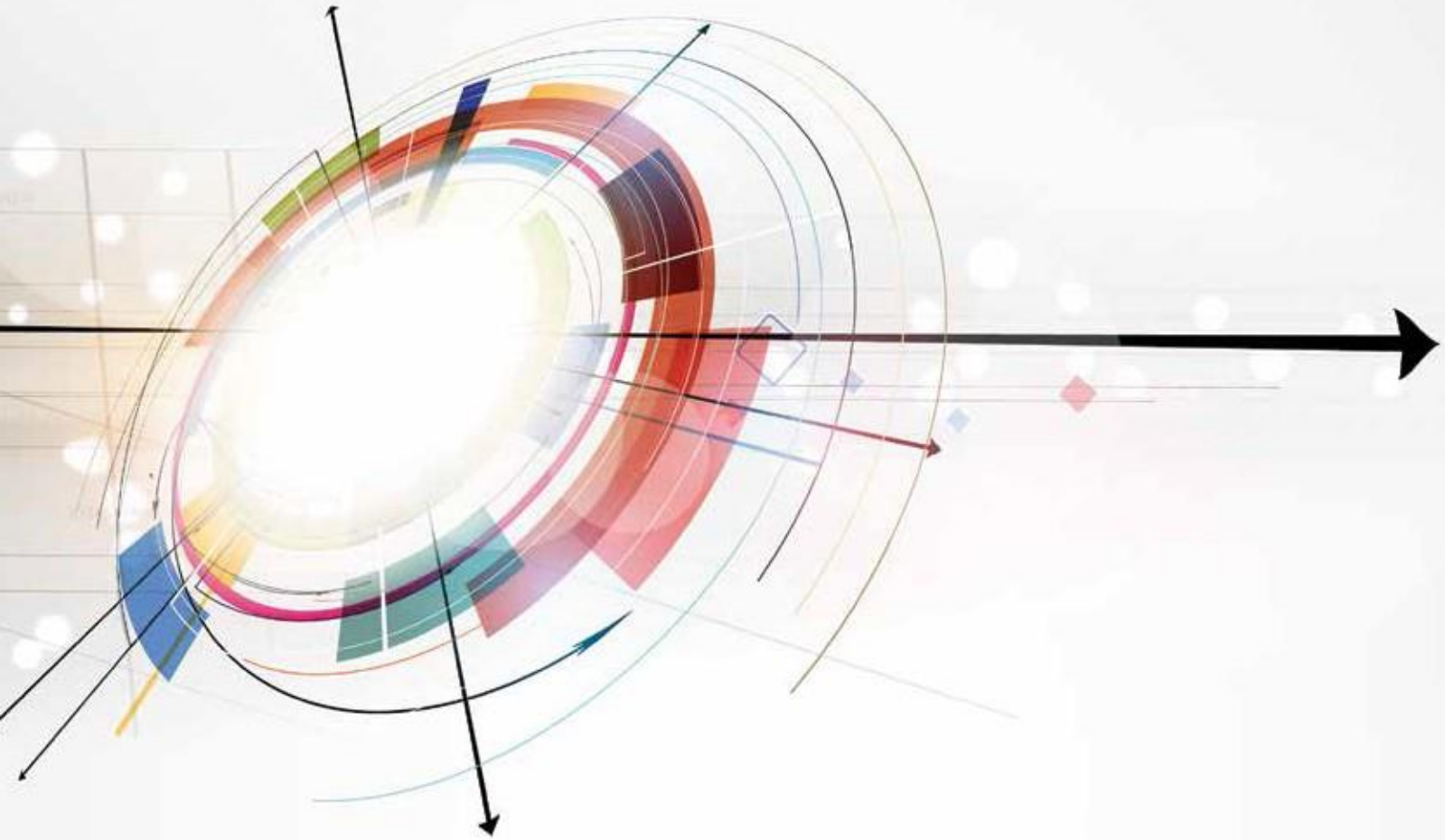


PERSPECTIVAS Y PERCEPCIONES GLOBALES

Auditoría interna y cumplimiento: claridad y colaboración para un gobierno más sólido

Traducción al Español Auspiciada por:

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors | Global

Ediciones anteriores

Para tener acceso las ediciones anteriores de Perspectivas y Percepciones Globales, visite: www.theiia.org/GPI

Comentarios del lector

Envíe preguntas o comentarios a: globalperspectives@theiia.org

Tabla de contenidos

Agradecimientos

El IIA agradece a los miembros y partes interesadas que contribuyeron a este documento, incluidos Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sorlie, Francis Nicholson, Jill Austin y IIA – Australia.

Acerca del IIA

El Instituto de Auditores Internos (IIA) es el defensor, educador y proveedor de normas, orientación y certificaciones más reconocido de la profesión de la auditoría interna. Fundado en 1941, el IIA sirve hoy a más de 200,000 miembros de más de 170 países y territorios. La sede mundial de la asociación está en Lake Mary, Florida, Estados Unidos. Para más información, visite: www.globaliia.org.

Exención de responsabilidad

Las opiniones expresadas en Perspectivas y Percepciones Globales no son necesariamente las de los colaboradores individuales o de los empleadores de los colaboradores.

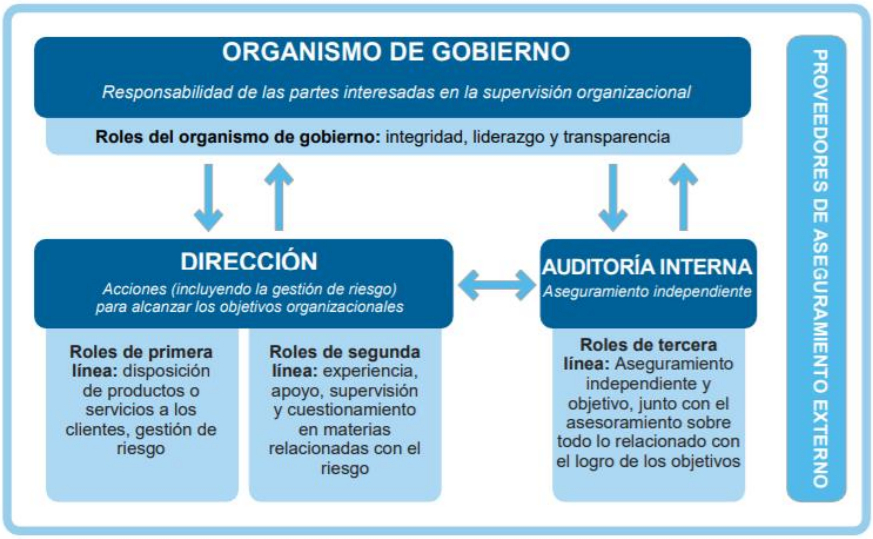
Derechos de autor

Introducción

La relación entre la auditoría interna y el cumplimiento es en ocasiones poco clara, lo que da lugar a importantes preguntas: ¿Puede la auditoría interna ser responsable del cumplimiento? ¿Es una función de cumplimiento responsable de todo el cumplimiento en una organización? Como director general de auditoría, ¿está bien estar a cargo del cumplimiento?

Este documento está diseñado para ayudar a aclarar estas complejidades y evitar la confusión, las brechas y la duplicación innecesaria. La comprensión clara es esencial, se recomienda firmemente la colaboración, y la independencia de la auditoría interna[1] es fundamentalmente importante.

Este *no* es un documento sobre cómo auditar el cumplimiento. En cambio, funciona como herramienta para los consejos de administración, la dirección, los profesionales del cumplimiento y los directores generales de auditoría, y utiliza el *Modelo de las Tres Líneas* como forma de explicar la relación entre la auditoría interna y el cumplimiento. Los Seis Principios del *Modelo de las Tres Líneas* y su aplicación al cumplimiento se examinan en profundidad más adelante en este documento.



