PRÁCTICAS DE BUEN GOBIERNO

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Gobierno del Riesgo de Cumplimiento

Relación entre Auditoría Interna y Cumplimiento Normativo

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.200 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.

AUDITORÍA INTERNA

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS

OBSERVATORIO SECTORIAL

PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

PRÁCTICAS DE BUEN GOBIERNO

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Gobierno del Riesgo de Cumplimiento

Relación entre Auditoría Interna y Cumplimiento Normativo

Junio 2018

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:
José Enrique Díaz Menaya, CIA, COSO, CRMA, ROAC. BERGÉ Y CÍA.

Carlos Balmisa García-Serrano, CIA. COMISIÓN NACIONAL DE MERCADOS Y COMPETENCIA (CNMC).
Mariano José Casado Carrillo de Albornoz, CFE. IBERDROLA.
José Antonio Castrillo Nuevo, CISA, CISM, CGEIT. MAZARS AUDITORES.
Enric Domenech Rey, CRMA, ROAC. BDO.
Cristina Fabre Chicano, ROAC. CEPSA.
Eduardo García Rivas. EY.
Cristina González Barreda, CIA. GRUPO BBVA.
Blanca Lantarón Martín, , CIA. RED ELÉCTRICA DE ESPAÑA.
Eva López de Sebastián Miro. VIESGO INFRAESTRUCTURAS ENERGÉTICAS.
Caroline Marion, COSO. EVO BANCO.
Carlos Méndez-Trelles García. RED ELÉCTRICA DE ESPAÑA.
María Isabel Morte Gómez, CIA. AMEC FOSTER WHEELER ENERGÍA.
Eduardo Navarro Villaverde. CALIDAD PASCUAL - CUMPLEN.
María de la Sierra Pérez García, CIA. GRUPO MUTUA MADRILEÑA.
José Antonio Rosich Parte, CIA. LIBERBANK.
Caridad Saboya Mariscal. FINTONIC

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Instituto de Auditores Internos de España

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

Depósito Legal: M-20681-2018
ISBN: 978-84-948405-2-4

Diseño y maquetación: desdecero, estudio gráfico

Impresión: Grafilia

El contexto regulatorio en el que operan las empresas es exigente y complejo y las consecuencias de no gobernarlo adecuadamente puede tener enormes impactos, que van desde la clausura temporal o total de la actividad de la empresa hasta pérdidas financieras derivadas de sanciones fijadas por un tribunal. A ellas se suma la pérdida de confianza por parte de clientes e inversores, entre otros grupos de interés.

Ante este contexto, el Gobierno del riesgo de Cumplimiento requiere que las organizaciones presten especial atención a la identificación, gestión y control de este riesgo dentro sus modelos y sistemas de gestión de riesgos dado que puede aparecer en cualquier proceso y actividad que lleve a cabo la empresa.

Al igual que todo el Sistema Integral de Gestión de Riesgos, corresponde al Consejo de Administración establecer y fomentar una cultura de cumplimiento alineada con la voluntad de cumplir, además de fijar una estructura que asegure la adecuada cobertura de este riesgo.

No existe un modelo único de Gobierno del riesgo de Cumplimiento en las organizaciones (salvo en las de sectores regulados, banca y seguros), que establezca cómo se debe desplegar en la estructura, organización interna y líneas de reporte; sino que deben considerarse el tamaño de la empresa, el grado de madurez y complejidad del sistema de control, así como los recursos disponibles y la existencia de otras funciones de aseguramiento.

Felicito a los autores de esta guía, profesionales de la Auditoría Interna y del Cumplimiento, por proponer un modelo abierto que asegure una adecuada relación y colaboración entre las áreas de Cumplimiento y Auditoría Interna que sirva para proteger el valor de empresas y organizaciones, fin último que debe guiar el Gobierno de este riesgo, complejo y transversal.

Instituto de Auditores Internos de España

Índice

Introducción

La naturaleza del riesgo de cumplimiento requiere mayor atención para su identificación, gestión y control, e integrarlo en los sistemas de gestión y control de riesgos.

Con un entorno regulatorio y una sociedad cada vez más exigentes, es indispensable que las entidades –más globales y complejas– identifiquen, gestionen y controlen los riesgos que puedan interferir en la consecución de sus objetivos.

Entre estos riesgos están los denominados "de cumplimiento", cuyo impacto puede provocar desde la clausura temporal o total de la sociedad, la administración judicial, sanciones o pérdidas financieras fijadas por un tribunal por incumplimientos legales, hasta incidencias reputacionales por compromisos adquiridos con terceros que podrían sacar a la sociedad del mercado. La naturaleza y repercusión de estos riesgos, que pueden darse a lo largo de todos los procesos y actividades de una organización hace que los órganos de administración, dada su obligada diligencia y responsabilidad[1], se muestren especialmente sensibles a su gestión y control.

En este contexto, es importante integrar el riesgo de cumplimiento normativo en la gestión y control de riesgos. El Cumplimiento de la entidad define una Cultura que contiene intrínsecamente un modo de relacionarse en el mercado de una manera ética y responsable con las obligaciones legales, regulatorias y sectoriales, contratos y, si cabe en mayor medida, satisfaciendo los compromisos autoimpuestos internamente.

Una regulación cada vez más clara y exigente en este sentido, y la naturaleza de este tipo de riesgos –que pueden aparecer a lo largo de todos los procesos y actividades de una organización– requieren que las organizaciones presten una mayor atención a la identificación, gestión y control de los riesgos de cumplimiento y a la necesidad de considerarlos dentro de sus modelos o sistemas de gestión de riesgos, por lo que cada vez más entidades han implantado, o van a implantar, modelos de *Corporate Compliance*[2] (Cumplimiento Corporativo).

Así, por ejemplo, la reforma del Código Penal español de 2015 en lo relativo a la responsabilidad penal de las personas jurídicas (Ley Orgánica 1/2015 de 30 de marzo, que modifi-

1. Artículo 225 de la ley 31/2014, de 3 de diciembre, por la que se modifica la Ley de Sociedades de Capital para la mejora del gobierno corporativo.

2. UNE-ISO 19600:2015, *Sistemas de Gestión de Compliance.*

ca la Ley Orgánica 10/1995[3]) supuso un impulso importante en la implantación y definición de modelos de Cumplimiento Corporativo estructurados y formalizados en las organizaciones. Estos modelos, si cumplen las condiciones previstas en las normativas que los contemplan, pueden mitigar e incluso eximir de determinadas responsabilidades al ser elementos que evidencian la debida diligencia y control con la que deben actuar directivos y administradores.

La Alta Dirección de la Organización, como responsable de la gestión, control y supervisión de este tipo de riesgos[4], debe definir el alcance de su compromiso y fomentar una cultura alineada con la voluntad de cumplir, siendo ejemplo de tal compromiso.

El gráfico a la derecha refleja una relación entre el grado de voluntad de la entidad con la Cultura de Cumplimiento, según el alcance de trabajo que tenga la función de Cumplimiento.

La pirámide parte de los requisitos básicos para operar en el mercado, pasando a los modelos de prevención de delitos, riesgos legales de continuidad de negocio (aquellos donde el impacto económico o reputacional dificultaría la continuidad normal del negocio), llegando a un alcance de cumplimiento normativo (donde pretendemos asegurar todos los cumplimientos legales aunque sean menores, códigos internos e instrucciones de la propia organización) hasta terminar en el *Compliance* (donde se amplía el alcance anterior con los compromisos voluntarios aceptados por la organización con el conjunto de los grupos de interés).

Fuente: Elaboración propia

No existe un modelo único que establezca cómo debe ser el desarrollo de la estructura, organización interna y líneas de reporte del área de Cumplimiento. Aunque en las organizaciones a partir de un nivel estructural medio existe una clara tendencia prospectiva al nombramiento de un Director de Cumplimiento *(Compliance Officer),* la solución práctica depende de diversos factores, como la existencia de regulación sectorial específica (caso del sector financiero), el tamaño de la empresa, el grado de madurez y los roles de otras funciones.

Por prescripción legal, el director de Cumplimiento debe disponer de la máxima independencia y autonomía para evitar posibles interferencias, conflictos de interés o represiones

3. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

4. Recomendaciones 45 y 46 del Código de Buen Gobierno de las Sociedades Cotizadas.

en el desarrollo de sus funciones. Lo más habitual es que dependa y/o tenga una línea directa de reporte por una parte, con la Alta Dirección y por otra, con los órganos de gobierno o alguna de sus comisiones delegadas que ejerzan las funciones de supervisión y control como, por ejemplo, la Comisión de Auditoría o la de Ética y Responsabilidad.

