AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del Marco de Gestión del Riesgo de Conducta

The Institute of Internal Auditors

40 años 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 3.500 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

OBSERVATORIO SECTORIAL

PRÁCTICAS DE BUEN GOBIERNO

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS

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.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del Marco de Gestión del Riesgo de Conducta

Noviembre 2023

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Cristina González Barreda, CIA. BBVA.

Eric Álvarez Naudó. DELOITTE.

Javier Arija Tejero. INDITEX.

David Bello Castro, CIA, CAMS. CREDIT ANDORRÁ.

Pablo Díaz Ortíz, CESCOM. EY.

María Gerbolés López, ICCP, CESCOM, EFPA. BANCO SABADELL.

Isabel Gracia de las Heras, CFE. SEAT.

Karina León Ávila. BANCO NACIONAL DE COSTA RICA.

Juan Luis Martín Fernández, CIA, CFSA. CAIXABANK.

Cristina Usó Blasco, COSO-ERM, CESCOM, ICECOM. INDEPENDIENTE.

The Institute of Internal Auditors

40 años 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

ISBN: 978-84-126682-4-7

Maquetación: desdecero, estudio gráfico

"La cultura organizacional es fundamental para el cumplimiento de objetivos. (...) ahora más que nunca una empresa debe asegurar que sus creencias, hábitos, valores, actitudes y tradiciones sean compartidos por todo su personal por ello, es de suma relevancia que la cultura organizacional esté claramente definida y alineada con la estrategia para obtener los resultados deseados". Auditoría de la cultura. **IIA Global 2017.**

"Para definir la Cultura Corporativa, las organizaciones deben plantearse cuáles son los riesgos para su sostenibilidad, objetivos estratégicos, reputación o permanencia que deriven de comportamientos no deseados concretos y, en función de estos, diseñar las herramientas que facilitarán a sus empleados cumplir con los criterios deseados mitigando los riesgos identificados". Auditoría interna de la cultura corporativa. **IAI España 2023.**

La gestión del riesgo de conducta es esencial para mantener la integridad y reputación de una organización. Este documento analiza el papel de Auditoría Interna en este proceso al evaluar los procesos de identificación y evaluación, valorar la efectividad de los controles establecidos y ofrecer recomendaciones para fortalecer el sistema de gestión del riesgo de conducta.

Índice

Resumen ejecutivo

El riesgo de conducta contempla la posibilidad de que los empleados o directivos actúen de manera contraria a los principios éticos, los valores y/o las políticas establecidas en la organización.

Este documento se centra en la importancia del riesgo de conducta en las organizaciones y el papel fundamental que desempeña Auditoría Interna en relación con el marco de gestión de este riesgo.

Partiendo de una explicación sobre el concepto de Riesgo de Conducta, el documento contempla la posibilidad de que los empleados o directivos de una organización actúen de manera contraria a los principios éticos, los valores y/o las políticas establecidas en la organización. Esto puede incluir, entre otras situaciones, comportamientos inapropiados, fraudes o conflictos de intereses. Comprender y gestionar la naturaleza de este riesgo es esencial para mantener la reputación de la organización y asegurar el cumplimiento de las normativas.

En segundo lugar, el documento aborda las características necesarias para disponer de un marco eficaz para la gestión del riesgo de conducta: un sistema que implica disponer de procesos para la identificación, evaluación, mitigación y seguimiento de las situaciones relacionados con la conducta indebida en el seno de la organización. Situación que implica establecer políticas claras, comunicar y formar a los empleados sobre los estándares de conducta esperados, así como implementar controles internos adecuados para prevenir y detectar las posibles irregularidades.

En tercer lugar, se profundiza en el papel fundamental que desempeña Auditoría Interna en este marco de gestión del riesgo de conducta. Su función principal será proporcionar aseguramiento sobre el proceso general de gestión de este riesgo (identificación, evaluación, etc.) y contrastar la efectividad de los controles y procesos diseñados e implementados para prevenir y detectar los comportamientos inadecuados.

En la última parte del documento, se abordan los principales beneficios derivados de los trabajos de Auditoría Interna sobre el marco de gestión del riesgo de conducta de la organización, entre los que destacan las capacidades de anticipación de situaciones no deseadas relacionadas con la conducta del personal; el aumento de confianza en los controles internos y en la efectividad del sistema de gestión de riesgos de conducta; la mejora de la cultura ética y de cumplimiento en la organización y la puesta a disposición de recomendaciones para fortalecer los procesos y controles existentes, ayudando a prevenir y mitigar potenciales riesgos de conducta con impactos significativos para la organización.

Cierra el documento un Anexo en el que se facilita una propuesta de programa de trabajo, a título de ejemplo, que puede servir de pauta a los auditores internos para poder afrontar los trabajos de revisión de un ele-

mento clave dentro de las organizaciones, como es el marco de gestión del riesgo de conducta.

En definitiva, la gestión del riesgo de conducta es esencial para mantener la integridad y reputación de una organización y este documento ayuda a entender que Auditoría Interna desempeña un papel vital en este proceso, al evaluar los procesos de identificación y evaluación, valorar la efectividad de los controles y procesos establecidos, y ofrecer recomendaciones para fortalecer el sistema de gestión del riesgo de conducta, en un proceso de mejora continua. Al hacerlo, Auditoría Interna contribuye a promover una cultura ética y de cumplimiento en la organización, así como a proteger sus intereses y reputación.

Introducción

RIESGO DE CONDUCTA – ENTENDER EL CONCEPTO

El perfil del auditor interno actual requiere de un profesional orientado al servicio, a la innovación, a la mejora constante y con visión anticipatoria, para ofrecer aseguramiento sobre la gestión de los riesgos de su organización. En este sentido, el riesgo de conducta se ha convertido en un factor elemental en la gestión de riesgos de las organizaciones, con independencia del sector en el que operen.

La mayoría de las organizaciones han avanzado significativamente en la gestión de los riesgos tradicionales que les pueden impactar. Sin embargo, aunque el riesgo de conducta ya se encuentra en el radar de muchas organizaciones, su control es más difícil que el de los riesgos más clásicos, ya que implica entender en profundidad el valor de lo intangible y el impacto que está teniendo en las entidades para las que trabajamos.

Es necesario prestar cuidado a aquellos aspectos en los que la visión, los valores y el propósito de una organización sean comprendidos, aplicados o vividos por todos los colaboradores y por la misma organización, de tal manera que los comportamientos se conviertan en un factor impulsor del negocio y no en un factor que afecte negativamente a su funcionamiento y continuidad.

La gestión del riesgo de conducta es esencial para mantener la integridad y reputación de una organización.

MOTIVACIÓN

La gestión del riesgo de conducta ganó atención en el sector financiero tras comprobar que la conducta no ética fue una de las principales causas de la crisis financiera que dio comienzo en 2007, y que tanto impacto tuvo en la economía global. Las organizaciones

que no consideran el impacto de sus valores y cultura sobre los distintos grupos de interés pueden ver afectadas sus operaciones, puesto que los comportamientos de sus equipos, proveedores y resto de colaboradores influyen, en mayor o menor medida, en la consecución de sus objetivos, en su reputación e, incluso, en su supervivencia. En los últimos años, y no solo a raíz de la crisis financiera comentada, se ha incrementado el foco de los distintos grupos de interés sobre las cuestiones de conducta que afectan al desempeño de la organización y a su entorno.

La gestión inadecuada del riesgo de conducta puede resultar en pérdidas financieras, daños a la reputación de la empresa, sanciones legales u otros impactos negativos.

El riesgo de conducta se ha considerado como un "riesgo no financiero", puesto que su origen es no financiero. Pero como se mencionaba antes, desde hace unos años la valoración de las organizaciones, por parte de los distintos grupos de interés, se ha ampliado para considerar no solo aspectos estrictamente económicos o financieros, sino también, otros factores como, por ejemplo, operar respetando la legalidad vigente (fraude y corrupción), disponer de políticas de sostenibilidad, respetar el medioambiente o implementar una cultura ética.

Nos encontramos en un contexto en el que la Responsabilidad Social Corporativa (RSC en adelante) y los criterios ESG (Environmental, Social and Governance) han cobrado una relevancia mayor en la toma de decisiones dentro y fuera de la organización. Es importante no perder de vista que los comportamientos de los individuos impactan en los resultados de una organización y que podrían convertirse en problemas traducibles en pérdidas y daños para la misma y, por tanto, es imprescindible que las organizaciones consideren el riesgo de conducta en sus análisis de riesgos.

"La cultura de una organización, no es un concepto novedoso, pero la importancia que ha adquirido durante los últimos años ha aumentado de manera considerable. La razón de este creciente interés no radica, exclusivamente, en el mayor escrutinio regulatorio y social al que se enfrentan las organizaciones, sino que también ha sido clave el entendimiento, por parte de los órganos de dirección, de que la cultura, a pesar de ser un elemento intangible, es fundamental para llevar a buen término los objetivos estratégicos definidos"[1]. Y esa cultura se refleja, precisamente, en los comportamientos, hábitos, actitudes y conductas de las personas que conforman una organización.

"La gestión inadecuada de los riesgos de conducta puede resultar en pérdidas financieras, daños a la reputación de la empresa, sanciones legales u otros impactos negativos en la organización"[2], por lo que para el auditor interno es un reto proporcionar una evaluación sobre este aspecto. Este planteamiento va más allá de un proceso de control enfocado en el cumplimiento de las normas, procedimientos o reglamentos definidos, ya que aborda el impacto más amplio que tiene la cultura y los comportamientos de la organización y sus individuos, en el cumplimiento de objetivos y en el valor percibido por los distintos grupos de interés.

Definir el riesgo de conducta permite a las organizaciones y a los auditores internos esta-

1. *Auditoría Interna de la Cultura Corporativa*, LA FÁBRICA DE PENSAMIENTO, Instituto de Auditores Internos de España, 2023.
2. Proyecto de Controles Blandos, Conglomerado Financiero del Banco Nacional de Costa Rica, 2022.

blecer los límites de su marco de gestión. En la actualidad existe desconocimiento y diferencias sobre los conceptos sobre el riesgo de conducta. En este documento, se clarifican algunos aspectos del riesgo de conducta en las organizaciones, para facilitar la función del auditor interno.

La información para evaluar el riesgo de conducta debe estar establecida en la estrategia corporativa e indicado en el *tone at the top.*

LA CONDUCTA EN LAS ORGANIZACIONES

El diccionario de la Real Academia de la Lengua Española define la conducta como *"la manera con que las personas se comportan en su vida y acciones".* Dependiendo del ámbito de estudio, la conducta puede catalogarse de un modo u otro (por ejemplo, conducta cívica o incívica en el ámbito jurídico, o conducta latente, voluntaria, adaptativa, patológica, etc. en el ámbito de la psicología). Adicionalmente, la conducta puede recibir un calificativo como "mala" o "buena", "deseable" o "indeseable", etc. dependiendo de la manera en que contribuya a alcanzar determinados objetivos.

A lo largo del documento se analiza cómo la conducta o el comportamiento de las personas vinculadas a una organización puede derivar en consecuencias negativas para la misma.

Tradicionalmente, las *soft skills* de las organizaciones no han sido el foco en las evaluaciones de las auditorías internas, porque *"existe el temor de brindar una opinión errónea sobre aspectos que se consideran subjetivos"*. Sin embargo, para una auditoría 4.0 es indispensable el seguimiento de aspectos clave de dichas *soft skills,* la cultura organizacional y su correlación con las competencias duras y el impacto conjunto en los resultados de la organización.

A continuación, se describen los aspectos clave para la gestión del riesgo de conducta.

Tone at the top

La información para evaluar el riesgo de conducta debe estar establecida en la estrategia de cada organización y debe estar indicado en el *tone at the top*, es decir, lo que dirige al auditor interno a comparar lo que se espera *versus* lo que sucede en la realidad diaria.

La expresión anglosajona *tone at the top* se refiere al liderazgo y está reflejada en metodologías de control interno, gestión de riesgos y *compliance*. Tal como indica el Instituto de Auditores Internos: *"es la condición necesaria para que toda la organización adopte la conducta deseable por la organización"*[3].

Las organizaciones que han comprendido su relevancia articulan mecanismos para implementarlo y difundirlo. El *tone at the top* es la condición necesaria para que todos los miembros de la organización se comporten según se recoge en su código de conducta y en su estrategia.

3. *Auditoría Interna y la ética empresarial,* LA FÁBRICA DE PENSAMIENTO, Instituto de Auditores Internos de España, 2022.

Habitualmente, las organizaciones disponen de un código de conducta, una declaración formal de principios que recoge los valores y estándares éticos que guían a la empresa.

Grupos de interés o stakeholders

Relacionados con la conducta, se han identificado grupos de interés internos y externos, del mismo modo que se definían en el documento *Auditoría Interna y los aspectos ESG* de la Fábrica de Pensamiento del IAI de España, siendo los más habituales los accionistas, empleados, inversores, instituciones financieras, proveedores, clientes, socios, colaboradores, competidores, autoridades, reguladores, organismos públicos, organizaciones de la sociedad civil, comunidades locales, entre otros.

La conducta de los miembros de la organización, entre ellos y con cada uno de los grupos de interés, puede derivar en un impacto en los resultados y/ o en la reputación de la organización.

Código de conducta

El riesgo de conducta, como cualquier otro riesgo, se puede prevenir y mitigar. Para ello, las organizaciones *pueden incluir "la implementación de políticas y procedimientos claros, programas de capacitación, sistemas de denuncia de irregularidades y una cultura corporativa que promueva la responsabilidad y la ética en el lugar de trabajo"*[4], así como una conducta determinada que apoye la estrategia.

Habitualmente esto se traduce en que las organizaciones dispongan de un código de conducta, es decir, una declaración formal de principios en la que se recogen los valores y estándares éticos por los que se guía la organización. Tomando como base este código, se diseñan las normas de comportamiento en términos de RSC, de ESG y, en general, debe servir de marco de referencia para el resto de normativa interna de la organización. Por lo general, el contenido de estos códigos hace referencia a la protección de los derechos fundamentales, laborales, medioambientales y prácticas contra la corrupción y el soborno. También puede contener directrices para las relaciones entre los empleados, entre el empleado y la organización y/o con los distintos grupos de interés, estableciendo sanciones en caso de la realización de ciertos comportamientos que van en contra de los valores y principios estipulados por la entidad, como pueden ser la prohibición de actividades ilegales, expectativas sobre confidencialidad y comportamiento con terceros.

Organización y sector

El tipo de organización y el sector en el que desempeña su actividad determinará el alcance del trabajo del auditor interno, tanto por las características específicas de la industria o la empresa, como por las exigencias normativas o legales que le sean aplicables. Por ejemplo, existen legislaciones de cumplimiento obligatorio para el sector financiero, sanitario, etc. *"El auditor interno, deberá tener muy en cuenta dónde se enmarca la actividad de su empresa en cuanto a las obligaciones legales que le sean de aplicación"*[5], a la hora de identificar y controlar sus riesgos y, en especial, el riesgo de conducta.

4. Chat GPT Mar 23 Version. Free Research Preview
5. *Auditoría Interna y los aspectos ESG,* LA FÁBRICA DE PENSAMIENTO, Instituto de Auditores Internos de España

DEFINICIÓN DEL RIESGO DE CONDUCTA

En el ámbito empresarial, la gestión del riesgo de conducta se enfoca en *"identificar y abordar los comportamientos de riesgo de los empleados de una organización, tales como el fraude, el acoso laboral, la discriminación o cualquier otra conducta inapropiada o perjudicial"*[6] que pueda suponer un impacto para la organización, ya sea directo o indirecto (por ejemplo, reputacional).

En ocasiones, estas conductas están ya expresamente prohibidas por la regulación, ya sean normas de protección de los consumidores, de salvaguarda de la competencia de los mercados o pueden, incluso, constituir un ilícito penal. Las conductas inadecuadas pueden ser deliberadas o negligentes, fruto de estructuras de gobierno inadecuadas, de marcos de control débiles o debido a la baja implantación de la cultura ética en la organización.