Los lectores deberían utilizar este documento para identificar, comprender, evaluar y aplicar claramente dentro de una estructura de gobierno, independientemente de la jurisdicción, el sector, la complejidad, la madurez o el tamaño, una gestión eficaz del cumplimiento y de la gestión de riesgos de cumplimiento en

[1] La naturaleza integral del cumplimiento como parte del gobierno sostenible es un enfoque clave y una acción política recomendada por el B20 Italia a los ministros del G20 en *B20 Italy Integrity & Compliance Policy Paper 2021* (en español, Documento de Política de Integridad y Cumplimiento de B20 Italia 2021). En particular, La acción política 2.1, en la página 11, menciona específicamente el rol de la auditoría interna tal y como se describe en *el Modelo de las Tres Líneas*.

sus diversos aspectos en relación con el *Modelo de las Tres Líneas.*[2] Las ilustraciones prácticas de los oficiales de riesgo y cumplimiento y de los auditores internos sobre los problemas de cumplimiento a los que se enfrentan en el campo ayudarán en la aplicación práctica de los Seis Principios del Modelo al evaluar la alineación de las actividades de cumplimiento de acuerdo con el *Modelo de las Tres Líneas*. (Véanse las páginas 8-16)

Responsabilidad, acciones y aseguramiento

El *Modelo de las Tres Líneas* describe cómo la responsabilidad del organismo de gobierno, las acciones de la dirección y el aseguramiento independiente mediante la auditoría interna proporcionan la base para un gobierno efectivo. También muestra cómo los Seis Principios ayudan en una evaluación de los respectivos roles y responsabilidades en una organización. La aplicación de los elementos centrales del Modelo y de los Seis Principios varía para cada organización, de acuerdo con sus objetivos, recursos y circunstancias. El Modelo ayuda a las organizaciones a identificar estructuras, diseñar procesos y asignar responsabilidades que mejor ayuden al logro de los objetivos. Esto incluye la gestión de riesgos de cumplimiento, que es una responsabilidad de la dirección[3], pero se logra a través de un esfuerzo de colaboración.

La gama de requisitos y expectativas de cumplimiento que una organización debe considerar comprende aquellos impuestos externamente, como leyes, reglas y regulaciones, y los impuestos internamente, como políticas, estándares, procedimientos y códigos de conducta o comportamiento. Pueden definirse formal y explícitamente o ser más implícitas, como las expectativas sociales, éticas y culturales. Este amplio y dinámico espectro de consideraciones se conoce en este documento como "requisitos y expectativas".

Las partes interesadas esperan que una organización cumpla su propósito y maximice su valor de forma legal y ética. En consecuencia, las organizaciones invierten en supervisar estrechamente el cumplimiento en áreas clave como la salud y la seguridad; el empleo; la protección de datos y la privacidad; las leyes y los códigos comerciales y de las personas jurídicas; la normativa del sector; las normas de calidad; la lucha contra el soborno y la corrupción; la protección de los inversores y los consumidores; los informes financieros y la fiscalidad; y los códigos de conducta individuales. La lista continúa. El cumplimiento puede entenderse y efectuarse en el contexto de la responsabilidad, las acciones y el aseguramiento, tal y como se describe en el *Modelo de las Tres Líneas*, como parte de un enfoque general de gobierno efectivo.

---

[2] En determinadas jurisdicciones e industrias, los roles y responsabilidades relacionados con el cumplimiento y la gestión de riesgos de cumplimiento están muy definidos y son objeto de una amplia legislación, regulación, jurisprudencia e investigación académica. Existen estudios más detallados, y se recomienda a los usuarios de este documento práctico que los consulten. Por ejemplo, véase del *American Law Institute, Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 (en español, Principios de la ley, cumplimiento, gestión de riesgos y aplicación de la ley nº 1) y *Principles of the Law, Compliance and Enforcement* No. 2 (en español, Principios de la ley, cumplimiento y aplicación de la ley nº 2).

[3] Para efectos de este documento, el término "dirección" se utiliza ampliamente para identificar los roles que no son responsabilidad del organismo de gobierno o de la auditoría interna.

¿Qué es el cumplimiento?

Las organizaciones deben adherirse (o cumplir con) las leyes aplicables y otros requisitos externos que son un requisito previo para hacer negocios. Estos requisitos de cumplimiento cubren todo, desde las relaciones con los empleados hasta el pago de impuestos. En ciertas industrias hay una variedad de organismos de establecimiento de normas, supervisores, de control y requisitos definidos, pero otros sectores tienen menos límites y restricciones legales y regulatorios impuestos externamente. Sin embargo, es difícil identificar una organización en el sector público o privado que no tenga requisitos de cumplimiento externos.

Al mismo tiempo, las organizaciones diseñan, desarrollan e implementan expectativas internas en forma de políticas y procedimientos y establecen estándares éticos para el comportamiento y la conducta. En ciertas industrias reguladas, los requisitos externos dictan que una organización debe establecer y adherirse a las políticas internas, estándares y códigos de comportamiento establecidos. Con esta red de muchos requisitos en capas, el concepto de "cumplimiento" en una organización adquiere una serie de dimensiones. En consecuencia, es útil considerar el cumplimiento en cada uno de sus aspectos amplios, relacionados, pero distintos, y cómo se discute en las organizaciones: como resultado; como categoría de riesgo;[4] como rol organizacional, departamento, función, etc. [5]; y un conjunto de actividades.

Cada uno de estos se discute a continuación.

El cumplimiento como un resultado

Las organizaciones participan en diversas actividades para cumplir con las leyes, reglas, políticas, códigos, etc., o "estar en cumplimiento". Lograr ciertos requisitos y expectativas de cumplimiento es a menudo una condición necesaria para operar y alcanzar objetivos estratégicos.

El cumplimiento como una categoría de riesgo

El Marco Internacional para la Práctica Profesional define el riesgo como *la posibilidad de que ocurra cualquier evento en la organización que genere impactos sobre el logro de los objetivos.* Esos impactos pueden ser favorables o adversos. Por lo tanto, al evaluar el riesgo, es esencial considerar los requisitos y expectativas de cumplimiento junto con la probabilidad de incumplimiento y su impacto potencial en los objetivos.

Existen riesgos para las organizaciones relacionados tanto con el cumplimiento como con el incumplimiento. Sus impactos pueden ser en forma de recompensas o sanciones, que pueden ser tangibles o intangibles. Por ejemplo, el cumplimiento de las normas de la Organización Internacional de Normalización (ISO) está diseñado para crear eficiencias operativas y otras ganancias y la atención favorable obtenida al seguir un código voluntario. El incumplimiento elimina esas ganancias positivas y

---

[4] Bajo la amplia categoría de riesgo de cumplimiento en una organización, una taxonomía de riesgos identifica una cascada de subcategorías que abordan tanto los riesgos específicos como los relacionados con las leyes, normas, reglamentos, políticas o comportamientos.

[5] Los roles pueden definirse para cubrir riesgos específicos, como el oficial de riesgo de conducta, el oficial de riesgo de protección de datos, etc.

puede resultar directamente en daño, así como incurrir en sanciones como la imposición de multas, retiro de licencias, sanciones, terminación de operaciones, enjuiciamiento civil o penal y pérdida de fondos o apoyo. Además, el incumplimiento puede causar riesgo de reputación en forma de posible insatisfacción de las partes interesadas, críticas públicas u otros daños.

La identificación, medición y evaluación del riesgo de cumplimiento y la determinación y las tolerancias del riesgo asumido de cumplimiento ayudan a determinar las respuestas apropiadas, incluidas las políticas, los procedimientos, los límites y los controles.[6]

El cumplimiento como un rol o departamento organizacional

Con frecuencia, el cumplimiento también se utiliza para referirse a un rol o departamento establecido para cumplir con requisitos y expectativas particulares o proporcionar supervisión, experiencia, verificación y desafío, monitoreo, prueba o aseguramiento en asuntos relacionados con el cumplimiento. Estos son característicos de varias funciones de primera o segunda línea como se describe en el *Modelo de las Tres Líneas,* permaneciendo dentro del ámbito general y las responsabilidades de la dirección y, dependiendo de las características específicas del rol, potencialmente ofreciendo apoyo especializado y gestión de riesgos a aquellos con roles de primera línea y ejecutivos de rango superior.

