y mantenimiento del marco de la gestión de riesgos y su política, como soporte para el Consejo a través de la Comisión de Auditoría.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Definición del apetito al riesgo.
- Imponer procesos de gestión de riesgos.
- Asumir funciones ejecutivas en el aseguramiento de riesgos o la respuesta a los mismos.
- Asumir responsabilidades sobre la gestión propia de los riesgos.

Anexo 7 · Sistemas Integrales de Gestión

MISIÓN Y OBJETIVOS

La misión y objetivos de la función del sistema de gestión integral es fusionar las normas ISO 9001:2008, ISO 14001:2004 y OHSAS 18001:2007 en un solo sistema, que implementa los elementos comunes simultáneamente y mantiene independientes los elementos de calidad, ambiente y ocupación, salud y seguridad, trabajando todo como un solo sistema sustentado en la mejora continua.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Estudio y coordinación de las actividades de innovación y desarrollo para satisfacer las expectativas de los clientes internos/externos, empleados y otros grupos de interés.
- Potenciación de la cultura de mejora continua en los productos y la gestión de los procesos de la sociedad, así como supervisión de la consecución del nivel de beneficio suficiente para la retribución correspondiente al capital empleado.
- Seguimiento del cumplimiento de la normativa, las leyes y otros compromisos en medio ambiente, prevención de riesgos laborales, etc.; así como seguimiento de la mejora de los indicadores financieros y no financieros (liderazgo, responsabilidad social, ambientales, seguridad).

Entregables:

- Planes de Auditoría de calidad, medio ambiente y prevención de riesgos laborales
- Informes de conclusiones de auditorías.
- Estado de las no conformidades/recomendaciones propuestas.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comités de calidad, medioambiente, prevención de riesgos laborales.
- Herramientas informáticas para la gestión documental de los informes de las auditorías, y seguimiento de no conformidades.
- Políticas, manuales de gestión y procedimientos del sistema de gestión integral.
- Planes de auditorías especializadas en: calidad, medio ambiente, prevención de riesgos laborales.

Anexo 7 · Sistemas Integrales de Gestión

REGULACIÓN Y MARCOS DE REFERENCIA

Externa:

- Legislación en materia medioambiental, de prevención de riesgos laborales, calidad y estandarización, ya sea de alcance global o sectorial.
- Recomendable: Normas ISO, Modelo EFQM, Prevención de Riesgos laborales: OHSAS 18001:2007.

Interna:

- Políticas y manuales de procedimientos internos de la función.
- Planes estratégicos y anuales de la función.
- Políticas corporativas de calidad, medio ambiente, prevención de riesgos laborales.
- Sistema de gestión integral de la compañía.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Emitir opinión respecto al alcance y suficiencia de los planes de auditorías especializadas.
- Revisar el cumplimiento con los planes de auditorías especializadas, asegurando que se realiza seguimiento de las no conformidades identificadas.
- Evaluar la competencia profesional de los auditores de calidad, medio ambiente o prevención de riesgos laborales.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Realizar auditorías en colaboración con los auditores de calidad, medio ambiente y prevención de riesgos laborales.
- Reuniones periódicas de coordinación y divulgación de actividades para establecer nexos de unión y colaboración.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Definir y aprobar políticas de calidad, medio ambiente, prevención de riesgos laborales.
- Diseño e implementación de un sistema de gestión integral.

Anexo 8 · Responsabilidad Corporativa y Reputación Corporativa

MISIÓN Y OBJETIVOS

La misión y objetivos de la responsabilidad corporativa y la reputación corporativa es gestionar las acciones de la compañía encaminadas a la transparencia informativa y las relaciones con grupos de interés en ámbitos como el gobierno corporativo, la ética en los negocios, los derechos humanos, los actores sociales en los que la compañía impacta en el desarrollo de sus actividades y en el medio ambiente.

FUNCIONES Y PRINCIPALES ENTREGABLES

Funciones:

- Seguimiento del posicionamiento de la organización en la sociedad, el prestigio de la marca y su propiedad intelectual, y elaboración de memorias de actividades, así como colaborar en la realización de la memoria anual.
- Estudio, diagnóstico y propuesta de políticas y acciones para el cumplimiento de los estándares de referencia y adaptación del desempeño de la organización a los requerimientos establecidos por determinados índices de sostenibilidad.
- Coordinación de los planes de acción para la ejecución de las acciones.

Entregables:

- Informe de responsabilidad corporativa anual que elabora el equipo gestor.
- Memorias de sostenibilidad incluidas en la comunicación corporativa.
- Informes de Auditoría Interna sobre empresas vinculadas/proveedores/subcontratas.

HERRAMIENTAS SOPORTE DE LA FUNCIÓN

- Comité de sostenibilidad
- Herramientas para elaborar los informes de responsabilidad corporativa (AA1000, ISAE 3000) y herramientas para recopilar y consolidar la información a través de la organización.
- Mapas de riesgo reputacionales.
- Políticas de recursos humanos en relación a igualdad, conciliación familiar, etc. y Política de marca corporativa.
- Plan anual de responsabilidad corporativa.
- Auditoría externa sobre la memoria de responsabilidad corporativa e informes externos sobre sostenibilidad.

Anexo 8 · Responsabilidad Corporativa y Reputación Corporativa

REGULACIÓN Y MARCOS DE REFERENCIA

Externa:

- Recomendable: United Nations, Global Reporting Iniciative, UNEP.

Interna:

- Principios de actuación de la función.
- Manual de procedimientos internos de la función.
- Planes estratégicos y plan director periódicos de responsabilidad corporativa y reputación corporativa.

ROL DE AUDITORÍA INTERNA RESPECTO A LA FUNCIÓN DE ASEGURAMIENTO

Actividades propias de Auditoría Interna en relación con esta función:

- Proporcionar aseguramiento respecto a los procesos de gestión de la responsabilidad corporativa y la imagen reputacional.
- Evaluar los procesos de gestión de los riesgos reputacionales y los impactos de dicha actividad en la sociedad.
- Evaluar la elaboración de las memorias anuales y la fiabilidad e integridad de la información del reporte integral a grupos de interés.

Actividades de Auditoría Interna en colaboración limitada con esta función:

- Colaborar en la evaluación del grado de cumplimiento de los estándares de referencia.
- Asesorar a la Dirección en la respuesta a los riesgos reputacionales.
- Revisión de los canales de denuncia.
- Colaborar en el mantenimiento del marco de la gestión del riesgo reputacional y su estrategia como soporte del Consejo.

Actividades que Auditoría Interna no debería desarrollar en relación con esta función:

- Asumir funciones ejecutivas en la elaboración del reporte integral a terceros.
- Asumir responsabilidades sobre la gestión propia de estos riesgos.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Esta nueva producción de LA FÁBRICA DE PENSAMIENTO, Guía práctica "Marco de relaciones de Auditoría Interna con otras Funciones de Aseguramiento", ayuda a fijar posiciones sobre la necesidad de mejorar la eficiencia de los recursos de las Direcciones de Auditoría interna para mantener el nivel adecuado de aseguramiento en coordinación con las distintas funciones de aseguramiento.

El documento aborda la necesidad de realizar un mapa de aseguramiento, que proporcione una visión global de las actividades de control llevadas a cabo por las distintas funciones de aseguramiento de una organización, proponiendo a Auditoría Interna como coordinador principal de todas ellas.

Esta guía práctica será de utilidad para los profesionales de Auditoría Interna y para todos aquellos profesionales que participan en los distintos niveles de aseguramiento de una organización.

Edita

Instituto de Auditores Internos de España

Patrocina

FUNDACIÓNMAPFRE