INSTITUTO DOMINICANO PARA LA CALIDAD

NORDOM ISO 37301:2021

Edición: 1ra.
Fecha de Aprobación: 2022-02-24
Coordinadora: Mercedes Suero Casilla

Norma Dominicana

Sistemas de gestión del cumplimiento — Requisitos con orientación para su uso.

CORRESPONDENCIA. Esta norma es una adopción idéntica de la norma internacional **ISO 37301:2021 Sistemas de gestión del cumplimiento — Requisitos con orientación para su uso.**

ICS: 03.100.01; 03.100.02; 03.100.70
Resolución: CTE-14-2022
Año de Publicación: 2022
Pág. 56 **Grupo** M

Editada e impresa por INDOCAL www.indocal.gob.do

Prefacio

EL Instituto Dominicano para la Calidad (INDOCAL) es el organismo oficial que tiene a su cargo el estudio y preparación de las Normas Dominicanas (NORDOM) a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO), Comisión Internacional de Electrotécnica (IEC), Comisión del Codex Alimentarius, y de la Comisión Panamericana de Normas Técnicas (COPANT), representando a la República Dominicana ante estos Organismos.

La Norma **NORDOM ISO 37301:2021 Sistemas de gestión del cumplimiento — Requisitos con orientación para su uso,** ha sido preparada por la Dirección de Normalización del Instituto Dominicano para la Calidad (INDOCAL).

La adopción de esta norma fue motivada a lo interno de la Dirección de Normalización, para que esté disponible al público para utilizarla como marco de referencia en la elaboración y aplicación de los procedimientos de evaluación de la conformidad en cualquier organización.

Ha sido estudiada por el Comité Técnico de adopción **03-3 Sistema de gestión de calidad**, en fecha **14 de septiembre 2021,** y publicada en un periódico de circulación nacional en fecha **23 de septiembre 2021**, para conocimiento de su adopción idéntica por todas las partes interesadas.

Finalmente, el INDOCAL solicitó a la Comisión Técnica de Expertos del CODOCA, a través de la Secretaria General del CODOCA, su oficialización como una Norma Dominicana

Esta es una adopción idéntica de la norma Internacional **ISO 37301:2021 Sistemas de gestión del cumplimiento — Requisitos con orientación para su uso,** desarrollada y publicada por el comité internacional de la ISO.

En el proceso de adopción formaron parte del Comité Técnico, las siguientes personas:

PARTICIPANTES:	**REPRESENTANTES DE:**
Julia Rodríguez	Depto. Normas de Servicios
Claudia Alonzo	Depto. Normas de Servicios
Karilyn Rodriguez	Direccion de Evaluación de la conformidad
Marlen Martinez	Direccion de Evaluación de la conformidad
Noemí Frías	Direccion de Evaluación de la conformidad
Fulgencio Batista	Direccion de Metrología
Rosa Asencio	Depto. Normas de Alimentos y Salud
Fredesvinda Selmo	Depto. Normas de Alimentos y Salud
Jose Guarino Contreras	Depto. Normas de Alimentos y Salud
Angela Urbaez	Depto. Normas de Alimentos y Salud
Modesta Acosta	Depto. Normas de Alimentos y Salud
Carmen Brito	Depto. Normas de Alimentos y Salud
Fabio Terrero	Depto. Normas de Ingeniería y Ciencias
Indira Diaz	Depto. Normas de Ingeniería y Ciencias
Esperanza Gonzales	Depto. Normas de Ingeniería y Ciencias
Mercedes Suero	Depto. Normas de Ingeniería y Ciencias

NORMA INTERNACIONAL

ISO 37301

Traducción oficial
Official translation
Traduction officielle

Primera edición
2021-04

Sistemas de gestión del *compliance* — Requisitos con orientación para su uso

Compliance management systems — Requirements with guidance for use

Systèmes de management de la conformité — Exigences et recommandations pour la mise en oeuvre

Publicado por la Secretaría Central de ISO en Ginebra, Suiza, como traducción oficial en español avalada por el *Grupo de Trabajo Spanish Translation Task Force (STTF)*, que ha certificado la conformidad en relación con las versiones inglesa y francesa.

Número de referencia
ISO 37301:2021 (traducción oficial)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Ginebra, Suiza
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Publicada en Suiza

Versión española publicada en 2021

Índice

Página

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase www.iso.org/directives).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de alguno o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de este documento se indicarán en la Introducción y/o en la lista ISO de declaraciones de patente recibidas (véase www.iso.org/patents).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html.

Este documento ha sido elaborado por el Comité Técnico ISO/TC 309, *Gobernanza de las organizaciones*.

Esta primera edición de la Norma ISO 37301 anula y sustituye a la Norma ISO 19600:2014, que ha sido revisada técnicamente.

Los principales cambios respecto de la Norma ISO 19600:2014 son los siguientes:

— este documento contiene ahora requisitos y orientación adicional basada en los mismos;

— este documento sigue los requisitos de ISO para una estructura armonizada para las normas de sistemas de gestión.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En www.iso.org/members.html se puede encontrar un listado completo de estos organismos.

Prólogo de la versión en español

Este documento ha sido traducido por el Grupo de Trabajo *Spanish Translation Task Force* (STTF) del Comité Técnico ISO/TC 309, *Gobernanza de las organizaciones*, en el que participan representantes de los organismos nacionales de normalización y representantes del sector empresarial de los siguientes países:

Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Guatemala, Panamá, Perú, Uruguay.

Esta traducción es parte del resultado del trabajo que el Grupo ISO/TC 309/STTF, viene desarrollando desde su creación en el año 2021 para lograr la unificación de la terminología en lengua española en el ámbito del *compliance*.

Introducción

Las organizaciones que pretenden ser exitosas a largo plazo necesitan establecer y mantener una cultura de cumplimiento, considerando las necesidades y expectativas de las partes interesadas. El *compliance*, por tanto, no sólo es la base, sino también una oportunidad para una organización exitosa y sostenible.

El *compliance* es un proceso continuo y el resultado de que una organización cumpla con sus obligaciones. El *compliance* se hace sostenible a través de su integración en la cultura de una organización y en el comportamiento y la actitud de las personas que trabajan para ella. Mientras mantenga su independencia, es preferible que la gestión del *compliance* esté integrada con los demás procesos de gestión de la organización y en sus requisitos y procedimientos operacionales.

Un sistema de gestión del *compliance* eficaz y que abarque a toda la organización permite que la organización demuestre su compromiso de cumplir con las leyes, requisitos regulatorios, códigos de la industria y las normas de la organización pertinentes, así como con las normas de buena gobernanza, las mejores prácticas generalmente aceptadas, la ética y las expectativas de la comunidad.

El enfoque de una organización para el *compliance* consiste en que los líderes apliquen los valores fundamentales y las normas generalmente aceptadas de buena gobernanza, de ética y de la comunidad. Incorporar el *compliance* en el comportamiento de las personas que trabajan para una organización depende, sobre todo, de sus líderes, en todos los niveles, y de que existan unos valores claros en la organización, así como de la aceptación e implementación de medidas que promuevan una conducta de cumplimiento. Si eso no sucede así en todos los niveles de la organización, existe riesgo de no cumplimiento de *compliance*.

En varias jurisdicciones, a la hora de determinar la sanción a imponer por contravenir las leyes pertinentes, los tribunales han tenido en cuenta el compromiso de cumplimiento de una organización a través de su sistema de gestión del *compliance*. Por ello, los organismos regulatorios y judiciales también se pueden beneficiar de tener este documento como punto de referencia.

Las organizaciones están cada vez más convencidas de que si aplican valores vinculantes y una gestión adecuada del *compliance*, pueden salvaguardar su integridad y evitar o minimizar los no cumplimientos de *compliance* con las obligaciones de *compliance* de la organización. Integridad y un *compliance* eficaz son, por tanto, elementos clave para llevar una buena y diligente gestión. El *compliance* también contribuye al comportamiento socialmente responsable de las organizaciones.

Uno de los objetivos de este documento es ayudar a las organizaciones a desarrollar y difundir una cultura positiva de *compliance*, teniendo en cuenta que una gestión eficaz y sólida de los riesgos relacionados con *compliance* debería considerarse como una oportunidad para perseguir y aprovechar, debido a los diversos beneficios que proporciona a la organización, como, por ejemplo:

— mejorar las oportunidades de negocio y la sostenibilidad;

— proteger y mejorar la reputación y la credibilidad de una organización;

— tener en cuenta las expectativas de las partes interesadas;

— demostrar el compromiso de la organización en la gestión de sus riesgos de *compliance* de forma eficaz y eficiente;

— aumentar la confianza de terceras partes en la capacidad de la organización para lograr un éxito sostenido;

— minimizar el riesgo de que se produzca una infracción que conlleve costos y daños a la reputación.

Este documento especifica requisitos y, además, proporciona una guía de los sistemas de gestión del *compliance* y prácticas recomendadas. Se pretende que tanto los requisitos como la guía que proporciona este documento sean adaptables, y su aplicación puede diferir dependiendo del tamaño y el nivel de

madurez del sistema de gestión del *compliance* de una organización y del contexto, la naturaleza y la complejidad de las actividades y los objetivos de la organización.

Este documento es adecuado para mejorar los requisitos relacionados con *compliance* en otros sistemas de gestión y para ayudar a la organización a que mejore la gestión global de todas sus obligaciones de *compliance*.

La Figura 1 proporciona una visión general de los elementos comunes de un sistema de gestión del *compliance*.

Figura 1 — Elementos de un sistema de gestión del *compliance*

En este documento se utilizan las siguientes formas verbales:

— “debe” indica un requisito;

— “debería” indica una recomendación;

— “puede” indica un permiso, una posibilidad o una capacidad.

La información indicada como “NOTA” se presenta a modo de orientación para la comprensión o clarificación del requisito correspondiente.

El Anexo A proporciona orientación para el uso de este documento.

Sistemas de gestión del *compliance* — Requisitos con orientación para su uso

1 Objeto y campo de aplicación

Este documento especifica los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión del *compliance* eficaz dentro de una organización.

Este documento es aplicable a toda clase de organizaciones independientemente del tipo, tamaño y naturaleza de la actividad, así como a organizaciones del sector público, privado o sin fines de lucro.

Todos los requisitos especificados en este documento que hagan referencia a un órgano de gobierno se aplican a la alta dirección en aquellos casos en los que una organización no tenga un órgano de gobierno como función independiente.

2 Referencias normativas

No existen referencias normativas en este documento.

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes.

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

— Plataforma de búsqueda en línea de ISO: disponible en https://www.iso.org/obp

— Electropedia de IEC: disponible en https://www.electropedia.org/

3.1
organización
persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus *objetivos* (3.6)

Nota 1 a la entrada: El concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización benéfica o institución, o una parte o combinación de estas, ya estén constituidas o no, públicas o privadas.

Nota 2 a la entrada: En el caso de que la organización forme parte de una entidad más grande, el término "organización" se refiere solo a aquella parte de la organización que está dentro del alcance del sistema de gestión.

3.2
parte interesada
persona u *organización* (3.1) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad

3.3
alta dirección
persona o grupo de personas que dirigen y controlan una *organización* (3.1) al más alto nivel

Nota 1 a la entrada: La alta dirección tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización.

Nota 2 a la entrada: Si el alcance del *sistema de gestión* (3.4) comprende solo una parte de una organización, entonces alta dirección se refiere a quienes dirigen y controlan esa parte de la organización.

Nota 3 a la entrada: Para los fines de este documento, el término "alta dirección" se refiere al más alto nivel de la dirección ejecutiva.

3.4
sistema de gestión
conjunto de elementos de una *organización* (3.1) interrelacionados o que interactúan para establecer *políticas* (3.5), *objetivos* (3.6) y *procesos* (3.8) para lograr esos objetivos

Nota 1 a la entrada: Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

Nota 2 a la entrada: Los elementos del sistema de gestión incluyen la estructura de la organización, los roles y las responsabilidades, la planificación y la operación.

3.5
política
intenciones y dirección de una *organización* (3.1) como las expresa formalmente su *alta dirección* (3.3)

Nota 1 a la entrada: La política también puede ser expresada formalmente por el *órgano de gobierno* (3.21) de una *organización* (3.1).

3.6
objetivo
resultado a lograr

Nota 1 a la entrada: Un objetivo puede ser estratégico, táctico u operativo.

Nota 2 a la entrada: Los objetivos pueden referirse a diferentes disciplinas (como las finanzas, la seguridad y salud y el medio ambiente). Pueden ser, por ejemplo, objetivos que abarquen a toda la organización o específicos para un proyecto, producto, servicio o *proceso* (3.8).

Nota 3 a la entrada: Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de *compliance* (3.26), o mediante el uso de términos con un significado similar (por ejemplo, finalidad o meta).