Sujeto a los requisitos legales y reglamentarios y al sector de la industria, el tamaño y la complejidad de la organización, un rol de cumplimiento de rango superior, dependiendo de sus responsabilidades específicas, puede reportar a una de varias funciones diferentes en la organización. Incluyen a la alta dirección ejecutiva (por ejemplo, el director ejecutivo, el director de riesgos, el director de operaciones, el asesor general u otros), sus respectivas cadenas de gestión y / o directamente al organismo de gobierno o subcomité designado. En ciertos casos, nuevamente sujeto a los factores identificados anteriormente y a un mecanismo para garantizar la independencia de la función de auditoría interna, un rol o departamento de cumplimiento puede informar al director ejecutivo de auditoría (DEA) o a una persona que supervisa tanto el departamento de cumplimiento como el departamento de auditoría interna. Se deben aplicar los Seis Principios descritos en el *Modelo de las Tres Líneas* para evaluar la alineación de las responsabilidades de cada rol para el cumplimiento de los requisitos y expectativas. Como se describe en el Modelo, se deben tomar medidas de mitigación si una alineación presenta un posible conflicto de intereses o deterioro de la objetividad o la independencia. El conflicto potencial o real o el menoscabo de la objetividad también deben notificarse al organismo de gobierno para su consideración y posibles medidas, incluida la notificación al organismo de control, cuando proceda.

El cumplimiento como un conjunto de actividades

El cumplimiento puede referirse a los procesos y controles diseñados para lograr, apoyar, supervisar, vigilar, verificar, probar, desafiar o confirmar el cumplimiento. Las personas que ejecutan estas medidas ayudan a garantizar que la organización y sus miembros cumplan con los requisitos y expectativas.

El cumplimiento en una organización se logra a través de las acciones y comportamientos de todos los que trabajan para o con la organización, apropiados para su rol y antigüedad.

---

[6] El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) ofrece marcos para la gestión de riesgos, y liderazgo de pensamiento, incluyendo nuevas orientaciones sobre la aplicación del marco de riesgos ERM a la gestión de los riesgos de cumplimiento.

La responsabilidad de los procesos, procedimientos y controles de rutina diseñados para satisfacer requisitos y expectativas específicas a un nivel determinado y con un grado aceptable de certeza puede estar en varios lugares dentro de la organización y también puede ser subcontratado. El *Modelo de las Tres Líneas* establece que un elemento clave en la evaluación de la alineación es la identificación de los derechos de decisión relacionados con las actividades de cumplimiento. (Véanse los roles y actividades detalladas que comprenden el cumplimiento en la sección de anexo.)

El Modelo de las Tres Líneas:

Cumplimiento

El organismo de gobierno es, en última instancia, responsable del gobierno, que se logra a través de las acciones y comportamientos del organismo, así como mediante la dirección y la auditoría interna.[7]

A medida que cada organización asigna responsabilidades para los aspectos de cumplimiento de acuerdo con sus propias circunstancias, sujeto a los requisitos externos prescritos, debe analizar qué tan bien los roles y responsabilidades específicas asignadas en toda la organización se alinean con los Seis Principios del *Modelo de las Tres Líneas.* La evaluación puede mostrar que algunas responsabilidades se alinean con los roles del organismo de gobierno; algunas con la dirección, incluidos los roles de cumplimiento y gestión de riesgos; y otros con los roles de auditoría interna.

Los roles de primera línea incluyen proporcionar productos y servicios a clientes o consumidores y proporcionar el soporte necesario para hacerlo de acuerdo con los requisitos y expectativas. Los roles de segunda línea proporcionan supervisión y asesoramiento especializados, evalúan el riesgo (particularmente sobre una base colectiva o de cartera) y realizan actividades de gestión de riesgos (incluido la supervisión, la vigilancia y las pruebas), desafiando de manera creíble la primera línea. El rol de auditoría interna de tercera línea proporciona un aseguramiento independiente, incluida el aseguramiento de qué tan bien la segunda línea desafía de manera creíble a la primera línea. Juntos, deben trabajar de manera efectiva a través de la coordinación, la comunicación y la colaboración adecuadas para garantizar que sus actividades estén alineadas adecuadamente sin superposición, duplicación y brechas indebidas, y sin conflictos o incompatibilidades.

El gráfico utilizado para representar el Modelo no identifica un rol o departamento de cumplimiento ni otras funciones, departamentos o responsabilidades específicos de segunda línea. Representa las relaciones entre los roles centrales del gobierno en oposición a una estructura organizativa prescrita.

Determinación de la responsabilidad de los roles y actividades de cumplimiento

La responsabilidad, las acciones y el aseguramiento son los ingredientes esenciales del gobierno. El establecimiento y las características de los departamentos especializados en gestión de riesgos, cumplimiento, ética, sostenibilidad, seguridad, privacidad de datos, asesoramiento legal, control financiero, etc. dependen de muchos factores. Incluyen la complejidad organizacional, el tamaño, el sector, los recursos, la regulación, la legislación y la cultura, la tolerancia y grado de aceptación de riesgo

[7] Las estructuras para los organismos de gobierno varían según la jurisdicción, los requisitos reglamentarios y el diseño de cada institución. Cuando nos referimos a los organismos de gobierno, incluimos la amplia gama de estructuras de organismo de gobierno que se encuentran en diversas jurisdicciones e industrias, y tanto en el sector público como en el privado. Pueden aplicarse las siguientes responsabilidades del organismo de gobierno: establecer la dirección de la organización; definir la visión, la misión, los valores y el riesgo asumido; y recibir informes de la dirección sobre los resultados planificados, reales y esperados y en riesgo y gestión de riesgos.

del organismo de gobierno y, lo que es más importante, los objetivos y responsabilidades de los roles dentro del departamento especializado respectivo.

Sujeto a mandatos regulatorios específicos en ciertas industrias, las organizaciones pueden no tener un departamento de cumplimiento designado por separado. Muchos no lo hacen, ni pueden tener personas cuyos cargos o descripciones de trabajo incluyan el cumplimiento.

Sin embargo, incluso sin un rol o departamento de cumplimiento designado, las organizaciones aún pueden tener un gobierno efectivo y cumplir con los requisitos y expectativas, siempre que asignen roles y responsabilidades, proporcionales a la organización, para lograr el cumplimiento de los requisitos y expectativas aplicables, y que las personas se adhieran a sus roles definidos.

Por lo general, a medida que las organizaciones se hacen más grandes, más complejas, ricas en recursos o fuertemente reguladas, pueden decidir o se les puede exigir que asignen responsabilidades y recursos separados a roles y departamentos individuales para diversos aspectos del cumplimiento.

Además, un empleado puede ser responsable de más de un rol. En este caso, debe haber una evaluación adecuada de la compatibilidad de estos múltiples roles, y una definición clara de las responsabilidades de cada rol y de la supervisión y aseguramiento sobre el desempeño de esos roles. En ciertos casos, puede ser necesaria la aprobación del organismo de gobierno y organismo de control.

Con múltiples roles, puede haber un mayor riesgo de incompatibilidad, conflicto de intereses y disminución de la claridad sobre la rendición de cuentas y la responsabilidad. Es posible que se requiera que la mitigación permanezca dentro del grado de aceptación de riesgo, junto con la presentación de informes al organismo de gobierno y organismo de control, cuando corresponda.

Un esfuerzo colectivo para lograr el cumplimiento

Incluso cuando hay un rol o departamento de cumplimiento designado, es importante reconocer que todas las actividades de cumplimiento no residen en un solo lugar dentro de la estructura de una organización. Los empleados en todos los niveles, así como los directores ejecutivos y no ejecutivos deben contribuir al esfuerzo de cumplimiento colectivo. La responsabilidad y la rendición de cuentas se distribuyen a lo largo de la jerarquía, los roles definidos y la estructura de jerarquía administrativa de una organización para lograr el cumplimiento, mitigar los riesgos de cumplimiento y supervisar el cumplimiento de los requisitos y expectativas.

El cumplimiento de los requisitos y las expectativas externas e internas suele ser gestionado por departamentos especializados o personas externas a un departamento de cumplimiento designado. Sus respectivos roles y responsabilidades pueden estar definidos de forma más estricta por la normativa del sector industrial o por una persona específica o un conjunto de requisitos o expectativas. Algunos ejemplos son: el cumplimiento de la legislación y los reglamentos en materia de recursos humanos (RR. HH.), a cargo del departamento de RR. HH., y el cumplimiento de los requisitos de información financiera y tributaria, a cargo del departamento de finanzas.