Cada organización debe evaluar la mejor forma de definir e implantar la función de Cumplimiento para lograr los objetivos que persigue.

Cada organización debe evaluar –en base a la normativa que le resulta de aplicación, su grado de madurez, disponibilidad de recursos, complejidad y otra serie de variables– la mejor manera de definir e implantar la función de Cumplimiento para lograr los objetivos que persigue. Los diferentes modelos de implantación se tratan al detalle en el apartado *Estructura de Cumplimiento* de este documento.

La creación de esta nueva función de Cumplimiento y su consolidación en aquellas organizaciones en las que ya estaba presente, así como una mayor sensibilización hacia los riesgos de Cumplimiento por parte de los *stakeholders*, afectan a la responsabilidad de Auditoría Interna sobre la evaluación de la eficacia y a la contribución por mejorar los procesos de gestión de riesgos, incluyendo en su ámbito de actuación los riesgos de cumplimiento a los que está expuesta su Organización.

Ahora, la cuestión que se plantea es cómo se debe articular la relación entre las áreas de Auditoría Interna y de Cumplimiento para que ambas alcancen sus objetivos. Si bien la respuesta estará claramente influenciada por el modelo establecido en la propia Organización, una adecuada definición de sus respectivos roles y responsabilidades, la existencia de protocolos de coordinación entre ambas y la comunicación de sus actividades al resto de la Organización serán factores clave del éxito y de la efectividad de las dos áreas.

Roles y responsabilidades

Antes de abordar el modelo de relación entre las áreas de Cumplimiento y Auditoría Interna conviene repasar los **OBJETIVOS PRINCIPALES** de ambas:

- **Cumplimiento.** Encargada de impulsar la cultura de cumplimiento, asesorar y apoyar a los órganos de Administración en la implantación y supervisión de los mecanismos necesarios para asegurar que se cumpla con las disposiciones legales, reglamentarias y administrativas que afecten a la entidad, así como de su normativa interna y compromisos autoimpuestos. Su función es supervisar el diseño de procesos y controles preventivos y detectivos para el aseguramiento y vigilar su eficacia.
- **Auditoría Interna.** Actividad independiente y objetiva de aseguramiento y consulta que se encarga de agregar valor y mejorar las operaciones de la organización para ayudarla a cumplir sus objetivos. Aporta un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno, incluyendo por tanto los riesgos de cumplimiento. Estos riesgos deben ser considerados por Auditoría Interna en la elaboración de su Plan Anual.

El Modelo de las Tres Líneas de Defensa para una efectiva gestión de riesgos y control[5] asigna las **RESPONSABILIDADES** en materia de gestión y supervisión de riesgos en tres niveles. Este modelo será la base para diferenciar los roles y responsabilidades de ambas funciones:

- La **gerencia operativa,** es decir, la Primera Línea de Defensa es realmente quien gestiona los riesgos.
- **Cumplimiento** se emplaza en la Segunda Línea de Defensa. Promueve y apoya a la organización en la implantación y supervisión de mecanismos que le permitan cumplir sus objetivos en materia de cumplimiento, asegurando el control y mitigación de los riesgos de cumplimiento, la prevención de delitos y la cultura de cumplimento, e informando de manera autónoma a los órganos de gobierno corporativo de la situación del sistema de cumplimiento. En su relación con Auditoría Interna, alertará de los riesgos presentes y futuros de cumplimiento para un correcto entorno de control.
- **Auditoría Interna** se emplaza en la Tercera Línea de Defensa. Revisa que los diferentes mecanismos establecidos por las funciones de la Primera y la Segunda Líneas de Defensa operen de manera correcta y cubran los objetivos pretendidos. Adicionalmente deberá evaluar periódicamente el diseño y la efectividad de los diferentes modelos de cumplimiento.

Por tanto, la **RELACIÓN** entre Cumplimiento y Auditoría Interna debe articularse como una relación de Segunda y Tercera Línea de Defensa, con objetivos comunes de prevención y mitigación de riesgos, preservando ambas un

Auditoría Interna y Cumplimiento deben preservar un grado de independencia que permita evaluar objetivamente el modelo de control y la gestión del riesgo de cumplimiento.

Fuente: Elaboración propia

5. ECIIA, Confederación Europea de Institutos de Auditores Internos, y FERMA (Federación Europea de Asociaciones de Gestión de Riesgos). *Modelo de las Tres Líneas de Defensa para una efectiva gestión de riesgos y control,* diciembre 2011.

grado de independencia que permita la evaluación objetiva de la eficacia del modelo de organización y control diseñado, y de la gestión de riesgos de cumplimiento.

A continuación y, siguiendo un enfoque basado en el marco de control interno propuesto por COSO[6] para cada uno de los cinco componentes de control interno, se recoge un resumen de los roles y responsabilidades clave de Cumplimiento y Auditoría Interna en el Modelo de Cumplimiento de una organización. Refleja un modelo generalista sujeto a las particularidades que sean aplicables en cada caso, especialmente cuando se responde a un requerimiento legal, ya sea a nivel sectorial o previsto en una normativa para una temática específica:

	ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA
ENTORNO DE CONTROL	Relación con la gestión	Independiente de las operaciones de la organización y responsable de la dirección/coordinación del riesgo de cumplimiento.	Independiente de las operaciones de la organización.
	Autoridad interna	Acceso a toda la Organización.	Acceso a toda la Organización.
	Código ético	Elabora y difunde, asegurando la comprensión y cumplimiento de las normas de conducta.	Audita y revisa su cumplimiento.
	Políticas y procedimientos	Propone, lidera e implanta políticas y procedimientos propios del área de Cumplimiento en función de las expectativas y objetivos de inversores y otros grupos de interés. Promueve la integración de las obligaciones de cumplimiento y de gestión de riesgos asociadas, en las políticas y procedimientos de la Organización.	Audita y verifica su implantación.
	Controles específicos	Desarrolla actividades de control e indicadores cuantificables y evaluables incorporados en los procesos de la organización en relación a los objetivos de cumplimiento.	Audita y revisa su cumplimiento.
	Evaluación del cumplimiento de las normas de conducta	Define indicadores de cumplimiento.	Audita su cumplimiento.

6. COSO (Committee of Sponsoring Organizations of the Treadway Commission). *Control Interno - Marco Integrado,* mayo 2013.

ENTORNO DE CONTROL

ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA
Canal ético	Define y asegura su adecuado funcionamiento, además de gestionarlo.	Audita el procedimiento, el funcionamiento y la gestión del canal.
Conductas irregulares	Previene, detecta e investiga.	Detecta e informa.
Conocimientos especializados relevantes	Jurídicos y regulatorios, Control Interno, gestión por procesos y gestión de riesgos.	*Marco Internacional para la Práctica Profesional de la Auditoría Interna,* Control Interno, gestión de riesgos, fraude y otras materias específicas para cubrir los distintos riesgos de la Organización, regulación, gestión por procesos, Financieros.
Desviaciones de objetivos	Mide valores esperados frente a valores reales en el ámbito de los objetivos de la Organización respecto al riesgo de cumplimiento.	Audita la gestión de las desviaciones.
Estructura de responsabilidades de control interno	Promueve la incorporación de responsabilidades en materia de Cumplimiento y control interno en las descripciones de puestos y en el sistema de evaluación de desempeño.	Asegura la existencia de mecanismos de rendición de cuentas, auditando su existencia y elaborando recomendaciones.
Sistema de control interno	Promueve, supervisa y define la estructura de Control Interno respecto al riesgo de cumplimiento, incorporando a toda la Organización.	Audita la adecuación y efectividad del sistema de Control Interno de toda la Organización.
Cambios en el entorno de negocio.	Reaccionan de manera dinámica ante los cambios, estudiando posibles impactos relacionados con el riesgo de cumplimiento en la Organización e informando a la Dirección y Consejo de Administración cuando proceda.	Actualiza el Análisis de Riesgos, pudiendo modificar su plan de auditoría para ser aprobado por la Comisión de Auditoría.
Régimen sancionador.	Promueve y define, junto con otras áreas de la Organización, la definición de un régimen sancionador adecuado frente a incumplimientos.	Revisa la existencia del procedimiento y audita el proceso de aplicación de sanciones disciplinarias.

	ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA
EVALUACIÓN DE RIESGOS	*Risk assessment*	Elabora junto con las unidades de negocio.	Audita el proceso de la Organización y propone recomendaciones de mejora. Elabora el plan de Auditoría Interna en base a un análisis de riesgos, con el input de la Alta Dirección y la Comisión de Auditoría.
	Evaluación del entorno regulatorio	Constante. Aborda nuevas implicaciones. Asegura el cumplimiento del negocio.	Periódica. Revisa el cumplimiento por parte de la Organización.
	Respuestas a los riesgos	Consensua con las unidades de negocio respuestas adecuadas a los riesgos de cumplimiento, siempre cumpliendo con los objetivos de la Organización y el nivel de Riesgo Aceptado por el Consejo de Administración.	Audita el sistema de respuesta a los riesgos de toda la Organización incluyendo los riesgos de cumplimiento.
	Parámetros de desempeño, incentivos y recompensas	Define junto con otras funciones de la Organización y asegura su revisión periódica.	Audita, en función de su plan de auditoría, las estructuras de recompensas y la medición de los resultados de la Organización, asegurando que estos respaldan un Sistema de Control Interno efectivo sin presiones excesivas.
	Apetito al riesgo	Define, con la aprobación del Consejo de Administración, el apetito al riesgo de Cumplimiento en la Organización, establece los mecanismos apropiados de gestión y vigilancia para asegurar que el valor real esté dentro del apetito definido e informa al Consejo de la situación de este con la frecuencia establecida y siempre que sea necesario.	Verifica la definición formal del apetito al riesgo validada por el Consejo de Administración. Audita su Cumplimiento y que la información que fluye hacia el Consejo sea veraz.

ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA	
Funciones de asesoramiento	Proporciona asesoramiento en materia de cumplimiento al gobierno y negocio de la Organización.	Proporciona asesoramiento en materia de gobierno, gestión de riesgos y control.	EVALUACIÓN DE RIESGOS
Enfoque de trabajo	Basado en Riesgos y procesos.	Basado en riesgos a nivel Organización, incluidos los de Cumplimiento.	
Responsabilidades operativas	Ostenta responsabilidades operativas relacionadas con el proceso de gestión del sistema de cumplimiento, y se encarga de supervisar su funcionamiento e integración con el resto de los procesos manteniendo la debida autonomía con las unidades operativas.	Es responsable de realizar los trabajos de auditoría interna. No ostenta ningún tipo de responsabilidad operativa.	ACTIVIDADES DE CONTROL
Programas de cumplimiento	Define, ejecuta y supervisa.	Audita su suficiencia y correcta ejecución.	
Metodología de trabajo	Basada en gestión de riesgos y procesos. No existe una metodología estandar generalmente aceptada para llevar a cabo las actividades de monitorización.	Basada en gestión de riesgos. Aporta un enfoque sistemático y disciplinado siguiendo las Normas Internacionales para la Práctica Profesional de la Auditoría Interna.	
Gestión por procesos	Incorpora en los procesos de la organización las actividades de control necesarias y suficientes para mitigar los riesgos de cumplimiento, que deben ser evaluables a través de indicadores específicos.	Audita los procesos y los controles existentes en base a riesgos.	
Integración con la evaluación de riesgos	Identifica y pone en marcha las acciones necesarias para llevar a cabo respuestas ante riesgos específicos de cumplimiento.	Audita la evaluación de riesgos y los controles establecidos para su mitigación.	
Integración con el resto de los procesos de la organización	Establece la dependencia y vinculación entre los procesos de negocio, riesgos de cumplimiento, actividades de control e indicadores de cumplimiento.	Revisa la efectividad del resultado.	

	ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA
ACTIVIDADES DE CONTROL	Planes de acción de mejora de control interno	En los procesos con impacto en el cumplimiento propone y coordina su implantación junto con las unidades de negocio.	Recomienda y realiza su seguimiento de implantación.
	Seguimiento	Define indicadores de desempeño claves en la ejecución de los planes de acción para la mejora del control interno en el ámbito del riesgo de cumplimiento.	Realiza el seguimiento de las recomendaciones realizadas para determinar si la dirección ha implantado adecuadamente sus compromisos.
	Definición de controles	Propone y promueve la implantación de mecanismos de control, asegurando un equilibrio de enfoques y metodologías para mitigar los riesgos de cumplimiento, teniendo en cuenta tanto controles manuales como automatizados y controles preventivos y de detección.	Recomienda la incorporación y/o mejora de controles clave para dar cobertura a los riesgos, y asesora sobre la eficacia e implantación de estos.
	Formación	Define e identifica las necesidades de formación y coordina su impartición junto con las unidades de negocio. Responsable de coordinar la formación a empleados de alto riesgo sobre materias específicas relacionadas con el cumplimiento.	Verifica conocimientos y cumplimiento del plan de formación, detecta necesidades de formación. No tiene responsabilidades específicas de formación. Provee formación profesional continua a los auditores internos para perfeccionar sus conocimientos, aptitudes y otras competencias.
INFORMACIÓN Y COMUNICACIÓN	Contenido del *reporting*	Informa sobre los riesgos de cumplimiento, mecanismos de control, resultado de las acciones mitigadoras, riesgos residuales y eventuales situaciones de incumplimiento.	Informa periódicamente sobre la actividad 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.
	Reporting interno en la organización	Reporta a la Alta Dirección y al Consejo de Administración.	A la Alta Dirección y/o al Consejo de Administración.
	Reporting a supervisores	Ejecuta.	Audita para asegurar su calidad y oportunidad.

ROLES Y RESPONSABILIDADES CLAVE	CUMPLIMIENTO	AUDITORÍA INTERNA	
Evaluación de la efectividad de los procesos y controles definidos	Lleva a cabo un control constante de los procesos relacionados con el riesgo de cumplimiento para asegurar que están funcionando según lo previsto.	Audita periódicamente determinados procesos seleccionados en base a riesgos.	SUPERVISIÓN
Evaluación del desempeño	Define indicadores y promueve su incorporación en los mecanismos de evaluación de desempeño.	Audita y recomienda mejoras.	
Oportunidades de mejora de control interno	Identifica, promueve y apoya su implantación.	Recomienda.	
Auditoría	Puede llevar a cabo auditoría o *testing* de operaciones de aquello sobre lo que no tiene responsabilidad.	Rol propio de Auditoría Interna. Los proyectos de Auditoría Interna se llevan a cabo de acuerdo con el *Marco Internacional para la Práctica Profesional de la Auditoría Interna.* En base a un análisis de riesgos, audita la existencia y efectividad del sistema de gestión de cumplimiento.	
Monitorización	Rol propio de Cumplimiento. El área de Cumplimiento es responsable de llevar a cabo una monitorización continua del cumplimiento en general.	Debe cumplir su programa de calidad y asegurar que periódicamente se revisa la actividad de Auditoría Interna.	

Fuente: Elaboración propia

Resumiendo, el área de Cumplimiento asume fundamentalmente responsabilidades relacionadas con el asesoramiento y la coordinación del sistema de gestión de cumplimiento, aplica una metodología basada en las mejores prácticas y normativa vigente, y sigue un enfoque basado en riesgos. Asimismo, vela por el funcionamiento global del sistema o modelo de cumplimiento de la organización a través de su supervisión. En cuanto a las responsabilidades de Auditoría Interna, están más relacionadas con la revisión de los resultados del modelo/sistema de cumplimiento. Y lo hace revisando la adecuación de su diseño y verificando la efectividad de los controles.

Ambas áreas requieren una posición de independencia con respecto a la línea ejecutiva y, en gran medida, se complementan. Existen organizaciones en las que Auditoría Interna desempeña roles propios de Cumplimiento.

En estas situaciones, hay que considerar la perspectiva de las Tres Líneas de Defensa, que

definen la estructura de responsabilidades en los sistemas de control interno, especialmente en lo relativo a la salvaguarda de aquellas responsabilidades propias e indelegables de la línea ejecutiva. Y, además, hay que sentar las bases para no comprometer la actuación de Auditoría Interna en cuanto a la independencia que debe mantener frente a las actividades y áreas que evalúa[7].

La Norma 1000 del *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (en adelante MIIP) establece que "el propósito, la autoridad y la responsabilidad de la actividad de Auditoría Interna deben estar formalmente definidos en un estatuto, en conformidad con la Misión de Auditoría Interna y los elementos de cumplimiento obligatorio del MIIP".

En el caso de las actividades propias del área de Cumplimiento –que Auditoría Interna puede realizar con las debidas salvaguardas– hay que considerar la Norma 1130.A2 del MIPP que establece que "los trabajos de aseguramiento para funciones por las cuales el Director de Auditoría Interna tiene responsabilidades deben ser supervisadas por alguien fuera de la actividad de Auditoría Interna"[8].