El riesgo de conducta se define entonces como **la posibilidad de que la organización sufra pérdidas derivadas de actuaciones o prácticas inadecuadas, indebidas, desleales o carentes de ética, que se traducen en un perjuicio para cualquiera de sus grupos de interés** (clientes, accionistas, proveedores, colaboradores, empleados, competidores, administraciones públicas o supervisores, los mercados o la estabilidad financiera, entre otros).

El denominador común de las actuaciones que constituyen el riesgo de conducta es la generación de un perjuicio ilegítimo, por la inobservancia de un deber de actuar conforme a las normas, incluidas las normas de la ética. Es necesario distinguir, en este punto, el riesgo de conducta del riesgo de cumplimiento.

El riesgo de cumplimiento hace referencia siempre a una norma o regulación externa que se ha de observar. **El riesgo de conducta va más allá,** puede ser anterior a la norma (conductas inapropiadas con clientes, proveedores, accionistas… que llevan al regulador a establecer límites, pero que incluso antes de la existencia de la norma, pueden ocasionar daño financiero o reputacional a una organización), **y está ligado a la cultura organizacional, al entorno en el que se mueve la organización, a lo que los grupos de interés de la organización esperan del comportamiento de la misma.**

Se ha de considerar que la conducta no es un concepto estático, cambia según las culturas y la época. Conductas que en el siglo XIX o XX eran aceptadas, hoy se encuentran penalizadas y otras conductas que en una cultura forman parte de la interacción diaria, en otras culturas pueden provocar un efecto no deseado. Por ello, se requiere de una revisión periódica de la conducta que la organización desea potenciar entre sus miembros.

En resumen, el riesgo de conducta debe ser definido y actualizado por cada organización, según su contexto cultural, sector de actuación y legislación vigente aplicable. Esto implica la identificación y mitigación de comportamientos de riesgo de los individuos en diferentes contextos, con los distintos grupos de interés y de manera alineada con su código de conducta, con el objetivo de prevenir consecuencias negativas para la organización.

El riesgo de conducta va más allá del riesgo de cumplimiento y está ligado a la cultura corporativa y al comportamiento que esperan los grupos de interés.

6. Chat GPT Mar 23 Version. Free Research Preview

DIMENSIONES DEL RIESGO DE CONDUCTA

Las dimensiones del riesgo de conducta son la siguientes y, para cada una de ellas, el riesgo de conducta se materializa a través de:

Clientes y consumidores	Prácticas y comportamientos que no aseguren el interés del cliente, especialmente la protección de los consumidores y de los clientes vulnerables.
Accionistas	Directrices y actuaciones que no preserven los legítimos intereses de los accionistas. En este sentido, se requiere que, cada vez que un miembro de una organización actúe en nombre de ésta, prevalezcan los intereses de la organización sobre los del propio individuo.
Empleados	Falta de trato justo con los empleados de la organización.
Proveedores	Trato injusto con los proveedores, ya sea en la negociación, contratación o pago a los mismos por parte de la organización.
Competencia	Prácticas y actuaciones que se traducen en competencia desleal.
Administración Pública y Supervisores	Actuaciones poco transparentes con los organismos públicos, como la obstrucción de sus labores de inspección.
Los mercados	El riesgo de conducta respecto a la protección de la integridad de los mercados se materializa en prácticas que perjudiquen ilegítimamente los intereses de los participantes de un mercado, tanto si se trata de un mercado regulado, como si no.
Estabilidad financiera y otros valores intangibles	Prácticas que externalizan riesgos propios de la compañía. El riesgo de conducta respecto a otros valores intangibles dignos de protección por parte de la empresa, como la estabilidad de precios o la confianza de los consumidores, se materializa en prácticas que atenten contra dichos bienes inmateriales sobre los que se asientan la economía de mercado.

Las dimensiones del riesgo de conducta, atendiendo al origen y a los factores que contribuyen a la generación de conductas inadecuadas o indebidas, se exponen en la tabla siguiente.

Clientes y consumidores

Estrategia	Inadecuada definición de estrategias y diseño del modelo de negocio, que propicien la adopción de decisiones que puedan conllevar perjuicios a clientes. P.ej.: estrategias de producción y comercialización de productos que no se ajustan a las necesidades de los clientes.
Gobierno y control	Falta de claridad en la asignación de roles y responsabilidades. Deficiencia en la prevención y gestión de los conflictos de interés con los clientes. Falta de monitorización y cuestionamiento sobre las acciones inapropiadas e inoportunas de la gestión de clientes. P.ej.: falta de medidas para identificar y evaluar vulneraciones de la conducta, por parte de la compañía, en la comercialización de productos no adecuados a las necesidades de los clientes.
Selección y formación	Falta de formación al personal sobre las normas y pautas de comportamiento. P.ej.: personal no cualificado para el asesoramiento y/o comercialización de productos que requieren de dicho conocimiento.
Retribución	Inadecuado diseño y fijación del sistema de remuneración e incentivos, de manera que se promueva la realización de conductas inadecuadas y comportamientos inapropiados. P.ej.: incentivos a las prácticas de venta agresiva o venta irregular por incentivos inapropiados.
Diseño de productos y servicios	Inadecuado diseño de productos y/o servicios, de manera que no estén desarrollados para satisfacer las necesidades de los clientes, o que no sean adecuados para ellos. P.ej.: falta de adaptación del producto a su público objetivo (incluido personas vulnerables), obsolescencia programada, recetar a un paciente un producto de un laboratorio, ya que se está trabajando con ellos en otros proyectos.
Comercialización de productos y servicios	Tratamiento inapropiado o perjudicial para los clientes en los procesos de venta y soporte de los productos, así como en los procesos de postventa y servicio, incluyendo la producción de daños y la generación de pérdidas para los mismos. P.ej.: falta de transparencia en la comercialización de productos y servicios, publicidad engañosa.

Accionistas

Estrategia	Inadecuada definición de estrategias y diseño del modelo de negocio. P.ej.: adopción de decisiones primando los intereses de los gestores de la compañía, en detrimento de los intereses de sus accionistas.
Gobierno y control	Diseño de estructuras organizativas que diluyan la responsabilidad de los gestores de la compañía. Mecanismos que dificulten a los accionistas el conocimiento de la situación de la organización. Deficiente prevención de los conflictos de interés. Falta de monitorización sobre las acciones inapropiadas e inoportunas de la gestión. P.ej.: formulación de cuentas anuales que no reflejen de forma fiel la situación contable o financiera de la organización.
Retribución	Inadecuado diseño y fijación del sistema de remuneración e incentivos. P.ej.: la adopción de un esquema de remuneraciones que prime la obtención cortoplacista de beneficios y/o promueva la adopción de riesgos no alineados con el apetito de riesgo.

Empleados

Estrategia

Inadecuada definición de estrategias que puedan derivar en un trato injusto hacia los empleados.

P.ej.: olvidar en la estrategia de la empresa la igualdad de oportunidades de los empleados en la selección, formación y/o promoción, o no evitar prácticas discriminatorias; no proporcionar a los empleados los medios necesarios o medidas de seguridad básicas para desarrollar su función, fomentar prácticas que generen un ambiente de trabajo intimidante, hostil, humillante u ofensivo.

Gobierno y control

Falta de un esquema de gobierno ético sobre el trato a los empleados, así como la ausencia de un programa de prevención y detección de conductas corruptas o de prevención de los conflictos de interés

P.ej.: inexistencias de canales de denuncias para empleados, inexistencias de políticas para la gestión de conflictos de interés entre empleados.

Selección y formación

Incorporación de personal no alineado con los valores corporativos de la Entidad. Políticas discriminatorias de selección y/o formación.

P.ej.: ofrecer oportunidades de formación con la condición de pertenecer a un colectivo o favorecer a empleados por realizar alguna practica contraria a las normas de conducta.

Retribución

Inadecuado diseño y fijación del sistema de remuneración e incentivos, de manera que se promueva la realización de conductas inadecuadas y comportamientos inapropiados por parte de los empleados para lograr los objetivos ligados a la incentivación.

P.ej.: objetivos en incentivación que no considera los conflictos de interés entre fuerza de ventas y clientes, o discriminatorios entre empleados.

Proveedores

Gobierno y control

Falta de un esquema de gobierno ético sobre el trato a proveedores o en el marco de su contratación. Ausencia de un programa de prevención y detección de conductas corruptas o de prevención de los conflictos de interés o de posición abusiva frente a proveedores.

P.ej.: el retraso deliberado del pago a proveedores, falta de transparencia en las negociaciones, conflictos de interés entre proveedores y adjudicadores (ej.: compra de producto farmacéutico de un laboratorio específico por parte de compras para favorecer una relación, cuando no es a priori el producto de mercado que represente una mejor condición de coste - beneficio para los pacientes). Cláusulas abusivas en los contratos. Crear falsas expectativas de trato sucesivo con un proveedor, para lograr mejores condiciones, y sabiendo que será una operación única.

Competencia

Estrategia

Inadecuada definición de estrategias y diseño del modelo de negocio promoviendo actuaciones que supongan competencia desleal o prácticas colusorias de limitación de la competencia.

P.ej.: adopción de estrategias de cártel.

Gobierno y control	Establecimiento de estructuras de gobierno de la compañía poco transparentes o la falta de monitorización sobre las acciones o estrategias de la compañía que puedan ir en detrimento de la libre y leal competencia. P.ej.: falta de control sobre la adecuación de los pactos empresariales.
Diseño de productos y servicios	Inadecuado diseño de los productos y/o servicios de manera que los mismos limiten la libre competencia. P.ej.: prácticas de *cross selling* o venta cruzada que limiten la libre competencia, distribución de un producto de un tercero y comenzar a trabajar al tiempo en el desarrollo de un producto sustitutivo.
Comercialización de productos y servicios	Tratamiento inapropiado o perjudicial para los clientes en los procesos de venta de manera que se limite la libre competencia. P.ej.: comercialización de productos de forma vinculada (prácticas de *cross selling)* que limiten la libre competencia.

Administración Pública y Supervisores

Estrategia	Inadecuada definición de estrategias y adopción de decisiones que puedan conllevar un aumento en el apetito de riesgo de conducta P.ej.: afecta a cómo se gestionan los requerimientos regulatorios (falta de transparencia, obstrucción de actividad inspectora, destrucción de pruebas, etc.), estrategias de eficiencia fiscal muy agresivas, prácticas de *cherry picking* regulatorio.
Gobierno y control	Falta de claridad en la asignación de roles y responsabilidades. Falta de medios adecuados para la gestión del riesgo, así como la falta de monitorización *(oversight)* de los procesos en los que la compañía interactúa con organismos públicos. P.ej.: la falta de un canal ético que permita a los empleados reportar actividades deshonestas o ilegales sin repercusiones.

Los mercados

Estrategia	Definición de estrategias o de modelos de negocio que no velen por la integridad de los mercados en los que opera la compañía o de los que participa; así como la falta de una cultura corporativa ética, que propicie la adopción de medidas que generen perjuicio al resto de los participantes de un mercado. P.ej.: prácticas de *insider dealing* (operar en mercados financieros con títulos en relación con los cuales se posee información privilegiada).
Gobierno y control	Falta de estructuras de gobierno y control sobre las acciones inapropiadas en relación con la protección de intereses (a veces difusos) de terceros ajenos a la compañía que merecen dicha protección, como los intereses de los consumidores. P.ej.: falta de controles para evitar prácticas de manipulación de índices de referencia (como el Libor) u otras formas de falsear mercados como la operativa constitutiva de abuso de mercado (recompra de acciones propias para generar falsa demanda de un valor).

Estabilidad financiera y otros valores intangibles

Estrategia	Inadecuada definición de estrategias empresariales que atenten contra valores intangibles que suponen un beneficio colectivo, así como a la falta de cultura corporativa ética que proteja dichos valores. P.ej.: definición de una estrategia de admisión de riesgos de forma que el riesgo asumido por la compañía supere el que puede ser cubierto por su capital social, de forma que, en caso de *default,* se externalizaran los efectos adversos (bancos considerados *too big to fail).*
Gobierno y control	Falta de estructuras de gobierno y control sobre las acciones o prácticas que atenten contra los referidos valores intangibles. P.ej.: falta de monitorización y control sobre la política de admisión de riesgos de un banco.

Sistema de gestión de riesgos de conducta

Para las organizaciones es de gran importancia la definición y puesta en marcha de un sistema eficaz y eficiente de gestión de riesgos, ya sea aprobado y formalizado o de manera informal. El objetivo de los marcos de gestión de riesgos es identificar los riesgos a los que la organización se ve expuesta por distintos factores de su actividad o entorno, cuantificarlos, predecir su impacto en caso de que se lleguen a materializar y establecer un marco que asegure su correcto control. Posteriormente, durante la realización de las actividades de la organización, se deberá revisar y actualizar dicho sistema de forma continua y disciplinada.

Los sistemas de gestión de riesgos incrementan la confianza de la organización y la continuidad de sus operaciones, contribuyendo a:

- Alcanzar sus objetivos.
- Facilitar la toma de decisiones.
- Mejorar el rendimiento y la reducción de costes.
- Aumentar la confianza de sus inversores.
- Incrementar su competitividad.

Existen distintos estándares y marcos que las organizaciones utilizan como guía para la definición de los sistemas de gestión de riesgos como son, por ejemplo, COSO ERM *(Committee of Sponsoring Organizations - Enterprise Risk Management);* ISO 31000 (Sistema de Gestión de Riesgos) o ISO 37301 (para Sistemas de Gestión de *Compliance).*

Respecto al riesgo de conducta también es necesario establecer un sistema o marco para su gestión.

A continuación, se indican los elementos a considerar en la configuración del marco de gestión de riesgos de conducta en una organización.

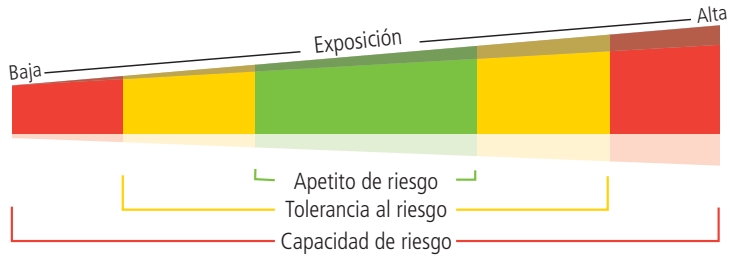
APETITO DE RIESGO DE CONDUCTA

El apetito de riesgo es la relación entre el riesgo que la organización está dispuesta a asumir y la consecución de sus objetivos, según la estrategia definida. La determinación de un buen umbral de apetito de riesgo permite conseguir una optimización de los recursos consiguiendo la rentabilidad, estrategia y objetivos esperados, a la vez que se realiza una correcta gestión de riesgos.

La definición de un correcto apetito de riesgo facilita la toma de decisiones por parte de la dirección de las organizaciones, ayudando en la identificación y asignación de recursos necesarios (personal, recursos económicos, activos, etc.) de forma que los objetivos y estrategias definidas se puedan, por un lado, alcanzar de la forma más eficiente posible y, por otro, con el nivel de riesgo asumible controlado.

La definición de un correcto apetito de riesgo facilita la toma de decisiones por parte de la dirección de las organizaciones.

Una representación gráfica del apetito de riesgo sería la siguiente[7]:



Cada empresa debe establecer su apetito para los distintos riesgos a los que se enfrenta, y para ello considerará factores internos y externos: la naturaleza del negocio, las practicas del sector, los objetivos de la empresa, el tamaño de la organización, la cultura corporativa, las condiciones del mercado, las expectativas de sus *stakeholders,* la regulación existente[8]...

En el caso de los riesgos de conducta, la organización deberá establecer también su apetito de riesgo. Algunas conductas pueden suponer un daño reputacional de tan alto impacto, que la organización llegue a establecer un apetito cero para el riesgo que se deriva de dichas conductas. Así se deberían recoger en el código de conducta de la organización, estableciendo una oposición frontal a riesgos críticos como, por ejemplo, riesgos de soborno u otros ilícitos penales. Es recomendable, por tanto, en la definición del apetito de riesgo, establecer unas líneas limítrofes claras en las que se identifiquen aquellas conductas que no son aceptables, bajo ninguna circunstancia, para la compañía.