Como se sugirió anteriormente, diferentes roles y departamentos pueden ser responsables de lograr el cumplimiento, así como el control, la supervisión y las pruebas de los aspectos del cumplimiento. Como resultado, es claramente importante aplicar los Seis Principios para identificar las características relacionadas con el cumplimiento de un rol individual y sus responsabilidades.

El gobierno efectivo se beneficia de la comunicación, coordinación y colaboración informales y formales y promueve la transparencia. Sin embargo, si las interacciones informales en las estructuras de gobierno y control eluden la identificación, el escalamiento y la mitigación adecuada de los problemas de cumplimiento, pueden socavar la eficacia de las estructuras formales de gobierno y control y desenfocar la determinación de la rendición de cuentas y la responsabilidad.

Al evaluar la efectividad de un modelo de gobierno, es esencial no solo evaluar la estructura de gobierno formal diseñada y desarrollada para lograr el cumplimiento, sino también sondear la organización en busca de líneas informales de comunicación, toma de decisiones y acción para identificar si, dónde y cuándo la estructura de gobierno informal socava o frustra la formal. En el *Modelo de las Tres Líneas* se fomentan fuertes interacciones formales e informales para promover la comunicación, la coordinación y la colaboración. Sin embargo, una estructura de gobierno informal puede bloquear el cumplimiento, eludir los controles y dar lugar a una gestión de riesgos de cumplimiento ineficaz, y oscurecer la claridad de la responsabilidad y la rendición de cuentas. La aplicación del *Modelo de las Tres Líneas* para identificar roles, responsabilidades y acciones permite a las organizaciones diseñar un marco de gobierno efectivo, incluido el desarrollo de salvaguardas para mitigar los riesgos del gobierno informal, la toma de decisiones y la acción que pueden conducir a fallas de cumplimiento.

Un programa de cumplimiento efectivo no solo impulsará la adopción y adhesión a una estructura formal y documentada de gobierno y control, sino que también será un elemento clave en el desarrollo y mantenimiento de una cultura de cumplimiento y control, facilitando la efectividad del *Modelo de las Tres Líneas.*

Aplicación de los Seis Principios

El *Modelo de las Tres Líneas* fomenta un enfoque basado en principios para evaluar y alinear roles y responsabilidades, teniendo en cuenta las circunstancias de una organización, incluidos sus requisitos y expectativas de cumplimiento específicos. Los Seis Principios del Modelo se pueden utilizar para comprender mejor el cumplimiento, como resultado, como categoría de riesgo, como rol o departamento, como conjunto de actividades, y su contribución a un marco de gobierno exitoso. (Para el lenguaje completo de los Seis Principios, véase el Modelo de las Tres Líneas).

Principio 1: Establecer requisitos de gobierno

El Principio 1 describe los requisitos mínimos de gobierno para ser:

- Responsabilidad (por parte de un organismo de gobierno a las partes interesadas para el éxito).
- Acciones y aplicación de recursos (por parte de la dirección para lograr los objetivos, incluye la gestión de riesgos y el cumplimiento).
- Aseguramiento y asesoramiento (desde un rol de auditoría interna independiente en todos los aspectos para permitir una supervisión y transparencia efectiva y promover la confianza y la mejora continua).

El organismo de gobierno es en última instancia responsable de garantizar que la organización se comporte de acuerdo con los estándares aceptados y las normas sociales. La dirección debe gestionar el riesgo asociado con el cumplimiento y el incumplimiento de acuerdo con la aceptación expresada por el organismo de gobierno. Esto puede incluir el establecimiento de roles individuales y equipos con un enfoque específico en los aspectos del cumplimiento, y la definición clara de los derechos de decisión entre la primera línea que posee los riesgos y la segunda línea para proporcionar un desafío creíble e impulsar la conformidad de la primera línea con el grado de aceptación de riesgo. La auditoría interna proporciona aseguramiento a la dirección y al organismo de gobierno sobre la adecuación y eficacia de los controles para el cumplimiento y asesoramiento para la mejora continua y la innovación.

Ilustraciones prácticas desde el campo

> **La atención médica es una industria altamente regulada y, como tal, la prestación de casi todos los servicios implica el cumplimiento de alguna regla, regulación o estándar. Las enfermeras, los médicos y otros profesionales clínicos deben asegurarse de que cada servicio prestado esté debidamente autorizado y documentado. Aquellos con responsabilidades de cumplimiento (roles individuales o un departamento) pueden asesorar a los departamentos clínicos sobre los requisitos de documentación y autorización de un procedimiento determinado, pero, en última instancia, los cuidadores de primera línea son responsables de implementar los procesos, controles y garantizar el cumplimiento de estos requisitos.**
>
> – Jefe de Cumplimiento y Auditoría Interna, Estados Unidos

Un ejemplo de mi industria es la clasificación de los principales riesgos de cumplimiento para la organización y los requisitos reglamentarios, y la alineación de actividades, controles, supervisión y responsabilidades para cumplir con los requisitos reglamentarios y en proporción a estos riesgos. Por ejemplo, una organización puede tener un oficial de cumplimiento contra el lavado de dinero, un oficial de privacidad, un oficial contra el soborno y la corrupción, etc., de acuerdo con los requisitos reglamentarios, y puede tener responsabilidades de productos, divulgación, empleo, quejas, etc., y recursos específicos para apoyar el cumplimiento y la gestión de estas áreas de riesgo clave. Se presentan informes periódicos al organismo de gobierno y todas las actividades están sujetas a una auditoría interna independiente.

– Director de Cumplimiento, Reino Unido

Un buen ejemplo de los desafíos que enfrentan las organizaciones hoy en día es el impulso para adoptar y adherir estándares "ambientales, sociales y de gobierno" o "ESG". El organismo de gobierno es responsable de hacer que la dirección rinda cuentas para que la organización se comporte de acuerdo con la estrategia, los estándares y las normas sociales establecidas por el organismo de gobierno. Los ESG abarcan todos los aspectos de la organización y a todos los empleados, proveedores y clientes, por lo que el organismo de gobierno debe garantizar que la dirección articule claramente los riesgos ESG aplicables a la organización, las leyes y reglamentos externos y las políticas y procedimientos internos, las medidas de rendimiento pertinentes y los datos fiables, auténticos y comparables que reflejen el cumplimiento de esos requisitos y expectativas internas. Además, tanto la dirección como el organismo de gobierno querrán o necesitarán aseguramientos sobre la consecución de los objetivos de cumplimiento ESG. Se requiere un complejo mapeo de responsabilidades y rendición de cuentas en toda la organización para captar los roles y departamentos respectivos y sus actividades necesarias para adoptar los ESG y demostrar su cumplimiento.

– Director de Cumplimiento, Estados Unidos

Principio 2: Mantener una supervisión adecuada del gobierno

El Principio 2 define los roles del organismo de gobierno para:

- Gobierno
- Supervisión de la gestión
- Establecer y supervisar una función de auditoría interna efectiva

El organismo de gobierno es en última instancia responsable del gobierno y se asegura de que existan estructuras y procesos apropiados. Esto incluye disposiciones para el cumplimiento, así como la supervisión del rol de la auditoría interna.

El organismo de gobierno debe determinar el grado de confianza que tiene y requiere sobre el cumplimiento de los requisitos y expectativas relacionados con el nivel de exposición al riesgo y el potencial de impacto en los objetivos estratégicos. Al determinar su grado de aceptación o tolerancia al riesgo de cumplimiento, el organismo de gobierno supervisará la ejecución de las actividades de la administración y el cumplimiento de las responsabilidades respectivas de los roles y departamentos

designados para lograr resultados de cumplimiento de acuerdo con la aceptación de riesgo de cumplimiento y las tolerancias relacionadas.

El organismo de gobierno debe garantizar que la auditoría interna esté adecuadamente posicionada y con los recursos necesarios para que pueda ofrecer aseguramiento y asesoramiento independientes y eficaces sobre el cumplimiento. El DEA debe ser responsable ante el organismo de gobierno, un comité de auditoría independiente o un comité designado equivalente del organismo de gobierno para asegurar su autoridad y su estado independiente.