Además de las funciones de Auditoría Interna y Cumplimiento, en muchas organizaciones existen otras actividades de aseguramiento que podrían funcionar como socios estratégicos del área de Cumplimiento a la hora de llevar a cabo la implantación y mejora continua de un modelo de cumplimiento. Asesoría Jurídica, Gestión de Riesgos, Comunicación Interna y Recursos Humanos, entre otras, han de tener un papel fundamental como integrantes del sistema de cumplimiento y con responsabilidades específicas relacionadas con la implantación y funcionamiento del programa de cumplimiento en la organización.

MATRIZ DE RESPONSABILIDADES DE CUMPLIMIENTO DE LAS ÁREAS DE CUMPLIMIENTO, AUDITORÍA INTERNA Y OTRAS FUNCIONES DE ASEGURAMIENTO DE LA ORGANIZACIÓN

- Coordina y dirige ejecución
- Interviene en la coordinación y dirección de ejecución en determinados aspectos que se encuentran dentro de su área de competencia
- Ejecuta en su área de responsabilidad atendiendo directrices de quien ostenta responsabilidad primaria

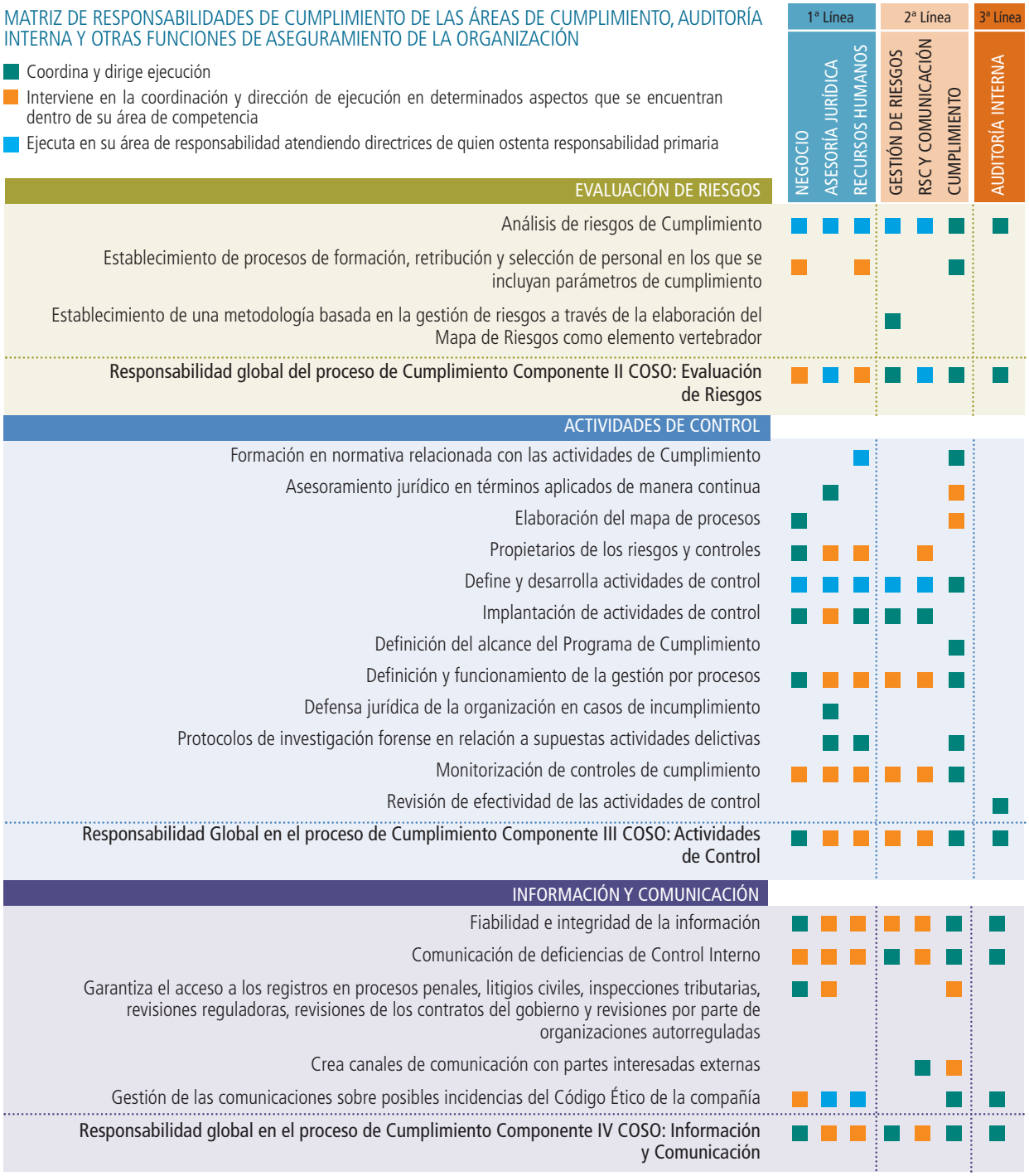
ENTORNO DE CONTROL	1ª Línea			2ª Línea			3ª Línea
	NEGOCIO	ASESORÍA JURÍDICA	RECURSOS HUMANOS	GESTIÓN DE RIESGOS	RSC Y COMUNICACIÓN	CUMPLIMIENTO	AUDITORÍA INTERNA
Impulsa la creación y modificación continua de normativa de la compañía relacionada con las actividades de Cumplimiento (Código ético, políticas anticorrupción, antifraude, etc.)	■		■	■		■	■
Establecimiento de una cultura ética y de cumplimiento en la organización y de su comunicación a todos los grupos de interés	■	■	■	■	■	■	■
Poner en marcha mecanismos de prevención y detección de conductas irregulares	■		■			■	
Definir estructura de responsabilidades de Control Interno relacionada con el Cumplimiento	■		■			■	
Realización de investigaciones de Cumplimiento	■		■			■	■
Aplicar regimen sancionador en caso de incumplimientos	■	■	■			■	
Coordinación del funcionamiento del modelo de Cumplimiento						■	
Responsabilidad global en el proceso de Cumplimiento Componente I de COSO: Entorno de Control.	■	■	■	■	■	■	■

7. Instituto de Auditores Internos de España. La Fábrica del Pensamiento. *Marco de Relaciones de Auditoría Interna con otras Funciones de Aseguramiento,* 2013.

8. The Global IIA. *Internal Audit and the Second Line of Defense Practice Guide,* 2016.

MATRIZ DE RESPONSABILIDADES DE CUMPLIMIENTO DE LAS ÁREAS DE CUMPLIMIENTO, AUDITORÍA INTERNA Y OTRAS FUNCIONES DE ASEGURAMIENTO DE LA ORGANIZACIÓN

- Coordina y dirige ejecución
- Interviene en la coordinación y dirección de ejecución en determinados aspectos que se encuentran dentro de su área de competencia
- Ejecuta en su área de responsabilidad atendiendo directrices de quien ostenta responsabilidad primaria



Fuente: Elaboración propia

MATRIZ DE RESPONSABILIDADES DE CUMPLIMIENTO DE LAS ÁREAS DE CUMPLIMIENTO, AUDITORÍA INTERNA Y OTRAS FUNCIONES DE ASEGURAMIENTO DE LA ORGANIZACIÓN

- Coordina y dirige ejecución
- Interviene en la coordinación y dirección de ejecución en determinados aspectos que se encuentran dentro de su área de competencia
- Ejecuta en su área de responsabilidad atendiendo directrices de quien ostenta responsabilidad primaria

SUPERVISIÓN	1ª Línea: NEGOCIO	1ª Línea: ASESORÍA JURÍDICA	1ª Línea: RECURSOS HUMANOS	2ª Línea: GESTIÓN DE RIESGOS	2ª Línea: RSC Y COMUNICACIÓN	2ª Línea: CUMPLIMIENTO	3ª Línea: AUDITORÍA INTERNA
Emprende mejoras de Control Interno	■	■	■	■	■	■	
Monitoriza de manera continua el Modelo de Cumplimiento. Estudia fallos de control	■				■		
Realiza auditorías proactivas de Cumplimiento	■					■	■
Recomienda mejoras de Control Interno						■	■
Revisión del entorno de control y recomendación de mejoras							■
Revisión del modelo de Cumplimiento							■
Estudio de la gestión de riesgos clave de cumplimiento a través de la monitorización continua	■	■	■	■	■	■	
Revisión de la gestión de riesgos clave de cumplimiento a través de la realización de auditorías	■					■	■
Evaluación del proceso de gestión de riesgos							■
Realiza seguimiento de las medidas correctivas						■	■
Responsabilidad global en el proceso de Cumplimiento Componente V COSO: Supervisión	■	■	■	■	■	■	■
Cumplimiento Componente I COSO III	■	■	■	■	■	■	■
Cumplimiento Componente II COSO III	■	■	■	■	■	■	■
Cumplimiento Componente III COSO III	■	■	■	■	■	■	■
Cumplimiento Componente IV COSO III	■	■	■	■	■	■	■
Cumplimiento Componente V COSO III	■	■	■	■	■	■	■
TOTAL TIPO DE RESPONSABILIDAD EN EL PROCESO DE CUMPLIMIENTO COSO III	■	■	■	■	■	■	■

Fuente: Elaboración propia

Relaciones entre Cumplimiento y Auditoría Interna

Si bien pueden existir diversas herramientas para establecer pautas en la relación entre las áreas de Cumplimiento y Auditoría Interna, así como con otras de la organización que tengan roles relevantes en la gestión de riesgos de cumplimiento, es necesario determinar y documentarla a través de un mapa de aseguramiento.