Nota 4 a la entrada: En el contexto de *sistemas de gestión* (3.4) del *compliance*, *la organización* (3.1) establece los objetivos de *compliance*, en concordancia con la *política* (3.5) de *compliance,* para lograr resultados específicos.

3.7
riesgo
efecto de la incertidumbre sobre los *objetivos* (3.6)

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positiva o negativa.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad.

Nota 3 a la entrada: Con frecuencia el riesgo se caracteriza por referencia a "eventos" potenciales (como se define en la Guía ISO 73) y "consecuencias" (como se define en la Guía ISO 73) , o a una combinación de estos.

Nota 4 a la entrada: Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios de las circunstancias) y la "probabilidad" (como se define en la Guía ISO 73) asociada de que ocurra.

3.8
proceso
conjunto de actividades interrelacionadas o que interactúan, que emplean o transforman elementos de entrada para obtener resultados

Nota 1 a la entrada: Que el resultado de un proceso se denomine salida, producto o servicio depende del contexto de referencia.

3.9
competencia
capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos

3.10
información documentada
información que una *organización* (3.1) tiene que controlar y mantener, y el medio en el que está contenida

Nota 1 a la entrada: La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

Nota 2 a la entrada: La información documentada puede hacer referencia a:

— el *sistema de gestión* (3.4), incluidos los *procesos* (3.8) relacionados;

— la información creada para que la organización opere (documentación);

— la evidencia de los resultados alcanzados (registros).

3.11
desempeño
resultado medible

Nota 1 a la entrada: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño se puede relacionar con actividades de gestión, *procesos* (3.8), productos, servicios, sistemas u *organizaciones* (3.1).

3.12
mejora continua
actividad recurrente para mejorar el *desempeño* (3.11)

3.13
eficacia
grado en el que se realizan las actividades planificadas y se logran los resultados planificados

3.14
requisito
necesidad o expectativa establecida, generalmente implícita u obligatoria

Nota 1 a la entrada: "Generalmente implícita" significa que es una costumbre o práctica común para la *organización* (3.1) y para las *partes interesadas* (3.2), que la necesidad o expectativa que se considera está implícita.

Nota 2 a la entrada: Un requisito especificado es el que está declarado, por ejemplo, en *información documentada* (3.10).

3.15
conformidad
cumplimiento de un *requisito* (3.14)

3.16
no conformidad
incumplimiento de un *requisito* (3.14)

Nota 1 a la entrada: Una no conformidad no es necesariamente un *no cumplimiento de compliance* (3.27).

3.17
acción correctiva
acción para eliminar las causas de una *no conformidad* (3.16) y evitar que vuelva a ocurrir

3.18
auditoría
proceso (3.8) sistemático e independiente para obtener las evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría

Nota 1 a la entrada: Una auditoría puede ser interna (de primera parte), o externa (de segunda o *tercera parte*, (3.30)), y puede ser combinada (combinando dos o más disciplinas).

Nota 2 a la entrada: Una auditoría interna es la que realiza la propia *organización* (3.1) o una parte externa en su nombre.

Nota 3 a la entrada: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

Nota 4 a la entrada: La independencia se puede demostrar por la ausencia de dependencia de la actividad objeto de la auditoría o por la ausencia de parcialidad y de conflicto de intereses.

3.19
medición
proceso (3.8) para determinar un valor

3.20
seguimiento
determinación del estado de un sistema, un *proceso* (3.8) o una actividad

Nota 1 a la entrada: Para determinar el estado puede ser necesario verificar, supervisar u observar de forma crítica.

3.21
órgano de gobierno
persona o grupo de personas que tienen la última responsabilidad y autoridad en las actividades, gobierno y *políticas* (3.5) de una *organización* (3.1) ante quienes la *alta dirección* (3.3) informa y rinde cuentas

Nota 1 a la entrada: No todas las organizaciones, particularmente las organizaciones pequeñas, tendrán un órgano de gobierno aparte de la alta dirección.

Nota 2 a la entrada: Un órgano de gobierno puede incluir, pero no está limitado a, un consejo directivo, comités de control, consejo de control, directores y supervisores.

3.22
personal
individuos en una relación reconocida como laboral en la legislación o práctica nacional, o en cualquier relación contractual cuya actividad dependa de la *organización* (3.1)

3.23
función de *compliance*
persona o grupo de personas con responsabilidad y autoridad para la operación del *sistema de gestión* (3.4) del *compliance* (3.26)

Nota 1 a la entrada: Preferiblemente se asignará la supervisión del sistema de gestión del *compliance* a un solo individuo.

3.24
riesgo de *compliance*
probabilidad de ocurrencia y las consecuencias del *no cumplimiento de compliance* (3.27) respecto a las *obligaciones de compliance* (3.25) de una *organización* (3.1)

3.25
obligaciones de *compliance*
requisitos (3.14) que una *organización* (3.1) tiene obligatoriamente que cumplir, así como aquellos que una *organización* elige voluntariamente cumplir

3.26
***compliance*/cumplimiento**
el cumplimiento de todas las *obligaciones de compliance* (3.25) de la *organización* (3.1)

3.27
no cumplimiento de *compliance*
incumplimiento de las *obligaciones de compliance* (3.25)

3.28
cultura de *compliance*
valores, ética, creencias y *conductas* (3.29) que existen en una *organización* (3.1) y que interactúan con las estructuras y sistemas de control de la organización para producir normas de comportamiento que conducen al *compliance* (3.26)

3.29
conducta
comportamientos y prácticas que repercuten en los resultados para los clientes, empleados, proveedores, mercados y comunidades

3.30
tercera parte
persona u organismo que es independiente de la *organización* (3.1)

Nota 1 a la entrada: Todos los socios de negocio son terceras partes, pero no todas las terceras partes son socios de negocio.

3.31
procedimiento
forma específica de llevar a cabo una actividad o un *proceso* (3.8)

[FUENTE: ISO 9000:2015, 3.4.5]

4 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos en su sistema de gestión del *compliance*.

Con este propósito, la organización debe considerar una gran variedad de cuestiones, que incluyen, pero no se limitan a:

— el modelo de negocio, que incluye la estrategia, la naturaleza, el tamaño y el nivel de complejidad y sostenibilidad de las actividades y operaciones de la organización;

— la naturaleza y el alcance de las relaciones comerciales con terceras partes;

— el contexto legal y regulatorio;

— la situación económica;

— los contextos social, cultural y ambiental;

— las estructuras, políticas, procesos, procedimientos y recursos internos, incluyendo la tecnología;

— su cultura de *compliance*.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

— las partes interesadas que son pertinentes al sistema de gestión del *compliance*;

— los requisitos pertinentes de estas partes interesadas;

— cuáles de esos requisitos se abordarán en el sistema de gestión del *compliance*.

4.3 Determinación del alcance del sistema de gestión del *compliance*

La organización debe determinar los límites y la aplicabilidad del sistema de gestión del *compliance* para establecer su alcance.

NOTA El alcance del sistema de gestión del *compliance* pretende aclarar los principales riesgos de *compliance* a los que se enfrenta la organización y los límites geográficos u organizacionales, o ambos, a los que se aplicará el sistema de gestión del *compliance*, especialmente si la organización es parte de otra entidad más amplia.

Cuando se determina este alcance, la organización debe considerar:

— las cuestiones externas e internas referidas en el apartado 4.1;

— los requisitos referidos en los apartados 4.2, 4.5 y 4.6.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión del *compliance*

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión del *compliance*, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

El sistema de gestión del *compliance* debe reflejar los valores, objetivos, estrategia y riesgos de *compliance* de la organización teniendo en cuenta el contexto de la organización (véase 4.1).

4.5 Obligaciones de *compliance*

La organización debe identificar sistemáticamente sus obligaciones de *compliance* como resultado de sus actividades, productos y servicios, y evaluar el impacto de estas en sus operaciones.

La organización debe disponer de procesos para:

a) identificar obligaciones de *compliance* nuevas y modificadas para asegurar un cumplimiento continuo;

b) evaluar el impacto de los cambios identificados e implementar cualquier cambio necesario en la gestión de las obligaciones de *compliance*.

La organización debe conservar la información documentada sobre sus obligaciones de *compliance*.

4.6 Evaluación de los riesgos de *compliance*

La organización debe identificar, analizar y valorar sus riesgos de *compliance* basándose en una evaluación de los riesgos de *compliance*.

La organización debe identificar los riesgos de *compliance* relacionando sus obligaciones de *compliance* con sus actividades, productos, servicios y aspectos pertinentes de sus operaciones.

La organización debe evaluar los riesgos de *compliance* relacionados con procesos contratados externamente y de tercera parte.

Los riesgos de *compliance* deben evaluarse periódicamente y siempre que haya cambios materiales en las circunstancias o el contexto de la organización.

La organización debe conservar información documentada sobre la evaluación de los riesgos de *compliance* y sobre las acciones para abordar sus riesgos de *compliance*.

5 Liderazgo

5.1 Liderazgo y compromiso

5.1.1 Órgano de gobierno y alta dirección

El órgano de gobierno y la alta dirección deben demostrar liderazgo y compromiso con respecto al sistema de gestión del *compliance*:

— asegurando que se establezcan la política de *compliance* y los objetivos de *compliance* y que estos sean compatibles con la dirección estratégica de la organización;

— asegurando la integración de los requisitos del sistema de gestión del *compliance* en los procesos de negocio de la organización;

— asegurando que los recursos que se necesitan para el sistema de gestión del *compliance* están disponibles;

— comunicando la importancia de una gestión del *compliance* eficaz y conforme con los requisitos del sistema de gestión del *compliance*;

— asegurando que el sistema de gestión del *compliance* logre sus resultados previstos;

— dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión del *compliance*;

— promoviendo la mejora continua;

— apoyando a otros roles pertinentes a demostrar su liderazgo en sus correspondientes áreas de responsabilidad.

NOTA Las referencias al término “negocio” en este documento se pueden interpretar ampliamente como aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

El órgano de gobierno y la alta dirección deben:

— establecer y defender los valores de la organización;

— asegurar que se desarrollan e implementan políticas, procesos y procedimientos para alcanzar los objetivos de *compliance*;

— asegurar que se les informa de manera oportuna de las cuestiones relacionadas con *compliance*, incluidos los casos de no cumplimiento de *compliance*, y asegurar que se toman las acciones adecuadas;

— asegurar que se mantiene el compromiso de *compliance* y que se gestionan adecuadamente los no cumplimientos de *compliance* y los comportamientos contrarios a *compliance*;

— asegurar que se incluyen las responsabilidades de *compliance* en las descripciones de los puestos de trabajo según corresponda;

— designar o nominar una función de *compliance* (véase 5.3.2);

— asegurar que se establece un sistema para el levantamiento y el tratamiento de inquietudes acorde con lo que establece el apartado 8.3.

5.1.2 Cultura de *compliance*

La organización debe desarrollar, mantener y promover una cultura de *compliance* a todos los niveles de la organización.

El órgano de gobierno, la alta dirección y la dirección deben demostrar un compromiso activo, visible, consistente y sostenido con un estándar común de comportamiento y conducta que se requiere en toda la organización.

La alta dirección debe fomentar comportamientos que creen y apoyen el *compliance*. Debe evitar y no tolerar comportamientos que comprometan el *compliance*.

5.1.3 Gobernanza del *compliance*

El órgano de gobierno y la alta dirección deben asegurar que se implementan los siguientes principios:

— el acceso directo de la función de *compliance* al órgano de gobierno;

— la independencia de la función de *compliance*;

— la autoridad y la competencia adecuadas de la función de *compliance*.

NOTA 1 El acceso directo puede incluir: tener una línea de información directa con el órgano de gobierno, presentar informes periódicamente al órgano de gobierno y participar en sus reuniones.

NOTA 2 Independencia significa ausencia de interferencia y/o presión indebida con la operación de la función de *compliance*.

5.2 Política de *compliance*

El órgano de gobierno y la alta dirección deben establecer una política de *compliance* que:

a) sea adecuada al propósito de la organización;

b) proporcione un marco de referencia para el establecimiento de los objetivos de *compliance*;

c) incluya el compromiso de cumplir los requisitos aplicables;

d) incluya el compromiso de mejora continua del sistema de gestión del *compliance*.

La política de *compliance* debe:

— estar alineada con los valores, objetivos y estrategia de la organización;

— requerir el cumplimento de las obligaciones de *compliance* de la organización;

— apoyar los principios de la gobernanza del *compliance* de acuerdo con el apartado 5.1.3;

— hacer referencia a la función de *compliance* y describirla;

— resumir las consecuencias de no cumplir con las obligaciones de *compliance*, las políticas, los procesos y los procedimientos de la organización;

— fomentar el planteamiento de inquietudes y prohibir cualquier tipo de represalia;

— estar escrita en un lenguaje sencillo de forma que todo el personal pueda entender fácilmente los principios y su intención;

— implementarse y hacerse cumplir de forma adecuada.