Ilustraciones prácticas desde el campo

> **Un organismo de gobierno eficaz es capaz de promulgar el cambio y tener una voz en toda la organización. A veces, las escalaciones y la presentación de informes se realizan de forma general, pero depende de qué tan actualizado esté el organismo de gobierno y de la calidad de la información para proporcionar una supervisión y dirección efectivas en el "ahora" en lugar de basarse retrospectivamente en datos históricos. La auditoría interna debe validar si el organismo de gobierno está obteniendo una visibilidad clara de los riesgos que se gestionan con el fin de anticipar, supervisar y orientar sobre dichos riesgos. El cumplimiento desempeña un importante papel de segunda línea para desafiar a la gestión sobre el cumplimiento y la eficacia del control y proporcionar al organismo de gobierno información sobre la efectividad de la gestión de riesgos de cumplimiento dentro del grado de aceptación del riesgo.**
>
> – Oficial de Cumplimiento, Singapur

> **En el cuidado de la salud y muchos otros sectores, un departamento de cumplimiento puede tener la responsabilidad diaria de ciertos elementos del programa de cumplimiento, incluida la capacitación y la educación, la supervisión de la línea directa, la promulgación de un código de ética, la realización de verificaciones de antecedentes, etc. Algunas de estas actividades tienen que ver con el logro del cumplimiento, otras pueden ser sobre el establecimiento de políticas, la supervisión o la presentación de informes sobre la efectividad del cumplimiento a la alta dirección y el organismo de gobierno. El departamento de auditoría interna no puede ofrecer aseguramiento independiente sobre la efectividad del programa de cumplimiento si el departamento de cumplimiento reporta al DEA. Sin embargo, en tales casos, se puede contratar a un tercero independiente para que ofrezca aseguramiento al organismo de gobierno.**
>
> – Jefe de Cumplimiento y Auditoría Interna, Estados Unidos

> **El organismo de gobierno debe tratar de garantizar que los riesgos de cumplimiento se evalúen / consideren a fondo en el plan de auditoría de auditoría interna, comprender la cobertura plurianual de la auditoría interna en los riesgos regulatorios clave y las áreas de enfoque del organismo de control, y revisar los resultados de los informes / actividades relacionadas con el cumplimiento.**
>
> – Director Ejecutivo de Auditoría, Reino Unido

> **El organismo de gobierno establece el tono para la gestión de riesgos de cumplimiento tanto para la dirección como para la auditoría interna. Para que el organismo de gobierno sea eficaz**

en su supervisión del cumplimiento, debe haber una examinación amplia, regular y frecuente de la información cuantitativa y cualitativa adecuada sobre el estado del cumplimiento, proporcionada tanto por la dirección como por la auditoría interna. El organismo de gobierno debe establecer como puntos permanentes del orden del día la gama de actividades de gestión de riesgos de cumplimiento para abordar la gestión de riesgos de cumplimiento con visión de futuro, y no simplemente un enfoque orientado hacia atrás basado en eventos en violaciones, incumplimientos y medidas de corrección.

– Director de Cumplimiento, Reino Unido

Principio 3: Definir los roles de la dirección en la primera y segunda línea

El Principio 3 describe los roles de la dirección (roles de primera y segunda línea que pueden combinarse o separarse según los recursos, los objetivos, la regulación, etc.).

Los roles de primera y segunda línea constituyen la dirección. Reflejan las responsabilidades de la primera línea para proporcionar los productos y servicios a los clientes, y la segunda línea para proporcionar supervisión especializada, evaluar el riesgo (particularmente sobre una base colectiva o de cartera) y realizar actividades de gestión de riesgos, desafiando de manera creíble la primera línea.

Se pueden establecer departamentos separados, como un departamento de cumplimiento, o el jefe del departamento o, en organizaciones más pequeñas y menos complejas, un individuo, puede ser nombrado con vías jerárquicas al organismo de gobierno, ya sea directamente o a través de un comité del organismo de gobierno. El jefe del departamento o individuo también puede tener que rendir cuentas conjuntamente al director ejecutivo o a una persona designada dentro de la dirección. Esta vía jerárquica o de rendición de cuentas ante el organismo de gobierno puede parecer que establece una mayor independencia para el jefe del departamento de cumplimiento o el individuo. Sin embargo, un aspecto clave de la independencia es la ausencia de responsabilidades en la toma de decisiones. Por lo general, una persona que desempeña el rol de cumplimiento mantiene cierto grado de responsabilidad en la toma de decisiones de la dirección, desde la aceptación del cliente, la concesión de excepciones a la política, la aprobación de nuevos productos, etc. En consecuencia, una vía jerárquica a un organismo de gobierno o a un comité del organismo de gobierno no crea para dicho departamento, jefe de departamento o individuo una verdadera independencia. La auditoría interna y el DEA, además de la independencia de la dirección en sus vías jerárquicas, tampoco tienen responsabilidades en la toma de decisiones operativas de la dirección, lo que proporciona un grado adicional de independencia.

En consecuencia, las características de los roles a través de las líneas pueden articularse de la siguiente manera:

- Roles de primera línea: lograr el cumplimiento de leyes, regulaciones, códigos de comportamiento, políticas organizacionales, etc., en la provisión de productos y servicios. El cumplimiento sigue siendo responsabilidad de la dirección.
- Roles de segunda línea: Los roles individuales de cumplimiento y los departamentos establecen marcos, ejecutan la supervisión, proporcionan asesoramiento, seguimiento y vigilancia, realizan pruebas, cuestionan la dirección y, en general, pueden tener la toma de decisiones operativas de

la dirección, los poderes de propiedad de riesgo (por ejemplo, puede incluir la aceptación del consumidor o del cliente, la aprobación de nuevos productos o servicios, la aprobación de transacciones, la aprobación del exceso de límites, las excepciones a las políticas, etc.).

- Roles de tercera línea: la auditoría interna proporciona un aseguramiento independiente sobre el cumplimiento, la efectividad de los esfuerzos de la dirección para lograr el cumplimiento y el trabajo del rol o departamento de cumplimiento para dar seguimiento y proporcionar supervisión y control de la gestión de riesgos de cumplimiento, pero no al revés. La auditoría interna no tiene responsabilidades de toma de decisiones de la dirección y reporta de forma independiente al organismo de gobierno.

Utilizando el *Modelo de las Tres Líneas,* una organización puede lograr el cumplimiento de los requisitos y expectativas, así como contribuir a un gobierno efectivo y sostenible y combatir la ilegalidad y la corrupción. El cumplimiento debe basarse en la transparencia, estableciendo un estándar adecuado dentro de una organización. Además, para las partes interesadas externas, incluidos los accionistas, los organismos gubernamentales, las agencias de control y las bolsas, los proveedores y la cadena de suministro, un programa de cumplimiento efectivo que promueva la transparencia infunde confianza en una organización.

Ilustraciones prácticas desde el campo

> **Los roles de primera y segunda línea deben trabajar juntos de manera efectiva para identificar, gestionar y supervisar la mitigación de los riesgos de cumplimiento de la organización. No debe depender de la auditoría interna para supervisar, probar y encontrar cosas. Esto debe hacerse y ser propiedad de los roles de primera y segunda línea.**
>
> – Director Administrativo, Estados Unidos

> **Un rol de cumplimiento debe apoyar al negocio, asegurándose de que los procesos y controles estén claramente alineados. Hay varios casos en los que un rol de cumplimiento como segunda línea brinda asesoramiento a la empresa. Los indicadores clave de rendimiento y los indicadores clave de riesgo ayudarán a la empresa a identificar y gestionar los riesgos para la eficacia del control.**
>
> – Director de Cumplimiento, México

> **Muchas industrias están sujetas a una infinidad de regulaciones complejas. El departamento de cumplimiento ofrece su experiencia y asesoramiento sobre los requisitos o los cambios normativos recientes en un departamento determinado. Por ejemplo, en el sector sanitario, la dirección de los distintos departamentos clínicos es responsable de diseñar y aplicar los controles necesarios para garantizar el cumplimiento de la normativa. Debido a su experiencia, el departamento de cumplimiento está idealmente situado para evaluar el cumplimiento de estos requisitos.**
>
> – Director de Cumplimiento, Estados Unidos

> **Un desafío clave, pero que se gestiona bien en las empresas más grandes, es la propiedad y las obligaciones de los requisitos y expectativas de cumplimiento y cómo son ejecutados por aquellos en roles de cumplimiento o departamentos de cumplimiento. Esto requiere un marco de gestión y control de riesgos muy claro que tenga líneas claras de rendición de cuentas y**

roles y responsabilidades con rutas de escalamiento efectivas a través de un gobierno sólido. Sin esto, la supervisión del cumplimiento es borrosa y difícil de ejecutar.