EL MAPA DE ASEGURAMIENTO

Es una herramienta de coordinación que permite identificar a los órganos de gobierno si existe una cobertura adecuada de los riesgos relevantes de la organización y si la gestión de estos se encuentra dentro de los parámetros establecidos para alcanzar los objetivos del negocio. En este mapa figuran, los riesgos de mayor relevancia para la organización y se completa con funciones específicas de aseguramiento (Cumplimiento, Auditoría Interna, Gestión de Riesgos, etc.) que realizan controles sobre esos riesgos.

Aporta información tanto al órgano de administración como a la Alta Dirección en cuanto al aseguramiento global de los principales riesgos de la organización, y permite identificar si existen riesgos críticos no adecuadamente gestionados o que se encuentran "sobrecontrolados". Eso implica una asignación ineficiente de recursos, con exceso de aseguramiento y/o duplicidad de esfuerzos en la cobertura de alguno de ellos (Norma 2050 - *Coordinación y Confianza* del *MIPP).*

La existencia de un mapa de aseguramiento ayuda a Auditoría Interna a coordinar sus actividades con otros proveedores de aseguramiento que existan en la compañía, cumpliendo así lo establecido en la Guía de Implementación 2050 *(Coordinación y confianza)* del *MIPP: "el Director de Auditoría Interna debería compartir información y coordinar las actividades con otros proveedores internos y externos de servicios de aseguramiento y consultoría para asegurar una cobertura adecuada y minimizar la duplicación de esfuerzos".* Una buena coordinación entre las distintas funciones de aseguramiento contribuirá a una adecuada cobertura de los riesgos clave y a una mejor asignación de los recursos de una organización.

En la definición del mapa de aseguramiento hay que condiderar, entre otros, el riesgo de cumplimiento. El mapa proporcionará información valiosa sobre el aseguramiento de estos y las interrelaciones que se producen entre Cumplimiento, Auditoría Interna y otras funciones o áreas que puedan realizar labores de aseguramiento al respecto en la organización.

Con relación al riesgo de cumplimiento se deben considerar las siguientes fases al elaborar el mapa de aseguramiento:

1. **Identificar los riesgos relevantes o críticos de cumplimiento** que pueda tener la organización (laboral, fiscal, contable, de prevención del blanqueo de capitales, etc).

   En esta etapa podría incluirse la identificación de los procesos en los que están localizados los diferentes riesgos, teniendo en cuenta la transversalidad de estos y, que en un único proceso podemos encontrarnos varios riesgos y varias funciones de aseguramiento que tengan encomendadas su control.

2. **Identificar las funciones de aseguramiento existentes** en la organización.

   También pueden existir funciones externalizadas que den cobertura a estos riesgos, e igualmente es necesario identificar y medir el grado de aseguramiento que proporcionan.

3. **Identificar y evaluar el grado de aseguramiento que proporcionan las distintas funciones** o áreas a cada uno de los riesgos identificados.

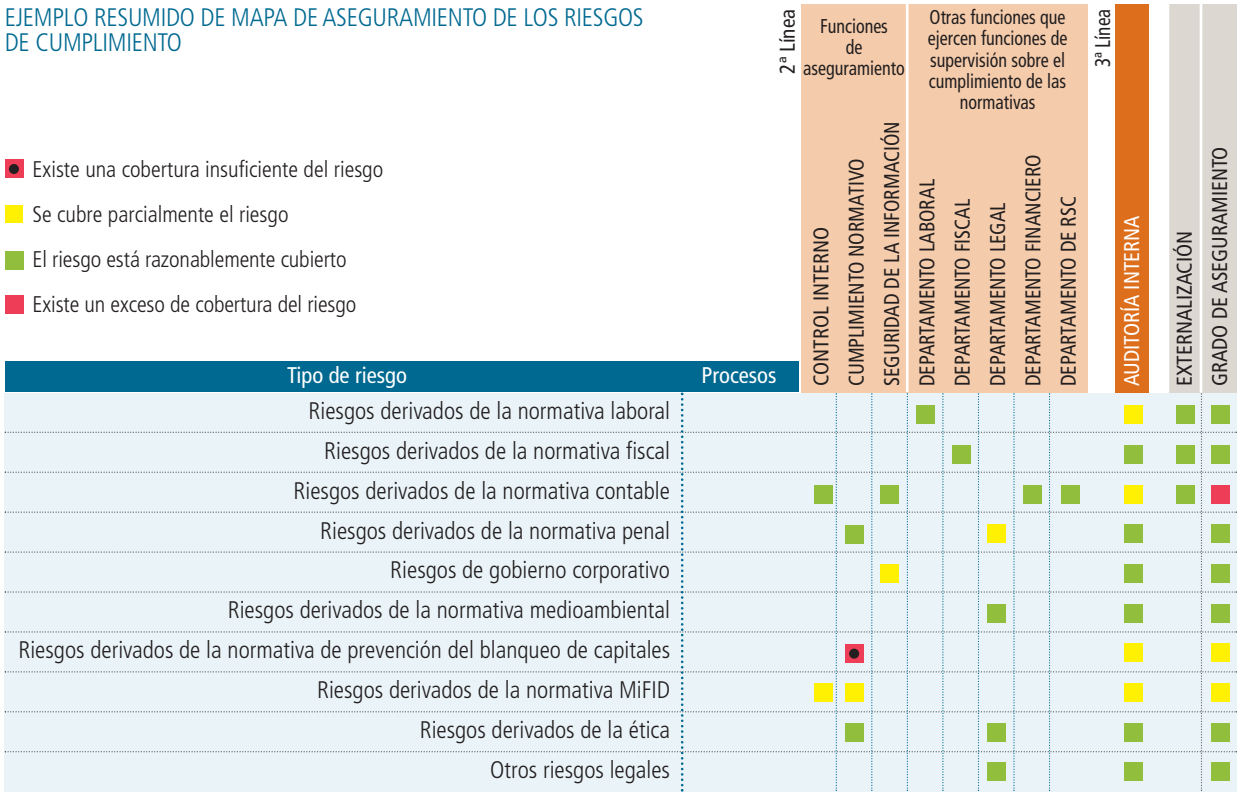
   Una vez evaluado el grado de aseguramiento de las distintas funciones, habría que determinar el grado de aseguramiento global existente para cada uno de los riesgos considerados, y se podría llegar a concluir sobre el grado de

aseguramiento global del riesgo de cumplimiento en general.

De esta manera, y a través del mapa, la organización podría disponer de una visión más desagregada de la cobertura del riesgo de cumplimiento, lo que permitirá identificar las posibles lagunas que se identifiquen en su gestión.

A su vez, este sub-mapa se integrará dentro de un mapa deaAseguramiento global de toda la organización, que incorporará el resto de los riesgos críticos.