— estar disponible como información documentada;

— comunicarse dentro de la organización;

— estar disponible para las partes interesadas, según corresponda.

5.3 Roles, responsabilidades y autoridades

5.3.1 Órgano de gobierno y alta dirección

El órgano de gobierno y la alta dirección deben asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización.

El órgano de gobierno y la alta dirección deben asignar la responsabilidad y autoridad para:

a) asegurar que el sistema de gestión del *compliance* cumple los requisitos de este documento;

b) informar al órgano de gobierno y a la alta dirección sobre el desempeño del sistema de gestión del *compliance*.

El órgano de gobierno debe:

— asegurar que a la alta dirección se la mide en función del logro de los objetivos de *compliance*;

— ejercer la supervisión sobre la alta dirección en relación con la operación del sistema de gestión del *compliance*.

La alta dirección debe:

— asignar recursos adecuados y apropiados para establecer, desarrollar, implementar, evaluar, mantener y mejorar el sistema de gestión del *compliance*;

— asegurar que existen sistemas eficaces para informar oportunamente sobre el desempeño del *compliance*;

— asegurar el alineamiento entre las metas estratégicas y las operativas y las obligaciones de *compliance*;

— establecer y mantener los mecanismos de rendición de cuentas, incluidas las consecuencias y acciones disciplinarias;

— asegurar la integración del desempeño del *compliance* en las evaluaciones de desempeño del personal.

5.3.2 Función de *compliance*

La función de *compliance* debe responsabilizarse de la operación del sistema de gestión del *compliance*, que incluye lo siguiente:

— facilitar la identificación de las obligaciones de *compliance*;

— documentar la evaluación de los riesgos de *compliance* (véase 4.6);

— alinear el sistema de gestión del *compliance* con los objetivos de *compliance*;

— medir y hacer seguimiento del desempeño del *compliance*;

— analizar y evaluar el desempeño del sistema de gestión del *compliance*; para identificar cualquier necesidad de acción correctiva;

— establecer un sistema de información y documentación del *compliance*;

— asegurarse de que el sistema de gestión del *compliance* se revise a intervalos planificados (véanse 9.2 y 9.3);

— establecer un sistema para plantear inquietudes y asegurar que se aborden las inquietudes.

La función de *compliance* debe ejercer la vigilancia de que:

— las responsabilidades para lograr las obligaciones de *compliance* identificadas se asignen de forma adecuada en toda la organización;

— las obligaciones de *compliance* estén integradas en las políticas, los procesos y los procedimientos;

— todo el personal pertinente esté formado como corresponda;

— estén establecidos indicadores de desempeño.

La función de *compliance* debe proporcionar:

— el acceso al personal a los recursos relacionados con las políticas, los procedimientos y los procesos de *compliance*;

— el asesoramiento a la organización en materias relacionadas con *compliance*.

NOTA Las tareas específicas de la función de *compliance* no exoneran a otros empleados de sus responsabilidades de *compliance*.

La organización debe asegurar que a la función de *compliance* se le ha dado acceso a:

— los tomadores de decisiones de alto nivel y a la oportunidad de contribuir en etapas tempranas de los procesos de toma de decisiones,

— todos los niveles de la organización;

— todo el personal, información documentada y datos necesarios;

— el asesoramiento experto en legislación, normativa, códigos y normas organizacionales pertinentes.

5.3.3 Dirección

La dirección debe ser responsable del *compliance* dentro de su área de responsabilidad:

— cooperando y apoyando a la función de *compliance* y animando a los empleados a hacerlo de la misma forma;

— asegurando que todo el personal bajo su control cumple con las obligaciones, las políticas, los procedimientos y los procesos de *compliance* de la organización;

— identificando y comunicando los riesgos de *compliance* en sus operaciones;

— integrando las obligaciones de *compliance* en las prácticas y procedimientos de negocio existentes en sus áreas de responsabilidad;

— asistiendo y apoyando las actividades formativas de *compliance*;

— desarrollando la concienciación del personal sobre las obligaciones de *compliance* y dirigiéndolos a que cumplan los requisitos de formación y competencia;

— animando al personal a plantear inquietudes en materia de *compliance* y apoyándoles e impidiendo cualquier forma de represalia;

— participando activamente en la gestión y resolución de incidentes y cuestiones relacionadas con *compliance* cuando corresponda;

— asegurando que una vez que se identifica la necesidad de una acción correctiva, se recomienda y se implementa la acción correctiva adecuada.

5.3.4 Personal

Todo el personal debe:

— observar las obligaciones, las políticas, los procesos y los procedimientos de *compliance* de la organización;

— informar sobre inquietudes, cuestiones y fallos de *compliance*;

— participar en la formación cuando corresponda.

6 Planificación

6.1 Acciones para abordar los riesgos y oportunidades

Al planificar el sistema de gestión del *compliance*, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2 y determinar los riesgos y oportunidades que necesitan abordarse para:

— asegurar que el sistema de gestión del *compliance* puede lograr los resultados previstos;

— prevenir o reducir los efectos no deseados;

— lograr la mejora continua.

Al planificar el sistema de gestión del *compliance*, la organización debe considerar:

— sus objetivos de *compliance* (véase 6.2);

— las obligaciones de *compliance* identificadas (véase 4.5);

— los resultados de la evaluación de los riesgos de *compliance* (véase 4.6).

La organización debe planificar:

a) las acciones para abordar los riesgos y oportunidades;

b) la forma de:

   1) integrar e implementar las acciones en sus procesos del sistema de gestión del *compliance*;

   2) evaluar la eficacia de estas acciones.

6.2 Objetivos de *compliance* y planificación para lograrlos

La organización debe establecer los objetivos de *compliance* en las funciones y niveles pertinentes.

Los objetivos de *compliance* deben:

a) ser coherentes con la política de *compliance*;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos aplicables;

d) ser objeto de seguimiento;

e) comunicarse;

f) actualizarse cuando corresponda;

g) estar disponibles como información documentada.

Cuando planifica cómo lograr sus objetivos de *compliance*, la organización debe determinar:

— qué se va a hacer;

— qué recursos serán necesarios;

— quién será responsable;

— cuándo se finalizará;

— cómo se evaluarán los resultados.

6.3 Planificación de los cambios

Cuando la organización determina la necesidad de hacer cambios en el sistema de gestión del *compliance*, los cambios deben realizarse de forma planificada.

La organización debe considerar:

— el propósito de los cambios y sus potenciales consecuencias;

— el diseño y la eficacia operacional del sistema de gestión del *compliance*;

— la disponibilidad de los recursos adecuados;

— la asignación o reasignación de las responsabilidades y autoridades.

7 Apoyo

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión del *compliance*.

7.2 Competencia

7.2.1 Generalidades

La organización debe:

— determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño del *compliance*;

— asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

— cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.

La información documentada para proporcionar evidencia de la competencia debe estar disponible.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.2.2 Proceso de empleo

En relación con todo su personal, la organización debe desarrollar, establecer, implementar y mantener procesos de manera que:

a) las condiciones de empleo requieran que el personal cumpla con las obligaciones, las políticas, los procesos y los procedimientos de *compliance* de la organización;

b) en un periodo de tiempo razonable desde su incorporación al empleo, el personal reciba una copia o se le dé acceso a la política de *compliance* y a formación relacionada con esa política;

c) se tomen las acciones disciplinarias adecuadas contra el personal que infrinja las obligaciones, las políticas, los procesos y los procedimientos de *compliance* de la organización.

Como parte del proceso de empleo, la organización debe considerar los riesgos de *compliance* que presentan los roles y el personal y aplicar los procedimientos de debida diligencia que corresponda antes de cualquier contratación, cambio de puesto o promoción.

La organización debe implementar un proceso que permita la revisión periódica de las metas de desempeño, las bonificaciones de desempeño y demás incentivos, para verificar que se aplican las medidas adecuadas para evitar que se fomente el no cumplimiento de *compliance*.

7.2.3 Formación

La organización debe proporcionar formación al personal pertinente de forma regular, desde su incorporación y a intervalos planificados determinados por la organización.

La formación debe:

a) ser adecuada a los roles del personal y a los riesgos de *compliance* a los que está expuesto el personal;

b) evaluarse en términos de eficacia;

c) revisarse regularmente.

Teniendo en cuenta los riesgos de *compliance* identificados, la organización debe asegurarse de que se implementan procedimientos para abordar la toma de conciencia y la formación en materia de *compliance* para terceras partes que actúan en su nombre y que pueden suponer un riesgo de *compliance* para la organización.

Los registros de formación se deben conservar como información documentada.

7.3 Toma de conciencia

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de:

— la política de *compliance*;

— su contribución a la eficacia del sistema de gestión del *compliance*, incluidos los beneficios de una mejora del desempeño del *compliance*;

— las implicaciones de no cumplir los requisitos del sistema de gestión del *compliance*.

— los medios y procedimientos para plantear inquietudes de *compliance* (véase 8.3);

— la relación entre la política de *compliance* y las obligaciones de *compliance* pertinentes para sus roles;

— la importancia de apoyar la cultura de *compliance*.

7.4 Comunicación

La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión del *compliance*, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) cómo comunicar.

La organización debe:

— considerar los aspectos de la diversidad y los obstáculos potenciales, al considerar sus necesidades de comunicación;

— asegurar que las opiniones de las partes interesadas se consideran al establecer los procesos de comunicación;

— al establecer los procesos de comunicación:

  — incluir las comunicaciones en su cultura de *compliance*, en sus objetivos y obligaciones de *compliance*;

  — asegurar que la información de *compliance* objeto de la comunicación es consistente con la información generada en el sistema de gestión del *compliance* y es fiable;

— responder a las comunicaciones pertinentes sobre el sistema de gestión del *compliance*;

— conservar la información documentada como evidencia de sus comunicaciones, cuando corresponda;

— comunicar internamente la información pertinente para el sistema de gestión del *compliance* a los distintos niveles y funciones de la organización, incluidos los cambios en el sistema de gestión del *compliance*, cuando corresponda;

— asegurar que sus procesos de comunicación permiten al personal contribuir a la mejora continua del sistema de gestión del *compliance*;

— asegurar que sus procesos de comunicación posibilitan que el personal pueda plantear inquietudes (véase 8.3);

— comunicar externamente la información pertinente para el sistema de gestión del *compliance*, como se establece en los procesos de comunicación de la organización e incluir la comunicación en su cultura de *compliance*, sus objetivos y obligaciones de *compliance*.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión del *compliance* de la organización debe incluir:

a) la información documentada requerida en este documento;

b) la información documentada que la organización ha determinado como necesaria para la eficacia del sistema de gestión del *compliance*.

NOTA La extensión de la información documentada para un sistema de gestión del *compliance* puede ser diferente de una organización a otra debido a:

— el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios;

— la complejidad de los procesos y sus interacciones;

— la competencia de las personas.

7.5.2 Creación y actualización de la información documentada

Al crear y actualizar información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

— la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

— el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

— la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión del *compliance* y por este documento se debe controlar para asegurarse de que:

a) está disponible y es adecuada para su uso, dónde y cuándo se necesite;

b) está protegida adecuadamente (por ejemplo, contra pérdida de confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según corresponda:

— la distribución, el acceso, la recuperación y el uso;

— el almacenamiento y la preservación, incluida la preservación de la legibilidad;

— el control de cambios (por ejemplo, control de versión);

— la retención y la disposición.

La información documentada de origen externo que la organización determina como necesaria para la planificación y operación del sistema de gestión del *compliance* se debe identificar, según sea apropiado, y controlar.

NOTA El acceso puede implicar una decisión en relación al permiso, solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el Capítulo 6 mediante:

— el establecimiento de criterios para los procesos;

— la implementación del control de los procesos de acuerdo con los criterios.

La información documentada debe estar disponible en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, según sea necesario.

La organización debe asegurarse de que los procesos, productos o servicios que se proporcionan externamente y son pertinentes al sistema de gestión del *compliance*, se controlan.

NOTA La contratación externa de las operaciones de una organización no le exime de sus responsabilidades legales o de sus obligaciones de *compliance*.

La organización se debe asegurar de que los procesos de terceras partes son controlados y se realiza un seguimiento de los mismos.

8.2 Establecimiento de controles y procedimientos

La organización debe implementar controles para gestionar sus obligaciones de *compliance* y los riesgos de *compliance* asociados. Estos controles se deben mantener, revisar y probar periódicamente para asegurarse de que continúan siendo eficaces.

NOTA Los controles de prueba implican realizar un ejercicio diseñado para ver si el control cumple su propósito o si no puede obviarse o si realmente es eficaz a la hora de reducir el impacto del riesgo o la probabilidad de que este se produzca.