– Director de Cumplimiento, Reino Unido

El cumplimiento es responsabilidad de todos. En industrias altamente reguladas, como la atención médica, esta responsabilidad abarca a todos los cuidadores y puede incluir el cumplimiento de los requisitos de autorización y documentación para cualquier procedimiento determinado. Si el departamento de cumplimiento desarrolla las políticas, procesos y controles sobre procesos o procedimientos específicos, o tiene la responsabilidad rutinaria del procedimiento, no podría ofrecer un aseguramiento objetivo. Sin embargo, asesorar y consultar sobre los requisitos reglamentarios asociados con un proceso o procedimiento no necesariamente perjudicaría la objetividad del departamento de cumplimiento.

– Jefe de Cumplimiento y Auditoría Interna, Estados Unidos

Principio 4: Definir el rol de la tercera línea

El principio 4 describe el rol de la auditoría interna como proveedor de aseguramiento y asesoramiento independiente.

El *Modelo de las Tres Líneas* amplía la necesidad crítica de asegurar la adecuación y eficacia de las respuestas al riesgo, incluidos los controles, como componente fundamental del gobierno. Las respuestas al riesgo y los controles incluyen los relativos a la consecución, el seguimiento y la supervisión del cumplimiento y la gestión de riesgo de cumplimiento. Esto se logra a través de la aplicación competente de procesos sistemáticos y disciplinados, experiencia y conocimiento por parte de la auditoría interna, como único proveedor de aseguramiento de la organización que es independiente de la gestión.

La coordinación y colaboración efectivas entre los roles de cumplimiento y los roles de auditoría interna se pueden lograr en beneficio de una organización sin afectar la efectividad de cada uno en el cumplimiento de sus distintos roles.

Como resultado de los diversos roles y responsabilidades en toda una organización, puede haber otras fuentes de seguridad que, en conjunto, podrían proporcionar una perspectiva integral y compuesta de una organización. Sin embargo, es importante analizar y evaluar roles específicos y su alineación de acuerdo con el *Modelo de las Tres Líneas* para evaluar la calidad y objetividad de dicho aseguramiento.

La auditoría interna mantiene la responsabilidad ante el organismo de gobierno y la independencia de las responsabilidades de la dirección. Esto es fundamental para comprender los roles de aseguramiento y la posición distintiva de la auditoría interna dentro de la estructura de gobierno. Si la independencia de la actividad de auditoría interna y la objetividad de los auditores internos se ven amenazadas, el DEA debe informar al organismo de gobierno para que tome medidas correctivas.

Los auditores internos, al evaluar la efectividad de los roles y departamentos de cumplimiento, deben estar abiertos a la comunicación, coordinación y colaboración para lograr la aplicación efectiva del *Modelo de las Tres Líneas* y promover una cultura de cumplimiento y control.

Ilustraciones prácticas desde el campo

> **Un elemento clave en el que hay que fijarse al evaluar la gestión de riesgo de cumplimiento es la eficacia de las actividades que se realizan para mitigar los problemas. Es importante una sólida evaluación de los riesgos específicos de cumplimiento y la alineación de las actividades en proporción a esos riesgos. De lo contrario, podrían realizarse muchas actividades sin que la organización se beneficie de salvaguardar los riesgos de incumplimiento.**
>
> – Director Ejecutivo de Auditoría, Sudáfrica

> **Un desafío particular para los auditores internos es la incorporación en su trabajo de auditoría y la presentación de informes de la identificación explícita de casos de incumplimiento: violaciones de leyes y reglamentos, infracciones de políticas, normas y códigos de conducta. Para ofrecer dicho aseguramiento se requiere acceso a recursos debidamente calificados para evaluar e informar de manera efectiva sobre el logro del resultado de cumplimiento deseado.**
>
> – Director Ejecutivo de Auditoría, Reino Unido

Principio 5: Mantener la independencia de tercera línea

El principio 5 describe la importancia de la independencia de la auditoría interna.

La auditoría interna como tercera línea tiene varias características que ayudan a definir su independencia. Estos incluyen una vía jerárquica funcional independiente al organismo de gobierno o a un comité del organismo de gobierno y, lo que es más importante, la independencia de la toma de decisiones de la dirección.

Las funciones de gestión de riesgos (incluidas las funciones de gestión de riesgos de cumplimiento), aunque a menudo tienen una vía jerárquica funcional al organismo de gobierno o a un comité del organismo de gobierno, generalmente también tienen dentro de sus respectivos roles responsabilidades de toma de decisiones de la dirección, particularmente con respecto a la toma, gestión, mitigación, control y notificación de riesgos, incluido el riesgo de cumplimiento.

La segunda línea puede mantener su responsabilidad de proporcionar un desafío efectivo y creíble de la primera línea. Sin embargo, la independencia de la auditoría interna de la toma de decisiones de gestión es un diferenciador significativo entre el rol de tercera línea y los roles de la segunda y primera línea, como se detalla anteriormente en el Principio 3.

Ilustraciones prácticas desde el campo

> **Para que la auditoría interna no entre en conflictos, los auditores internos no deben haber diseñado o ejecutado controles ni haber participado en la toma de decisiones de la dirección; su objetivo es la observación, la comprobación y la evaluación para determinar si los riesgos clave se identifican y se controlan según lo previsto. No deben tener ningún sesgo ni expectativas preconcebidas.**
>
> – Director Ejecutivo de Auditoría, Australia

La parte interesada clave de la auditoría interna es el organismo de gobierno, y la independencia organizativa de la auditoría interna le permite informar resultados y recomendaciones sin filtrar. No hay expectativa ni necesidad de garantizar que los mecanismos de control y quienes los ejecutan se vean de manera favorable. La auditoría interna tiene la responsabilidad final de informar la verdad.

– Director de Auditoría y Cumplimiento, Estados Unidos

Los roles de segunda línea en materia de cumplimiento definen las políticas, asesoran a las empresas en cuanto al diseño de los controles, asesoran y revisan los riesgos asumidos de las empresas y ofrecen aseguramiento. Los individuos o departamentos de cumplimiento pueden tener responsabilidades asignadas para ejecutar funciones operativas en nombre de la primera línea. En estos casos, la persona o el departamento de cumplimiento no es totalmente independiente de la primera línea. La auditoría interna es la única actividad totalmente independiente debido a su independencia de la toma de decisiones de la dirección de la primera y segunda línea.

– Jefe de Riesgo Empresarial y Auditoría Interna, Estados Unidos

Principio 6: Crear y proteger el valor a través de la colaboración

El principio 6 describe la importancia de garantizar la coordinación y la colaboración entre todos estos roles.

Un gobierno eficaz no sólo requiere una asignación adecuada de responsabilidades, sino también una fuerte alineación de las actividades a través de la coordinación, la colaboración y la comunicación. Los organismos de gobierno se basan en los informes de la dirección, la auditoría interna y otros para ejercer la supervisión y proporcionar directrices a la dirección para alcanzar los objetivos, gestionar el riesgo y crear valor. Los roles del organismo de gobierno, junto con los de primera, segunda y tercera línea, contribuyen colectivamente a la creación y protección de valor cuando están alineados entre sí y con los intereses prioritarios de las partes interesadas. En consecuencia, la comunicación clara de las responsabilidades de cumplimiento en toda la organización, los derechos de decisión, las obligaciones de información, el riesgo asumido, las taxonomías comunes, las entidades o unidades de evaluación bien definidas, la información sobre el rendimiento y el riesgo en relación con los requisitos y las expectativas, y los programas de pruebas y aseguramiento sirven para mejorar la coordinación y la colaboración.