EJEMPLO RESUMIDO DE MAPA DE ASEGURAMIENTO DE LOS RIESGOS DE CUMPLIMIENTO

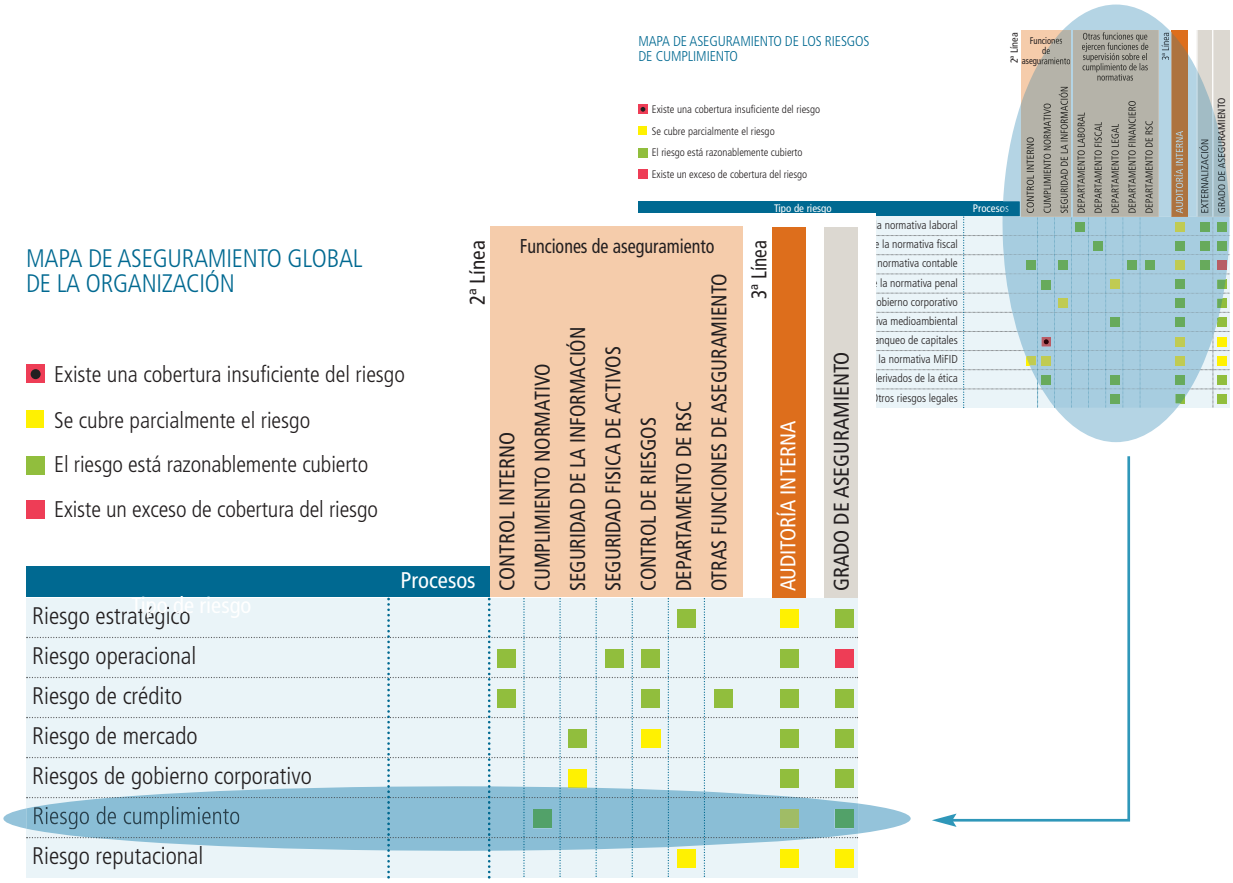


Fuente: Elaboración propia

RIESGOS CON ENFOQUE DE AUDITORÍA INTERNA

El Plan de Auditoría Interna se prepara a partir de una evaluación preliminar de los riesgos que amenazan la consecución de los objetivos de la organización. El riesgo de cumplimiento es un factor más a considerar dentro del proceso más amplio de identificación y evaluación de riesgos, el que se realiza a partir del inventario de procesos de la organización o a partir del universo auditable.

La información proporcionada por el mapa de aseguramiento podrá servir de base y punto de partida para que Auditoría Interna planifique y priorice sus trabajos, que también podrá utilizar la propia evaluación de riesgos realizada por



Fuente: Elaboración propia

Cumplimiento (y documentada, por ejemplo, a través de una herramienta como un mapa de riesgos normativo) y su programa anual de actividades.

En este caso, Auditoría Interna realizará a la misma los ajustes que considere necesarios en función de su experiencia y conocimiento de los procesos y actividades afectados por estos riesgos de cumplimiento, antes de incorporarlos a su propia evaluación.

Finalmente Auditoría Interna determinará un plan basado en riesgos a partir de su propia metodología, dando prioridad a aquellas áreas, funciones o procesos de la empresa con riesgos de cumplimiento más relevantes o con un nivel de aseguramiento inadecuado o insuficiente. En el plan puede incluir:

- Trabajos específicos de Auditoría Interna cuyo objetivo sea evaluar la eficacia del aseguramiento proporcionado por Cumplimiento.
- Revisiones detalladas de los requerimientos establecidos en las distintas normas de aplicación en la empresa (por ejemplo, RGPD, blanqueo de capitales, etc.).
- Revisiones de los requerimientos establecidos en la normativa que aplica a un proceso o ac-

tividad más amplio/global dentro de la compañía.

Por otra parte, cualquier encargo de Auditoría Interna, independientemente del tipo, debiera incorporar también una identificación y evaluación de los riesgos de cumplimiento inherentes al proceso o actividad auditada dentro de la evaluación preliminar de riesgos que realiza el auditor interno durante la planificación y preparación del programa de trabajo.

EVALUACIÓN DEL ASEGURAMIENTO PROPORCIONADO POR CUMPLIMIENTO

Cualquier encargo de Auditoría Interna debería incorporar la identificación de los riesgos de cumplimiento inherentes al proceso auditado.

En aquellos casos en los que la organización disponga de una unidad propia de Cumplimiento, los principales aspectos a considerar en una auditoría interna cuyo objetivo sea la evaluación de la eficacia del aseguramiento proporcionado por esta son:

1. **Obtener un profundo conocimiento de la regulación a aplicar** a la organización, así como de la normativa interna aplicable a sus actividades. En general, los principales riesgos que se encuentran bajo la responsabilidad de una unidad de Cumplimiento están relacionados, dependiendo del sector, con legislación y normas cuyo origen es la prevención del blanqueo de capitales y financiación del terrorismo, la prestación de servicios de inversión (MiFID), la protección de datos de carácter personal, la prevención de riesgos penales y el cumplimiento de los códigos de ética, entre otros.

   Además, la revisión de actas del Consejo de Administración, Comisión de Auditoría y Cumplimiento y Comité de Riesgos proporcionarán al auditor interno información muy relevante y una visión general de las estrategias, filosofía, metodología de gestión de riesgos, apetito y aceptación de riesgos de cumplimiento.

2. **Verificar el cumplimiento de los requisitos organizativos y principios** sobre los que debe asentarse el desempeño eficaz de la actividad de cumplimiento normativo, entre ellos:
   - Verificar que los roles y responsabilidades del órgano de administración, de la Alta Dirección y de Cumplimiento se han definido y comunicado de forma clara y precisa a toda la organización.
   - Independencia del área de Cumplimiento, cuya posición y línea de reporte dentro de la organización le permita cumplir con sus responsabilidades.
   - Verificar que existen las condiciones necesarias para evitar posibles conflictos de intereses por parte de los miembros del área de Cumplimiento y que no existen limitaciones o restricciones al acceso a la información, al personal y a los bienes necesarios que les permitan realizar su trabajo con objetividad y libre de interferencias.
   - Verificar que los recursos asignados a Cumplimiento son suficientes y apropiados y que los miembros de la unidad tienen una competencia profesional adecuada.

3. **Verificar la existencia de políticas y procedimientos** que regulen los procesos de gestión del riesgo de cumplimiento en la compañía y de la función de aseguramiento proporcionada por la unidad de Cumplimiento Normativo, comprobando, además, que han sido aprobados formalmente y comunicados de forma efectiva a toda la organización.

4. **Verificar la integración de los procesos de gestión de riesgos de cumplimiento** dentro de los procesos globales de gestión de riesgos de la organización.

5. **Revisar y evaluar la eficacia de los procesos relacionados con la identificación, documentación y evaluación de los riesgos de cumplimiento** que afectan a la organización, verificando, por ejemplo:
   - que se ha establecido y definido un programa de cumplimiento sobre la base del inventario de riesgos regulatorios.
   - que se ha documentado un mapa de riesgos regulatorios.

6. **Comprobar la eficacia y la efectividad de los controles internos existentes** en la organización que mitigan o reducen a niveles óptimos los riesgos de cumplimiento identificados.

7. **Comprobar la existencia de un sistema de comunicación y reporte** de los resultados de los trabajos de aseguramiento proporcionados por Cumplimiento, incluyendo la existencia de planes de acción en caso de coberturas insuficientes o inadecuadas, así como el seguimiento de su efectiva implantación.