7. *Definición e implantación de Apetito de Riesgo,* LA FÁBRICA DE PENSAMIENTO. Instituto de Auditores Internos de España.
8. Para más información, sobre la definición y formulación del apetito al riesgo se puede consultar: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

Como se ha mencionado antes, el riesgo de conducta es un factor clave para alcanzar la visión, el propósito y los objetivos estratégicos de una organización. Los comportamientos deben ser palancas impulsoras del negocio y no factores que afecten negativamente a su funcionamiento y continuidad. Por ello, la consideración del riesgo de conducta es un elemento crítico dentro del apetito de riesgo de una organización.

IDENTIFICAR EL UNIVERSO DE RIESGOS DE CONDUCTA

Identificar los factores de riesgo de conducta a los que se enfrenta la organización es crucial para construir una buena defensa.

Para identificar el universo de factores de riesgo donde se puede materializar el riesgo de conducta, se ha de comenzar definiendo y concretando el riesgo de conducta para la organización de forma específica, es decir, definir aquellas actuaciones, comportamientos o prácticas inadecuadas, indebidas, desleales o carentes de ética, que pueden producir un perjuicio económico o reputacional para la organización o traducirse en un daño para cualquiera de sus grupos de interés.

Identificar los factores de riesgo de conducta a los que se enfrenta día a día la organización es crucial para construir una buena defensa frente a ellos. Para armar este universo, hay que identificar los comportamientos inapropiados o poco éticos que pueden ocurrir en la organización, y para ello se puede:

- **Revisar la normativa externa (supranacional, nacional, regional o local), las prácticas y recomendaciones sectoriales y la normativa interna** para identificar cualquier brecha o inconsistencia que pueda conducir a comportamientos inapropiados.
- **Analizar incidentes** de conductas poco éticas sucedidos en la organización o en el sector, para identificar los factores que contribuyeron a ellos y para detectar cualquier riesgo potencial de conducta en el futuro.
- **Entender las expectativas de los distintos grupos de interés,** en materia de conducta.

De una manera más concreta, se podrán detectar riesgos de conducta en la organización mediante las siguientes técnicas:

- **Análisis de datos históricos** para detectar patrones de comportamiento inusual o inconsistencias en el desempeño.
- **Entrevistas y encuestas** a empleados, proveedores, colaboradores y otros grupos de interés para obtener información sobre los riesgos de conducta en la organización.
- **Análisis de los canales éticos/ de denuncias** para identificar conductas o denuncias frecuentes.
- **Análisis del entorno** para identificar los riesgos de conducta en la industria, en el negocio y en la comunidad en general.
- **Evaluación del control interno** de la compañía para determinar si existen deficiencias, en su diseño o implementación, que puedan conducir a riesgos de conducta.
- **Evaluación de la cultura corporativa** para determinar si fomenta o desalienta el comportamiento ético y la toma de decisiones correctas.

En este proceso de identificación de riesgos de conducta, se deberán tener en cuenta factores culturales, el tipo de mercado y el tipo de negocio en el que opera la organización. Estos factores pueden influir en los comporta-

mientos inapropiados que pueden surgir y, por lo tanto, en los riesgos a los que se enfrenta la organización. Por ejemplo:

- En algunas culturas puede ser común el **uso de prácticas poco éticas para conseguir resultados comerciales,** ello aumenta el riesgo de conducta inapropiada. Además, en algunos mercados altamente competitivos, puede haber una mayor presión para alcanzar objetivos comerciales a corto plazo, lo que también puede aumentar el riesgo de comportamientos inapropiados por parte de las fuerzas de ventas.
- El **tipo de negocio** también puede influir en los riesgos de conducta. Una empresa de servicios financieros y de construcciones internacionales puede estar más expuesta a riesgos de fraude y corrupción, mientras que una empresa de fabricación industrial puede estar más expuesta a riesgos de seguridad y salud.

ANÁLISIS Y EVALUACIÓN DE RIESGOS

Una vez identificado el universo de los riesgos de conducta, conviene evaluar sus **probabilidades e impactos,** de forma que se pueda determinar cuáles son los más críticos y, por tanto, requieren mayor atención.

Para evaluar la probabilidad de un riesgo es importante considerar la facilidad con la que se pueden producir los comportamientos inapropiados que pueden llevar a dicho riesgo, así como los factores culturales, el tipo de negocio, el mercado y otros factores que puedan influir en su probabilidad de ocurrencia.

Para evaluar el impacto de un riesgo, es importante considerar los posibles efectos negativos sobre la organización al materializarse: daños a la reputación, pérdida de clientes, sanciones financieras y legales, entre otros. También se debe considerar el alcance y la magnitud del impacto, así como el tiempo que llevaría a la organización recuperarse de dichos efectos negativos.

La organización debe valorar todos los riesgos del universo de riesgos existentes, el impacto que pueden tener dentro y fuera de la organización y la probabilidad de que estos se materialicen. Una vez valorados, la organización podrá clasificarlos **de más a menos críticos, priorizando así la asignación de recursos** sobre aquellos riesgos de conducta más relevantes, sobre aquellos que superen el apetito de riesgo definido o sobre los que no existen mecanismos de control suficientes.

La realización de un **mapa de riesgos** en el que se represente el nivel de criticidad tras la valoración de la probabilidad y el impacto puede ser de gran ayuda para visualizar la importancia de los riesgos sobre la organización.

El análisis de riesgos debe ser un proceso continuo, ya que estos pueden evolucionar con el tiempo, debido a cambios en el entorno de la organización, cambios en la regulación, en el comportamiento de los empleados y en las expectativas de otros actores relevantes. El análisis continuo es especialmente relevante en el riesgo de conducta por el carácter temporal de la propia definición de conducta inadecuada. Además, este proceso de análisis

Un mapa de riesgos que represente criticidad tras valorar la probabilidad y el impacto permite visualizar la importancia de los riesgos.

El análisis continuo es especialmente relevante en el riesgo de conducta por el carácter temporal de la propia definición de conducta inadecuada.

implica examinar con atención las situaciones que presentan incertidumbre, las fuentes de riesgo que las causan, las posibles consecuencias que podrían resultar, la probabilidad de que ocurran los eventos que se podrían presentar, las diferentes situaciones posibles, así como los controles existentes y su eficacia. Es importante tener en cuenta que un solo evento puede tener varias causas y consecuencias y afectar a múltiples objetivos.

También es de gran ayuda **establecer indicadores** que conviertan la valoración inicial y estática de los riesgos en un proceso dinámico que se adapte a la realidad de la compañía, sin un decalaje temporal que pueda generar errores en la priorización de los riesgos. Para ello, muchas organizaciones establecen indicadores de riesgo que se monitorizan periódicamente para identificar cambios en su nivel de criticidad y poder, así, anticiparse a las consecuencias derivadas de una mala o insuficiente gestión de riesgos.

Por ejemplo, una empresa que opera con el sector público puede identificar el riesgo de corrupción como un riesgo con alta criticidad por su probabilidad e impacto, mientras que otra que opere en los mercados de valores, puede considerar como crítico el riesgo de utilización de información privilegiada. Una compañía que comienza a internacionalizarse en diferentes áreas geográficas deberá comenzar a considerar la discriminación por razón de raza o etnia como un potencial riesgo de conducta.

En resumen, la evaluación de la probabilidad y del impacto de los riesgos identificados es crucial para determinar cuáles son más críticos y requieren mayor atención en la implementación de controles adecuados. Además, es importante tener en cuenta los factores condicionantes que pueden influir en la probabilidad de ocurrencia e impacto de los riesgos, así como establecer indicadores de riesgo que permitan su gestión dinámica y adaptativa.

MARCO DE CONTROL DEL RIESGO DE CONDUCTA

La creación de un marco de control del riesgo de conducta es imprescindible para gestionar los riesgos identificados y valorados. El marco de control debe ser un sistema sólido, aprobado por el nivel adecuado en la organización (órganos de gobierno, alta dirección), promovido de forma activa para que se ejecute conforme a su definición y para que se actualice periódicamente.

Para el diseño del marco de control del riesgo de conducta se debe tener en cuenta:

"Tone at the top"

Como se ha comentado anteriormente, el *tone at the top* o tono directivo de la organización debe promover valores éticos y fomentar una cultura de cumplimiento. La alta dirección debe establecer un tono desde arriba que muestre un compromiso fuerte con la ética y el cumplimiento, y que promueva la transparencia y la responsabilidad en todos los niveles de la organización.

Este *tone at the top* debe estar reflejado en metodologías de control interno y gestión de riesgos, y es la condición necesaria para que todos los miembros de la organización se comporten de acuerdo a su código de conducta. Pero para ello es imprescindible el compromiso de la alta dirección con los comportamientos y conductas exigidas a los empleados.

Ejemplos de *tone at the top* pueden ser los siguientes, adaptados a diferentes factores:

- **Modelo de negocio.** Si la organización se dedica, por ejemplo, a la venta de productos o servicios financieros, el *tone at the top* adecuado debería incluir la promoción, por parte de la alta dirección, de prácticas transparentes y responsables en la comercialización de productos financieros, así como la protección de los intereses de los clientes.
- **Cultura.** Si la organización tiene una cultura orientada hacia el trabajo en equipo y la colaboración, el *tone at the top* adecuado debería incluir la promoción de la honestidad, la integridad y el respeto en las relaciones interpersonales, desde la alta dirección y en todos los niveles de la organización.
- **Geografía.** Si la organización opera en un país donde existen prácticas comerciales corruptas, el *tone at the top* adecuado debería fomentar la promoción de prácticas comerciales éticas y la lucha contra la corrupción, así como el cumplimiento de las leyes y regulaciones aplicables.
- **Industria.** Si la organización opera en una industria altamente regulada, el tono ético adecuado debe exigir el cumplimiento de las leyes y regulaciones aplicables, así como la promoción de prácticas responsables en relación con la seguridad, salud y medio ambiente.

  Un ejemplo específico puede ser una empresa de tecnología que opera en una cultura empresarial altamente competitiva y centrada en la innovación. El *tone at the top* adecuado puede incluir la promoción de la innovación responsable, que tenga en cuenta los impactos sociales y ambientales de los productos y servicios ofrecidos. También puede incluir la promoción de la transparencia y la responsabilidad en la gestión de datos de los clientes, la protección de la privacidad y la seguridad de la información. Además, puede promover la diversidad y la inclusión en la cultura empresarial, fomentando la igualdad de oportunidades y el respeto por las diferencias culturales y de género en la empresa.

Gobernanza

Los marcos de control deben contar con una estructura de gobierno específica en la que se establezcan **roles y responsabilidades** concretos de los distintos miembros de la organización. Aunque cada compañía debe estructurar su gobernanza como mejor convenga,

La alta dirección debe establecer un tono desde arriba que muestre un compromiso fuerte con la ética y el cumplimiento, y que promueva transparencia y responsabilidad.

El responsable de RRHH puede jugar un papel fundamental en la adopción de medidas preventivas contra riesgos de conducta relacionados con el personal.

es conveniente que existan órganos de decisión que se encuentren informados con cierta periodicidad sobre la eficacia de los controles implantados sobre los riesgos de conducta y que vele por su actualización, cuando sea necesario.

A modo de ejemplo, entre los roles más significativos para la gestión del riesgo de conducta en las organizaciones pueden encontrarse los siguientes:

- **La alta dirección:** como se ha mencionado antes, normalmente es responsable de establecer la cultura y valores, de asegurar el *tone at the top* con su ejemplo y compromiso, de asignar los recursos y de definir el marco de gestión del riesgo de conducta a aprobar por los órganos de gobierno.
- **El comité de riesgos de conducta,** o cualquier otro ya existente en la organización que vele por los riesgos de conducta (por ejemplo, comité de compliance, ESG, ética, riesgos…), normalmente compuesto por representantes de las áreas, debe asegurar una visión global y completa de todos los riesgos de conducta a los que hace frente la organización, con funciones de supervisión sobre el marco de gestión, evaluación y monitorización de los riesgos de conducta.
- **Los empleados** deben recibir la capacitación necesaria para identificar y gestionar, a su nivel y conforme a su cometido, los riesgos de conducta asociados a su función y deben saber cómo reportar cualquier conducta inapropiada o sospechosa. En este sentido no sólo es clave la existencia de canales de denuncia, sino la adopción de medidas para difundir su conocimiento y utilización.

Adicionalmente, en organizaciones con un sistema de control interno maduro, organizado de acuerdo al modelo de tres líneas, los roles y responsabilidades respecto al riesgo de conducta podrían ser los siguientes:

- **La primera línea, enfocada en la gestión operativa y de riesgos,** también del riesgo de conducta:

  Tras la identificación de los riesgos de conducta que afectan a la organización, o como parte casi de la misma identificación, si se atiende a la relevancia que reviste, es conveniente que cada riesgo concreto tenga asociado un propietario, responsable de su gestión y seguimiento, porque es importante que alguien tenga encomendada la función de desarrollar una estrategia de respuesta ante dicho riesgo.

  Adicionalmente, el responsable de Recursos Humanos y/o Formación puede jugar un papel fundamental en la adopción de medidas preventivas contra riesgos de conducta relacionados con el personal (bien de carácter general, como los derivados de acoso laboral, discriminación, etc., o bien sectorial, como los derivados de pautas de comercialización inadecuadas, falta de transparencia, etc.). Entre las medidas preventivas más significativas que, desde Recursos Humanos y/o Formación, pueden impulsarse se encuentran la impartición de formación y la comunicación para asegurar que todos los empleados disponen del conocimiento requerido para la gestión del riesgo de conducta.

- **La segunda línea supervisa la eficacia de la gestión del riesgo de conducta** considerando su impacto de forma transversal en

cada uno de los procesos de la organización, en concreto:

- Participando en el diseño de políticas y procedimientos que garanticen que la organización desarrolla sus actividades y negocios conforme a las pautas de conducta definidas.
- Estableciendo y gestionado los canales de denuncia y éticos.
- Monitoreando que se cumplan los requisitos de la normativa interna y externa donde se establecen las pautas de conducta para los distintos procesos de la organización y acorde a su cultura corporativa.
- Velando porque los procedimientos de identificación y evaluación de riesgos incluyan los riesgos de conducta.

Esta segunda línea podría ser asumida por la Función de Cumplimiento, ya que puede aportar una visión coordinada de la gestión del riesgo de conducta, dado su vínculo directo con el cumplimiento de las normas externas y por su contacto con la alta dirección y con el comité de riesgos de conducta.

- **La tercera línea asumirá un papel de aseguramiento** (evaluación independiente de la eficacia y eficiencia del control interno y el cumplimiento de la legislación) **o de asesor de confianza** (dando respuesta a las solicitudes concretas de los stakeholders), según el enfoque definido en su plan de auditoría.

Políticas y procedimientos

La organización debe tener políticas y procedimientos claros que establezcan las expectativas de comportamiento ético y legal, y que proporcionen orientación sobre cómo manejar situaciones difíciles. Es importante que estas políticas y procedimientos estén alineadas con el código de conducta, que sean comunicadas de manera efectiva a todos los empleados y que se brinde capacitación para asegurar que las comprenden.

Evaluación de riesgos

La organización debe llevar a cabo una evaluación periódica de los riesgos de conducta (como se ha indicado en apartados anteriores) y ajustar sus controles y procesos en consecuencia. Esto asegurará que se aborden adecuadamente los riesgos emergentes y que se identifiquen oportunidades para mejorar los controles existentes.

Monitorización y supervisión

La organización debe establecer sistemas de seguimiento y supervisión efectivos para detectar comportamientos inapropiados y riesgos de conducta. Esto puede incluir la implementación de controles específicos para prevenir y detectar fraudes, la revisión de transacciones, la monitorización del comportamiento del mercado, etc.[9] Dicha monitorización sobre el riesgo de conducta debe ser comunicada periódicamente a la alta dirección y a los órganos de gobierno, como responsables últimos de dicho marco.