8.3 Planteamiento de inquietudes

La organización debe establecer, implementar y mantener un proceso para animar y permitir que se informe (en caso de que haya motivos razonables para pensar que la información es cierta) sobre los intentos de infracción, las infracciones supuestas o reales de la política o de las obligaciones de *compliance*.

Este proceso debe:

— ser visible y accesible en toda la organización;

— tratar los informes de forma confidencial;

— aceptar los informes anónimos;

— proteger a aquellos que realizan los informes de las represalias;

— permitir al personal que reciba asesoramiento.

La organización debe asegurarse de que el personal toma conciencia de los procedimientos de información, sus derechos y protección y de que pueden usarlos.

8.4 Procesos de investigación

La organización debe desarrollar, establecer, implementar y mantener procesos para valorar, evaluar, investigar y cerrar los informes sobre casos supuestos o reales de no cumplimiento de *compliance*. Estos procesos deben asegurar que la toma de decisiones es justa e imparcial.

Los procesos de investigación deben realizarse de forma independiente y sin ningún conflicto de intereses por parte del personal competente.

La organización debe usar los resultados de las investigaciones para la mejora del sistema de gestión del *compliance* cuando corresponda (véase el Capítulo 10).

La organización debe informar regularmente sobre las cantidades y los resultados de las investigaciones al órgano de gobierno y a la alta dirección.

La organización debe conservar la información documentada sobre la investigación.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

9.1.1 Generalidades

La organización debe realizar seguimiento del sistema de gestión del *compliance* para asegurar que se alcanzan los objetivos de *compliance*.

La organización debe determinar:

— qué debe ser objeto de seguimiento y qué es necesario medir;

— los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

— cuándo se deben llevar a cabo el seguimiento y la medición;

— cuándo se deben analizar y evaluar los resultados del seguimiento y la medición.

La información documentada para proporcionar evidencia de los resultados debe estar disponible.

La organización debe evaluar el desempeño de *compliance* y la eficacia del sistema de gestión del *compliance*.

9.1.2 Fuentes de opinión sobre el desempeño del *compliance*

La organización debe establecer, implementar, evaluar y mantener procesos para buscar y recibir opiniones de su desempeño del *compliance* de una serie de fuentes. La información debe analizarse y evaluarse críticamente para identificar las causas raíz de no cumplimiento de *compliance*, asegurar que se toman las acciones adecuadas y reflejar esta información en la evaluación periódica de riesgos requerida en el apartado 4.6.

9.1.3 Desarrollo de indicadores

La organización debe desarrollar, implementar y mantener un conjunto de indicadores adecuados que ayuden a la organización a evaluar el logro de sus objetivos de *compliance* y a evaluar su desempeño del *compliance*.

9.1.4 Informes de *compliance*

La organización debe establecer, implementar y mantener procesos para proporcionar información en materia de *compliance* con el fin de asegurar que:

a) se definen los criterios adecuados para la presentación de informes;

b) se establecen plazos para la presentación periódica de informes;

c) se implementa un sistema de informes de excepciones que facilita información ad hoc;

d) se implementan sistemas y procesos para asegurar la exactitud e integridad de la información;

e) se facilita una información exacta y completa a las funciones o áreas de la organización apropiadas, para permitir que se adopten acciones preventivas, correctivas y correcciones de manera oportuna.

Cualquier informe emitido por la función de *compliance* para el órgano de gobierno o la alta dirección debe protegerse adecuadamente de modificaciones.

9.1.5 Mantenimiento de registros

Se deben mantener registros exactos y actualizados de las actividades de *compliance* de la organización con objeto de ayudar en los procesos de seguimiento y revisión y para demostrar la conformidad con el sistema de gestión del *compliance*.

9.2 Auditoría interna

9.2.1 Generalidades

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión del *compliance*:

a) cumple:

   — los requisitos propios de la organización para su sistema de gestión del *compliance*;

   — los requisitos de este documento;

b) se implementa y mantiene eficazmente.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener programas de auditoría que incluyan la frecuencia, los métodos, responsabilidades, requisitos de planificación e informes.

A la hora de establecer los programas de auditoría interna, la organización debe considerar la importancia de los procesos involucrados y los resultados de las auditorías previas.

La organización debe:

a) para cada auditoría, definir los criterios, los objetivos y el alcance de la misma;

b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

c) asegurarse de que los resultados de las auditorías se comunican a los directivos pertinentes y a la dirección.

NOTA 1 La dirección pertinente puede incluir la función de *compliance*, la alta dirección y el órgano de gobierno.

La información documentada para proporcionar evidencia de la implementación del programa de auditoría y de los resultados de las auditorías debe estar disponible.

NOTA 2 La Norma ISO 19011 contiene directrices para la auditoría de los sistemas de gestión.

9.3 Revisión por la dirección

9.3.1 Generalidades

El órgano de gobierno y la alta dirección deben revisar el sistema de gestión del *compliance* de la organización a intervalos planificados, para asegurarse de su idoneidad, adecuación y eficacia continuas.

9.3.2 Entradas para la revisión del sistema

La revisión por la dirección debe incluir:

a) el estado de las acciones de las revisiones por la dirección previas;

b) los cambios en las cuestiones externas e internas que sean pertinentes para el sistema de gestión del *compliance*;

c) los cambios en las necesidades y las expectativas de las partes interesadas que son pertinentes para el sistema de gestión del *compliance*;

d) la información sobre el desempeño del *compliance*, incluidas las tendencias relativas a:

— las no conformidades, no cumplimientos de *compliance* y acciones correctivas;

— el seguimiento y los resultados de las mediciones;

— los resultados de las auditorías;

e) las oportunidades de mejora continua.

La revisión por la dirección debe tener en cuenta:

— la adecuación de la política de *compliance*;

— la independencia de la función de *compliance*;

— el grado en el que se han cumplido los objetivos de *compliance*;

— la adecuación de los recursos;

— la adecuación de la evaluación de riesgos de *compliance*;

— la eficacia de los controles e indicadores de desempeño existentes;

— la comunicación por parte de las personas que plantean inquietudes, partes interesadas, que incluye opiniones (véase 9.1.2) y quejas;

— las investigaciones (véase 8.4);

— la eficacia del sistema de informes.

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión del *compliance*.

La información documentada para proporcionar evidencia de los resultados de la revisión por la dirección debe estar disponible.

10 Mejora

10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión del *compliance*.

10.2 No conformidades y acciones correctivas

Cuando ocurra una no conformidad o un no cumplimiento de *compliance*, la organización debe:

a) reaccionar ante la no conformidad o no cumplimiento de *compliance* y, según sea aplicable:

1) tomar acciones para su control y corrección;

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad y/o no cumplimiento de *compliance*, o ambas con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

1) la revisión de la no conformidad y/o no cumplimiento de *compliance*;

2) la determinación de las causas de la no conformidad y/o no cumplimiento de *compliance*;

3) la determinación de si existen no conformidades y/o no cumplimientos de *compliance* similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas;

e) si es necesario, hacer cambios en el sistema de gestión del *compliance*.

Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades y/o no cumplimientos de *compliance* encontrados.

Debe estar disponible la información documentada para proporcionar evidencia de:

— la naturaleza de las no conformidades y/o no cumplimientos de *compliance* y cualquier acción tomada posteriormente;

— los resultados de cualquier acción correctiva.

Anexo A
(informativo)

Guía para el uso de este documento

A.1 Antecedentes y alcance

A.1.1 Generalidades

El propósito de la guía contenida en este anexo es indicar los enfoques y tipos de acciones que puede tomar una organización al implementar su sistema de gestión del *compliance*. No pretende ser exhaustiva o preceptiva, ni que las organizaciones estén obligadas a implementar todas las sugerencias recogidas en esta guía con el fin de tener un sistema de gestión del *compliance* que cumpla los requisitos de este documento. Los pasos dados por la organización deben ser razonables respecto de la naturaleza y extensión de los riesgos de *compliance* a los que se enfrenta para cumplir con sus obligaciones de *compliance*.

Una organización puede elegir implementar este sistema de gestión del *compliance* como un sistema aparte, sin embargo, lo ideal sería implementarlo junto con el resto de sus sistemas de gestión, como los de riesgos, antisoborno, calidad, ambiental, seguridad de la información y responsabilidad social, por poner algunos ejemplos. En estos casos, la organización puede consultar las Normas ISO 31000, ISO 37001, ISO 9001, ISO 14001 e ISO/IEC 27001, así como la Norma ISO 26000.

A.1.2 Alcance

Las organizaciones de cualquier tamaño, complejidad o industria pueden aplicar esta norma para crear un sistema de gestión del *compliance*, siguiendo sus requisitos. Ello les permitirá comprender su contexto, sus operaciones de negocio, obligaciones resultantes y riesgos de *compliance* y les ayudará a implementar pasos razonables para que cumpla sus obligaciones. Se debe seguir cada uno de los requisitos de este documento. Sin embargo, la guía contenida en este anexo tiene carácter informativo.

En la práctica, a menudo es más sencillo implementar un sistema de gestión del *compliance* en línea con esta norma en organizaciones pequeñas, porque son menos complejas. Las organizaciones pequeñas y medianas mejorarán las prácticas de la organización mediante el uso de los principios de los requisitos de esta norma.

El documento hace referencia al órgano de gobierno y a la alta dirección y define lo que significan estos términos en una variedad de contextos y lugares. De igual modo que la norma puede utilizarse en todas las organizaciones, si su organización en particular no utiliza estos términos, entonces hay que fijarse en el propósito de su uso: los requisitos o direcciones se aplicarían a la persona o grupo de personas que tienen la autoridad y responsabilidad en lo más alto de la organización.

A.2 Referencias normativas

En este documento no existen referencias normativas. Los usuarios pueden consultar la bibliografía para obtener más información y conocer las normas internacionales pertinentes para el *compliance*.

A.3 Términos y definiciones

Este documento ha adoptado la "estructura de alto nivel" (HLS, por sus siglas en inglés) desarrollada por ISO para mejorar el alineamiento entre sus normas internacionales para sistemas de gestión. La estructura HLS establece la secuencia de capítulos, terminología y definiciones comunes y un texto principal idéntico que forma el núcleo de las normas ISO de sistemas de gestión (MSS, por sus siglas

en inglés). Esto significa que algunas de estas definiciones podrían no utilizarse de una forma que le resulte familiar. Las definiciones facilitadas podrían considerarse al usar este documento a modo de aclaración.

Este enfoque común hacia las MSS incrementa el valor de dichas normas para los usuarios. Es particularmente útil para esas organizaciones elegir operar un sistema de gestión único (a veces llamado «integrado») que cumpla los requisitos de dos o más MSS simultáneamente. Las organizaciones que no hayan adoptado MSS o un marco de gestión del *compliance* pueden adoptar fácilmente este documento como una guía independiente en su organización.

Se puede encontrar más información sobre MSS y la estructura HLS en:

https://www.iso.org/management-system-standards.html.

A.4 Contexto de la organización

A.4.1 Comprensión de la organización y de su contexto

El propósito de este capítulo es que las organizaciones establezcan un alto grado de comprensión (por ejemplo, estratégica) de las cuestiones importantes que puedan afectar su sistema de gestión del *compliance*. Los conocimientos obtenidos se utilizan entonces para orientar el enfoque hacia la planificación, implementación, operación y mejora del sistema de gestión del *compliance*.

Consiste en el proceso de revisar toda la información disponible de la organización: lo que hace, dónde, cómo y por qué. Se realiza una evaluación de factores externos y factores clave por su impacto en la organización en términos de sus obligaciones de *compliance*.

Las obligaciones de *compliance* más obvias proceden de los contextos legales y regulatorios en los que su organización opera, pero las obligaciones o los riesgos también podrían surgir de otros factores como se sugiere en este documento. Su organización debería también considerar las tendencias futuras pertinentes que podrían tener un impacto.

Los factores internos también deberían tomarse en consideración. En el documento se incluyen algunos ejemplos. La lista no es exhaustiva, pudiendo haber otros que sean pertinentes para su organización.

A.4.2 Comprensión de las necesidades y expectativas de las partes interesadas

Las organizaciones deberían establecer una comprensión de las necesidades y expectativas de las personas u organizaciones que pueden afectar, verse afectadas o percibirse como afectadas por el sistema de gestión del *compliance*.

Algunas son obligatorias porque se han incorporado a los requisitos formales, como: leyes, reglamentos, permisos y licencias y acciones gubernamentales o judiciales. Puede haber otros requisitos formales que no están incluidos aquí y que se apliquen.

Otras necesidades y expectativas de una parte interesada se convierten en obligaciones cuando se especifican y la organización decide adoptarlas voluntariamente al formalizar un acuerdo o contrato. Una vez que la organización ha decidido sobre ellas, se convierten en obligaciones de *compliance*.

Entre los ejemplos de partes interesadas externas pueden incluirse, entre otras:

— los gobiernos y las agencias gubernamentales;

— los organismos reguladores;

— los clientes;

— los contratistas;

— los proveedores;

— las terceras partes intermediarias;

— los propietarios, los accionistas e inversores;

— las organizaciones no gubernamentales;

— la sociedad y los grupos de la comunidad;

— los socios comerciales.

Entre los ejemplos de partes interesadas internas pueden incluirse, entre otras:

— el órgano de gobierno;

— la dirección;

— los empleados;

— las funciones internas tales como la gestión del riesgo, el control interno, la auditoría interna, los recursos humanos.

A.4.3 Determinación del alcance del sistema de gestión del *compliance*

La determinación del alcance de un sistema de gestión del *compliance* es el proceso por el que las organizaciones establecen los límites físicos y organizacionales a los que se aplica el sistema de gestión del *compliance*. Al hacerlo, la organización tiene la libertad y la flexibilidad de elegir implementar el sistema de gestión del *compliance* en toda la organización, en una unidad específica o en una función específica dentro de la organización.

Típicamente, un sistema de gestión del *compliance* se implementará en toda la organización y -en caso de grupos de organizaciones- en todo el grupo de organizaciones para evitar la dualidad de normas de conducta ética y *compliance*.

El alcance debería ser razonable y proporcionado teniendo en cuenta la naturaleza y la extensión de los riesgos de *compliance* a los que se enfrenta la organización.

Al establecer el alcance del sistema de gestión del *compliance* y al determinar los requisitos que la organización va a adoptar conviene entender el contexto y los requisitos de las partes interesadas pertinentes.

A.4.4 Sistema de gestión del *compliance*

Un sistema de gestión del *compliance* es un marco que integra estructuras, políticas, procesos y procedimientos esenciales para conseguir los resultados del *compliance* deseados y actuar para prevenir, detectar y reaccionar ante un no cumplimiento de *compliance*.

Típicamente, el marco de un sistema de gestión del *compliance* es una cuestión estructural: la infraestructura necesaria sobre la que se construye este sistema. Luego es necesario hacerlo operativo a través de la implementación de políticas, procesos y procedimientos. Después, es necesario mantener y mejorar continuamente el sistema de gestión del *compliance*.

Hay muchos elementos en un sistema de gestión del *compliance*. Algunos elementos del sistema de gestión del *compliance* se diseñarán para apoyar comportamientos deseados, mientras que otros se diseñarán para evitar comportamientos no deseados. Algunos elementos sirven únicamente para realizar un seguimiento del desempeño del *compliance* de la organización o emitir alertas ante no cumplimientos de *compliance*.

El sistema de gestión del *compliance* reconocerá que los errores ocurren y contará con procesos que aseguren que hay una reacción adecuada. Una reacción adecuada incluirá remediar los procesos y sistemas y las partes afectadas.

El sistema de gestión del *compliance* debería basarse en los principios de buena gobernanza, proporcionalidad, integridad, transparencia, rendición de cuentas y sostenibilidad.

El sistema de gestión del *compliance* debería estar disponible de forma documentada.

A.4.5 Obligaciones de *compliance*

La organización debería tomar las obligaciones de *compliance* como base para establecer, desarrollar, implementar, evaluar, mantener y mejorar su sistema de gestión del *compliance*.

Los requisitos con los que una organización debe cumplir obligatoriamente pueden incluir:

— las leyes y las reglamentaciones;

— los permisos, las licencias u otras formas de autorización;

— las órdenes, las reglas u orientaciones emitidas por agencias reguladoras;

— las sentencias de cortes o tribunales administrativos;

— los tratados, las convenciones y los protocolos.

Los requisitos que una organización elige cumplir voluntariamente pueden incluir:

— los acuerdos con grupos comunitarios u organizaciones no gubernamentales;

— los acuerdos con autoridades públicas y clientes;

— los requisitos organizacionales, como políticas y procedimientos;

— los principios voluntarios o códigos de práctica;

— el etiquetado voluntario o compromisos medioambientales;

— las obligaciones derivadas de acuerdos contractuales con la organización;

— las normas organizacionales e industriales pertinentes.

La organización debería identificar obligaciones de *compliance* por departamentos, funciones y diferentes tipos de actividades organizacionales para determinar quiénes se ven afectados por estas obligaciones de *compliance*.

Los procesos para obtener información sobre cambios en leyes y en otras obligaciones de *compliance* pueden incluir:

— estar en las listas de distribución de los reguladores pertinentes;

— ser miembros de grupos profesionales;

— suscribirse a servicios de información pertinentes;

— asistir a foros de la industria y seminarios;

— revisar las páginas web de los reguladores;

— mantener reuniones con los reguladores;

— llegar a acuerdos con asesores legales;

— revisar las fuentes de las obligaciones de *compliance* (por ejemplo, pronunciamientos regulatorios y sentencias judiciales).

Se debería adoptar un enfoque basado en el riesgo, es decir, una organización debería comenzar con la identificación de la obligación de cumplimiento más importante pertinente para el negocio y luego centrarse en todas las demás obligaciones de *compliance* (principio de Pareto).

Cuando sea apropiado, la organización debería establecer y mantener un solo documento (como un registro o bitácora) que establezca todas sus obligaciones de *compliance* y tener un proceso para actualizar el documento de manera regular.

Además de establecer las obligaciones de *compliance*, el documento debería incluir, pero no limitarse a:

— el impacto de las obligaciones de *compliance*;

— la gestión de las obligaciones de *compliance*;

— los controles vinculados a las obligaciones de *compliance*;

— la evaluación de riesgos.

A.4.6 Evaluación de los riesgos de *compliance*

La evaluación de los riesgos de *compliance* constituye la base para la implementación del sistema de gestión del *compliance* y la asignación de recursos y de procesos adecuados y apropiados para gestionar los riesgos de *compliance* identificados.

Los riesgos de *compliance* se pueden caracterizar por la probabilidad de ocurrencia y por las consecuencias del no cumplimiento de *compliance* de la política y las obligaciones de *compliance* de la organización.

Los riesgos de *compliance* incluyen riesgos de *compliance* inherentes y residuales. Los riesgos de *compliance* inherentes hacen referencia a todos los riesgos de *compliance* a los que se enfrenta una organización en una situación sin control y sin ninguna de las medidas correspondientes para el tratamiento de los riesgos de *compliance*. Los riesgos de *compliance* residuales son los riesgos de *compliance* que no controlan de forma eficaz las medidas existentes para el tratamiento de los riesgos de *compliance*.

La organización debería analizar los riesgos de *compliance* considerando las causas raíz de los no cumplimientos de *compliance* y sus consecuencias, al mismo tiempo que se incluye la probabilidad de que se produzcan estas repercusiones. Las consecuencias pueden incluir, por ejemplo, daño personal y ambiental, pérdidas económicas, daño en la reputación, cambios administrativos y responsabilidades civiles y penales.

La identificación de los riesgos de *compliance* incluye la identificación de las fuentes de los riesgos de *compliance* y la definición de las situaciones de riesgo de *compliance*. Las organizaciones deberían identificar las fuentes de los riesgos de *compliance* dentro de diversos departamentos, funciones y distintos tipos de actividades organizacionales de acuerdo con las responsabilidades del departamento, las responsabilidades del puesto y los distintos tipos de actividades organizacionales. La organización debería identificar de forma regular las fuentes de los riesgos de *compliance* y definir las situaciones de riesgo de *compliance* correspondientes a cada fuente de riesgo de *compliance* para desarrollar una lista de fuentes de riesgos de *compliance* y una lista de situaciones de riesgo de *compliance*.

La evaluación del riesgo implica comparar el nivel del riesgo de *compliance* que es aceptable para la organización con el nivel de riesgo de *compliance* que se establece en la política de *compliance*.

Los riesgos de *compliance* deberían reevaluarse periódicamente y en todo caso cuando haya:

— actividades, productos o servicios nuevos o modificados;

— cambios en la estructura o en la estrategia de la organización;

— cambios externos significativos, tales como circunstancias económico-financieras, condiciones de mercado, pasivos y relaciones con los clientes;

— cambios en las obligaciones de *compliance*;

— fusiones o adquisiciones;

— no cumplimientos de *compliance* (incluso un único caso de no cumplimiento de *compliance* puede constituir un cambio material de las circunstancias) o situaciones cercanas al no cumplimiento.

El alcance y el nivel de detalle de la evaluación de riesgos de *compliance* dependen de la situación de riesgo, el contexto, el tamaño y los objetivos de la organización y pueden variar para sub-áreas específicas (por ejemplo, ambiental, financiera, social).

El enfoque basado en el riesgo en la gestión del *compliance* no significa que para situaciones de riesgo bajo de no cumplimientos de *compliance*, la organización acepte no cumplimientos de *compliance*. Ayuda a las organizaciones a centrar la atención primaria y los recursos en los riesgos más elevados de forma prioritaria y, en última instancia, cubrirá todos los riesgos de *compliance*. Todos los riesgos/situaciones de *compliance* identificados son objeto de seguimiento y tratamiento.

Cuando se lleva a cabo una evaluación de los riesgos (véase como orientación la Norma ISO 31000) se debería prestar atención a las técnicas adecuadas (como las detalladas en la Norma IEC 31010).

A.5 Liderazgo

A.5.1 Liderazgo y compromiso

A.5.1.1 Órgano de gobierno y alta dirección

Para que el *compliance* sea eficaz requiere un compromiso activo por parte del órgano de gobierno y de la alta dirección que permee toda la organización.

Para el sistema de gestión del cumplimiento es vital que el órgano de gobierno y la alta dirección demuestren de forma clara y visible su compromiso con el logro de los objetivos del sistema de gestión del *compliance*.

Los no cumplimientos de *compliance* pueden tener un impacto negativo en el negocio como daño en la reputación, pérdida de licencia para operar o de oportunidad y derivar en un coste considerable. Por ello, el órgano de gobierno y la alta dirección deberían reconocer la importancia estratégica de una gestión del *compliance* eficaz.

Esta norma enumera muchas formas en las que los líderes pueden demostrar su compromiso. La forma primordial de hacerlo es a través del apoyo activo y visible al establecimiento y mantenimiento del sistema de gestión del *compliance*.

El grado de compromiso se pone de manifiesto por el grado en el que:

— el órgano de gobierno y todos los niveles de la dirección, a través de sus acciones y decisiones, demuestran activamente su compromiso por establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión del *compliance* eficaz y que genera respuesta por parte de la organización;

— la política de *compliance* está formalmente aprobada por el órgano de gobierno;

— la alta dirección asume la responsabilidad de asegurar que el compromiso de *compliance* en la organización es plenamente alcanzado;

— todos los niveles de la dirección transmiten a todo el personal de forma consistente un mensaje claro (demostrado de palabra y acción) de que la organización cumplirá con sus obligaciones de *compliance*;

— el compromiso hacia el *compliance* se comunica ampliamente a todo el personal y a las partes interesadas pertinentes en declaraciones claras y convincentes y apoyadas por acciones;

— la función de *compliance* tiene personal con la competencia, la autoridad y la independencia adecuadas que reflejan la importancia de que el *compliance* sea eficaz y tiene acceso directo al órgano de gobierno;

— se asignan recursos adecuados para establecer, desarrollar, implementar, evaluar, mantener y mejorar una cultura de *compliance* robusta a través de actividades de concienciación y formación para todo el personal y las partes interesadas pertinentes;

— las políticas, los procesos y los procedimientos reflejan, no solo los requisitos legales, sino también códigos voluntarios y los valores fundamentales de la organización;

— la organización asigna y exige la rendición de cuentas en materia de *compliance* a la dirección en todos los niveles de la organización;

— se realizan revisiones periódicas del sistema de gestión del *compliance* (se recomienda, al menos, una al año);

— el desempeño del *compliance* en la organización se mejora de forma continua;

— las acciones correctivas se toman oportunamente;

— el órgano de gobierno y la alta dirección siguen el sistema de gestión del *compliance* de la organización.

A.5.1.2 Cultura de *compliance*

Los factores que apoyarán el desarrollo de una cultura de *compliance*, entre otros, son:

— un conjunto claro de valores publicados;

— una dirección que implementa y respeta activa y visiblemente los valores;

— la consistencia en el tratamiento de no cumplimientos de *compliance*, con independencia de la posición;

— guiar, entrenar y predicar con el ejemplo;

— una evaluación adecuada del personal potencial previa a su incorporación para funciones críticas que incluyen la debida diligencia;

— un programa de iniciación u orientación que enfatice el *compliance* y los valores de la organización;

— la formación continua en *compliance*, que incluye actualizaciones de la formación a todo el personal y a las partes interesadas pertinentes;

— la comunicación continua de las cuestiones de *compliance*;

— los sistemas de evaluación del desempeño que consideren la evaluación del comportamiento de *compliance* y que incluyan retribuciones del desempeño en base al logro de objetivos y parámetros clave de *compliance*;

— un reconocimiento visible de los logros en la gestión del *compliance* y en sus resultados;

— las medidas disciplinarias rápidas y proporcionadas en caso de infracciones de las obligaciones de *compliance* intencionadas o negligentes;

— una relación clara entre la estrategia de la organización y los roles individuales, que enfatizan el *compliance* como esencial para alcanzar los resultados de la organización;

— la comunicación abierta y adecuada sobre el *compliance*, interna y externamente.

La evidencia de una cultura de *compliance* se mide por el grado en que:

— se implementan los puntos señalados arriba;

— las partes interesadas (especialmente el personal) creen que se han implementado los puntos señalados arriba;

— el personal entiende la relevancia de las obligaciones de *compliance* relativas a sus propias actividades y a las de sus unidades de negocio;

— las acciones correctivas para abordar los no cumplimientos de *compliance* se asumen como propios y se gestionan en todos los niveles adecuados de la organización cuando sea necesario;

— se valora el papel de la función de *compliance* y sus objetivos;

— al personal se le permite y anima a plantear inquietudes relativas al *compliance* al nivel adecuado de la dirección, incluyendo a la alta dirección y al órgano de gobierno.

La organización debería:

a) medir su cultura de *compliance*;

b) recabar aportaciones de todos los empleados para determinar si perciben el compromiso de *compliance* del órgano de gobierno, la alta dirección y la dirección media;

c) establecer planes de acción basados en los resultados de los indicadores de la cultura de *compliance* de la organización.

A.5.1.3 La gobernanza del *compliance*

La gobernanza del *compliance* se apoya en los siguientes principios fundamentales.

La función de *compliance* tiene acceso directo al órgano de gobierno y a la alta dirección. Pueden obviar a otros dentro de la organización en caso necesario y comunicarse directamente con otra persona o personas con la máxima autoridad para actuar. Esto beneficia directamente al órgano de gobierno y a la alta dirección de forma que pueden ejercer sus tareas. Este acceso debería planificarse y ser sistemático. Por ejemplo, la función de *compliance* podría tener una línea de información directa con el primer ejecutivo y una línea de información discontinua con el comité de auditoría, el presidente o con toda la junta.

La función de *compliance* debería ser independiente y no estar en conflicto con la estructura de la organización u otros elementos. Son libres para actuar sin ninguna interferencia con la línea de mando.

La función de *compliance* tiene autoridad. La función de *compliance* no es una posición menor que se pueda desautorizar o a la que puedan modificar sus informes o información los que tienen más autoridad. La función de *compliance* puede dirigir a otros empleados en caso necesario. La función de *compliance* debería tener voz ("voice at the table") para defender y plantear cualquier inquietud relativa al *compliance*.

La función de *compliance* dispone de los recursos adecuados para apoyar a la organización a llevar a cabo el trabajo necesario y las responsabilidades del sistema de gestión del *compliance* sin restricciones, incluido el acceso a la tecnología para permitir que el sistema de gestión del *compliance* sea exhaustivo y apoye de forma eficaz a la organización en el logro de sus objetivos de *compliance*.

A.5.2 Política de *compliance*

La política de *compliance* establece los principios generales y el compromiso de acción de una organización para lograr el *compliance*. Establece el nivel de responsabilidad y de desempeño que se requiere y establece las expectativas bajo las que se evaluarán las acciones. La política debería ser adecuada para las obligaciones de *compliance* de la organización que se derivan de sus actividades.

La política de *compliance* debería ser aprobada por el órgano de gobierno.

La política de *compliance* debería especificar:

— la aplicación y el contexto del sistema de gestión del *compliance* en relación con el tamaño, la naturaleza y la complejidad de la organización y del entorno en el que opera;

— el grado en el que el *compliance* se va a integrar con otras funciones, tales como gobernanza, riesgos, auditoría y asesoría jurídica;

— los principios según los cuales se van a gestionar las relaciones con partes interesadas internas y externas.

La política de *compliance* no debería ser un documento único, sino que debería estar apoyado por otros documentos, que incluyen políticas y procesos, operacionales.

La política de *compliance* debería estar traducida a otros idiomas en caso de ser necesario.

La política de *compliance* debería ser adecuada para las obligaciones de *compliance* de la organización que se derivan de su alcance y sus actividades.

Al desarrollar la política de *compliance*, se debería considerar lo siguiente:

a) las obligaciones específicas internacionales, las regionales o las locales;

b) la estrategia, los objetivos, la cultura y el enfoque de gobernanza de la organización;

c) la estructura de la organización;

d) la naturaleza y el nivel de riesgo asociado a los no cumplimientos de *compliance*;

e) las normas, los códigos, las políticas internas y los procedimientos adoptados;

f) las normas de la industria.

Las políticas de *compliance* pueden constar de:

— una declaración de la misión;

— una declaración de política general;

— las estrategias de gestión y la asignación de responsabilidades y los recursos;

— los procedimientos estándar de *compliance*;

— la auditoría, la debida diligencia y el *compliance*.

A.5.3 Roles, responsabilidades y autoridades

A.5.3.1 Órgano de gobierno y alta dirección

El involucramiento activo y la supervisión por parte de un órgano de gobierno es una parte integral de un sistema de gestión del *compliance* eficaz. Lo anterior contribuye a asegurar que los empleados comprenden plenamente la política de *compliance* y los procedimientos operacionales de *compliance* de la organización y cómo se aplican en sus trabajos, así como a que las obligaciones de *compliance* se lleven a cabo con eficacia.

Para que un sistema de gestión del *compliance* sea eficaz, se necesita que el órgano de gobierno y la alta dirección prediquen con el ejemplo, adhiriéndose y apoyando activa y visiblemente al *compliance* y el sistema de gestión del *compliance*.

Muchas organizaciones -dependiendo de su tamaño- también tienen a una persona que tiene la responsabilidad general de la gestión del *compliance*, aunque también puede ser algo adicional a otros roles o funciones, incluidos comités existentes, unidades organizacionales, o contratar externamente algunos elementos a expertos en *compliance*.

La alta dirección debería fomentar comportamientos que crean en el *compliance* y lo apoyen y no debería tolerar comportamientos que comprometen el *compliance*.

La alta dirección debería asegurar:

— el alineamiento de los compromisos de *compliance* de la organización con sus valores, objetivos y estrategia para posicionar el *compliance* de forma adecuada;

— el impulso para que todos los empleados acepten la importancia de alcanzar los objetivos de *compliance* de los que son responsables o sobre los que tienen que rendir cuentas;

— la creación de un entorno en el que se fomente que se informe sobre los no cumplimientos de *compliance* y en el que se proteja de represalias al empleado que informe;

— que el *compliance* se incorpora a la cultura más amplia de la organización y a las iniciativas de cambio cultural;

— la identificación de los no cumplimientos de *compliance* y actuar de forma inmediata para corregirlos o gestionarlos;

— que los objetivos y metas operacionales no comprometen un comportamiento adecuado.

La alta dirección debería revisar el desempeño del sistema de gestión del *compliance* a intervalos planificados (por ejemplo, trimestral o mensualmente) haciendo referencia a los KPIs y otra información clave para asegurar que el sistema de gestión del *compliance* logre sus objetivos.

La eficacia de un sistema de gestión del *compliance* requiere de un compromiso de la alta dirección mediante el establecimiento de normas y un ejercicio de supervisión razonable. La alta dirección debería tener conocimiento del contenido y la operación del sistema de gestión del *compliance* y debería asegurarse de que la organización tiene los procesos adecuados para un sistema de gestión del *compliance* eficaz.

A.5.3.2 Función de *compliance*

Muchas organizaciones tienen una persona dedicada (por ejemplo, un responsable de *compliance* o *compliance officer*) responsable de la gestión del *compliance* en el día a día, y otras tienen un comité de *compliance* multifuncional para coordinar el *compliance* en toda la organización. La función de *compliance* trabaja en conjunto con la dirección.

No todas las organizaciones crearán una función de *compliance* separada, algunas pueden asignar esta función a una posición existente o contratar externamente esa función. Cuando se contrate externamente, las organizaciones deberían considerar no asignar la totalidad de la función de *compliance* a terceras partes. Incluso si contrata externamente parte de la función, debería considerar mantener la autoridad sobre ella y vigilar esas funciones.

Cuando se asigne la responsabilidad del sistema de gestión del *compliance*, se debería considerar asegurar que la función de *compliance* demuestra:

— la integridad y el compromiso con el *compliance*;

— las habilidades de comunicación eficaz y de capacidad de influencia;

— la capacidad y el prestigio para que sus consejos y directrices tengan aceptación;

— la competencia pertinente para diseñar, implementar y mantener los sistemas de gestión del *compliance*;

— la firmeza, los conocimientos del negocio y la experiencia para probar y afrontar desafíos;

— un enfoque estratégico y proactivo hacia el *compliance*;

— que dispone de tiempo suficiente para cumplir las necesidades del puesto.

La función de *compliance* debería tener autoridad, respaldo e independencia. Autoridad significa que el órgano de gobierno y la alta dirección conceden poderes suficientes a la función de *compliance*. Respaldo significa que es probable que otros empleados escuchen y respeten su opinión. Independencia significa que el involucramiento personal de la función de *compliance* se encuentra lo más alejada posible de las actividades expuestas a riesgos de *compliance*.

La función de *compliance* debería estar libre de conflictos de intereses para cumplir su papel.

A.5.3.3 Dirección

Las responsabilidades de la alta dirección no deberían verse como una exoneración a otros niveles de la dirección de sus responsabilidades de *compliance*, ya que todos los directivos tienen un papel que jugar con relación al sistema de gestión del *compliance*. Es, por tanto, importante que se establezcan claramente sus respectivas responsabilidades y que se incluyan en sus descripciones de puesto de trabajo.

Las responsabilidades de *compliance* de los directivos variarán, necesariamente, en función de los niveles de autoridad, influencia y otros factores, tales como la naturaleza y el tamaño de la organización. Sin embargo, es probable que algunas responsabilidades sean probablemente comunes a través de una variedad de organizaciones.

A.5.3.4 Personal

Se espera que todo el personal cumpla con las obligaciones de *compliance*.

El personal debería asegurarse de que conoce sus responsabilidades de *compliance* y de que las lleva a cabo de forma eficaz. Para ello, recibirán el apoyo de los elementos del sistema de gestión del *compliance*, como formación, políticas y procedimientos y el código de conducta.

El personal debería ser proactivo y contribuir al conocimiento y las mejoras que podrían ayudar en el desempeño del sistema de gestión del *compliance*.

A.6 Planificación

A.6.1 Acciones para abordar los riesgos y oportunidades

La planificación para el sistema de gestión del *compliance* se realiza a nivel estratégico, frente a la planificación de las operaciones que se realiza para la planificación y el control operacional.

El propósito de planificar es anticipar escenarios y consecuencias potenciales y, por tanto, tiene carácter preventivo. Basándose en los resultados de la evaluación de los riesgos de *compliance*, la organización debería planificar cómo abordar los efectos no deseados antes de que ocurran y cómo beneficiarse de las condiciones o circunstancias favorables que pueden apoyar la eficacia del sistema de gestión del *compliance*.

La planificación debería también incluir la determinación de cómo incorporar las acciones consideradas necesarias o beneficiosas para el sistema de gestión del *compliance* en las actividades y procesos de negocio. La incorporación puede lograrse mediante el establecimiento de objetivos, control operacional u otras cláusulas específicas (por ejemplo, provisión de recursos, competencia). También se deberían planificar las medidas para evaluar la eficacia del sistema de gestión del *compliance*. Estas pueden incluir, el seguimiento, las técnicas de medición, la auditoría interna o la revisión por la dirección.

A.6.2 Objetivos de *compliance* y planificación para lograrlos

Los objetivos deberían especificarse de forma que se puedan medir los resultados.

Un ejemplo de objetivo de *compliance*: impartir formación en *compliance* al personal pertinente al menos una vez al año.

Se deberían determinar las acciones que se requieren para lograr los objetivos (es decir, "qué") y un marco temporal asociado (es decir, "cuándo") y la persona responsable (es decir, "quién"). El estado y progreso de los objetivos debería ser objeto de seguimiento periódico, registrarse, evaluarse y actualizarse cuando sea necesario.

A.7 Apoyo

A.7.1 Recursos

Los recursos incluyen recursos financieros, humanos y técnicos, así como el acceso a asesoramiento externo y a habilidades especializadas, infraestructura organizacional, desarrollo profesional, tecnología y material de referencia actual sobre la gestión del *compliance* y las obligaciones legales.

A.7.2 Competencia

A.7.2.1 Generalidades

El término "competencia" significa la capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos. La competencia requiere de conocimientos, experiencia y habilidades para que esa persona pueda realizar su función de forma eficaz. La organización debería determinar para todo el personal la experiencia y los conocimientos necesarios para que cumplan con sus tareas de modo que la organización pueda proporcionar sus productos y servicios a los clientes. La organización debería establecer evidencia de la competencia (por ejemplo, descripciones de los puestos de trabajo, declaraciones de posiciones) que se puedan considerar al cubrir los puestos.

Las medidas (por ejemplo, la formación) deberían adoptarse para asegurar que las competencias existentes se mantienen y se adquieren nuevas. Debería existir documentación adecuada de las competencias, así como de las medidas adoptadas para mantener o adquirir esas competencias.

A.7.2.2 Proceso de empleo

Antes de contratar personal o de promocionar al personal existente, la organización debería llevar a cabo la debida diligencia que podría incluir comprobaciones de referencias o de antecedentes.

A.7.2.3 Formación

El órgano de gobierno, la dirección y el personal con obligaciones de *compliance* deberían ser capaces de cumplirlas de forma eficaz. La obtención de esa capacidad se puede lograr de muchas maneras, incluso las habilidades y conocimientos que se requieran, a través de educación, formación o experiencia profesional.

El objetivo de un programa de formación es asegurar que el personal es competente para cumplir con su rol profesional de forma consistente con la cultura de *compliance* de la organización y con el compromiso que tiene con el *compliance*.

Una formación diseñada y ejecutada adecuadamente puede proporcionar una manera eficaz para que el personal comunique riesgos de *compliance* que previamente no hubieran sido identificados.

La educación y formación deberían:

— cuando sea necesario, estar basadas en una evaluación de las carencias de conocimientos y competencias del empleado;

— ser lo suficientemente flexibles como para tener en cuenta varias técnicas para adaptarse a las diferentes necesidades de las organizaciones y del personal;

— diseñarse, desarrollarse e impartirse por personal experimentado y cualificado;

— impartirse en la lengua local cuando sea aplicable;

— ser valoradas y evaluadas desde el punto de vista de su eficacia de forma periódica.

La formación interactiva puede ser la mejor forma de impartir formación si los no cumplimientos de *compliance* pudieran tener consecuencias serias.

La organización debería proporcionar formación en el ámbito en el que se han producido malas prácticas.

Se debería considerar la necesidad de impartir formación adicional en *compliance* siempre que haya:

— unos cambios en la posición o en las responsabilidades;

— un cambio en las políticas, procesos y procedimientos internos;

— un cambio en la estructura organizacional;

— unos cambios en las obligaciones de *compliance*, especialmente en los requisitos legales y los requisitos de las partes interesadas;

— unos cambios en las actividades, productos y servicios;

— unas cuestiones identificadas en el seguimiento, auditorías, revisiones, reclamaciones y no cumplimientos de *compliance*, incluidas las opiniones de las partes interesadas.

A.7.3 Toma de conciencia

La toma de conciencia implica que las políticas de *compliance* son accesibles y están disponibles para todo el personal y que se comprenden.

La toma de conciencia relativa al *compliance* se puede lograr mediante métodos como, pero no limitados a:

— la formación (presencial o virtual);

— la comunicación desde la alta dirección;

— los materiales de referencia fáciles de seguir y fácilmente accesibles;

— las actualizaciones regulares sobre cuestiones de *compliance*.

Comunicar su compromiso con el *compliance*:

— sensibiliza y motiva al personal para que adopte el sistema de gestión del *compliance*;

— anima a los empleados a que hagan sugerencias que faciliten la mejora continua del desempeño del *compliance*.

A.7.4 Comunicación

Se debería adoptar un enfoque práctico de comunicación externa, dirigido a todas las partes interesadas, de acuerdo con la política de la organización.

Las partes interesadas pueden incluir organismos reguladores, clientes, contratistas, proveedores, inversores, servicios de emergencia, organizaciones no gubernamentales y vecinos.

La organización debería asignar los recursos adecuados y personas con los conocimientos pertinentes para coordinar y facilitar la interacción reglamentaria.

Los métodos de comunicación pueden incluir páginas web y correos electrónicos, comunicados de prensa, anuncios y boletines periódicos, informes anuales (o con otra periodicidad), discusiones informales, jornadas de puertas abiertas, grupos de trabajo, diálogo con la comunidad, involucramiento en eventos de la comunidad y líneas telefónicas directas. Estos enfoques pueden apoyar el entendimiento y la aceptación del compromiso con el *compliance* de una organización.

Las comunicaciones deberían observar los principios de transparencia, adecuación, credibilidad, capacidad de respuesta, accesibilidad y claridad.

A.7.5 Información documentada

A.7.5.1 Generalidades

La información documentada puede incluir:

— la política y los procedimientos de *compliance* de la organización;

— los objetivos, las metas, la estructura y el contenido del sistema de gestión del *compliance*;

— la asignación de roles y las responsabilidades de *compliance*;

— un registro de las obligaciones de *compliance* pertinentes;

— los registros de los riesgos de *compliance* y la priorización del tratamiento basada en el proceso de evaluación de riesgos de *compliance*;

— un registro de los no cumplimientos de *compliance*, conatos de no cumplimientos y de las investigaciones;

— los planes anuales de *compliance*;

— los registros personales, que incluyen, pero no se limitan a, los registros de formación;

— el proceso de auditoría, el calendario de auditoría y los registros de auditoría asociados.

La información documentada puede incluir materias relacionadas con los requisitos de información regulatorios. La información documentada puede comprender todo tipo de medios (digitales y no digitales).

A.7.5.2 Creación y actualización de información documentada

La información documentada debería actualizarse para reflejar los cambios internos y externos y así demostrar que están y permanecen actualizados.

A.7.5.3 Control de la información documentada

La información documentada se puede preparar con el propósito de obtener asesoramiento legal y, por tanto, puede estar sometida a privilegio legal.

A.8 Operación

A.8.1 Planificación y control operacional

Un sistema de gestión del *compliance* bien diseñado comprende medidas (es decir, políticas, procesos y procedimientos) que aportan tanto contenido como efectos a la cultura de *compliance*. Abordan y tienen por objetivo reducir los riesgos identificados como parte del proceso de evaluación de los riesgos de *compliance*.

Un elemento básico del control operacional es un código de conducta que establece, entre otras cosas, el compromiso total de la organización con las obligaciones de *compliance* pertinentes. Un código de conducta debería ser aplicable a todo el personal y ser accesible a todos ellos. Basadas y derivadas de un código de conducta, las medidas de *compliance* deberían incorporarse a las operaciones diarias de la organización para fomentar la cultura de *compliance*.

Los controles operacionales se requieren para situaciones relacionadas con los procesos de negocio cuando la falta de tales controles podría llevar a desviaciones de la política de *compliance* o a un

incumplimiento de las obligaciones de *compliance*. Estas situaciones pueden relacionarse con todas las situaciones, actividades o procesos de negocio (ejemplo: producción, instalación, revisión o mantenimiento) o con contratistas, proveedores o vendedores.

El grado de control puede variar dependiendo de varios factores, como la importancia o la complejidad de las funciones realizadas, las consecuencias potenciales de no cumplimiento de *compliance* o el apoyo técnico involucrado o disponible.

Cuando los controles operacionales fallan, es necesario tomar acciones para abordar cualquier resultado o efecto no deseado.

En caso de uso de procesos de terceras partes o de contratación externa de las actividades de la organización, la organización debería llevar a cabo una debida diligencia eficaz para asegurar que sus estándares y compromisos con el *compliance* no se rebajan. Un ejemplo de terceras partes podría estar relacionado con el suministro de productos y servicios y la distribución de productos. La organización debería asegurar que los acuerdos de nivel de servicio (SLAs, por sus siglas en inglés) adecuado que especifican las obligaciones de *compliance* para el proveedor de servicio se formalizan.

Un proceso contratado externamente bien diseñado considera lo siguiente:

— la debida diligencia anterior de la asignación y continua;

— la implementación de controles adecuados;

— la realización de un seguimiento continuo;

— una revisión adecuada de acuerdos legales/contractuales;

— la consideración de acuerdos de nivel de servicio (SLAs, por sus siglas en inglés);

— utilizar terceras partes certificadas conforme a este documento.

Al contratar con terceras partes, la organización debería implementar controles para asegurar que los aspectos relativos a las compras, los aspectos operativos, comerciales y otros aspectos no financieros de sus actividades se estén gestionando adecuadamente. Dependiendo del tamaño de la organización y de la transacción, los controles sobre las compras y los controles operativos, comerciales y otros controles no financieros implementados por una organización pueden reducir los riesgos de *compliance*.

A.8.2 Establecimiento de controles y procedimientos

Se necesitan controles eficaces para asegurar que se cumplen las obligaciones de *compliance* y que se previenen, o se detectan y corrigen, los no cumplimientos de *compliance*. Los controles deberían diseñarse con el rigor suficiente para facilitar el logro de las obligaciones de *compliance* específicas de las actividades de la organización y del entorno en el que opera. Cuando sea posible, dichos controles deberían estar integrados en los procesos organizacionales normales.

Los controles pueden incluir:

— las políticas operativas, los procesos, los procedimientos, e instrucciones de trabajo documentados, claros, prácticos y fáciles de seguir;

— los sistemas e informes de excepciones;

— las autorizaciones;

— la segregación de roles y las responsabilidades incompatibles;

— los procesos automatizados;

— los planes anuales de *compliance*;

— los planes de desempeño de empleados;

— las evaluaciones de *compliance* y las auditorías;

— el compromiso demostrado de la dirección y comportamiento ejemplarizante y otras medidas para promover un comportamiento cumplidor;

— la comunicación activa, abierta y frecuente sobre el comportamiento esperado de los empleados (estándares y valores, códigos de conducta).

Al desarrollar los procedimientos que apoyan la gestión del *compliance*, se debería considerar lo siguiente:

— la integración de las obligaciones de *compliance* en procedimientos, incluidos los sistemas informáticos, los formularios, los sistemas de información, los contratos y otra documentación legal;

— la consistencia con otras funciones de revisión y el control de la organización;

— el seguimiento y medición continuos;

— la evaluación e información (incluida la supervisión de la dirección) para asegurar que los empleados cumplen con los procedimientos;

— las disposiciones específicas para identificar, informar y comunicar a niveles superiores casos de no cumplimientos de *compliance* y riesgos de no cumplimientos de *compliance*.

A.8.3 Planteamiento de inquietudes

Cuando sea necesario, la comunicación a niveles superiores debería llegar a la alta dirección y al órgano de gobierno, incluidos los comités pertinentes.

Incluso en los casos en los que no lo requiera la reglamentación local, las organizaciones deberían considerar desarrollar un mecanismo de denuncias que permita el anonimato o la confidencialidad, a través de los cuales los empleados y agentes de la organización puedan informar o buscar orientación en términos de no cumplimiento de *compliance* sin miedo a represalias.

Para información adicional sobre sistemas de gestión de los canales de denuncia, véase la Norma ISO 37002.

A.8.4 Procesos de investigación

Una característica de un sistema de gestión del *compliance* eficaz es un mecanismo que funcione bien para las investigaciones oportunas y exhaustivas de cualquier alegación o sospecha de malas prácticas por parte de la organización, su personal o terceras partes pertinentes. Esto incluye la documentación de la respuesta de la organización, incluidas las medidas disciplinarias o de remediación tomadas y las revisiones del sistema de gestión del *compliance* que consideran las lecciones aprendidas.

Un mecanismo de investigación eficaz identifica las causas raíz de malas prácticas, vulnerabilidades del sistema de gestión del *compliance* y los fallos en la rendición de cuentas, incluso entre directivos, la alta dirección y el órgano de gobierno. Un análisis profundo de las causas raíz aborda el alcance y la generalización del no cumplimiento de *compliance*, la cantidad y el nivel del personal involucrado, la gravedad, duración y frecuencia del no cumplimiento de *compliance*.

Las organizaciones deberían asegurarse de que las investigaciones sean justas e independientes. Deberían considerar, cuando corresponda, la creación de comités independientes para supervisar las investigaciones y asegurar que sean completas e independientes.

La organización debería establecer un mecanismo de información de las investigaciones que incluya el nivel superior al que tienen que informar de los hallazgos de las investigaciones.

NOTA En ocasiones, la ley exige que las organizaciones informen sobre los no cumplimientos de *compliance*. En esos casos, las autoridades regulatorias necesitan ser informadas de acuerdo con la legislación aplicable o según lo convenido.

Aun cuando la legislación no requiera que las organizaciones informen sobre los no cumplimientos de *compliance*, estas pueden considerar hacer declaraciones voluntarias de los no cumplimientos de *compliance* a las autoridades regulatorias para mitigar las consecuencias de los no cumplimientos de *compliance*.

A.9 Evaluación del desempeño

A.9.1 Seguimiento, medición, análisis y evaluación

A.9.1.1 Generalidades

El seguimiento es el proceso por el que se recoge información con el objetivo de evaluar la eficacia del sistema de gestión del *compliance* y el desempeño del *compliance* de la organización.

El seguimiento del sistema de gestión del *compliance* típicamente incluye:

— la eficacia de la formación;

— la eficacia de los controles (por ejemplo, a través de los resultados de análisis sobre una muestra);

— la asignación eficaz de responsabilidades para cumplir con las obligaciones de *compliance*;

— la actualización de las obligaciones de *compliance*;

— la eficacia en la gestión de fallos de *compliance* previamente identificados;

— los casos en los que no se llevan a cabo inspecciones internas de *compliance* según lo previsto;

— las revisiones de la estrategia de negocio frente a los riesgos de *compliance*, con ánimo de poder actualizarla apropiadamente.

El seguimiento del desempeño del *compliance* típicamente incluye:

— los no cumplimientos de *compliance* y conatos (es decir, incidentes sin efectos adversos);

— los casos en los que no se cumplen las obligaciones de *compliance*;

— los casos en los que no se alcanzan los objetivos;

— el estado de la cultura de *compliance*;

— los indicadores predictivos y reactivos establecidos.

A.9.1.2 Fuentes de opinión sobre el desempeño del *compliance*

Las fuentes incluyen:

— el personal (por ejemplo, a través de canales de denuncias, líneas de ayuda, buzones de opinión y de sugerencias);

— los clientes, por ejemplo, a través de un sistema de gestión de reclamaciones;

— las terceras partes;

— los proveedores;

— los contratistas,

— los reguladores;

— los registros de control de procesos y registros de actividad (incluidos tanto electrónicos como en papel).

Las opiniones del desempeño del *compliance* pueden incluir:

— las cuestiones de *compliance;*

— los no cumplimientos de *compliance* e inquietudes relativas al *compliance*;

— las cuestiones de *compliance* que emerjan;

— los cambios continuos regulatorios y organizacionales;

— los comentarios sobre la eficacia y el desempeño del *compliance*.

Existen muchos métodos para recoger información. Cada método que se relaciona más abajo es pertinente en distintas circunstancias y se deberían seleccionar con cuidado las diferentes herramientas para que sean adecuadas al tamaño, escala, naturaleza y complejidad de la organización.

La recopilación de información puede incluir:

— los informes ad hoc de no cumplimientos de *compliance* cuando aparecen o son identificados;

— la información obtenida en líneas directas, reclamaciones y otras fuentes, incluido el canal de denuncias,

— las discusiones informales, los talleres de trabajo y los grupos temáticos;

— las pruebas integrales y por muestreo, tales como cliente espía (*mystery shopping*);

— los resultados de encuestas de percepción;

— las observaciones directas, las entrevistas formales, las visitas a las instalaciones e inspecciones;

— las auditorías y las revisiones;

— las consultas a las partes interesadas, peticiones de formación y opiniones recogidas durante la formación (especialmente las de los empleados).

Se debería desarrollar un sistema para la clasificación, el almacenamiento y la recuperación de la información.

Los sistemas de gestión de la información deberían registrar tanto las cuestiones como las reclamaciones y permitir la clasificación y el análisis de aquellas relacionadas con el *compliance*. El análisis debería considerar los problemas sistémicos y recurrentes para proceder a su corrección o mejora ya que es probable que conlleven riesgos de *compliance* significativos para la organización y pueden ser más difíciles de identificar.

Los criterios para la clasificación de la información pueden incluir:

— la fuente;

— el departamento;

— la descripción del no cumplimiento de *compliance*;

— las referencias de la obligación;

— los indicadores;

— la severidad;

— el impacto real o potencial.

A.9.1.3 Desarrollo de indicadores

Este proceso debería tener en cuenta los resultados de la evaluación de los riesgos de *compliance* para asegurar que los indicadores están relacionados con las principales características de los riesgos de *compliance* de la organización. La cuestión de qué y cómo medir el desempeño del *compliance* puede ser compleja en ocasiones, pero sin embargo es un factor vital para demostrar la eficacia del sistema de gestión del *compliance*. Además, los indicadores necesarios variarán a medida que la organización madure, así como con el ritmo y alcance de los programas nuevos y revisados que se implementen.

Los indicadores pueden incluir:

— el porcentaje de empleados a los que se haya impartido formación de forma eficaz;

— la frecuencia de los contactos con los reguladores;

— la utilización de mecanismos para obtener opiniones (incluidos los comentarios sobre el valor de dichos mecanismos por parte de los usuarios).

Los indicadores reactivos pueden incluir:

— las cuestiones de no cumplimientos de *compliance* identificados y comunicados, por tipo, área y frecuencia;

— las consecuencias de los no cumplimientos de *compliance*, que pueden incluir una valoración del impacto que resulte de compensaciones monetarias, multas y otras sanciones, coste de remediación, pérdida de reputación o coste del tiempo de los empleados;

— la cantidad de tiempo utilizado para informar y tomar acciones correctivas.

Los indicadores predictivos pueden incluir:

— los riesgos de no cumplimientos de *compliance*, medidos como la pérdida/ganancia potencial de los objetivos (ingresos, salud y seguridad, reputación, etc.) a lo largo del tiempo;

— las tendencias de no cumplimientos de *compliance* (la tasa de *compliance* esperada basada en tendencias pasadas).

A.9.1.4 Informes de *compliance*

Mientras que los informes de problemas sistémicos y recurrentes son particularmente importantes, un no cumplimiento de *compliance* puntual puede ser igualmente preocupante si es grave o deliberado. Incluso un fallo pequeño puede indicar una gran debilidad en los procesos actuales y en el sistema de gestión del *compliance*. Si no se informa sobre él oportunamente, puede llevar a pensar que el fallo no importa y puede dar lugar a que dicho fallo se convierta en un problema sistémico.

Los informes de *compliance* pueden incluir:

— cualquier materia sobre la que la organización deba notificar a cualquier autoridad reguladora;

— los cambios en las obligaciones de *compliance*, en su impacto en la organización y las propuestas para cumplir con las nuevas obligaciones;

— la medición del desempeño del *compliance*, que incluye los no cumplimientos de *compliance* y la mejora continua;

— el número y los detalles de posibles no cumplimientos de *compliance* y su análisis subsiguiente;

— las acciones correctivas adoptadas;

— la información sobre la eficacia del sistema de gestión del *compliance*, sus logros y tendencias;

— los contactos y el desarrollo de las relaciones con los reguladores;

— los resultados de las auditorías, así como de las actividades de seguimiento;

— el seguimiento de la ejecución completa de los planes de acción, especialmente aquellos derivados de informes de auditoría y/o requisitos del regulador.

La política de *compliance* debería fomentar el informe inmediato de cuestiones significativas que surjan fuera de los periodos previstos para el informe periódico.

A.9.1.5 Mantenimiento de registros

El mantenimiento de registros debería incluir el registro y clasificación de las cuestiones de *compliance* y los presuntos no cumplimientos de *compliance* y los pasos dados para resolverlos.

Los registros deberían almacenarse de manera que se asegure que permanecen legibles, fácilmente identificables y recuperables.

Estos registros deberían protegerse contra cualquier adición, borrado, modificación, uso no autorizado u ocultación.

Los registros del sistema de gestión del *compliance* de la organización pueden incluir:

— la información sobre el desempeño del *compliance*, incluidos los informes de *compliance*;

— los detalles de los no cumplimientos de *compliance* y acciones correctivas;

— los resultados de las revisiones y de las auditorías de los sistemas de gestión del *compliance* y las acciones adoptadas.

A.9.2 Auditoría interna

Las funciones de auditoría, ya sean internas o externas, deberían estar libres de conflicto de intereses y ser independientes para cumplir su rol.

Véase la Norma ISO 19011 para obtener información sobre cómo realizar una auditoría de un sistema de gestión.

A.9.3 Revisión por la dirección

La revisión por la dirección debería incluir también recomendaciones sobre:

— la necesidad de cambios en la política de *compliance* y en sus objetivos, sistemas, estructura y personal asociados;

— los cambios en los procesos de *compliance* para asegurar la integración eficaz con las prácticas operacionales y los sistemas;

— las áreas sobre las que hacer seguimiento de no cumplimientos de *compliance* futuros potenciales;

— las acciones correctivas respecto a los no cumplimientos de *compliance*;

— las lagunas o carencias en los sistemas del *compliance* actuales e iniciativas de mejora continua más a largo plazo;

— el reconocimiento de un comportamiento de *compliance* ejemplar dentro de la organización.

Al órgano de gobierno se le debería facilitar una copia de los resultados documentados y cualquier recomendación de la revisión por la dirección.

A.10 Mejora

A.10.1 Mejora continua

La eficacia de un sistema de gestión del *compliance* se caracteriza por el hecho de tener la capacidad de mejorar y evolucionar continuamente. El entorno interno y externo y el negocio de la organización cambian con el tiempo, igual que cambia la naturaleza de sus clientes y las obligaciones de *compliance* aplicables.

La adecuación y eficacia del sistema de gestión del *compliance* debería evaluarse de forma continuada y regular mediante varios métodos, por ejemplo, con revisiones o auditorías internas.

La organización debería establecer medidas para revisar su sistema de gestión del *compliance* y asegurar que se mantiene actual y adecuado a su propósito. Al determinar el alcance y el marco temporal de las acciones que apoyan la mejora continua, la organización debería considerar su contexto, factores económicos y otras circunstancias pertinentes.

Algunas organizaciones realizan encuestas a los empleados para medir la cultura de *compliance* y evaluar la solidez de los controles. Otras fuentes de información para la mejora continua pueden ser los resultados de las encuestas realizadas a los clientes, los informes en los que se plantean inquietudes, los seguimientos regulares, las auditorías periódicas o las revisiones por la dirección.

La organización debería considerar los resultados y aportaciones de estas evaluaciones para determinar si existe la necesidad o la oportunidad de cambiar el sistema de gestión del *compliance*.

Con el fin de ayudar a asegurar que se mantienen la integridad y eficacia del sistema de gestión del *compliance*, los cambios en los elementos individuales del sistema de gestión deberían tener en cuenta la dependencia y el impacto de tales cambios en la eficacia del sistema de gestión en su conjunto.

Al realizar cambios en el sistema de gestión del *compliance*, la organización debería considerar las implicaciones que los cambios tienen en el sistema de gestión del *compliance*, sus operaciones, la disponibilidad de recursos, las evaluaciones de los riesgos de *compliance*, las obligaciones de *compliance* de la organización y sus procesos de mejora continua.

A.10.2 No conformidades y acciones correctivas

La falta de prevención o detección de un no cumplimiento de *compliance* puntual no significa necesariamente que el sistema de gestión del *compliance* no sea eficaz para prevenir y detectar un no cumplimiento de *compliance*.

La información obtenida del análisis de una no conformidad o de un no cumplimiento *de compliance* puede usarse para considerar:

— evaluar el desempeño del producto y servicio;

— mejorar o rediseñar productos y servicios;

— cambiar las prácticas y procedimientos de la organización;

— repetir la formación de los empleados;

— reevaluar la necesidad de informar a las partes interesadas;

— proporcionar una alerta temprana sobre un potencial no cumplimiento de *compliance*;

— rediseñar o revisar los controles;

— mejorar las etapas de notificación e información a niveles superiores (internos y externos);

— comunicar los hechos que rodean el no cumplimiento de *compliance* y la posición de la organización en relación con el no cumplimiento de *compliance*.

La organización debería identificar las causas raíz por las que no se han seguido las políticas y/o los procedimientos, que hayan contribuido a una conducta desviada y actualizar la política y el procedimiento en base a las lecciones aprendidas.

Bibliografía

[1] ISO 9000, *Sistemas de gestión de la calidad — Fundamentos y vocabulario*

[2] ISO 9001, *Sistemas de gestión de la calidad — Requisitos*

[3] ISO 14001, *Sistemas de gestión ambiental — Requisitos con orientación para su uso*

[4] ISO 19011, *Directrices para la auditoría de los sistemas de gestión*

[5] ISO 22000, *Sistemas de gestión de la inocuidad de los alimentos — Requisitos para cualquier organización en la cadena alimentaria*

[6] ISO 26000, *Guía de responsabilidad social*

[7] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO 31000, *Gestión del riesgo — Directrices*

[9] IEC 31010, *Risk management — Risk assessment techniques*

[10] ISO 37000, *Guidance for the governance of organizations*

[11] ISO 37001, *Sistemas de gestión antisoborno — Requisitos con orientación para su uso*

[12] ISO 37002, *Whistleblowing management systems — Guidelines*

[13] ISO Guide 73, *Risk management — Vocabulary*

ICS 03.100.01; 03.100.02; 03.100.70

Precio basado en 40 páginas

Traducción oficial/Official translation/Traduction officielle

Calle Olof Palme, Esq. Núñez de Cáceres, San Gerónimo.
Santo Domingo, República Dominicana.
(809) 686-2205