A la hora de llevar a cabo una evaluación de la eficacia del aseguramiento proporcionada por Cumplimiento, hay que indicar que –como se ha señalado en apartados anteriores– en muchas organizaciones no existe un departamento específico, unidad o responsable de cumplimiento, sino que las funciones y responsabilidades relacionadas con el cumplimiento pueden ser desempeñadas, de forma descentralizada, por las propias unidades operativas/de negocio.

En estos casos, los objetivos y aspectos a considerar en una auditoría interna para evaluar la eficacia del aseguramiento proporcionado por esa función, no deberían variar de forma significativa en comparación con el trabajo realizado cuando existe un área o departamento específico de Cumplimiento. Sin embargo, es necesario que Auditoría Interna, a la hora de planificar y preparar el programa de trabajo, disponga de un conocimiento general del ámbito de actuación, de los roles y responsabilidades establecidos y del grado de cobertura de las distintas unidades que ejercen funciones de cumplimiento normativo dentro de la organización. La existencia de un Mapa de Aseguramiento y la información proporcionada por esta herramienta sería de enorme ayuda.

Para preparar el plan de trabajo, Auditoría Interna debe conocer el ámbito de actuación, roles y cobertura de las unidades que ejerzan funciones de cumplimiento en una organización.

Auditoría Interna no sólo comunicará el resultado de los trabajos específicos realizados sobre el área de Cumplimiento a esta última, sino que deberá dar a conocer también los hallazgos identificados en otros trabajos de auditoría de procesos y/o actividades que afecten al riesgo de cumplimiento.

Auditoría Interna realizará propuestas de mejora que Cumplimiento podría incorporar en su modelo o sistema de gestión del cumplimiento normativo (por ejemplo, en el mapa de riesgos, en su plan o programa de cumplimiento).

RIESGOS CON ENFOQUE DE CUMPLIMIENTO

El Mapa de Aseguramiento de la organización proporcionará también información a Auditoría Interna de aquellos riesgos de cumplimiento de los cuales el área de Cumplimiento es directamente responsable o cuya responsabilidad sea coordinar actividades de aseguramiento para ese riesgo.

De esta forma, se plantean dos escenarios posibles para Auditoría Interna con relación a los riesgos que deben ser cubiertos por Cumplimiento Normativo:

- **Decisión de no confiar en el aseguramiento proporcionado por parte de Cumplimiento** con relación a los riesgos de los cuales es responsable. En este caso, se tendrá en cuenta este hecho durante el proceso de elaboración del Plan de Auditoría (y en la correspondiente evaluación del riesgo de cumplimiento), pudiéndose incluir trabajos en áreas con cobertura inadecuada o insuficiente.

- **Decisión de confiar en el aseguramiento proporcionado por Cumplimiento.** Auditoría Interna debería estar coordinada con Cumplimiento para garantizar que los recursos son utilizados de la manera más eficiente y efectiva posible y proporcionar a la organización un nivel de aseguramiento global de los riesgos de cumplimiento a los que está expuesta.

  Esta decisión debe venir avalada por:

  · Una evaluación previa (realizada por Auditoría Interna) del aseguramiento proporcionado por parte de Cumplimiento. Esta evaluación podría ser el resultado de trabajos de auditoría interna realizados en años anteriores, o determinada en función de diversos factores como el grado de madurez de la unidad, su independencia, objetividad, competencias y cualificación de sus miembros, suficiencia en el alcance de los trabajos y adecuación de las pruebas realizadas por Cumplimiento, existencia de procedimientos adecuados de seguimiento de acciones correctivas para solucionar las deficiencias, debilidades o incumplimientos identificados en el aseguramiento proporcionado por Cumplimiento Normativo.

  · Los resultados proporcionados por parte de Cumplimiento derivados de su propio proceso de monitorización continua sobre riesgos de cumplimiento y sus correspondientes controles internos, como Segunda Línea de Defensa.

En caso de confiar en el trabajo realizado por Cumplimiento, Auditoría Interna podrá incorporar los resultados de la revisión y aseguramiento realizados por la primera en sus informes, haciendo referencia a esta circunstancia.

Los directores de Auditoría Interna y de Cumplimiento deben mantener comunicación fluida y compartir información sobre cambios normativos, nuevos riesgos de cumplimiento, etc.

Independientemente de cualquier tipo de relación que se establezca entre ambas áreas, el Director de Auditoría Interna y el director o responsable de Cumplimiento deben mantener una comunicación fluida, promoviendo reuniones periódicas para compartir información relevante en relación con cambios normativos que puedan afectar a la organización, a la identificación de nuevos riesgos de cumplimiento, etc.

Además, Auditoria Interna puede asesorar en la definición y alcance de la cultura de cumplimiento y en el contenido de las formaciones necesarias para la implantación de un

modelo de prevención de riesgos de cumplimiento.

Independientemente de cómo esté estructurada la organización, el área de Cumplimiento, y de la decisión de confiar o no en el trabajo realizado por esta, Auditoría Interna debería verificar que todos los riesgos de cumplimiento cuya responsabilidad recae en Cumplimiento se encuentran gestionados convenientemente, de forma que no queden riesgos sin la debida cobertura, pudiendo emitir una opinión sobre la efectividad de la función de aseguramiento desempeñada por Cumplimiento.

Por último, en su labor de supervisión y evaluación de los procesos de gestión de riesgos, el trabajo de Auditoría Interna se convierte en una fuente de información útil para enriquecer y completar los programas de cumplimiento y mejorar el entorno de control y de cumplimiento.

El trabajo de Auditoría Interna es útil para enriquecer y completar los programas de cumplimiento y mejorar el entorno de control.

Estructura de Cumplimiento

La estructura de cumplimiento es una de las cuestiones más complejas, ya sea porque en determinados sectores (financiero, seguros, etc.) el diseño viene condicionado de forma taxativa por el derecho derivado de la Unión Europea o su trasposición al ordenamiento jurídico español, o bien porque la propia fisonomía de las personas jurídicas (tamaño, número de empleados, recursos, etc.) condiciona inexorablemente la realidad orgánica de las áreas de Cumplimiento, cuando puedan existir, o de las personas que, finalmente, asuman tales cometidos.

En cualquier caso, la existencia de una persona física o un órgano que asuma las funciones de *Compliance Officer* (Director de Cumplimiento), de forma permanente y exclusiva, u ocasional y a tiempo parcial, es muy recomendable en el escenario holístico ya descrito en la introducción.

A continuación, se detallan las particularidades orgánicas y competenciales que entraña el cumplimiento.

ESTRUCTURA ORGÁNICA

La naturaleza y fisonomía jurídica de las organizaciones (sociedades cotizadas, entidades financieras, pequeñas y medianas empresas, etc.) hace que haya divergencia de formas organizativas. A continuación se describen dos potenciales modelos, pero la casuística permitirá tantas combinaciones como una adecuada implantación de la cultura de cumplimiento permita.

Modelos centralizados

Aquellos donde Cumplimiento dispone de recursos (humanos y materiales) suficientes, con

personas con conocimiento de la gestión de riesgos de cumplimiento (legales, fiscales, contables, medioambientales, etc.) y llevan a cabo las acciones documentales, formativas e informativas necesarias al fin pretendido, vigilan el cumplimiento, gestionan el Canal Ético y verifican la idoneidad del modelo. Podrían coordinar con Auditoría Interna la verificación del modelo, llegando a un mapa de aseguramiento que genere un entorno de control confiable.

Las ventajas de este modelo residen en una mayor autonomía y facilidad en la coordinación. Las desventajas se centran en el coste del modelo, la posible "no implicación" de todo el colectivo de la organización y la potencial ineficiencia derivada de tal desconexión.

Modelos descentralizados

Aquellos donde el área de Cumplimiento –muchas veces unipersonal– hace de núcleo del modelo al que reportan indirectamente aquellas funciones expertas con el conocimiento técnico preciso para la gestión de riesgos de cumplimiento (contable, fiscal, prevención de blanqueo de capitales, laborales, etc.) y con la que colaboran en el desarrollo de las acciones formativas técnicas e investigación que procedan.

En este modelo, Cumplimiento debe facilitar a esas funciones expertas un modelo estándar de trabajo, una coordinación de planes de acción y la "protección" precisa para el desempeño de su trabajo con autonomía y sin conflicto de intereses. Además, podría coordinar con Auditoría Interna la verificación del modelo, llegando a un mapa de aseguramiento que genere un entorno de control fiable.

Las ventajas de este modelo residen en el coste y velocidad con la que Cumplimiento se integra en la cultura corporativa. A su vez, las desventajas residen inicialmente en las resistencias de los responsables directos de las áreas identificadas para colaborar en el sistema y la coordinación.