Reporte de conductas y respuesta

La organización debe establecer canales de reporte seguros y confidenciales para que los empleados puedan informar sobre comporta-

La organización debe tener políticas y procedimientos claros que establezcan las expectativas de comportamiento ético y legal, y que proporcionen orientación sobre cómo manejar situaciones difíciles.

9. Se detallan algunos de estos controles en el apartado 2.5 de este documento.

Hay que comunicar políticas, procedimientos y expectativas de comportamiento ético a todos los empleados y grupos de interés.

mientos inapropiados sin temor a represalias. Además, se debe contar con un plan de respuesta para manejar adecuadamente los incidentes y para tomar medidas correctivas y preventivas en caso de que se produzca algún riesgo de conducta.

Comunicación y formación

Es importante que la organización comunique sus políticas y procedimientos, así como sus expectativas de comportamiento ético a todos los empleados y grupos de interés. También es necesario proporcionar formación regular para que los empleados estén actualizados y sean conscientes de los riesgos de conducta. Para comunicar adecuadamente los riesgos de conducta, es importante contar con canales que sean efectivos, accesibles, confidenciales y seguros.

En este sentido, es importante que las organizaciones cuenten con **planes formativos actualizados** que favorezcan el conocimiento, por parte de todos los empleados de la compañía, de las conductas esperadas y las consideradas inapropiadas o que puedan suponer un riesgo. La formación puede ser interna y/o externa (particularmente útil para organizaciones que operan en mercados muy regulados o con riesgos de conducta complejos); formación al inicio de la relación laboral (permitirá conocer las expectativas de la organización en términos de comportamiento ético y los requisitos relacionados con el riesgo de conducta) y formación continua (actualizada en función de las novedades en el mercado y los cambios normativos).

CONTROLES DE GESTIÓN DEL RIESGO DE CONDUCTA

Se recomienda establecer controles para la gestión del riesgo de conducta que sean integrales y abarquen desde la cultura corporativa hasta la implementación de actividades y procesos específicos, con el objeto de mitigar los riesgos de conducta identificados. La supervisión y la monitorización continua es esencial para asegurar que los controles son efectivos y que se abordan adecuadamente los riesgos emergentes.

Se distinguen dos niveles de controles:

Controles generales

Buscan disminuir de forma global el conjunto de los riesgos de conducta identificados.

- Existencia de un **código ético o de conducta** debidamente informado a los integrantes de la compañía. Dicho código será el marco de referencia para la **normativa interna** de la organización, que también desarrollará la conducta esperada por empleados y con los distintos grupos de interés (incluyendo procedimientos de identificación y gestión de los conflictos de interés entre la organización y éstos).
- Existencia de una **figura responsable** de velar por el cumplimiento de los estándares de conducta buscados por la compañía, y/o de un conjunto de responsables con funciones definidas en el gobierno del riesgo de

conducta (conforme se ha explicado en apartados anteriores).

- **Canal de denuncias o de reporte interno:** se trata de un canal interno para que los empleados puedan informar sobre cualquier comportamiento inapropiado o sospechoso que pueda dar lugar a un riesgo de conducta. Este canal debe ser seguro y confidencial para garantizar que los empleados se sientan cómodos al informar sobre el comportamiento inapropiado sin temor a represalias.

- **Línea directa:** se trata de una línea directa de comunicación para que cualquier interesado (empleado o externo) pueda informar o preguntar sobre comportamientos inapropiados o sospechosos. La línea directa puede ser administrada interna o externamente y debe ser accesible de manera fácil y segura.

  Es muy importante que se comuniquen los canales de reporte de riesgos de conducta de manera clara y efectiva a todos los empleados de la organización. Además, se debe asegurar que los canales de reporte sean monitorizados y gestionados adecuadamente para garantizar que los informes se investiguen y se tomen medidas adecuadas para abordar los riesgos de conducta identificados, asegurando la independencia y la ausencia de conflictos de interés de los gestores de los mensajes recibidos.

- **Reuniones y entrevistas individuales:** los empleados pueden ser invitados a participar en reuniones y entrevistas individuales con el fin de comunicar cualquier inquietud o riesgo de conducta. Estas reuniones deben ser confidenciales y deben proporcionar a los empleados un ambiente seguro para discutir cualquier preocupación que puedan tener.

- **Evaluación de satisfacción del cliente:** la organización también puede utilizar las evaluaciones de satisfacción del cliente para detectar cualquier comportamiento inapropiado o riesgo de conducta. Los clientes pueden proporcionar comentarios sobre el comportamiento de los empleados y la calidad de los servicios, lo que puede ayudar a detectar cualquier problema.

- **Establecimiento de un sistema de sanciones** que ayude a evitar la existencia de conductas contrarias a la ética de la organización.

Controles específicos

Buscan mitigar la posibilidad de que se materialicen riesgos de conducta en los procesos de la organización y con sus distintos *stakeholders*.

Para ello es importante que se identifiquen las actividades concretas en las que se pueden dar las conductas contrarias a los principios y ética de la compañía, para poder identificar posteriormente actividades de control que disminuyan su probabilidad de ocurrencia. Los controles pueden ser **detectivos o preventivos, automáticos o manuales.**

Algunos de estos controles serían, por ejemplo: la definición de procedimientos para la recepción de regalos por los empleados de parte de proveedores o colaboradores; procedimientos y herramientas de declaración y gestión de conflictos de interés; mecanismos de detección de uso de información privilegiada; revisión de pagos a miembros de la administración pública; indicadores de venta

El canal interno de denuncias debe ser seguro y confidencial para que los empleados informen sobre comportamientos inapropiados sin temor a represalias.

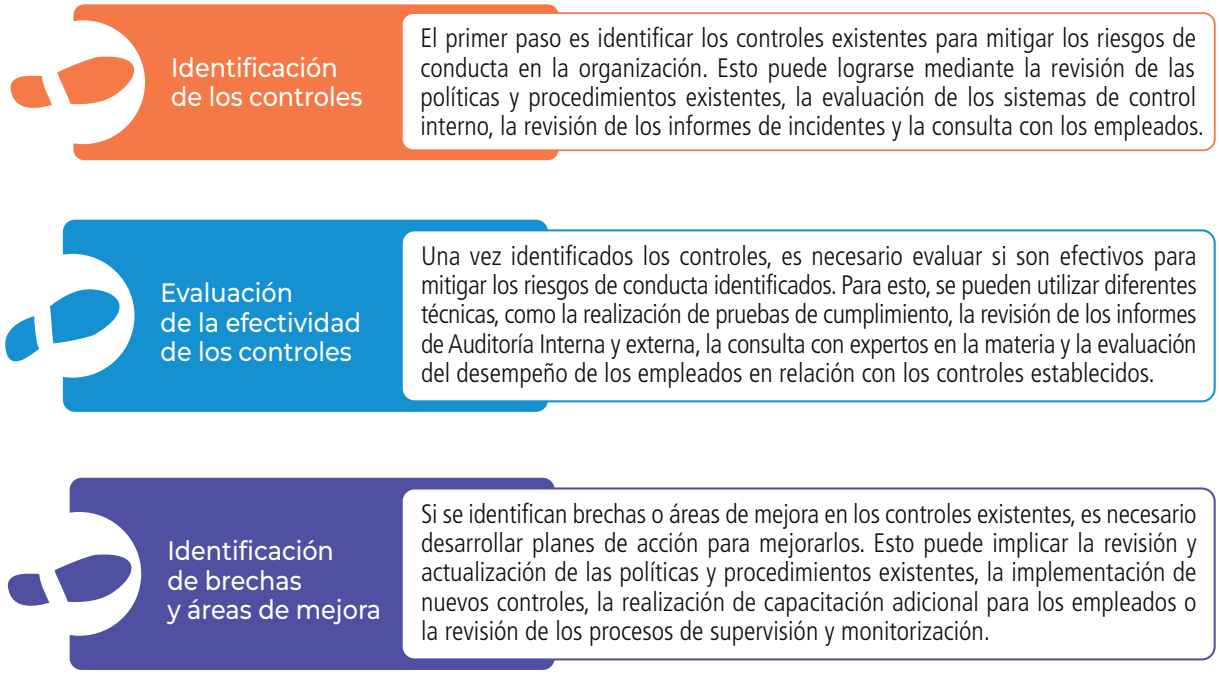
cruzada o de ventas improductivas (devoluciones o cancelaciones de ventas); inclusión en los comités de incentivación de una figura que vele por los intereses de los clientes; políticas de gobierno de producto donde se definan especificaciones mínimas de los mismos, publico objetivo, condiciones de comercialización, etc.

EVALUACIÓN Y MEJORA CONTINUA

La gestión del riesgo de conducta debe ser un proceso continuo y en constante evolución. Por lo tanto, es importante evaluar regularmente los controles implementados y realizar mejoras cuando sea necesario.

La evaluación de los controles del riesgo de conducta es un proceso clave para determinar si los controles establecidos son efectivos para mitigar los riesgos identificados de comportamiento inapropiado en una organización.

A continuación, se presentan los pasos fundamentales para evaluar los controles del riesgo de conducta.



La evaluación de los controles del riesgo de conducta debe ser un proceso continuo y debe ser revisada periódicamente para asegurar que sigan siendo efectivos en la mitigación de los riesgos de conducta. Además, los resultados de la evaluación de los controles deben ser reportados a la alta dirección y al Consejo de Administración de la organización para su revisión y consideración.

COMUNICACIÓN Y REPORTE A LA ALTA DIRECCIÓN Y ÓRGANOS DE GOBIERNO

Por último, los órganos de gobierno y la alta dirección, como últimos responsables del modelo de gestión del riesgo de conducta, deben ser informados periódicamente sobre el mismo, sobre su funcionamiento y eficacia. Este reporte debería incluir al menos:

- El seguimiento del apetito de riesgo de conducta.
- Los resultados de la evaluación periódica del riesgo de conducta en la compañía, destacando los factores de riesgo con mayor probabilidad e impacto y aquellos cuya valoración haya cambiado con respecto a ejercicios de evaluación anteriores.
- La efectividad de los controles generales y específicos sobre el riesgo de conducta:
  - Adhesión de empleados al código de conducta.
  - Denuncias y comunicaciones en el canal de denuncias.
  - Resultados de encuestas a clientes y proveedores.
  - Acciones de formación y comunicación a empleados, en relación con el riesgo de conducta.
  - Etc.
- Las conductas inapropiadas o indebidas ocurridas en la compañía y su impacto sobre los distintos grupos de interés.
- Los resultados de la evaluación y mejora continua del sistema de gestión de riesgo de conducta.
- Cualquier otro aspecto relevante sobre la gestión del riesgo de conducta.

Hay que reportar periódicamente sobre la evaluación del riesgo de conducta.

Papel de Auditoría Interna en el marco de gestión del riesgo de conducta

De acuerdo con *El Modelo de las Tres Líneas, nuevo marco teórico para auditores internos* publicado del Instituto de Auditores Internos, en su principio número 4[10], se otorga a Auditoría Interna una **misión de aseguramiento y asesoramiento independiente** sobre la adecuación y la eficacia del gobierno y sobre la gestión de riesgos de la organización.

Para conseguir ese objetivo, Auditoría Interna debe basar su metodología en un proceso sistemático y disciplinado que utilice el conoci-

10. https://www.theiia.org/en/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/

Auditoría Interna debe revisar alguno(s) procesos en los que se puede materializar el riesgo de conducta.

miento y la pericia de los auditores internos y los hallazgos identificados durante sus trabajos para comunicarlos tanto a la alta dirección como a los órganos de gobierno, bajo la perspectiva de la mejora continua de la organización.

Un eje fundamental que vertebra el Modelo de las Tres Líneas es la independencia del Función de Auditoría Interna, entendida con respecto a las actividades de gestión y operativas del negocio, que son desarrolladas por la alta dirección, bien sea en relación con la primera o la segunda línea.

Con el objetivo de **proporcionar confort sobre la adecuada gestión del riesgo de conducta,** Auditoría Interna puede realizar:

- Trabajos focalizados en la **eficacia del marco de gestión del citado riesgo** en la organización.
- **Considerar transversalmente este riesgo en todas o algunas de sus revisiones** (aquellas en que así se considere conveniente, como resultado de los trabajos de planificación de cada auditoría).
- **Revisar específicamente alguno o algunos de los distintos procesos donde se materializa el riesgo de conducta** en los que pueda incurrir la organización como, por ejemplo, las prácticas de comercialización de productos, los sistemas de incentivación de la fuerza de ventas, la gestión del canal de denuncias, la implementación de las políticas de conflictos de interés con proveedores, la publicidad engañosa, la revisión de controles y procedimientos para evitar conductas inadecuada en la selección y gestión de los empleados, el funcionamiento de los mecanismos establecidos para evitar el uso de información privilegiada, entre otros.

Factores como la madurez, el tamaño, la ubicación geográfica y el sector de la organización pueden influir en la adopción de estos enfoques. Especialmente si el objeto de la auditoría es el propio marco de gestión del riesgo de conducta en sí, total o parcialmente, Auditoría Interna debe obtener y revisar la documentación relacionada con el marco de gestión del riesgo de conducta, incluyendo políticas, procedimientos, manuales y otros documentos relevantes.

Deberá comprobar si cada documento cuenta con la aprobación de la instancia que por su contenido requieran, en su caso, la normativa externa y/o interna aplicable en materia de gestión de riesgos, en general o de los riesgos de conducta concretos que pudieran contar con requerimientos al respecto. Esto será condición *sine qua non* para concluir favorablemente sobre la adecuada formalización y gobernanza del marco de gestión. Adicionalmente, habrá que opinar si las políticas y procedimientos son claros y suficientes para guiar la gestión del riesgo de conducta y si los controles definidos son eficaces para mitigar los riesgos identificados.

APETITO DE RIESGO DE CONDUCTA

Como se ha indicado anteriormente, el establecimiento del apetito de riesgo de conducta de una organización no es, una función de Auditoría Interna, sino de sus órganos de gobierno y/o gestión.

En este sentido, Auditoría Interna debe asegurarse de que el riesgo de conducta está considerado entre los riesgos que debe gestionar la organización, pero más allá de eso, que es básico, resulta crucial obtener un **aseguramiento razonable de que el nivel de riesgo de conducta asumido permite a la organización cumplir con los objetivos de su estrategia, con las expectativas de los distintos grupos de interés y con el marco legal** que le resulte aplicable, todo ello alineado con el marco de apetito de riesgo general de la organización.

Adicionalmente, Auditoría Interna debe comprobar que el nivel de riesgo de conducta objetivo de la organización está aprobado por las instancias pertinentes de la misma, de acuerdo con las facultades aplicables en materia de asunción de riesgos, aprobadas por los órganos de gobierno.

IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE CONDUCTA DE LA ORGANIZACIÓN

Auditoría Interna debe asegurarse de que la organización entiende adecuadamente los riesgos de conducta a los que está expuesta y que su marco de gestión está alineado con los objetivos estratégicos y la cultura de la organización. Es decir, debe tener claro que todos los riesgos de conducta han sido identificados y evaluados por la organización.

En este sentido, resulta crucial tener identificada la legislación supranacional, nacional, regional o local (entre otros, de los ámbitos penal, mercantil, administrativo…), así como la normativa y buenas prácticas sectoriales propias del ámbito de actividad de la organización, y considerar los ámbitos de actividad y las características de los grupos de interés que podrían estar afectados en caso de materializarse: tales como pudieran ser clientes/consumidores, accionistas, empleados o proveedores. Así mismo, puede llevar a cabo entrevistas con los responsables y empleados de la organización para obtener una comprensión clara de sus prácticas y culturas y evaluar el grado de conciencia y comprensión de los riesgos de conducta.

Como se ha indicado previamente en el apartado anterior, identificar el universo de riesgos de conducta a los que se enfrenta día a día la organización es imprescindible para realizar su adecuada gestión. En este sentido, Auditoría Interna puede recomendar a las áreas de control que tengan identificados estos riesgos mediante su mapeo entre las distintas líneas de negocio, productos, procesos y/o servicios de la organización. De este modo, el mapeo se presenta como una herramienta de validación de la integridad de riesgos de conducta que acechan en la actividad diaria.

Auditoría Interna deberá evaluar de forma independiente los riesgos identificados, en términos de probabilidad e impacto, para dedicar sus mayores esfuerzos a verificar que aquellos riesgos más críticos para la organización son los primeros que incluye en sus revisiones. Puede tener en cuenta en sus revisiones sobre el riesgo de conducta la frecuencia, periodicidad o circunstancias desencadenantes de revisiones en su proceso de identificación de riesgos. En este sentido, puede valo-

Hay que asegurarse de que los riesgos de conducta están bien identificados y evaluados.

rarse la conveniencia de establecer periodicidades mínimas de revisión anuales o ligadas al ejercicio contable o fiscal, así como la consideración de cambios normativos que impacten en la adecuación de las conductas de la actividad diaria de la organización. Pero siempre proporcionando *assurance* sobre los riesgos más críticos.

EVALUAR EL MARCO DE CONTROL DEL RIESGO DE CONDUCTA

Evaluación del "tone at the top"

Como se ha mencionado previamente, tradicionalmente, las *soft skills* de las organizaciones no han sido el foco principal de auditorías internas, porque *"existe el temor de brindar una opinión errónea sobre aspectos que se consideran subjetivos".*

No se trata de **evaluar** la conducta individual de un empleado, sino **la cultura general que mueve la conducta de los empleados:** las directrices, escritas o no, que inducen a los empleados a comportarse de cierta manera.

En este sentido, para evaluar el *tone at the top,* el auditor interno deberá verificar si:

- Existe un código de conducta o pautas de conducta definidas y claras.
- Las directrices de la alta dirección no contradicen los principios del código de conducta, ni de la regulación aplicable.
- La alta dirección se preocupa por que los empleados entiendan sus responsabilidades en materia de conducta.
- En definitiva, existe un marco efectivo de gestión del riesgo de conducta promovido desde la alta dirección de la compañía.

Cuando la alta dirección no hace honor a la cultura de la ética, se empezará a producir un deterioro del control interno y del cumplimiento de las normas que, en el medio plazo, podrá afectar gravemente a la consecución de la misión, visión y estrategia de la compañía.

Asignar roles y responsabilidades para la gestión del riesgo de conducta

Un elemento clave en la gestión del riesgo de conducta es la asignación de roles y responsabilidades, de tal manera que cada integrante de la organización esté implicado en la gestión de este riesgo en la medida adecuada: la implicación no debe ser idéntica para todos, sino que estará condicionada por las funciones que cada uno realiza.

Auditoría Interna debe asegurarse de que existe en la organización esta asignación de roles y responsabilidades y de que abarca a todos sus integrantes, empezando por los órganos de gobierno y la alta dirección.

En la asignación de roles y responsabilidades puede tenerse en cuenta también el Modelo de las Tres Líneas, cuya flexibilidad permite adaptarlo a todo tipo de organizaciones, con independencia de su naturaleza, actividad o tamaño.

En este sentido, Auditoría Interna debe estar alerta en sus revisiones a la separación de roles de primera línea (funciones de negocio, relacionadas con la elaboración y comercialización de productos y prestación de servicios a los clientes, pero también implementan acciones relacionadas con la gestión de riesgos) y segunda línea (soporte en materia de riesgos, dando apoyo y monitorizando la gestión del riesgo realizada por la primera línea). Es decir, debe verificar la existencia de una adecuada separación de funciones entre propietarios/gestores de riesgos y supervisores de riesgos.

Auditoría Interna debe dar confort sobre el hecho de que el propietario de los riesgos, en el caso de que esté definido, sea efectivamente alguien de la organización en las mejores condiciones para comprender e implementar las acciones necesarias y con la suficiente autonomía para ello. Encontrar la respuesta a las siguientes cuestiones puede ayudar en esta evaluación de idoneidad de los propietarios de riesgos de conducta:

- ¿Quién entiende mejor las posibles causas de incumplimiento, el riesgo en sí y su impacto en la organización?
- ¿Quién tiene más experiencia en gestión de riesgos?
- ¿Quién estaría en las mejores condiciones para responder si se materializara el riesgo?
- ¿Quién tiene la capacidad de monitorizar proactivamente el riesgo?

Monitorización y supervisión del marco de gestión del riesgo de conducta

Las entidades pueden tener diferentes esquemas de monitorización de cara a evaluar desviaciones en los objetivos de negocio derivados de conductas inadecuadas en sus procesos, que pueden variar en función de su organización, mayor o menor cercanía a los mismos, nivel de segregación de funciones, aspectos que en gran parte pueden estar influenciados por el nivel de regulación de sus actividades.

Pese a ello, a continuación, se identifican elementos comunes para todos ellos, que son consecuencia de la materialización de diferentes riesgos de conducta de la entidad con impacto económico, y podrían ser evaluados durante la auditoría:

- Análisis de los procedimientos jurídicos abiertos y su impacto en la provisión contable de contingencias y gasto del ejercicio, y cuantificaciones de impactos máximos por esas operativas.
- Aprobación de las dotaciones a las provisiones financieras por contingencias relacionadas con el riesgo de conducta (por ejemplo, provisiones por aplicación de cláusulas suelo, compensación a clientes por interrupción del servicio, etc.).
- Análisis de cuentas de gasto para evaluar multas, sanciones, compensaciones comerciales.

- Medidas complementarias adoptadas para identificación y mitigación inmediata de los asuntos.
- Identificación de *gaps*.
- Establecimiento y seguimiento de planes de acción para solucionar los *gaps*.
- Contrastes de la valoración del riesgo conducta realizada por el área de gestión de riesgos o equivalente.
- Elaboración de cuadros de mando por parte de la organización y por Auditoría Interna.

Reporte periódico a la alta dirección y los órganos de gobierno sobre el desempeño de la organización en materia de gestión del riesgo de conducta

Como se ha comentado anteriormente, la organización debe tener un proceso efectivo de reporte y comunicación de riesgos de conducta a la alta dirección y órganos de gobierno y Auditoría Interna debe comprobar la existencia y efectividad de dicho proceso.

En este sentido, es relevante verificar la adecuación de los aspectos objeto de reporte, entre los que podrían incluirse:

- Los eventos de materialización de riesgo de conducta más relevantes, desde el punto de vista cualitativo o cuantitativo, así como su impacto para la organización en términos económicos, reputacional, de pérdida de cuota de mercado, etc.
- Los eventos de funcionamiento anómalo de los controles más relevantes sobre riesgo de conducta.
- Las provisiones financieras significativas para dotar sobre riesgos de conducta, su metodología de cálculo y su histórico.
- KPIs sobre riesgo de conducta, su metodología de cálculo y su histórico.
- Conclusiones de los trabajos de auditoría más relevantes en materia de riesgo de conducta.
- Las expectativas de los distintos grupos de interés.
- Novedades normativas y/o sectoriales.
- Noticias relacionadas con los riesgos de conducta de la organización.

Adicionalmente, Auditoría Interna debería evaluar otros aspectos más formales, pero no menos importantes sobre la gestión del riesgo de conducta, como, por ejemplo, la trazabilidad y coherencia de los aspectos puestos de manifiesto en reportes sucesivos, y/o el seguimiento de las acciones de remediación requeridas según los informes anteriores.

Promoción de una cultura ética en la organización: formación, sensibilización y comunicación continua sobre las normas éticas y normas de conducta

La formación es una herramienta clave para facilitar que los diferentes usuarios (generalmente empleados, aunque también clientes, proveedores o colaboradores y otros grupos de interés) entiendan los riesgos y las oportunidades de las características de productos y servicios que comercializan las entidades, así como también de los derechos y las obligaciones a los que hacen frente.

La formación es un complemento a la regulación interna y externa, y como consecuencia, debe ser un aspecto para considerar en el programa de trabajo del auditor interno.

En esta parte de la auditoría, se puede considerar la evaluación de aspectos tales como:

- Existencia de un plan de formación definido, o bien si las características básicas del comportamiento esperado por los principales agentes de los procesos auditados se están considerando en las formaciones existentes, de forma directa o indirecta.
- El perímetro de aplicación de planes de formación se encuentra adecuadamente definido, e incluye a los usuarios que realizan las actividades que tienen riesgo específico de conducta.
- Si la formación sobre los usuarios que desempeñan actividades de mayor riesgo de conducta incluye cuestiones específicas sobre su conducta esperada en su actividad, de forma que sea suficientemente entendible y refleje las actitudes deseadas, y no deseables.
- Si la frecuencia de la formación establecida es adecuada en función de las características de su actividad y su riesgo.

Actualización del marco de gestión del riesgo de conducta

Como se ha tratado anteriormente, la organización debe disponer de un proceso periódico de actualización de su marco de gestión del riesgo de conducta y Auditoría Interna debe comprobar su cumplimiento.

En este sentido, Auditoría Interna debe comprobar si la organización tiene un proceso efectivo de revisión continua del marco de gestión del riesgo de conducta, mediante el cual las novedades significativas y, en particular, las legislativas, pero también las procedimentales, culturales, técnicas, informáticas, etc., así como los resultados de los controles internos y las revisiones periódicas, se utilizan para mejorar y actualizar el citado marco de gestión. En definitiva, se trata de que el marco contemple su propia actualización como mecanismo de mejora continua, basada en el aprendizaje y la retroalimentación.

Igualmente, y en aras del buen gobierno, es importante que Auditoría Interna revise si los principales documentos del marco tienen formalmente identificados un responsable y una periodicidad de revisión y, en su caso, de actualización, así como una obligación de reporte a la instancia de aprobación del resultado de dicha revisión, para su conocimiento y/o conformidad con la misma.

EVALUACIÓN DE CONTROLES ESPECÍFICOS PARA MITIGAR LOS RIESGOS DE CONDUCTA DE LA ORGANIZACIÓN

Auditoría Interna debe ser capaz de identificar los mecanismos de control específicos sobre los riesgos de conducta identificados de manera oportuna y adecuada, de modo que se garantice la protección de los distintos grupos de interés afectados, evitando que se pro-

duzcan conductas no deseadas y sus efectos. Como ya ha sido visto, se pueden revisar controles generales o transversales a la organización o específicos en los distintos procesos o con los distintos grupos de interés.

Controles generales

Un elemento común para identificar potenciales conductas inadecuadas será la evaluación del adecuado funcionamiento del código de conducta, la gestión del canal de denuncias de la entidad y el sistema sancionador.

Un sistema de gestión del riesgo de conducta sin un adecuado esquema de sanciones puede resultar poco eficaz.

Código de conducta

En primer lugar, el auditor interno puede revisar el diseño del contenido del código de conducta, para evaluar cuestiones como su alcance de aplicación (mercados, sociedades, actividades, terceros), y su adecuación a la misión y visión de la organización, a la regulación del sector y a las mejores prácticas.

También puede evaluar el diseño y la efectividad de los mecanismos establecidos para su cumplimiento, incluyendo en el mismo la revisión de su difusión, el desarrollo de procedimientos sobre los distintos principios recogidos en el código, los mecanismos de control para su cumplimiento y el reporte a los Comités establecidos.

Canal de denuncias

Auditoría Interna puede revisar los asuntos informados a través del canal de denuncias de la entidad, para evaluar cuestiones como:

- Evolución y tipología de denuncias recibidas, y su alineamiento con el alcance del código de conducta.
- Gestión efectiva de expedientes: Identificación de denuncias no investigadas o no resueltas/comunicadas.
- Evolución de KPIs por tipología e identificación de casuísticas esperables en los colectivos que no tienen reflejo en denuncias, o son residuales.
- Existencia de un protocolo de actuación y comunicación de decisiones a adoptar en función de su relevancia.
- Existencias de mecanismos para no adoptar represalias contra los denunciantes.

Esquema de sanciones

Un sistema de gestión del riesgo de conducta sin un adecuado esquema de sanciones puede resultar poco eficaz. En este sentido, Auditoría Interna deberá revisar:

- La existencia de un esquema de sanciones para conductas no deseadas.
- La aprobación de este esquema por parte del nivel adecuado de la organización.
- La correcta aplicación de dicho esquema en los casos de conducta inapropiada.

Controles específicos

Entrando en las distintas dimensiones del riesgo de conducta tratadas en el primer apartado de este documento, y sin ser exhaustivos puesto que, como se ha comentado, el riesgo de conducta se ha de concretar en cada organización, se señalan a continuación los principales aspectos a analizar por parte de los auditores internos.

Clientes y consumidores

Con carácter general, y dada su relevancia, se recomienda prestar atención a aquellos factores que afectan a la comercialización de productos y servicios para los clientes, evaluando el lugar que ocupan las áreas que llevan a cabo los mecanismos de soporte al negocio que resultan clave en el aseguramiento de una adecuada conducta en los productos o servicios comercializados. En este campo, pueden evaluarse, entre otros, la conducta en los procesos que afectan a su diseño; sus procesos productivos internos y su cadena de suministro; los mecanismos de información de sus características ante el consumidor (tales como etiquetas, anuncios, redes sociales) o la atención al cliente.

Para ello, Auditoría Interna puede servirse de un mapeo de productos y servicios con los principales procesos de la organización, o en su caso, del proceso específico que esté auditando, con la finalidad de identificar los principales controles o esfuerzos organizativos y de recursos que mantiene implantados la organización en esta materia.

La auditoría de la gestión del riesgo de conducta para la protección de consumidores y clientes puede incluir los siguientes ámbitos de alcance, en la medida en que éstos resulten de riesgo para la organización.

1.- **Gobernanza de los flujos comerciales con clientes y consumidores.** En este ámbito, se podrían evaluar cuestiones tales como:

   a. *Los servicios de atención al cliente.*
      - Análisis de la evolución de la tipología de las comunicaciones de los consumidores, y su resolución e identificación de casos anómalos.
      - Atención de las consultas sobre sus derechos en materia de transparencia y protección de la clientela o sobre los cauces legales para el ejercicio de sus derechos.
      - Evaluar cómo se ha producido la resolución de conflictos surgidos con los consumidores.
      - Nivel de confidencialidad existente en los procesos de atención al cliente.

   b. *Si la compañía vela por la seguridad de los medios de pago utilizados,* para garantizar el adecuado funcionamiento y la trazabilidad de los procedimientos de facturación y cobro, en el sentido de evitar prácticas abusivas o discriminatorias, garantizando la protección de los datos de los clientes y actuando con debida diligencia en la prevención del fraude a los consumidores.
      - KPIs sobre reclamaciones de clientes en relación con incidencias en sus pagos.
      - Los medios de pago aceptados y sus características se encuentran adecuadamente explicitados (web de venta, carteles en tienda).
      - Se realiza una comunicación adecuada sobre el tratamiento de los datos y una gestión acorde con los mismos.
      - Existe un adecuado tratamiento de los datos de las tarjetas de los clientes.

   c. *Si hay una gestión adecuada en materia de devoluciones* y ésta se encuentra a disposición de los clientes.
      - Existencia de estándares o normativa interna en materia de devoluciones y *gap* análisis del

alineamiento con la normativa vigente y/o estándares de buen gobierno de la entidad.

- Evaluación del cumplimiento de los estándares en base a casos reales.
- Elaboración u obtención y análisis de KPIs sobre la evolución de las devoluciones, que puedan denotar comportamientos anómalos en determinados productos.
- Elaboración u obtención y análisis de KPIs sobre el cumplimiento de los plazos establecidos en las políticas comerciales de las devoluciones.

d. ***Si existe una gestión adecuada en materia de gestión de rebajas,*** descuentos, usos posteriores del producto.

- Existencia de estándares o normativa interna en relación con rebajas, descuentos, trazabilidad suficiente sobre los cambios en los precios y *gap* análisis en relación con la normativa aplicable.
- Evaluar si está adecuadamente visible para las áreas comerciales de la empresa y el consumidor.
- Revisión de que los descuentos anunciados se encuentran acordes con los aplicados.
- Revisión de las fechas de comienzo, finalización y que los diferentes cambios de precios aplicados sean adecuados.
- Analizar qué gestión se realiza con el *stock* sobrante, taras, prácticas relacionadas con el tratamiento de residuos, reutilizaciones posteriores del producto.

2.- Diseño y gobierno de productos y servicios

a. ¿Está suficientemente definido en la normativa interna de la entidad, el marco de actuación en relación con las ***características esenciales de los elementos que se pueden diseñar,*** contratar, producir, y/o elementos no permitidos?

b. ¿Existen ***mecanismos de decisión previos al lanzamiento de nuevos productos*** o servicios, o modificación de los actuales?

- Evaluar en qué medida se consideran en ellos los factores establecidos por la alta dirección, relativos al riesgo de conducta.
- Analizar cómo se tiene en cuenta la posible existencia de colectivos de consumidores con características singulares y cómo podrían verse afectados.
- Comprobar si existe un proceso de homologación de nuevos materiales que se incorporan en los artículos nuevos o existentes, que asegure que su origen, composición y calidad es adecuada.
- Verificar si se dispone de un maestro de artículos y un proceso para su gestión, en el que se incluyen las características básicas que pueden afectar al cumplimiento de la conducta esperada por la entidad en su comercialización.
- Comprobar la existencia de servicios de preventa (instrucciones) y postventa (más allá del puro cumplimiento de la normativa de garantías aplicable), acordes en base a las características del bien o servicio comercializado.

3.- Sistemas de retribución e incentivación de los equipos.

En este apartado, se pueden evaluar cuestiones tales como la existencia de elementos que hagan de contrapeso sobre el volumen de ventas o rentabilidad económica, como, por ejemplo, el cumplimiento de requisitos de sostenibilidad en la cadena de suministro, normas internas de conducta, indicadores de malas ventas…

4.- La publicidad de las características de productos y servicios comercializados (etiquetado, merchandising, web de venta, redes sociales). Habitualmente se identifican diferentes canales de comunicación con los consumidores, con relación a las características de los bienes y servicios que se comercializan.

Existen requerimientos regulatorios en esta materia en muchas industrias, pero en general:

a. ¿Están suficientemente definidas en la normativa interna de la entidad y difundidas las directrices sobre ***cómo realizar una exposición o publicidad responsable*** de los productos o servicios comercializados?
   - Identificar normativa interna sobre etiquetado de artículos, o procesos implantados para una adecuada gestión de las etiquetas, su alcance y difusión.
   - Identificar los procedimientos sobre gestión de las redes sociales relacionadas con los productos y servicios, y si estos incluyen comportamientos personales de los empleados en relación a información de la entidad.

b. ***¿Se identifican artículos o servicios*** comercializados por la entidad, en los que promocionan características o estándares genéricos, ***que no se encuentran suficientemente definidos?***
   - Evaluar en qué medida, en caso de darse, se corresponden a conceptos propios de la entidad, y cuáles a estándares de mercado.
   - Analizar las descripciones y su adecuación a las características del producto o servicio.

c. ¿Se dispone de ***trazabilidad suficiente en la cadena de suministro*** para asegurar que los elementos incorporados en los artículos son acordes con las características anunciadas?
   - Evaluación de características trazadas y no trazadas.
   - Análisis de suficiencia del eslabón de la cadena trazada vs necesaria para garantizar los compromisos adquiridos frente al consumidor.

d. Existe normativa interna relativa a ***componentes no permitidos,*** se encuentra actualizada y adecuadamente difundida (tanto internamente como en la cadena de suministro).

e. Podría realizarse, bien mediante un análisis global, o bien a través de la selección de una muestra de artículos comercializados por la entidad, la ***identificación y análisis de toda la información que se ha emitido de productos o servicios.***
   - Etiquetas: evaluación de información contenida en la etiqueta física, control de las composiciones, homogeneidad y cumplimiento normativo.
   - Web de venta: evaluación de información adicional contenida en la web de venta y su alineamiento con las políticas internas o estándares éticos de la entidad.
   - Redes sociales y otras fuentes de información: identificación y análisis de información proporcionada sobre las características de servicios y productos, tanto por fuentes internas, como por fuentes externas (grupos de influencia). En este apartado, evaluar si la información es responsable, y su comunicación y tono se encuentran alineados con la ética profesional y conductas esperadas.

Accionistas

La protección de los derechos e intereses legítimos de todos los accionistas, con independencia del lugar donde residan y, en especial, de los accionistas minoritarios, es un aspecto relevante para considerar en el riesgo de conducta de las entidades. En relación con el mismo, Auditoría Interna puede:

a. Evaluar si la estrategia definida para la compañía prima los **intereses de los accionistas** frente a los de los gestores.

b. Evaluar si las **estructuras de la organización son claras,** evitando estructuras complejas que diluyan

la responsabilidad de los gestores de la compañía o que dificulten el conocimiento por parte de los accionistas.

c. Respecto de la **información privilegiada:**

- Evaluar si existe un marco normativo y de gestión sobre el tratamiento de la información privilegiada por parte de los usuarios que participan en su gestión.
- Analizar la relación de personas (que incluye empleados, pero también asesores externos), que, de forma temporal o transitoria, tienen acceso a información privilegiada de la entidad con motivo de su participación o involucración en una operación, durante el tiempo que requiera dicho proyecto.
- Evaluar si estos individuos son conocedores del comportamiento establecido en la normativa interna.
- Identificar los principales flujos de generación de dicha información y evaluar si la cobertura de la relación actual de personas es adecuada.

d. **Operaciones personales** relacionadas con instrumentos financieros de la entidad:

- Evaluar si existe un marco para que consejeros, altos directivos, personas vinculadas o empleados que posean, por el ejercicio de sus funciones, información privilegiada, realicen operaciones por cuenta propia relativa a los Valores e Instrumentos Afectados conforme a lo previsto en la normativa aplicable.
- Revisar la accesibilidad a dicho marco por parte todos los miembros de la organización (tales como comunicación inicial, publicación intranet, correos recordatorios, formación periódica).
- Analizar si se dispone de un registro, se encuentra actualizado y existe un procedimiento establecido para asegurar su cumplimiento.

e. Concluir sobre si el **sistema de remuneración** a empleados prima exclusivamente la consecución de beneficios a corto plazo, y/o si la remuneración de las áreas de control compromete su independencia.

f. Analizar si los **sistemas de retribución** promueven la adopción de riesgos no alineados con el apetito de riesgo de la compañía.

Proveedores

En relación con la evaluación del riesgo de conducta de la entidad que afecte a la cadena de suministro (proveedores, franquicias, colaboradores, socios de negocio), Auditoría Interna puede evaluar la gestión de los conflictos de interés y regalos de los suministradores hacia otros colectivos (empleados, accionistas, clientes).

a. **Conflictos de interés.** La adecuada gestión de los conflictos de interés es un elemento relevante del buen gobierno. Se trata de evitar o mitigar situaciones en las que un interés personal del empleado o proveedor (conflicto de interés directo) o de una persona vinculada al mismo (conflicto de interés indirecto) se contrapone (conflicto de interés real) o puede contraponerse (conflicto de interés potencial) al interés de la entidad, pudiendo interferir en sus grupos de interés, al poder comprometer la necesaria objetividad o profesionalidad de los empleados en el desempeño de sus funciones. En este apartado el auditor interno puede revisar:

- Existencia de marco de conducta que regula estas situaciones, que contiene una adecuada descripción de las casuísticas potencialmente habituales, definición de responsabilidades y proceso definido de consulta, evaluación y seguimiento.
- Identificación de un proceso definido de gestión.

- Obtención del registro de casos y análisis de su mantenimiento y supervisión periódica de las medidas de control a adoptar.

b. **Gestión de regalos, hospitalidades.** Evaluar la posición formal de la entidad hacia sus empleados y proveedores, en el contexto de regalos o hospitalidades entendidos como símbolo de gratitud en el contexto de las prácticas comerciales, y en qué medida éstas pueden influir las decisiones comerciales en perjuicio de otros proveedores.

   - *Evaluación del marco normativo* relacionado con regalos y hospitalidades, su alcance, difusión y proporcionalidad, analizando:
     - Que resulten acorde con las leyes aplicables.
     - Que no se realicen con la intención de influir a terceros o para obtener de éstos algún beneficio indebido.
     - Que no se realicen con la finalidad de obtener o mantener un determinado negocio o una ventaja empresarial.
     - Que no tengan por objeto obtener o intercambiar tratos de favor.
     - Que sean ofrecidos o recibidos de forma abierta y transparente.
     - Que no puedan dar lugar a conflictos de interés.
     - Que no tengan un valor superior a una cantidad económica definida.
   - ***Identificación de actividades y áreas especialmente sensibles,*** sobre las cuales se puede llevar a cabo:
     - Identificación de la difusión, formación y adhesión al marco normativo interno.
     - Existencia y adecuado mantenimiento de registros de regalos, y su gestión.
   - *Identificación de anomalías sobre los requerimientos de la normativa* (volumen en determinados momentos del año, mercados, áreas de actividad).

c. **Prácticas de compra abusivas.** Analizar si hay conductas de compra abusivas o no acordes con los estándares de comportamiento establecidos por la entidad. Para ello, pueden realizarse diversas verificaciones, según el sector. Algunas de ellas:

   - Identificación de ***cargos emitidos anómalos*** tanto en importe como en volumen, a través de los que se puedan identificar abusos o conducta no adecuada.
   - Análisis entre fechas de pedido y entrega donde puedan ponerse de manifiesto ***requerimientos de producción "imposibles".***
   - Identificación de anulaciones de pedidos en fecha muy próxima a la entrega, donde puedan manifestarse ***conductas abusivas con perjuicios a la cadena de suministro.***

Empleados

Adicionalmente, en el alcance de las revisiones, Auditoría Interna puede considerar la inclusión de riesgos de conducta que, de materializarse, perjudiquen a empleados, evaluando las medidas implantadas por la entidad para evitar conductas no deseadas como, discriminación por cuestiones de género, origen étnico o social, características genéticas, lengua, religión, edad u orientación sexual. Esto incluye, con carácter no limitativo, las políticas de contratación, los planes de desarrollo empresarial, la remuneración, el acceso a formación, o posibilidad de optar a vacantes internas.

A este respecto, pueden revisarse cuestiones como:

- Medidas implantadas para prevenir que otros empleados o personas externas ejerzan una influencia inadecuada, tales como la existencia de **políticas de**

prevención de cualquier tipo de acoso, discriminación, conducta o comportamiento inapropiado, políticas retributivas.

- **Accesibilidad a dichas políticas** por parte de todos los miembros de la organización (publicación intranet, correos recordatorios).
- Existencia de un **procedimiento de queja o denuncia,** ante incumplimientos en los estándares establecidos en las mismas, adecuadamente difundido en la organización.
- Evaluación de **KPIs de denuncias recibidas** por motivos de cualquier tipo de acoso, discriminación, conducta o comportamiento inapropiado.
- Extracción de datos para **identificación de sesgos no justificados.**

Otros grupos de interés

El Consejo de Administración, como órgano supervisor (al más alto nivel) de la Información Económico-Financiera, No Financiera y Corporativa, ha de asegurar la máxima difusión y calidad de la información suministrada a los grupos de interés y al mercado en general. En el ámbito de una auditoría de riesgo de conducta, deberían evaluarse, más allá del cumplimiento de los requerimientos normativos aplicables para la formulación de los estados de información financiera y no financiera, aspectos relativos a los mecanismos de comunicación y procesos de elaboración de contenidos, fundamentalmente en la información corporativa emitida en las webs y redes sociales corporativas, donde, en general, no existen estándares legales establecidos de reporte.

Para valorar este aspecto, podrían evaluarse cuestiones tales como:

- ¿La difusión de Información es adecuada, y de calidad para los accionistas y demás grupos de interés, y existen marcos de control interno con el objetivo de proporcionar una información razonable?
- ¿La información contenida es transparente, veraz, objetiva y simétrica?
- ¿Existe igualdad de trato en el reconocimiento y el ejercicio de los derechos de todos los accionistas que se encuentren en condiciones idénticas?
- ¿Se encuentran a disposición de los accionistas y de los grupos de interés los cauces efectivos para conocer y seguir la actualidad de la entidad, las novedades más relevantes de su actividad de acuerdo con la legislación aplicable y sus normas de gobierno corporativo?

Beneficios de la Auditoría Interna del marco de gestión del riesgo de conducta

En algunos sectores existe conciencia sobre la importancia del riesgo de conducta (por ejemplo, en el financiero, altamente regulado), dedicando un porcentaje relevante de su plan de auditoría a esta cuestión. Sin embargo, no todas las organizaciones se encuentran dis-

puestas a dedicar recursos de Auditoría Interna a dicho riesgo. A continuación, se exponen las principales razones y beneficios derivados de llevar a cabo este tipo de revisiones.

CONTRIBUYE A LOGRAR LA MISIÓN Y VISIÓN Y A ALCANZAR LA ESTRATEGIA DE UNA ORGANIZACIÓN

Como se ha ido señalando a lo largo de este documento, **el riesgo de conducta indebidamente gestionado (por haber sido ignorado o asumido plenamente) puede suponer un auténtico obstáculo para el propósito de la organización: su misión, visión, y estrategia a medio y corto plazo para lograrlas.**

Según se ha visto, el riesgo de conducta versa sobre una "conducta inapropiada y perjudicial" y tiene, en todas sus dimensiones, una vertiente estratégica. No identificar, por sesgo o negligencia, las instancias en las que el riesgo de conducta puede presentarse, puede hacer que la misión y visión de la organización no se alcance, ya que los comportamientos de los miembros de la organización pueden divergir de éstas, o les sean directamente contrarios.

Por ello, auditar la cultura ética de la organización y su riesgo de conducta, contribuye a la consecución de los objetivos de la organización, conforme a su propósito.

Dedicar los recursos necesarios a comunicar de forma abierta y honesta los potenciales riesgos de conducta, en Comisiones de Auditoría y otros foros adecuados, no es una señal de debilidad sino todo lo contrario; representa un adecuado conocimiento de los riesgos que afronta la organización y un cumplimiento del mandato recibido como auditor interno.

Aun así, puede ser que en algunas organizaciones los principales *stakeholders* o grupos de interés requieran de un plus de convencimiento antes de autorizar o participar en auditorías que incluyan este riesgo. En estas circunstancias, el auditor interno puede considerar los siguientes argumentos para proponer auditar el marco de gestión del riesgo de conducta:

- Ayuda a identificar situaciones que pueden derivar en riesgos de incumplimiento o fraude.
- Permite entender por qué se cumplen, o dejan de cumplir, las políticas y procedimientos de la organización.
- Es una forma de aumentar el engagement de los grupos de interés con la misión y la visión de la organización, al reforzar y explicar cómo éstas se despliegan en el día a día.

En definitiva, *"la cultura organizacional es fundamental para el cumplimiento de objetivos. (…) ahora más que nunca una empresa debe asegurar que sus creencias, hábitos, valores, actitudes y tradiciones sean compartidos por todo su personal; por ello, es de suma relevancia que la cultura organizacional esté claramente definida y alineada con la estrategia para obtener los resultados deseados"*[11]. Y en este sentido, se hace imprescindible asegurar que los comportamientos y conductas, como

Mal gestionado, el riesgo de conducta puede impedir a la organización lograr sus objetivos estratégicos.

11. The IIA Global, *Practice Guide: Auditing Culture,* 2019

elementos invisibles de la cultura organizacional[12], sean adecuados y contribuyan a la estrategia y objetivos de la organización, minimizando el riesgo que, de ellos, pudiera surgir.

GARANTIZA LA APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE GESTIÓN DE RIESGOS

Tras conocer qué es el riesgo de conducta y como auditar y valorar las respuestas y estrategias que las organizaciones puedan poner en marcha respecto al mismo, queda pendiente preguntarse de qué manera podemos integrar este riesgo no financiero dentro del panorama de riesgos de nuestra organización. O **¿cómo encaja un riesgo tan amplio, y quizás tan complejo de gestionar, en nuestros programas de control interno?**

El riesgo de conducta es un elemento subyacente clave en los sistemas de control interno y de gestión de riesgos de los principales estándares.

Aunque la respuesta pueda ser diferente en cada organización, merece la pena detenerse sobre una justificación a la par tan sencilla como relevante: el riesgo de conducta es un elemento subyacente clave en los sistemas de control interno y de gestión de riesgos construidos sobre los principales estándares de mercado. Tanto en el marco COSO de Control Interno de 2013 como en el de COSO ERM de 2017 existen obligaciones para las tres líneas respecto a los riesgos, y también referidas al riesgo de conducta.

Incluso podría señalarse que esta transversalidad es reconocida ya por los autores de ambos marcos que establecen la obligatoriedad de gestionarlo como una de las *best practices* para cumplir con dichos marcos.

El riesgo de conducta dentro del marco COSO ERM

Existen dos componentes del marco COSO ERM estrechamente ligados con el riesgo de conducta:

- **Gobierno y cultura.** El principio de *Definir la cultura,* establece que la alta dirección debe definir de qué manera espera que sus empleados y colaboradores se comporte *(the way we do things here).* Es decir, la alta dirección debe tratar de prevenir el riesgo de conducta mediante guías claras de comportamiento. En otro de los principios, *Demostrar compromiso con los valores fundamentales* se establece que se deben fijar los mecanismos para detectar y castigar los comportamientos contrarios a los valores.

- **Evaluación y revisión.** Dentro de este componente la gestión del riesgo de conducta se encarna en el principio de *Perseguir la mejora en la Gestión de Riesgos Corporativos.* Esta mejora no solo requiere de mejoras técnicas, como puede ser un análisis más detallado del apetito de riesgo, sino también exige poner los medios para que los principios señalados en el componente anterior se lleven a cabo. Comunicaciones, formaciones y manifestaciones de los valores clave y advertencias sobre el riesgo de conducta forman, por lo tanto, parte im-

12. *Auditoría Interna de la Cultura Corporativa,* LA FÁBRICA DE PENSAMIENTO, Instituto de Auditores Internos de España, 2023

prescindible del ciclo de mejora continua de un sistema ERM bien engrasado.

Parece claro que una organización no podrá operar un sistema de gestión de riesgos adecuado al marco COSO ERM si no se compromete a trabajar el riesgo de conducta, al menos de forma preventiva.

El riesgo de conducta dentro del marco COSO de Control Interno

Si se pone foco en lo que dice el marco COSO de Control Interno al respecto, ¿se sostiene la afirmación de que el riesgo de conducta sigue siendo un aspecto clave? Será labor del lector llegar a la conclusión, teniendo en cuenta lo que el marco dice en los siguientes componentes:

- **Ambiente de control.** En dos de sus principios *(Demostrar compromiso con la ética y los valores* y *Hacer cumplir la responsabilidad)* el marco COSO CI establece la obligación para las organizaciones de definir, desde las más altas esferas y para toda la organización, medidas para combatir el riesgo de conducta. La pública y reiterada adhesión de la alta dirección a ir más allá del mero cumplimiento y a favorecer, recompensando y castigando, un comportamiento acorde a la misión y la visión (de forma adicional al mero riesgo de cumplimiento).
- **Actividades de supervisión.** En el marco de este componente y explicitado a través del principio de *Evaluar y Comunicar Deficiencias* se observa otro llamado a actuar sobre el riesgo de conducta. En este caso proponiendo a las organizaciones ir más allá del papel meramente preventivo y generalista centrado en comunicar buenas intenciones y mandatos de comportamiento. Este principio espera que la organización sea capaz de detectar situaciones en las que el riesgo de conducta se haya cristalizado en un evento de riesgo, para luego comunicar las lecciones aprendidas y sus consecuencias al resto de la organización. Esta es una palanca increíblemente potente para generar organizaciones honestas y abiertas en las que los *stakeholders* conozcan el compromiso real, pues se basa en situaciones específicas, y no en declaraciones generalistas, de la dirección relacionadas con gestionar el riesgo de conducta y asegurar que se trabaja de acuerdo a los principios y maneras de hacer que han sido comunicadas.

La adecuada gestión del riesgo de conducta no es un añadido, es más bien un fundamento para dar cumplimiento a los requerimientos de un sistema de control interno efectivo. Así, por ejemplo, una organización que no contemple o actúe sobre el riesgo de conducta difícilmente podrá decir que cumple con las exigencias de la normativa respecto al SCIIF[13], basada precisamente en este marco teórico.

Una empresa no podrá operar un sistema de gestión de riesgos adecuado al marco COSO ERM si no trabaja el riesgo de conducta.

REFUERZA LA CULTURA CORPORATIVA

En el documento *Auditoría Interna y la ética empresarial,* de la Fábrica de Pensamiento del IAI de España, los autores se preguntaban sobre cómo trabajar en algo tan etéreo como la cultura corporativa. Concluía dicho documento afirmando la importancia de la cultura

13. Sistema de Control Interno sobre la Información Financiera.

corporativa y demostrando que se pueden realizar pruebas sobre la misma, su cumplimiento y su madurez.

Merece la pena señalar la necesidad de enlazar ese documento con el presente, pues, como se ha ido comentando, el riesgo de conducta puede ser una amenaza frontal a la cultura de las organizaciones. Yendo más allá, se debe considerar el riesgo de conducta y su gestión como una palanca más para dar alas a la cultura de las organizaciones.

A continuación, se señalan algunas maneras mediante las cuales la Tercera Línea, mediante su trabajo sobre el riesgo de conducta, puede ayudar a reforzar la cultura corporativa de una organización:

- **Comunicar las debilidades detectadas en sus revisiones:** contrariamente a lo que pueda parecer, la comunicación interna, y por canales adecuados, de las situaciones en las que se ha producido un riesgo de conducta proporciona varios efectos positivos; demuestra el compromiso de la organización para combatir estos comportamientos dañinos; sirve como aviso para otros actores que consideren conductas análogas al señalar que estas prácticas son detectadas y castigadas por la organización; y proporciona un ejemplo adicional de las conductas que se quieren evitar, favoreciendo que personas que pudieran conocer situaciones similares se sientan respaldadas para levantar la voz y denunciarlas por los canales correspondientes.
- **Conmemorar mejores prácticas:** no debemos olvidar tampoco el felicitar y compartir aquellos casos en los que, en situaciones complejas, observemos que los distintos grupos de interés supieron mitigar o reaccionar al riesgo de conducta. Esto no solo estimula la repetición de estos comportamientos, sino que demuestra el compromiso de la alta dirección de una forma mucho más amable que las más comunes reprimendas o castigos.
- **Crear un repositorio de conductas:** finalmente, mediante los trabajos de auditorías sobre el riesgo de conducta, el auditor interno acumula una cantidad de información muy relevante a compartir con las otras dos Líneas de aseguramiento. La experiencia acumulada, propia y específica de la organización, puede utilizarse para el *benchmark* en el caso de incorporar nuevas unidades de negocio o como material formativo para nuevos empleados o directivos.

La comunicación interna, y por canales adecuados, de las situaciones en las que se ha producido un riesgo de conducta proporciona efectos positivos.

PERMITE VISUALIZAR LOS BENEFICIOS Y SINERGIAS ENTRE LAS TRES LÍNEAS

Como se ha indicado anteriormente, y adaptado al grado de madurez del sistema de control interno de la organización, la auditoría del modelo de gestión del riesgo de conducta pone de manifiesto los beneficios y sinergias de la coordinación e integración del Modelo de Tres Líneas. La primera línea, encargada de la operativa y de la gestión del riesgo de conducta, la segunda como soporte y supervisión de la eficacia de la gestión de dicho riesgo, y, por último, la tercera, Auditoría Interna, aportando su independencia y objetividad para proporcionar aseguramiento y asesoramiento sobre la gestión del riesgo de conducta.

LA GESTIÓN DEL RIESGO DE CONDUCTA COMO PALANCA DE ESG

Del mismo modo, el documento *Auditoría Interna y los aspectos ESG,* también de la Fábrica de Pensamiento del Instituto de Auditores Internos de España, puede ayudar a entender que el riesgo de conducta podría llegar a afectar también a factores ESG.

Hoy en día, la Responsabilidad Social Corporativa (RSC) y los criterios ESG *(Environmental, Social and Governance)* tienen una gran relevancia en la toma de decisiones de las organizaciones y de sus grupos de interés. Los criterios ESG apoyan una visión renovada y más amplia de creación de valor por parte de la organización, aportación que hasta hace muy poco se vinculaba exclusivamente con criterios económicos y de rentabilidad.

La "G" de ESG se refiere al Gobierno de las organizaciones y, como se ha visto, la gestión adecuada del riesgo de conducta es un elemento clave. Por ello, el aseguramiento o asesoramiento del auditor interno en la gestión del riesgo de conducta y de los principios de ESG, así como el aprovechamiento de las sinergias entre ambos, resultará altamente beneficioso para la organización.

Adicionalmente, y de forma específica, empiezan a existir exigencias regulatorias en materia de conducta tanto en la normativa española, como en la futura normativa[14] europea, mostrando la unión entre ambos conceptos y reforzando la idea de la gestión del riesgo de conducta como una palanca sobre ESG. Como ejemplo, en la normativa europea se menciona:

- Considerando 27: mediante el desarrollo del proceso de diligencia debida detectar, prevenir, mitigar y reparar los principales efectos negativos reales y potenciales relacionados con sus actividades y que determina cómo subsanan esos efectos, que son directamente causados por la empresa, aquellos a los que contribuye y/o los que, de alguna manera, están relacionados con su cadena de valor.
- Considerando 39: que regulará que las normas de presentación de información en materia de sostenibilidad tengan en cuenta los principios y marcos reconocidos internacionalmente sobre conducta empresarial responsable, responsabilidad social de las empresas y desarrollo sostenible, incluidos los Objetivos de Desarrollo Sostenible de las Naciones Unidas, los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas, las Líneas Directrices para Empresas Multinacionales de la OCDE, la Guía sobre Diligencia Debida para una Conducta Empresarial Responsable de la OCDE y las directrices sectoriales conexas, el Pacto Mundial de las Naciones Unidas, la Declaración Tripartita de Principios de la organización internacional del Trabajo sobre Empresas Multinacionales y Política Social, la norma ISO 26000 sobre responsabilidad social y los Principios para la Inversión Responsable de las Naciones Unidas.

Algunos indicadores que los auditores internos pueden considerar en sus revisiones, y

La "G" de ESG se refiere al Gobierno de las organizaciones, donde la gestión adecuada del riesgo de conducta es un elemento clave.

14. En el momento de redacción de este documento se habla del futuro reglamento de sostenibilidad: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0189

que relacionan la gestión del riesgo de conducta con factores ESG son:

- Existencia de estándares o normativa interna que regule el riesgo de conducta vinculado a criterios ESG.
- Desarrollo del código de conducta que dé cobertura y recoja expresamente los criterios ESG y, además, incluya ejemplos de conductas y comportamientos acordes a los mismos.
- Comunicaciones recibidas en el canal de denuncias vinculadas al incumplimiento de normas o principios ESG.

La creación y publicación transparente de estos riesgos de conducta en los informes de sostenibilidad es recomendable.

La buena comunicación, influye en la efectividad del desarrollo de los criterios en la empresa, potenciando su transversalidad y gestión coordinada entre varias áreas, en su caso. Este método empleado para los criterios de sostenibilidad ayudará también a la comunicación de los riesgos de conducta a los diferentes *stakeholders* o grupos de interés. Se destacan a continuación alguno de ellos:

- Se debe implementar un proceso efectivo de reporte y comunicación de los riesgos de conducta a la alta dirección, a los órganos de gobierno, y también a los responsables de Sostenibilidad. Auditoría Interna comprobará la existencia y efectividad de éstos.
- Además de este reporte periódico interno, conviene definir el proceso de comunicación interna a los responsables de gestión de los riesgos para la ejecución y mejora continua de la gestión de los principios ESG y su impacto en el riesgo de conducta.
- La creación y publicación transparente de estos riesgos de conducta en los informes de sostenibilidad es recomendable y se considera beneficioso para la transparencia en todas las industrias, como generador de beneficio para el valor de la propia organización en la sociedad en la que opere, independientemente de que se trate de empresas cotizadas o no, multinacionales o empresas locales.
- La publicación y seguimiento de aceptación en web y encuestas periódicas a los grupos de interés posibilitará esa mejora continua y desarrollo mutuo.

La especialización y formación de profesionales de auditoría interna especializados en este ámbito, hasta hace poco desconocido, será muy interesante para poder generar valor en la organización.

LECCIONES APRENDIDAS TRAS ESCÁNDALOS DE CONDUCTA POCO ÉTICA

Como se ha visto, el papel de **Auditoría Interna en el aseguramiento y/o asesoramiento del riesgo de conducta tiene numerosas ventajas para la organización.**

No solo eso, a lo largo de la historia se ha visto que la conducta no ética y la no detección o comunicación de esta, por parte de los responsables de una organización, incluidos la Tercera Línea, ha acarreado importantes impactos económicos, reputacionales, e incluso alguna crisis más allá de una organización concreta. En este sentido, se señalan algunas lecciones aprendidas tras escándalos y crisis causadas por conductas poco éticas:

- Resulta necesario integrar la ética en la estrategia y cultura corporativa, como palan-

ca de cambio progresivo de las organizaciones.

- Las quiebras y conductas inadecuadas del pasado han ayudado a la concienciación social, y a que exista una tolerancia cada vez más limitada a los casos de corrupción o mala praxis corporativas, eliminando del tejido empresarial, o sancionando con la quiebra, a organizaciones que no han cumplido con los criterios éticos.
- El buen Gobierno Corporativo es otra de las lecciones aprendidas, destacando la importancia de que el Consejo de Administración inspire, cumpla y se esfuerce por hacer cumplir.
- El valor de la independencia de los auditores internos se ha visto reforzado tras los escándalos de conducta poco ética.
- De igual forma, se ha desarrollado la necesidad de crear dentro de las organizaciones, órganos de control que supervisen la actividad empresarial de forma efectiva, y que gocen de autonomía e independencia (por ejemplo, función de *Compliance* u otras áreas de control interno).
- El incremento de la importancia sobre la transparencia y la adecuada gestión de conflictos de interés de la empresa, sus profesionales y sus clientes, así como entre los mismos.
- La necesidad de crear reglas transnacionales que ayuden a impulsar a gran escala los comportamientos éticos y tolerancia cero a la corrupción, con el incremento de normativa extraterritorial como FCPA o SAPIN II[15].
- Los criterios ESG también están ayudando a revisar la cultura corporativa y a enfocar a la organización para que no solo compute la cuenta de resultados económicos en la toma de decisiones.

Se requieren reglas transnacionales que impulsen comportamientos éticos y tolerancia cero ante la corrupción.

UN EJEMPLO DE LOS BENEFICIOS DE LA GESTIÓN DEL RIESGO DE CONDUCTA Y EL PAPEL DE AUDITORÍA INTERNA: LA INNOVACIÓN

El riesgo de conducta vinculado a la innovación cobra cada día más relevancia para la labor del auditor interno debido al avance en los desarrollos tecnológicos y su creciente aplicación en la mejora de productos y servicios, así como en el entorno empresarial. Una adecuada gestión de este riesgo potenciará la estrategia de innovación de la compañía y su crecimiento y competitividad en el sector y geografías en las que desarrolle su actividad.

El auditor interno puede apoyarse en diferentes guías emitidas por diversos organismos supervisores y expertos que ayudarán a reforzar el Marco de Gestión del Riesgo de Conducta en innovación[16].

15. FCPA, Foreign Corrupt Practices Act, o Ley de Prácticas Corruptas en el Extranjero de los Estados Unidos. SAPIN II, ley francesa basada en la FCPA y la UK Bribery Act, que tiene como objetivo prevenir y detectar los sobornos y la corrupción.
16. Entre otros; Libro Blanco de la Inteligencia Artificial, futuro reglamento de Inteligencia Artificial, Guías emitidas por la Agencia Española de Protección de Datos AEPD, relativas a medidas de seguridad de la información, privacidad en el diseño y por defecto, gestión de riesgos vinculados a la protección de datos, Reglamento Europeo de Protección de Datos.

Una innovación corporativa responsable debe preserva la privacidad y seguridad de la información.

Una innovación corporativa responsable, que valore los impactos sociales, medioambientales y que promueva la transparencia y responsabilidad de la gestión de los datos de los usuarios, su privacidad y la seguridad de la información, es fundamental y estratégicamente necesaria. En especial en sectores como el tecnológico o el sanitario, donde cada día cobra mayor relevancia la asignación adecuada de recursos, la eficiencia, la colaboración público-privada y el desarrollo de inteligencia artificial aplicada a la mejora en la predicción o prevención de la salud.

Ejemplo: Riesgo de conducta y desarrollo de Inteligencia Artificial

Incluso organizaciones maduras y muy acostumbradas a innovar deben considerar estos riesgos. Un ejemplo es lo que sucedió a una conocida compañía tecnológica, cuando introdujo un software de Inteligencia Artificial con capacidades de *machine learning* en su proceso de selección de personal.

La compañía empezó a utilizar en 2014 un software que debía simplificar y agilizar la selección de programadores, para ello revisaba a los actuales candidatos teniendo en cuenta las características de los candidatos presentados en el pasado. Pero dado que históricamente la mayoría de los candidatos había sido hombres, se generó un sesgo en contra de las candidatas que no fue detectado hasta un año después. Esto no solo fue embarazoso para la compañía, sino que llevó a tener que desechar toda la inversión realizada en este sistema.

¿Cómo llegó a esta situación la compañía? En primer lugar, porque no consideró que una máquina que tome decisiones está afectada también por el riesgo de conducta. Derivado de ello, no tomó medidas para detectar la presencia de conductas contrarias a su misión y visión, como en este caso. En segundo lugar, no se dotó de mecanismos para auditar el proceso de innovación que asegurase la mitigación de los riesgos asociados al mismo.

Algunos indicadores que los auditores internos pueden considerar en sus revisiones, y que relacionan la gestión del riesgo de conducta con la innovación son:

- Existencia de estándares o normativa interna que regule el riesgo de conducta vinculado a la innovación.
- Evaluación periódica del desarrollo de proyectos de innovación de la organización.

  Inclusión en el código de conducta de las consideraciones y principios en materia de innovación ética. Inclusión de ejemplos de conductas y comportamientos acordes a los mismos.
- Comunicaciones recibidas en el canal de denuncias vinculadas al incumplimiento de normas de conducta en desarrollos tecnológicos e innovación.
- Seguimiento del clima interno y conocimiento de los profesionales sobre los riesgos de conducta vinculados a innovación.

Bibliografía

THE INSTITUTE OF INTERNAL AUDITORS GLOBAL

- *Practice Guide: Auditing Culture,* 2019.
- *Practice Guide: Auditing Conduct Risk,* 2020.
- *Marco Profesional para la Práctica Profesional de Auditoría Interna (MIPP).* 2017.

INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

- LA FÁBRICA DE PENSAMIENTO. *Definición e implantación de Apetito de Riesgo,* 2012
- *El Modelo de las Tres Líneas, nuevo marco teórico para auditores internos,* 2020
- LA FÁBRICA DE PENSAMIENTO. *Auditoría Interna y los aspectos ESG,* 2021.
- LA FÁBRICA DE PENSAMIENTO. *Auditoría Interna y la ética empresarial,* 2022.
- LA FÁBRICA DE PENSAMIENTO. *Auditoría Interna de la Cultura Corporativa,* 2023.

THE INSTITUTE OF INTERNAL AUDITORS AUSTRALIA

- *Managing Culture - A good practice guide,* 2017.
- *Auditing Risk Culture: A practical guide,* 2021.

INFORMES Y ESTUDIOS

- Management Solutions, *Riesgo de Conducta. Tendencias y desafíos para el sector financiero,* 2016.
- Management Solutions, *Confianza y reputación: gestión activa del riesgo reputacional,* 2021.
- Harvard Business Review. *Reputation and Risks,* 2007.
- Conglomerado Financiero Banco Nacional de Costa Rica, Proyecto Controles Blandos, 2022.

BLOGS, ARTÍCULOS Y OTROS ENLACES DE INTERÉS

- Vilches abogados. Hernandez-vilches.com, *Buena conducta cívica, ¿qué es?*
- Psicología y Mente. psicologiaymente.com. Los 15 tipos de conductas, y sus características, https://psicologiaymente.com/psicologia/tipos-de-conductas
- Wikipedia, la enciclopedia libre, Mal comportamiento, https://es.wikipedia.org/wiki/Mal_comportamiento
- Elderecho.com. Cómo hacer un código de conducta de la empresa sin limitar derechos de los empleados, https://elderecho.com/guia-para-elaborar-un-codigo-de-conducta-de-la-empresa
- Chat GPT. Consultado en marzo 2023 Versión. Free Research Preview

Anexo-Programa de trabajo para auditar el marco de gestión del riesgo de conducta

FACTOR DE RIESGO	CÓMO AUDITARLO
No consideración del riesgo de conducta en el marco de apetito de riesgo de la compañía	• Comprobar que el marco de apetito de riesgo de la organización considera el riesgo de conducta. • Verificar que el apetito de riesgo de conducta está aprobado por las instancias pertinentes. • Verificar que el apetito de riesgo de conducta está alineado con el apetito de riesgo general de la compañía: - que se realiza un seguimiento periódico del mismo, analizando eventos en materia de conducta acontecidos, rotura de umbrales si los hay, etc. - se considera el riesgo de conducta en las actualizaciones periódicas del marco de apetito de riesgo de la organización.
No se identifican y/o valoran adecuadamente todos los riesgos de conducta que puedan afectar a la compañía.	• Comprobar que los riesgos de conducta han sido identificados en la organización conforme a la regulación, normativa interna y buenas prácticas sectoriales; se han considerado las novedades al respecto previstas; nuevos riesgos emergentes y riesgos potenciales. • Asegurar la consideración de todos los grupos de interés para la identificación de los riesgos de conducta de la organización. • Revisar el mapa de riesgos de conducta de la organización, verificando que los riesgos inherentes, controles mitigantes y riesgo residual se han identificado y valorado según la metodología definida en la compañía. • Comprobar que se han tenido en cuenta las materializaciones previas del riesgo para la valoración del riesgo de conducta. • Asegurar que la compañía focaliza esfuerzos y/o recursos en los riesgos de conducta más relevantes *(risk based approach).*
La alta dirección de la compañía no promueve de forma efectiva una cultura general de cumplimiento de las obligaciones de conducta.	• Verificar si están definidos, por parte de la alta dirección, los valores, la cultura y los comportamientos deseados en la organización. Comprobar si existe un código de conducta o pautas de conducta definidas y claras para los distintos grupos de interés. • Verificar que la alta dirección divulga estas pautas o código de conducta, y se preocupa porque los empleados y otros grupos de interés entiendan sus responsabilidades en materia de conducta, tanto con campañas de comunicación y sensibilización, como a través de la definición de políticas corporativas. • Determinar si existe alineación entre los valores clave, comportamientos y la toma de decisiones. Analizar que las directrices de la alta dirección no contradicen ninguno de los principios del código de conducta, ni de la regulación aplicable. • Determinar si existe un reporte oportuno y completo a la alta dirección y órganos de gobierno sobre la gestión del riesgo de conducta.

FACTOR DE RIESGO	CÓMO AUDITARLO
Inexistencia de un marco efectivo de gestión del riesgo de conducta en la compañía.	• Verificar si existe un código de conducta o pautas de conducta definidas y claras para los distintos grupos de interés. • Determinar si existen políticas y procedimientos asociadas a la cultura y cumplimiento del código de conducta, que desarrollen con más detalle las pautas y principios del código de conducta. • Verificar que el resto de normativa interna de la organización está alineada con las pautas y principios del código de conducta. • Verificar la adhesión de empleados al código de conducta, el conocimiento de los valores y principios éticos por parte de estos. • Verificar que el mapa de riesgos de la organización contempla los riesgos de conducta. • Determinar si existe un diagnóstico de la cultura e indicadores asociados con el riesgo de conducta dentro de la organización. • Verificar si en los procesos de admisión de riesgos se contempla, como uno más, el riesgo de conducta y se definen los controles para su mitigación. • Analizar si el proceso de rendición de cuentas hacia los órganos de gobierno incluye el riesgo de conducta. • Concluir sobre la existencia de un programa de formación y sensibilización para empleados, que sensibilice sobre el riesgo de conducta.
Las personas que integran la organización no están implicadas en la gestión del riesgo de conducta. La estructura organizativa de la compañía no contempla una adecuada asignación de roles y responsabilidades en relación con el riesgo de conducta.	• Comprobar que en la organización existe una adecuada estructura organizativa, una clara asignación de roles y responsabilidades (incluidos los órganos de gobierno y la alta dirección), y que ésta contempla las responsabilidades individualizadas (individual accountability) en materia de conducta. • Asegurar que la estructura organizativa tiene en cuenta el Modelo de las Tres Líneas que permite una adecuada separación de funciones entre propietarios/gestores de riesgos y supervisores de riesgos de conducta. Verificar la existencia e idoneidad de funciones y competencias de un responsable u órgano de control del riesgo de conducta. Asegurar que, entre sus funciones, se ocupa de velar porque los riesgos se gestionen de acuerdo con el apetito de riesgo y el fomento de una sólida cultura de riesgos en toda nuestra organización.
Controles ineficientes y/o insuficientes para la adecuada mitigación de los riesgos de conducta	Controles generales • Comprobar el diseño del código de conducta o pautas de conducta de la organización, para determinar si se corresponde con las necesidades de la organización. Verificar que se consideran los riesgos de conducta más relevantes para la organización y comprobar su actualización periódica. • Realizar una comparativa con otros códigos de conducta de entidades comparables para determinar si se incluyen todas las secciones y compromisos habitualmente detallados en estos. • Verificar si para la gestión del canal de denuncias de la entidad, existe un protocolo y una política formal, conforme con la normativa interna, la regulación y las buenas prácticas. • Comprobar la efectividad de los métodos establecidos para su cumplimiento, entre otros la difusión y el desarrollo de procedimientos que detallan la implantación de los principios recogidos en el código. • Comprobar el desarrollo de métricas que soporten el seguimiento y mejora continua en la gestión del código de conducta y el canal de denuncias. • Obtener copia de las comunicaciones realizadas para dar a conocer el compromiso de la dirección con la no represalia al denunciante • Verificar los mecanismos existentes (seguimientos, entrevistas, revisión de evaluaciones de desempeño, etc..) que se han aplicado para asegurar la no represalia. • Verificar la existencia de un adecuado esquema de sanciones, para conductas no deseadas, el cual ha sido aprobado al nivel apropiado. • Verificar, mediante la revisión de la documentación soporte de una muestra de casos, el cumplimiento del proceso de denuncia y de sanciones aprobado.

FACTOR DE RIESGO	CÓMO AUDITARLO
	Controles específicos • Asegurar que la compañía enfoca sus esfuerzos y recursos para mitigar con controles adecuados los riesgos de conducta más relevantes. Para ello, y en función de cada compañía, evaluar el diseño y efectividad de los controles sobre los riesgos más relevantes en materia de conducta con los distintos grupos de interés.
Inadecuada supervisión y monitorización de conductas inapropiadas.	• Análisis de los indicadores de monitorización del riesgo de conducta; revisión de las variables y metodologías para su cálculo, con el objeto de determinar que los mismos son apropiados para monitorizar el riesgo de conducta. • Revisión de los procedimientos y documentación relacionada con la monitorización y supervisión de riesgos, para concluir sobre oportunidad e integridad de dicha supervisión. • Verificar la ejecución de los planes de remediación establecidos en relación con el riesgo de conducta: acciones, responsables, plazos y resultados esperados; revisando la documentación soporte de la ejecución.
Inadecuada comunicación a los órganos de gobierno y/o alta dirección de los aspectos relacionados con la gestión del riesgo de conducta. Incorrecta implementación de las decisiones adoptadas tras dicho *reporting*.	• Solicitar los resultados de los controles que mitigan el riesgo de conducta, eventos acaecidos, actas de comités sancionadores, etc., para asegurar que se ha comunicado al nivel adecuado cualquier aspecto relevante relacionado con el riesgo de conducta. • Verificar que el *reporting* a los órganos de gobierno y/o alta dirección sobre el riesgo de conducta cubre todas las áreas de riesgo significativas y permite una visión completa del riesgo de conducta. • Verificar que las decisiones tomadas por la alta dirección y/u órganos de gobierno son transmitidas a los responsables de implementarlas. • Revisar actas de la alta dirección y/o órganos de gobierno para verificar que se realiza un seguimiento adecuado de las decisiones tomadas por ellos, en materia de conducta.
Los diferentes grupos de interés desconocen, por falta de formación o inadecuada divulgación, los riesgos y oportunidades a los que hace frente la organización en materia de conducta.	• Asegurar que la compañía dispone de programas de formación y/o sensibilización sobre el riesgo de conducta. • Verificar la impartición de formación/sensibilización. Revisar la integridad de los colectivos que conforman el perímetro de destinatarios de los programas de formación. • Verificar la aprobación de los programas de formación por las instancias adecuadas, de acuerdo con las facultades establecidas al respecto en la organización. • Asegurar que los contenidos y el diseño de los programas de formación resultan adecuados para promocionar los comportamientos esperados por los distintos destinatarios. Verificar la graduación y adaptación de los contenidos a los destinatarios / grupos de interés, poniendo mayor énfasis en aquellos más expuestos al riesgo de conducta. • Comprobar la actualización de los programas de formación con la periodicidad establecida y/o si acontecen eventos que lo hacen necesario.
El marco de gestión del riesgo de conducta no se encuentra actualizado	• Comprobar la existencia y efectividad de un programa de revisión continua del marco de gestión del riesgo de conducta. • Asegurar la adecuación de los inputs empleados en la actualización y mejora continua del marco de gestión del riesgo de conducta (novedades legislativas, procedimentales, culturales, técnicas, informáticas, etc… así como el aprendizaje interno y retroalimentación: resultados de los controles internos y las revisiones periódicas).

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA DE LA CULTURA CORPORATIVA

Este documento tiene como objetivo impulsar el entendimiento de la cultura corporativa como un elemento más del universo auditable y, con un enfoque práctico, servir como guía para utilizar y adaptar a las características y naturalezas propias de sus organizaciones.

NUEVAS FORMAS DE TRABAJO EN REMOTO DE AUDITORÍA INTERNA

Esta guía de buenas prácticas analiza todos los aspectos necesarios para desarrollar el trabajo en remoto en la Dirección de Auditoría Interna, incluyendo sus implicaciones en las relaciones con los stakeholders y los retos y limitaciones –y cómo hacerles frente– de esta forma de trabajar.

AUDITORÍA INTERNA DE LA GESTIÓN DE CRISIS Y RESILIENCIA DEL NEGOCIO

Abarca el rol de Auditoría Interna en la supervisión de los mecanismos de gestión de crisis y la resiliencia del negocio, así como el papel que asume en la fase previa, durante y después de que se produzca una crisis, e identifica las mejores prácticas relacionadas con la actuación de Auditoría Interna en este tipo de trabajos.

GESTIÓN ESTRATÉGICA DEL TALENTO EN AUDITORÍA INTERNA

La gestión del talento es fundamental para la consecución de los objetivos de la compañía y de cada uno de los departamentos que la integran. Este documento abarca distintas dimensiones de la gestión del tallento desde la óptica de la consecución de los objetivos de la Dirección de Auditoría Interna y en el ámbito del *Marco Internacional para la Práctica Profesional de la Auditoría Interna*.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

La gestión del riesgo de conducta es esencial para mantener la integridad y reputación de una organización. Este documento analiza el papel de Auditoría Interna en este proceso al evaluar los procesos de identificación y evaluación, valorar la efectividad de los controles establecidos y ofrecer recomendaciones para fortalecer el sistema de gestión del riesgo de conducta.

40 años Instituto de Auditores Internos de España
The Institute of Internal Auditors