Ilustraciones prácticas desde el campo

Una ilustración de coordinación y colaboración es, por ejemplo, la privacidad de los datos. El cumplimiento, o en ciertas organizaciones el cumplimiento en colaboración con el departamento legal identifica los requisitos reglamentarios, los comunica a la organización y garantiza que se implementen los procesos y controles apropiados. Los equipos de negocios (operaciones, TI, seguridad de la información, etc.) implementan las actividades, incluyendo supervisión, escalamiento y reportando la información según sea necesario. El equipo de seguridad de la información y los equipos de cumplimiento supervisan las áreas de riesgo clave para garantizar que los equipos de negocios sigan los procedimientos y supervisen e informen

adecuadamente. La auditoría interna evalúa el marco de gestión de los riesgos pertinentes, incluido el riesgo de cumplimiento, y los procesos y controles conexos realizados por los equipos de la empresa al auditar esas áreas.

– Director de Cumplimiento, Reino Unido

El ESG es un gran ejemplo de coordinación y colaboración en toda la organización para lograr el cumplimiento de los requisitos y expectativas. Los roles de primera, segunda y tercera línea deben trabajar juntos, dentro de sus respectivos roles y con la supervisión del organismo de gobierno, para lograr los resultados ESG deseados. Aquellos con diversas responsabilidades de cumplimiento trabajarán con otros en la organización para lograr los objetivos ESG de la organización:

- **El organismo de gobierno establece la estrategia y grado de aceptación del riesgo y proporciona el tono para la cultura y el comportamiento.**
- **La dirección integra los requisitos y expectativas de ESG en el gobierno y las operaciones de la organización.**
  - **Proporciona asesoramiento, marco y requisitos sobre el contenido, el diseño y la aplicación de estructuras, sistemas y procesos adecuados para la planificación estratégica y operativa, el establecimiento de objetivos, la recopilación de datos, la toma de decisiones y la elaboración de informes relacionados con ESG.**
  - **Evalúa los riesgos asociados con el logro del cumplimiento de los requisitos y estándares externos de ESG, así como de las políticas y objetivos internos.**
  - **Desarrolla estándares, marcos, principios o modelos que deben adoptarse para medir, supervisar y reportar los impactos en el logro de los resultados de ESG.**
  - **Evalúa la precisión y consistencia de los datos y las metodologías utilizadas para recopilar datos utilizados en la sostenibilidad y los informes ESG.**
  - **Establece mediciones y procesos de evaluación; definición de la materialidad y lista de indicadores pertinentes (KPI); introducción de métodos, directrices y herramientas de presentación de informes (tanto internos como externos).**
- **La auditoría interna proporciona aseguramiento independiente al organismo de gobierno sobre las actividades anteriores y el logro de los objetivos ESG por parte de la dirección, así como sobre la conformidad de los informes a la dirección con requisitos y expectativas.**

– Director de Cumplimiento, Reino Unido

Datos clave sobre el cumplimiento

Diez puntos importantes para tener en cuenta:

1. Es posible que no haya un recurso dedicado, departamento, gerente, etc., para el cumplimiento. No todas las organizaciones pueden o necesitan asignar recursos de esta manera. A menudo, a medida que las organizaciones se vuelven más complejas, alta o específicamente reguladas, más grandes, sujetas a un mayor escrutinio, comienzan a operar en entornos que cambian rápidamente (regulatorios, comerciales, etc.) y comienzan a abordar factores similares que deciden que los individuos, equipos, sistemas y / u otros recursos deben asignarse a aspectos de cumplimiento como una división del trabajo y un componente formal del diseño organizacional. Esos recursos pueden ser externos en algunas organizaciones; por ejemplo, a través de la subcontratación de ciertos controles de cumplimiento o experiencia en la materia.

2. Al aplicar los Seis Principios del *Modelo de las Tres Líneas* para evaluar los roles relacionados con el cumplimiento, es útil considerar los resultados de los que el rol es responsable:

- Lograr el cumplimiento de las leyes, regulaciones, contratos, políticas, procedimientos, códigos de conducta u otros requisitos en la provisión de productos y servicios.
- Proporcionar supervisión especializada; evaluar el riesgo (en particular sobre una base colectiva o de cartera) y realizar actividades de gestión de riesgos; y desafiar de manera creíble la primera línea para promover y lograr el cumplimiento en toda la organización de acuerdo con los códigos de conducta aplicables o los estándares, requisitos y expectativas.
- Proporcionar una evaluación sobre la adecuación y efectividad del programa de cumplimiento.
- Proporcionar un desafío experto sobre la efectividad del programa de cumplimiento y sus componentes en toda la organización.

3. Un solo rol o departamento de cumplimiento dentro de una organización puede no cubrir todos los asuntos relacionados con el cumplimiento para esa organización[8]. En tales casos, la organización debe documentar claramente el alcance de los roles de cumplimiento o departamento(s), así como qué roles tienen responsabilidad por otros requisitos y expectativas. Esto es tan importante para las organizaciones más pequeñas, donde a un individuo se le pueden asignar múltiples responsabilidades y roles y algunas responsabilidades pueden ser subcontratadas, como lo es para las organizaciones más grandes, donde puede haber múltiples roles o departamentos encargados de diversas actividades de cumplimiento.

4. Un rol de cumplimiento o jefe de un departamento de cumplimiento puede, en la práctica y sujeto a requisitos legales y reglamentarios, reportar a uno de varios roles diferentes en una organización, incluyendo: la alta dirección ejecutiva (por ejemplo, el director ejecutivo, el director de riesgos, el director

[8] La ética, la sostenibilidad, la información financiera, la privacidad de los datos, los recursos humanos y las obligaciones legales, como ejemplos, pueden tener su propio recurso interno y/o externo para lograr el cumplimiento o proporcionar una supervisión adicional y una gestión de riesgos para componentes específicos del cumplimiento. Por ejemplo, la evolución de los aspectos medioambientales, sociales y de gobierno (ESG) está dando lugar a una serie de nuevos roles, responsabilidades, actividades y departamentos dentro de varias organizaciones, centrados en el cumplimiento de los amplios aspectos de los ESG.

de operaciones, el asesor general u otros) y / o el organismo de gobierno o comité de este. En algunos casos, el cumplimiento, aunque es parte de la administración, puede informar al DEA. La idoneidad de la línea de reporte puede determinarse en parte mediante la evaluación de responsabilidades de acuerdo con el *Modelo de Tres Líneas* y los requisitos legales y reglamentarios respectivos.

5. Un rol de cumplimiento o jefe de un departamento de cumplimiento puede tener una vía jerárquica o reportar la responsabilidad a uno o más comités del consejo o presidente de uno o más comités del consejo. Sin embargo, esto no equivale a independencia de la dirección y no reemplaza la necesidad de una garantía independiente proporcionada por la auditoría interna.

6. Los roles individuales de cumplimiento y los departamentos de cumplimiento pueden incluir responsabilidades que incluyen, pero no se limitan a: la gestión de riesgos de cumplimiento en general, el seguimiento, las pruebas, el análisis, la evaluación, el asesoramiento, el aseguramiento, el establecimiento de políticas, el desarrollo y la aplicación de sistemas y controles, las decisiones de la dirección, la supervisión y la formación.

7. Los roles y departamentos de cumplimiento también pueden incluir responsabilidades que están estrecha o directamente relacionadas con la provisión de productos y servicios. Esto requeriría una documentación clara de las responsabilidades, la autoridad y la responsabilidad en el rol (por ejemplo, la capacidad de prevenir el incumplimiento en el suministro del producto o servicio al prohibir una transacción o vetar una decisión de la dirección).