El Consejo debe mostrar compromiso con Cumplimiento asegurando su existencia, recursos adecuados y su buen funcionamiento.

DEPENDENCIA JERÁRQUICA

El Consejo de Administración, en defensa de los intereses propios y, principalmente, de los accionistas de la empresa, debe mostrar el compromiso con Cumplimiento asegurando su existencia, una adecuada dotación de recursos y su buen funcionamiento, promoviendo una cultura de cumplimiento y buenas prácticas.

En los sistemas centralizados Cumplimiento dependería directamente del máximo órgano societario.

De igual forma, el Consejo de Administración debe garantizar la autonomía íntegra del modelo mediante la dependencia directa de quien lidere el modelo y todas aquellas funciones identificadas para participar en él. Debe asegurarse para ellos una correcta gestión del conflicto de intereses que podría diferir en un momento dado entre el negocio y el cumplimiento, garantizarles la inexistencia de represalias ante cualquier decisión de cumplimiento y asegurarles la confidencialidad precisa.

REPORTE FUNCIONAL

Si bien la dependencia debe ser del órgano de administración, esta podrá ejecutarse a través de una comisión delegada o cualquier otra estructura que tenga la organización. Entre la casuística posible, y para aquellas empresas que presenten cuenta de pérdidas y ganancias abreviada, el administrador puede realizar la función de Cumplimiento.

Para el día a día, el Consejo de Administración, la comisión correspondiente o el administrador podrían encargar o apoyarse en Cumplimiento para realizar la supervisión del modelo.

Si bien la dependencia debe ser del órgano de administración, puede realizarse a través de una comisión u otra estructura de la organización.

Consideraciones finales

Concluyendo, la organización deberá diseñar una estructura que optimice la relación entre Auditoría Interna y Cumplimiento Normativo, de manera que la primera pueda cumplir su misión y contribuir así a agregar valor a la organización, incorporándose de la forma más apropiada posible a los distintos procesos definidos para garantizar el cumplimiento de las responsabilidades de la segunda.

Ambas áreas tienen varios aspectos comunes que se centran, básicamente, en ayudar a la organización a lograr un gobierno corporativo responsable y un sistema de control de los riesgos eficaz. La clave para alcanzar el éxito en este objetivo pasará por identificar y definir un ambivalente equilibrio de coordinación/colaboración en el que Auditoría Interna y Cumplimiento puedan y deban interactuar, sin perder de vista el Modelo de las Tres Líneas de Defensa y sus especiales circunstancias que les obliga a ser libres respecto de lo que dicen y piensan.

Auditoría Interna podrá aportar a Cumplimiento su experiencia y la metodología propia de un área ya implantada para conseguir mejorar en aspectos como los siguientes:

- Focalizar los esfuerzos de la organización en dar **cobertura a los principales riesgos de cumplimiento** a los que se enfrenta, previa evaluación de estos y de su criticidad.
- Proponer **procesos de mejora continua,** mediante el análisis de los procesos, detección de debilidades de carácter normativo e implantación de los planes de acción diseñados al efecto.
- Dirigir a la organización hacia **modelos preventivos avanzados de monitorización** de cumplimiento de leyes, regulaciones y políticas, anticipándose a los impactos que pueden derivarse de infracciones normativas.
- Participar en las **estrategias y procesos de transformación del cambio,** adaptando el modelo de cumplimiento normativo a los nuevos desafíos de las organizaciones.
- Establecer **modelos de *reporting* a los órganos de dirección y de administración**

que les permitan cumplir con sus responsabilidades de forma eficaz.

En definitiva, Auditoría Interna y Cumplimiento comparten roles y responsabilidades similares en diferentes espacios funcionales y temporales, y –en la medida en que puedan converger cuando sea necesario– podrán compartir recursos y conocimientos para desempeñar sus respectivas funciones sin perjuicio de la independencia y objetividad de cada una de ellas. Auditoría Interna tendrá oportunidades para ayudar a la organización a garantizar que los riesgos derivados del cumplimiento son gestionados de forma aceptable.

Puesto que los principales roles de Auditoría Interna relacionados con la gestión de riesgos forman parte inherente de su misión de aseguramiento, y considerando que durante los últimos años a este rol de "asegurador[9]" se viene sumando un rol cada vez más demandado de "asesor de confianza", se detallan a continuación los roles legítimos de Auditoría Interna:

1. **Actuar como facilitador en la identificación y evaluación de riesgos.** Auditoría Interna puede aportar valor, asumiendo un papel proactivo en la identificación de riesgos de cumplimiento. A tal efecto, podría liderar el establecimiento de un sistema de comunicación efectivo con Cumplimiento.

2. **Asesorar a Cumplimiento sobre cómo responder a los riesgos.** Si bien no puede imponer procesos de gestión de riesgos o tomar decisiones sobre la respuesta a los mismos, sí podría ejercer una labor de "asesor" o "consultor", aportando su visión global de los procesos de la entidad y alertando sobre posibles *gaps* en la cobertura de los riesgos de cumplimiento. En este marco, resultaría interesante que Auditoría Interna participara –manteniendo siempre su independencia y dejando claro su rol de asesor– en comités en materia de cumplimiento, dando su opinión sobre aquellos aspectos en los que pueda hacer aportaciones e impulsando acciones que mejoren la gestión de los riesgos de cumplimiento.

3. **Coordinar actividades de gestión de riesgos de cumplimiento o liderar la implantación del sistema de gestión de riesgos de cumplimiento.** En estructuras que por tamaño, eficiencia, experiencia, capacitación o visión de los órganos de gobierno o en entornos menos maduros, Auditoría Interna podría impulsar la implantación del sistema de gestión de riesgos de cumplimiento. En estos casos, es necesario asegurar que existen las salvaguardas necesarias para mantener la independencia y objetividad necesarias del área. En ocasiones, este modelo evoluciona hacia otro en el que las dos áreas se segregan, proceso que debe asegurar que se realiza manteniendo la adecuada independencia de ambas áreas con respecto a la línea ejecutiva.

4. **Mantener y desarrollar el marco de gestión de riesgos empresarial.** La elaboración o la coordinación de la elaboración del mapa de aseguramiento, en el que se incluyen los riesgos de cumplimiento, hace que Auditoría Interna pueda aportar un valor extra a esta área, estableciendo un lenguaje y un marco común de interrelación entre la Primera, la Segunda y la Tercera Línea de Defensa en materia de gestión de riesgos.

9. Para ampliación, ver el documento del Instituto de Auditores Internos de España. La Fábrica del Pensamiento. *Más allá del aseguramiento. El auditor interno como asesor de confianza,* 2017.

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

MARCO DE RELACIONES DE AUDITORÍA INTERNA CON OTRAS FUNCIONES DE ASEGURAMIENTO

Es la primera guía en español que clarifica el papel de Auditoría Interna como coordinadora de todas las funciones de aseguramiento. Establece qué funciones de aseguramiento deben darse en una empresa y qué puede y no hacer Auditoría Interna en su papel de coordinación para asegurar que se cumplen y evitar duplicidades.

GUÍA DE SUPERVISIÓN PARA COMISIONES DE AUDITORÍA. CÓMO MAXIMIZAR EL VALOR DE AUDITORÍA INTERNA

Analiza el marco en el que se desarrolla la relación de supervisión de las Comisiones de Auditoría con Auditoría Interna, y propone buenas prácticas que aseguren el éxito de Auditoría Interna como soporte de la Comisión y que evite o mitigue riesgos cuya materialización impediría obtener el máximo valor de su actividad.

MÁS ALLÁ DEL ASEGURAMIENTO: EL AUDITOR INTERNO COMO ASESOR DE CONFIANZA

La labor de Auditoría Interna abarca mucho más que el aseguramiento clásico: examina hechos, identifica mejoras, emite recomendaciones... Este documento define los roles de asesoramiento, identifica áreas y cualidades para llevarlos a cabo, y marca los límites y riesgos cuando Auditoría Interna realiza estas tareas.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

La complejidad y exigencia del entorno regulatorio requiere que las organizaciones establezcan un Gobierno del riesgo de Cumplimiento en el que se preste especial atención a la identificación, gestión y control de este riesgo, que puede aparecer en cualquier proceso y actividad de la empresa.

Este documento propone un modelo abierto del Gobierno del riesgo de Cumplimiento que asegure una adecuada relación y colaboración entre las áreas de Cumplimiento y Auditoría Interna que sirva para proteger el valor de empresas y organizaciones, fin último que debe guiar el Gobierno de este riesgo, complejo y transversal.

Instituto de Auditores Internos de España

The Institute of Internal Auditors