8. Los roles de primera y segunda línea deben estar separados. Los miembros de la primera línea deben ser dueños del riesgo que asuman, mientras que los de la segunda línea deben establecer y supervisar los marcos y estándares para ayudar a la primera línea a gestionar los riesgos que poseen, al tiempo que proporcionan un desafío creíble a las decisiones y actividades de la primera línea. En la práctica, dependiendo de los requisitos jurisdiccionales o de la industria, y del tamaño, la complejidad y otros factores de la organización, puede haber roles combinados. En ese caso, debe llevarse a cabo una evaluación de la compatibilidad de dichos roles y mitigarse cualquier riesgo relacionado. Esto puede requerir ajustes en la composición de los roles para mitigar efectivamente los riesgos de un conjunto incompatible de actividades dentro de un rol. La responsabilidad de gestionar el riesgo sigue siendo parte de los roles de primera línea y dentro del alcance de la gestión.

9. Independientemente de cómo las organizaciones estructuren sus recursos dedicados a las obligaciones de cumplimiento, la dirección mantiene la responsabilidad de garantizar que la organización cumpla con sus requisitos y expectativas dentro de los parámetros de riesgos asumidos establecidos por el organismo de gobierno.

10. Una responsabilidad esencial del rol de cumplimiento de segunda línea es la evaluación de la efectividad del programa de cumplimiento de la organización y los esfuerzos necesarios para lograr los requisitos y expectativas de cumplimiento de la organización.

ANEXO: Alinear la responsabilidad de los roles y actividades de cumplimiento

Las actividades de cumplimiento son un componente esencial de las actividades de gobierno, gestión de riesgos y control interno de una organización. La responsabilidad de las acciones necesarias para lograr, apoyar, verificar y confirmar el cumplimiento, y la ejecución de esas responsabilidades, puede asignarse a varias partes de la organización. Los responsables de las actividades de cumplimiento deben definir los resultados esperados que constituyen el cumplimiento y definir las medidas apropiadas para demostrar el logro de esos resultados.

Las actividades que comprenden el cumplimiento pueden incluir, entre otras, las siguientes:

- Identificar leyes, reglas, regulaciones y políticas internas, estándares, procedimientos y códigos de conducta externos relevantes y un comportamiento aceptable consistente con los objetivos de la organización.
- Determinar la medición de riesgos adecuada para el cumplimiento y el incumplimiento de las leyes, reglas, regulaciones y políticas internas, estándares, procedimientos y códigos de conducta externos relevantes y el comportamiento aceptable consistente con los objetivos de la organización.
- Realizar evaluaciones de riesgos para el cumplimiento de las leyes, reglas, regulaciones externas relevantes y políticas, estándares y procedimientos internos, incluidos los riesgos futuros y emergentes, y los códigos de conducta y el comportamiento aceptable consistente con los objetivos de la organización.
- Diseñar, desarrollar e implementar procesos y controles para lograr el cumplimiento de las leyes, reglas, regulaciones y políticas internas, estándares, procedimientos y códigos de conducta externos relevantes y un comportamiento aceptable consistente con los objetivos de la organización.
- Realizar, mantener y administrar procesos y controles para lograr el cumplimiento de leyes, reglas, regulaciones y políticas internas externas, estándares, procedimientos y códigos de conducta y un comportamiento aceptable consistente con los objetivos de la organización.
- Evaluar, probar y supervisar el cumplimiento de las leyes, reglas, regulaciones y políticas internas externas relevantes, estándares, procedimientos y códigos de conducta y el comportamiento aceptable consistente con los objetivos de la organización.
- Proporcionar un desafío creíble a la administración con respecto al riesgo de cumplimiento.
- Gestionar y mitigar el riesgo de cumplimiento.
- Determinar casos de cumplimiento o incumplimiento.
- Informar y escalar casos de incumplimiento.

- Reportar cumplimiento o incumplimiento de acuerdo con requerimientos externos e internos.
- Fomentar una cultura propicia para el cumplimiento.
- Sensibilizar a través de la comunicación, la formación, la promoción y la educación.
- Consultar y asesorar sobre aspectos de cumplimiento.
- Establecer y mantener un programa de ética o denuncia de irregularidades.
- Desarrollar y proporcionar capacitación, educación y concientización sobre el cumplimiento.
- Realizar las responsabilidades de enlace regulatorio entre las agencias de control y la organización.
- Establecer y mantener relaciones con organizaciones profesionales y organismos de la industria para identificar estándares, códigos o pautas relevantes por los cuales la organización y sus respectivas actividades deben o pueden optar por adherirse, así como facilitar la recopilación y presentación de informes de información de referencia.
- Establecer y mantener relaciones de enlace con las organizaciones de infraestructura de la industria que pueden establecer y requerir la conformidad con los requisitos o expectativas para los usuarios de la infraestructura y las contrapartes.

Es importante que las responsabilidades, y los resultados deseados, de cada rol sean claros. Algunos de estos roles y actividades son incompatibles con otros roles, como la aprobación de transacciones, la aceptación del cliente u otra toma de decisiones de riesgo comercial dentro de las responsabilidades de tercera línea, como se detalla en el *Modelo de las Tres Líneas.* Cuando se pide a la auditoría interna que asuma tales roles, se necesitan salvaguardias clave, incluido el consentimiento del organismo de gobierno o del comité de auditoría, el uso de un tercero para proporcionar un aseguramiento independiente en las áreas afectadas y, en su caso, la aprobación reglamentaria.

Del mismo modo, incluso con las mejores intenciones para lograr el resultado de proporcionar productos y servicios a los clientes en cumplimiento, una organización debe estar atenta para identificar roles, cuyas responsabilidades están diseñadas tanto para lograr el cumplimiento en la provisión del producto o servicio, como para proporcionar la supervisión y una gestión de riesgos de cumplimiento más amplia. Se aplican los principios básicos de separación de funciones e independencia, así como la expectativa de mitigar los riesgos que surgen cuando se identifican actividades incompatibles en roles.

Del mismo modo, a veces existe la tentación de quienes están en roles de supervisión, al identificar brechas o deficiencias en las actividades de gestión y control de riesgos que sustentan la provisión de productos o servicios, de ampliar su propio alcance más allá de la supervisión hacia la ejecución. Lo inverso también puede ser cierto, donde la primera línea puede confiar demasiado en aquellos roles que proporcionan supervisión o con responsabilidades de gestión de riesgos. Esto socava los beneficios de una supervisión objetiva. En tales casos, corresponde al rol de supervisión identificar, escalar y supervisar la brecha o deficiencia, y la remediación de la administración. Estos elementos deben alinearse y documentarse de acuerdo con los roles y responsabilidades de gobierno establecidos.

Acerca de las declaraciones de posición

El Instituto de Auditores Internos (The Institute of Internal Auditors o IIA) promulga las declaraciones de posición en temas principales de interés para las partes interesadas y los practicantes con el fin de promover un buen gobierno y educar a aquellos involucrados en ella. Las posiciones esbozadas ofrecen percepciones sobre diversos aspectos del proceso de gobierno y el rol fundamental de la auditoría interna en la mejora del gobierno en todos los niveles y la adición de valor a la organización. Las declaraciones de posición se desarrollan y revisan a través de un proceso riguroso que solicita aporte y crítica de los profesionales practicantes de la auditoría interna y otros voluntarios del IIA que actúan en el Comité Global de Defensa del IIA, la Junta de Normas del IIA y el Comité de Responsabilidad Profesional y Ética del IIA.

Acerca del Instituto de Auditores Internos

El Instituto de Auditores Internos (IIA) es el defensor, educador y proveedor de normas, orientación y certificaciones más ampliamente reconocido de la profesión de auditoría interna. Establecido en 1941, el IIA atiende hoy a más de 200,000 miembros de más de 170 países y territorios. La sede mundial del IIA se encuentra en Lake Mary, Florida. Para obtener más información, visite: www.globaliia.org.

Cláusula de exención de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no pretende proporcionar respuestas definitivas a determinadas circunstancias individuales y, como tal, sólo se pretende utilizar como guía. El IIA recomienda que siempre busque asesoramiento independiente de expertos que se relacionen directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona colocando su dependencia exclusiva de este material.

Derechos de autor

La traducción al español de este documento fue autorizada por The Institute of Internal Auditors, Inc. y fue realizada por la Fundación Latinoamericana de Auditores Internos – FLAI. Traductora: Suzzet González (servicios contratados), revisor: Roberto Loo y Jorge Badillo, CIA, CRMA, CCSA, CGAP, CISA.

Traducción al Español Auspiciada por:

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS