norma española

UNE-ISO 19600

Abril 2015

TÍTULO

Sistemas de gestión de *compliance*

Directrices

Compliance management systems. Guidelines.

Systèmes de management de la conformité. Lignes directrices.

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO 19600:2014.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 307 *Gestión de riesgos* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 12496:2015

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

36 Páginas

Índice

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de las normas internacionales normalmente se realiza 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, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica.

En la parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar esta norma y para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Esta norma se redactó de acuerdo a las reglas editoriales de la parte 2 de las Directivas ISO/IEC. 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 cualquiera o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de esta norma se indican en la introducción y/o en la lista ISO de declaraciones de patente recibidas. www.iso.org/patents.

Cualquier nombre comercial utilizado en esta norma es información a la atención de los usuarios y no constituyen una recomendación.

Para obtener una explicación sobre el significado de los términos específicos de ISO y expresiones relacionadas con la evaluación de la conformidad, así como información de la adhesión de ISO a los principios de la OMC (Organización Mundial del Comercio) respecto a los obstáculos técnicos al comercio (TBT), véase la siguiente dirección: http://www.iso.org/iso/home/standards_development/resources-for-technical-work/foreword.htm.

El comité responsable de esta norma es el Comité de Proyecto ISO/PC 271, *Sistemas de Gestión del Cumplimiento*.

0 Introducción

Las organizaciones cuya meta es tener éxito a largo plazo necesitan mantener una cultura de integridad y de cumplimiento, así como tomar en consideración las necesidades y expectativas de las partes interesadas. Integridad y *compliance*, por tanto, no sólo son la base, sino también una oportunidad para una organización de éxito y sostenible.

Compliance es el resultado de que una organización cumpla con sus obligaciones, y se hace sostenible introduciéndola en la cultura de la organización y en el comportamiento y en la actitud de las personas que trabajan en ella. Mientras mantenga su independencia, es preferible que la gestión de *compliance* esté integrada con los procesos de gestión de finanzas, riesgos, calidad, medio ambiente y salud y seguridad, y en sus requisitos y procedimientos operacionales.

Un sistema de gestión de *compliance* eficaz y que abarque a toda la organización permite que la organización demuestre su compromiso de cumplir con la normativa, incluyendo los requisitos legales, los códigos de la industria y los estándares de la organización, así como con los estándares de buen gobierno corporativo, las mejores prácticas, la ética y las expectativas de la comunidad en general.

El enfoque ideal de una organización hacia *compliance* consiste en que su dirección aplique los valores fundamentales y los estándares de gobierno corporativo, de ética y de relaciones con la comunidad generalmente aceptados. El que se interiorice a *compliance* en el comportamiento de las personas que trabajan en una organización depende, sobre todo, de sus directivos, en todos los niveles, y de que existan unos valores claros en la organización, así como de la aceptación y aplicación de medidas que promuevan un comportamiento de cumplimiento. Si eso no sucede así en todos los niveles de la organización, existe riesgo de incumplimiento.

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

Las organizaciones están cada vez más convencidas de que si aplican valores obligatorios y una gestión adecuada de *compliance*, pueden salvaguardar su integridad y evitar o minimizar los incumplimientos legales. Integridad y un *compliance* eficaz son, por tanto, elementos clave para llevar una buena y diligente gestión. *Compliance* también contribuye al comportamiento socialmente responsable de las organizaciones.

Esta norma internacional no especifica requisitos, sino que proporciona una guía para los sistemas de gestión de *compliance* y prácticas recomendadas. Se pretende que la guía que proporciona esta norma internacional sea adaptable, por lo que el uso de esta guía puede diferir de acuerdo con el tamaño y el nivel de madurez del sistema de gestión de *compliance* de una organización y de acuerdo con el contexto, la naturaleza y la complejidad de las actividades de la organización, incluyendo su política de *compliance* y sus objetivos.

El flujograma de la figura 1 es coherente con otros sistemas de gestión y está basado en el principio de mejora continua (Planificar-Hacer-Verificar-Actuar).

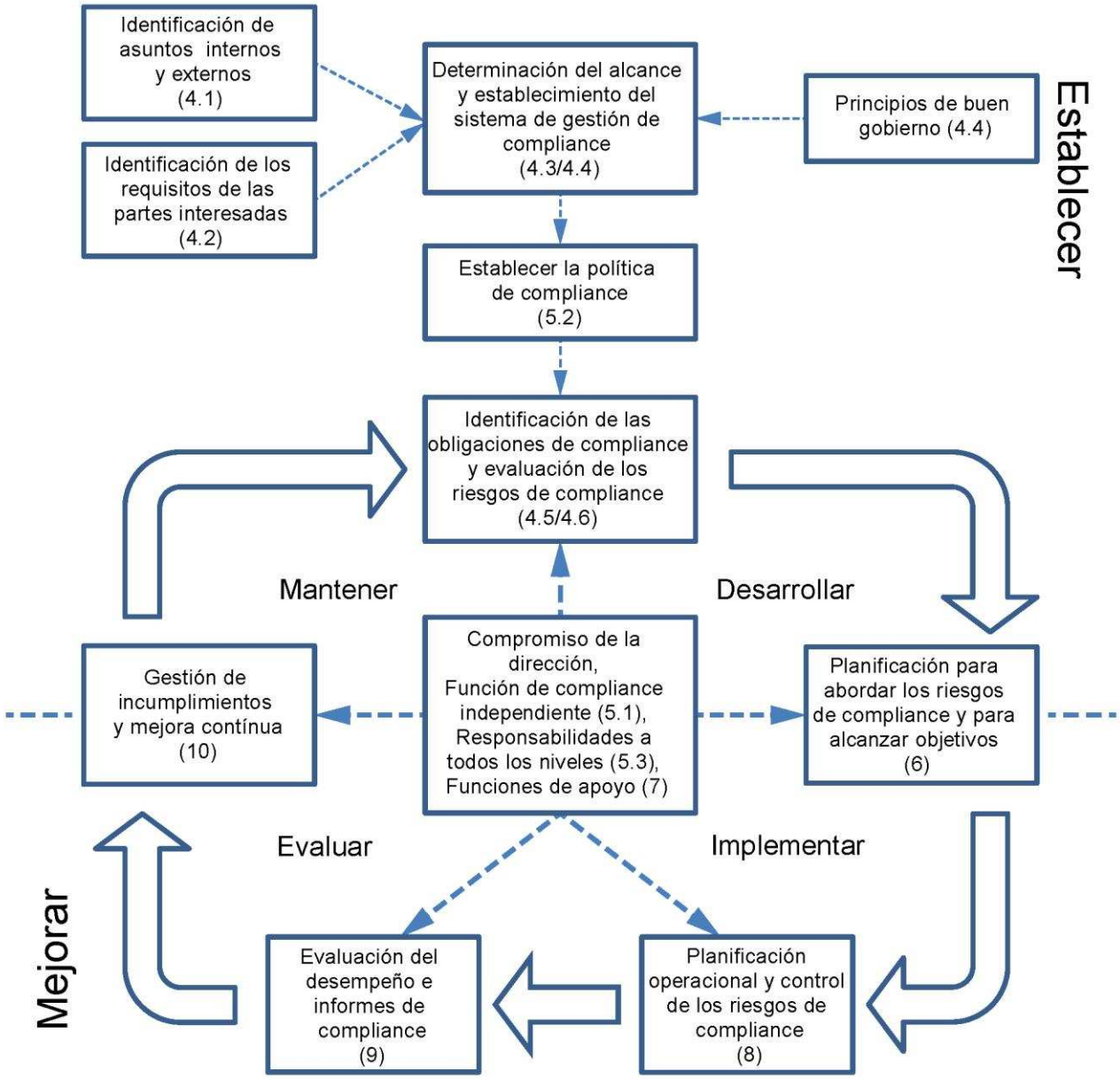

Figura 1 – Organigrama de un sistema de gestión de *compliance*

Esta norma internacional ha adoptado la "estructura de alto nivel" (es decir, secuencia de cláusulas, texto común y terminología común) desarrollada por ISO para mejorar el alineamiento entre sus normas internacionales para sistemas de gestión. Además de una guía genérica sobre un sistema de gestión de *compliance*, esta norma internacional también proporciona un marco para ayudar en la implementación de cuestiones relacionadas con *compliance* en cualquier sistema de gestión.

Las organizaciones que no hayan adoptado normas de sistemas de gestión o un marco de gestión de *compliance* pueden adoptar fácilmente esta norma internacional como una guía independiente en su organización.

Esta norma internacionales adecuada 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*.

Esta norma internacional puede combinarse con normas de sistemas de gestión existentes (por ejemplo, las Normas ISO 9001, ISO 14001, ISO 22000) y con guías genéricas (por ejemplo, ISO 31000, ISO 26000).

1 Objeto y campo de aplicación

Esta norma internacional proporciona orientación para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de *compliance* eficaz y que genera respuesta por parte de la organización.

Las directrices sobre sistemas de gestión de *compliance* son aplicables a todo tipo de organizaciones. El alcance de la aplicación de estas directrices depende del tamaño, estructura, naturaleza y complejidad de la organización. Esta norma internacional se basa en los principios de buen gobierno, proporcionalidad, transparencia y sostenibilidad.

2 Normas para consulta

No hay normas para consulta.

3 Términos y definiciones

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

3.1 organización:
Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus *objetivos* (3.9).

NOTA 1 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 éstas, ya estén constituidas o no , públicas o privadas.

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

NOTA a la versión en español Los términos en inglés “interested party” y “stakeholder” tienen una traducción única al español como “parte interesada”.

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

NOTA 1 La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

NOTA 2 Si el alcance del sistema de gestión (3.7) comprende sólo una parte de una organización, entonces “alta dirección” se refiere a quienes dirigen y controlan esa parte de la organización.

3.4 órgano de gobierno:
Persona o grupo de personas que gobiernan una *organización* (3.1), establecen las direcciones y a quienes la *alta dirección* (3.3) rinde cuentas.

3.5 empleado:
Individuo con una relación que está reconocida como relación laboral en la legislación nacional o en la práctica.

3.6 función de *compliance*:
Persona(s) con responsabilidad para la gestión de *compliance* (3.17).

NOTA 1 Preferiblemente se asignará la responsabilidad global de la gestión de *compliance* a un solo individuo.

3.7 sistema de gestión:
Conjunto de elementos de una *organización* (3.1) interrelacionados o que interactúan para establecer *políticas* (3.8), *objetivos* (3.9) y *procesos* (3.10) para lograr estos objetivos.

NOTA 1 Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 2 Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, etc.

NOTA 3 El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

3.8 política:
Intenciones y dirección de una *organización* (3.1), como las expresa formalmente su *alta dirección* (3.7).

3.9 objetivo:
Resultado a lograr.

NOTA 1 Un objetivo puede ser estratégico, táctico u operativo.

NOTA 2 Los objetivos pueden referirse a diferentes disciplinas (como financieras, de seguridad y salud y ambientales) y se pueden aplicar en diferentes niveles (como estratégicos, para toda la organización, para proyectos, productos y *procesos* (3.10)).

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

NOTA 4 En el contexto de sistemas de gestión de *compliance*, la organización establece los objetivos de *compliance*, en concordancia con la política de *compliance*, para lograr resultados específicos.

3.10 proceso:
Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

3.11 riesgo:
Efecto de la incertidumbre en los *objetivos* (3.9).

NOTA 1 Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

NOTA 2 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 Con frecuencia el riesgo se caracteriza por referencia a eventos potenciales (Guía ISO 73:2009, 3.5.1.3) y a consecuencias potenciales (Guía ISO 73:2009, 3.6.1.3), o a una combinación de éstos.

NOTA 4 Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad (Guía ISO 73:2009, 3.6.1.1) de que ocurra.

3.12 riesgo de *compliance*:
Efecto de la incertidumbre en los *objetivos* (3.9) de *compliance*.

NOTA 1 El riesgo de *compliance* se puede caracterizar por la probabilidad de que ocurran y las consecuencias de los incumplimientos de *compliance* (3.18) respecto a las obligaciones de *compliance* (3.16) de una organización.

3.13 requisito:
Necesidad o expectativa establecida, generalmente implícita u obligatoria.

NOTA 1 “Generalmente implícita" significa que es una costumbre o práctica común en la organización y en las partes interesadas, que la necesidad o expectativa que se considera está implícita.

NOTA 2 Un requisito especificado es el que está declarado, por ejemplo, en información documentada.

3.14 requisito de *compliance*:
Requisito (3.13) que una *organización* (3.1) tiene que cumplir.

3.15 compromiso de *compliance*:
Requisito (3.13) que una *organización* (3.1) elige cumplir.

3.16 obligación de *compliance*:
Requisito de compliance (3.14) o *compromiso de compliance* (3.15).

3.17 *compliance*:
Cumplir con todas las *obligaciones de compliance* (3.16) de una organización.

NOTA 1 *Compliance* se sostiene a través de su integración en la cultura de una *organización* (3.1) y en el comportamiento y la actitud de las personas que trabajan en ella.

3.18 incumplimiento de *compliance*:
No cumplir con una *obligación de compliance* (3.16).

NOTA 1 Un incumplimiento de *compliance* puede ser un evento único o múltiple y puede ser o no ser el resultado de una *no conformidad* (3.33).

3.19 cultura de *compliance*:
Valores, ética y creencias 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 a resultados de *compliance* (3.17).

3.20 código:
Declaración de buenas prácticas desarrollada internamente o por un organismo internacional, nacional o de la industria o por otra *organización* (3.1).

NOTA 1 El código puede ser obligatorio o voluntario.

3.21 normas organizativas y de la industria:
Códigos (3.20) documentados, buenas prácticas, estatutos, normas técnicas y estándares de la industria que se consideran relevantes para una *organización* (3.1).

3.22 autoridad regulatoria:
Organización (3.1) responsable de regular o hacer cumplir *compliance* (3.17) con *requisitos* (3.13) regulatorios y de otro tipo.

3.23 competencia:
Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

3.24 información documentada:
Información que una *organización* (3.1) tiene que controlar y mantener, y el medio en el que está contenida.

NOTA 1 La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2 La información documentada puede hacer referencia a:

- el *sistema de gestión* (3.7), incluidos los *procesos* (3.10) relacionados,
- la información creada para que la organización opere (documentación),
- la evidencia de los resultados alcanzados (registros).

3.25 procedimiento:
Forma específica de llevar a cabo una actividad o *proceso* (3.10).

3.26 desempeño:
Resultado medible.

NOTA 1 El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

NOTA 2 El desempeño se puede relacionar con la gestión de actividades, *procesos* (3.10), productos (incluidos servicios), sistemas u *organizaciones* (3.1).

3.27 mejora continua:
Actividad o *proceso* (3.10) recurrente para mejorar el *desempeño* (3.26).

3.28 externalizar (verbo):
Establecer un acuerdo mediante el cual una *organización* (3.1) externa realiza parte de una función o *proceso* (3.10) de una organización.

NOTA 1 Una organización externa está fuera del alcance del *sistema de gestión* (3.7), aunque la función o proceso externalizado forme parte del alcance.

3.29 seguimiento:
Determinación del estado de un sistema, un *proceso* (3.10) o una actividad.

NOTA 1 Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

NOTA 2 El seguimiento no es una actividad que se realice una sola vez, sino un proceso en el que se observa una situación de forma regular o continua.

3.30 medición:
Proceso (3.10) para determinar un valor.

3.31 auditoría:
Proceso (3.10) sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1 Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

NOTA 2 “Evidencia de auditoría” y “criterios de auditoría” se definen en la Norma ISO 19011.

NOTA 3 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.

3.32 conformidad:
Cumplimiento de un *requisito* (3.13).

3.33 no conformidad:
Incumplimiento de un *requisito* (3.13).

NOTA 1 Una no conformidad no es necesariamente un incumplimiento de c*ompliance* (3.18).

3.34 corrección:
Acción para eliminar una *no conformidad* (3.33) o un *incumplimiento de compliance* (3.18) detectados.

3.35 acción correctiva:
Acción para eliminar la causa de una *no conformidad* (3.33) o un *incumplimiento de compliance* (3.18) y evitar que vuelvan a ocurrir.

4 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

La organización debería determinar las cuestiones externas e internas que son pertinentes para su propósito, tales como las que se refieren a riesgos de *compliance*, y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de *compliance*. Para ello, la organización debería considerar un conjunto amplio de aspectos internos y externos, tales como el contexto regulatorio, social y cultural, la situación económica y las políticas internas, los procedimientos, los procesos y los recursos.

4.2 Compresión de las necesidades y expectativas de las partes interesadas

La organización debería determinar:

– las partes interesadas que son pertinentes al sistema de gestión de *compliance*; y

– los requisitos de estas partes interesadas.

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

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

NOTA El alcance del sistema de gestión de *compliance* pretende determinar los límites geográficos y/u organizativos a los que se aplicará el sistema de gestión de *compliance*, especialmente si la organización es parte de otra organización más amplia en una zona determinada.

Cuando se determina este alcance, la organización debería considerar:

– las cuestiones externas e internas referidas en 4.1; y

– los requisitos referidos en 4.2 y en 4.5.1

El alcance debería estar disponible como información documentada.

4.4 Sistema de gestión de *compliance* y principios de buen gobierno

La organización debería establecer, implementar, mantener y mejorar continuamente un sistema de gestión de *compliance*, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta norma internacional, tomando en consideración los siguientes principios de gobierno:

– acceso directo de la función de *compliance* al órgano de gobierno;

– independencia de la función de *compliance;*

– asignación a la función de *compliance* de la autoridad correspondiente y de recursos adecuados.

El sistema de gestión de *compliance* debería reflejar los valores, objetivos, estrategia y riesgos de *compliance* de la organización.

4.5 Obligaciones de *compliance*

4.5.1 Identificación de las obligaciones de *compliance*

La organización debería identificar sistemáticamente sus obligaciones de *compliance* y las implicaciones que éstas tienen para sus actividades, productos y servicios. La organización debería considerar estas obligaciones al establecer, desarrollar, implementar, evaluar, mantener y mejorar su sistema de gestión de *compliance*.

La organización debería documentar sus obligaciones de *compliance* de forma adecuada a su tamaño, complejidad, estructura y operaciones.

Las fuentes de las obligaciones de *compliance* deberían incluir requisitos de *compliance* y pueden incluir compromisos de *compliance*.

EJEMPLO 1 Ejemplos de requisitos de *compliance* incluyen:

– normas legales,

– permisos, licencias u otras formas de autorización,

– órdenes, reglas o guías emitidas por agencias regulatorias,

– sentencias de juzgados o de tribunales administrativos,

– tratados, convenciones y protocolos.

EJEMPLO 2 Ejemplos de compromisos de *compliance* incluyen:

– acuerdos con grupos de la comunidad u organizaciones no gubernamentales,

– requisitos organizativos, tales como políticas y procedimientos,

– principios voluntarios o códigos de prácticas,

– etiquetado voluntario o compromisos ambientales,

– obligaciones derivadas de acuerdos contractuales con la organización,

– normas y estándares relevantes para las organizaciones y la industria.

4.5.2 Mantenimiento de las obligaciones de *compliance*

Las organizaciones deberían disponer de procesos que identifiquen novedades y modificaciones en la legislación, los códigos y otras obligaciones de *compliance* para asegurar un cumplimiento continuo. Las organizaciones deberían tener procesos para evaluar el impacto de los cambios identificados y para implementar cualquier cambio en la gestión de las obligaciones de *compliance*.

EJEMPLO Ejemplos de procesos para obtener información sobre cambios en leyes y en otras obligaciones de *compliance* incluyen:

– estar en las listas de distribución de los reguladores relevantes,

– ser miembros de grupos profesionales,

– suscribirse a servicios de información relevantes,

– 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).

4.6 Identificación, análisis y evaluación de los riesgos de *compliance*

La organización debería identificar y evaluar sus riesgos de *compliance*. Esta evaluación puede estar basada en una apreciación de riesgos formal o bien puede llevarse a cabo a través de enfoques alternativos. La aperciación de riesgos de *compliance* constituye la base para la implementación del sistema de gestión de *compliance* y para planificar la asignación de recursos y de procesos que sean adecuados y apropiados para gestionar los riesgos de *compliance* identificados.

La organización debería identificar los riesgos de *compliance* relacionando sus obligaciones de *compliance* con sus actividades, productos, servicios y aspectos relevantes de sus operaciones, con objeto de identificar situaciones en las que pueden ocurrir incumplimientos de *compliance*. La organización debería identificar las causas y las consecuencias de los incumplimientos de *compliance*.

La organización debería analizar los riesgos de *compliance* considerando las causas y las fuentes de los incumplimientos de *compliance* y la gravedad de sus consecuencias, así como la probabilidad de que ocurran los incumplimientos de *compliance* y las consecuencias asociadas. Las consecuencias pueden incluir, por ejemplo, daño personal y ambiental, pérdidas económicas, daño reputacional y responsabilidades administrativas.

La evaluación de riesgos incluye comparar el nivel del riesgo de *compliance* identificado durante el proceso de análisis con el nivel de riesgo de *compliance* que la organización puede y está dispuesta a aceptar. Basándose en esta comparación, se pueden establecer las prioridades como base para determinar la necesidad de implementar controles y la extensión de dichos controles (véase 6.1).

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* (véase 4.5);

– incumplimiento(s) de *compliance*.

NOTA 1 La extensión y el nivel de detalle de la apreciación de riesgos de *compliance* dependen de la situación de riesgo, el contexto, el tamaño y los objetivos de la organización y puede variar para sub-áreas específicas (por ejemplo, ambiental, financiera, social).

NOTA 2 El enfoque basado en el riesgo en la gestión de *compliance* no significa que para situaciones de riesgo bajo de incumplimientos de *compliance*, la organización acepte incumplimientos de *compliance*. Sirve de ayuda a la organización para 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 son objeto de seguimiento, corrección y acciones correctivas.

NOTA 3 La Norma ISO 31000 facilita una guía detallada sobre apreciación de riesgos.

5 Liderazgo

5.1 Liderazgo y compromiso

La alta dirección debería demostrar liderazgo y compromiso con respecto al sistema de gestión de *compliance*:

a) estableciendo y defendiendo los valores fundamentales de la organización;

b) 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 (véase 6.2);

c) asegurando que se desarrollan e implementan las políticas, procedimientos y procesos para alcanzar los objetivos de *compliance*;

d) asegurando que los recursos que se necesitan para el sistema de gestión de *compliance* están disponibles, distribuidos y asignados;

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

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

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

h) apoyando a otros roles de dirección relevantes a demostrar en sus correspondientes áreas su liderazgo en relación a sus responsabilidades en materia de *compliance*;

i) asegurando el alineamiento entre los objetivos operacionales y las obligaciones de *compliance*;

j) estableciendo y manteniendo mecanismos de contabilidad, incluyendo la información puntual de cuestiones relacionadas con *compliance*, incluyendo los incumplimientos de *compliance*;

k) asegurando que el sistema de gestión de *compliance* logre los resultados previstos;

l) promoviendo la mejora continua.

EJEMPLO Para que *compliance* sea eficaz se requiere un compromiso activo del órgano de gobierno y de la alta dirección que penetre en el conjunto de la organización. El nivel de compromiso se indica 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 para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de *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 eficaz,

– todos los niveles de la alta dirección transmiten a todos los empleados de forma consistente un mensaje claro (demostrado de palabra y acción) de que la organización cumplirá con sus obligaciones de *compliance*,

– el compromiso hacia *compliance* se comunica ampliamente en declaraciones claras y convincentes y apoyadas por actuaciones,

– se otorga a la función de *compliance* un nivel de autoridad que refleje la importancia de que *compliance* sea eficaz y se le da acceso directo al órgano de gobierno,

– se asignan recursos para establecer, desarrollar, implementar, evaluar, mantener y mejorar una cultura de *compliance* robusta a través de actividades de concienciación y formación,

– las políticas, procedimientos y procesos reflejan, no sólo los requisitos estrictamente legales, sino también códigos voluntarios y los valores fundamentales de la organización,

– la organización asigna y exige responsabilidades de *compliance* a la dirección en todos los niveles de la organización,

– se requieren revisiones periódicas del sistema de gestión de *compliance*,

– el desempeño de *compliance* en la organización se mejora de forma continua,

– se toman acciones correctivas.

5.2 Política de *compliance*

5.2.1 Generalidades

El órgano de gobierno y la alta dirección, preferiblemente tras consultar con los empleados, debería establecer una política de *compliance* que:

– sea adecuada al propósito de la organización;

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

– incluya el compromiso de cumplir los requisitos aplicables; e

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

La política de *compliance* debería definir:

– el alcance del sistema de gestión de *compliance*;

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

– la medida en la que *compliance* va a estar integrada con otras funciones, tales como gobernanza, riesgos, auditoría y asesoría jurídica;

– el grado en el que *compliance* estará embebida en las políticas, procedimientos y procesos operacionales;

– el grado de independencia y autonomía de la función de *compliance*;

– la responsabilidad para gestionar e informar de cuestiones de *compliance*;

– los principios bajo los cuales se van a gestionar las relaciones con partes interesadas internas y externas;

– la norma/niveles exigida/exigibles de conducta y responsabilidad;

– las consecuencias de los incumplimientos de *compliance*.

La política de *compliance* debería:

– estar disponible como información documentada;

– estar escrita en un lenguaje sencillo de forma que los empleados puedan entender fácilmente los principios y su intención;

– estar traducida a otros idiomas en caso de ser necesario;

– comunicarse de forma clara dentro de la organización y estar fácilmente disponible para todos los empleados;

– estar disponible para las partes interesadas, según corresponda;

– actualizarse en caso de que sea necesario, asegurándose de que sigue siendo pertinente.

La política de *compliance* debería establecerse en línea con los valores, objetivos y estrategia de la organización, y debería ser respaldada por el órgano de gobierno.

La política de *compliance* establece los principios generales y el compromiso de acción de una organización para lograr *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* no debería ser un documento único sino que debería estar apoyado por otros documentos, incluyendo políticas, procedimientos y procesos operacionales.

5.2.2 Desarrollo

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

a) obligaciones específicas internacionales, regionales o locales;

b) la estrategia, los objetivos y los valores de la organización;

c) la estructura y el marco de gobierno de la organización;

d) la naturaleza y el nivel de riesgo asociado a los incumplimientos de *compliance*;

e) otras políticas, normas y códigos internos.

5.3 Roles, responsabilidades y autoridades en la organización

5.3.1 Generalidades

La alta dirección debería asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización.

La alta dirección debería asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de *compliance* es conforme con los requisitos de esta norma internacional; e

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

NOTA Las tareas específicas de la función de *compliance* no exoneran a otros empleados de las responsabilidades que puedan existir de informar sobre cuestiones de *compliance*.

5.3.2 Asignación de responsabilidades de *compliance* en la organización

La involucración activa y la supervisión por parte del órgano de gobierno y de la alta dirección es una parte integral de un sistema de gestión de *compliance* eficaz. Lo anterior contribuye a asegurar que los empleados comprendan plenamente la política y los procedimientos operacionales 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 de *compliance* sea eficaz, se necesita que el órgano de gobierno y la alta dirección prediquen con el ejemplo, adhiriéndose y apoyando activamente a *compliance* y al sistema de gestión de *compliance*.

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

Algunas organizaciones- dependiendo de su tamaño- también tienen a una persona que tiene una responsabilidad general de la gestión de *compliance*, aunque también puede ser algo adicional a otros roles o funciones, incluyendo comités existentes, unidad(es) organizativas, o externalizar algunos elementos a expertos en *compliance*.

Esto no debería 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 de *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 tamaño de la organización. Sin embargo, es probable que algunas responsabilidades sean comunes a través de una variedad de organizaciones.

NOTA Esta norma internacional no distingue entre el concepto de responsabilidad y el de rendición de cuentas. Rendición de cuentas está implícito en el término “responsabilidad”.

5.3.3 Rol y responsabilidad del órgano de gobierno y de la alta dirección

El órgano de gobierno y la alta dirección deberían:

a) establecer una política de *compliance* de acuerdo con lo indicado en 5.2.2;

b) asegurar que se mantiene el compromiso hacia *compliance* y que se gestionan adecuadamente los incumplimientos de *compliance* y los comportamientos contrarios a *compliance*;

c) incluir las responsabilidades de *compliance* en las declaraciones de posiciones de los altos directivos;

d) designar o nominar una función de *compliance* con:

   1) autoridad y responsabilidad para el diseño, consistencia e integridad del sistema de gestión de *compliance*,

   2) apoyo claro y sin ambigüedad del órgano de gobierno y la alta dirección y acceso directo a los mismos,

   3) acceso a:

      – tomadores de decisiones de alto nivel y oportunidad de contribuir en etapas tempranas de los procesos de toma de decisiones,

      – todos los niveles de la organización,

      – toda la información documentada y los datos necesarios para desarrollar las tareas de *compliance*,

      – asesoramiento experto en legislación, códigos y normas organizativas relevantes,

   4) la autoridad y capacidad de ejercer como contrapoder al mostrar cualquier consecuencia para *compliance* en los procesos de toma de decisión relevantes,

e) asegurar que la función de *compliance* tiene autoridad para actuar de forma independiente y que no se ve comprometida por otras prioridades que entren en conflicto, especialmente cuando *compliance* está integrado en el negocio.

La alta dirección debería:

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

– asegurar que se asignan las responsabilidades y autoridades para los roles relevantes y que son comunicadas a toda la organización;

– asegurar que hay sistemas de información y comunicación eficaces y puntuales;

– medirse contra baremos o resultados de desempeño clave de *compliance*;

– asignar la responsabilidad de informar sobre el desempeño del sistema de gestión de *compliance* al órgano de gobierno y a la alta dirección.

5.3.4 Función de *compliance*

No todas las organizaciones crearán una función de *compliance* separada, algunas pueden asignar esta función a una posición existente.

La función de *compliance*, trabajando conjuntamente con la dirección, debería ser responsable de:

a) identificar las obligaciones de *compliance*, con el apoyo de los recursos necesarios, y traducir esas obligaciones en políticas, procedimientos y procesos viables;

b) integrar las obligaciones de *compliance* en las políticas, procedimientos y procesos existentes;

c) proporcionar u organizar apoyo formativo continuo a la plantilla para garantizar que todos los empleados relevantes son formados con regularidad;

d) promover la inclusión de las responsabilidades de *compliance* en las descripciones de puestos de trabajo y en los procesos de gestión del desempeño de los empleados;

e) poner en marcha un sistema de información y documentación de *compliance*;

f) desarrollar e implementar procesos para gestionar la información, tales como las reclamaciones y/o comentarios recibidos de líneas directas, un canal de denuncias anónimas u otros mecanismos;

g) establecer indicadores de desempeño de *compliance* y supervisar y medir el desempeño de *compliance*;

h) analizar el desempeño para identificar la necesidad de acciones correctivas;

i) identificar los riesgos de *compliance* y gestionar aquellos riesgos que relacionados con terceras partes, tales como proveedores, agentes, distribuidores, consultores y contratistas;

j) asegurar que el sistema de gestión de *compliance* se revisa a intervalos planificados;

k) asegurar que hay acceso a un asesoramiento profesional adecuado para el establecimiento, implementación y mantenimiento del sistema de gestión de *compliance*;

l) proporcionar a los empleados acceso a los recursos de los procedimientos y referencias de *compliance*;

m) proporcionar asesoramiento objetivo a la organización en materias relacionadas con *compliance*.

NOTA La Norma ISO 10002 proporciona directrices para el tratamiento de las quejas.

Cuando se asigne la responsabilidad de la gestión de *compliance*, se debería considerar la forma de asegurar que la función de *compliance* no tiene conflictos de intereses y que ha demostrado:

– integridad y compromiso con *compliance*;

– habilidades de comunicación eficaz y de capacidad de influencia;

– capacidad y prestigio para que sus consejos y directrices tengan aceptación;

– competencia necesaria.

5.3.5 Responsabilidades de la dirección

La dirección debería ser responsable de *compliance* dentro de su área de responsabilidad. Esto incluye:

a) cooperar con y apoyar a la función de *compliance* y animar a los empleados a hacerlo de la misma forma;

b) cumplir personalmente, y que se le vea que cumple, con las políticas, procedimientos y procesos y atender y apoyar las actividades formativas de *compliance*;

c) identificar y comunicar los riesgos de *compliance* en sus operaciones;

d) llevar a cabo de forma activa y fomentar las actividades de orientación, entrenamiento y supervisión de empleados para promover un comportamiento de cumplimiento;

e) animar a los empleados a que planteen sus preocupaciones de *compliance*;

f) participar activamente en la gestión y resolución de incidentes y cuestiones relacionadas con *compliance*;

g) desarrollar la concienciación de los empleados sobre las obligaciones de *compliance* y dirigirlos a que completen los requisitos de formación y competencia;

h) asegurar que *compliance* se introduce en las descripciones de puestos de trabajo;

i) integrar el desempeño de *compliance* en las evaluaciones del desempeño de los empleados (por ejemplo, indicadores clave de desempeño, objetivos y criterios de promoción);

j) integrar las obligaciones de *compliance* en las prácticas y procedimientos de negocio existentes en sus áreas de responsabilidad;

k) junto con la función de *compliance*, asegurar que, una vez que se identifica la necesidad de una acción correctiva, ésta se implementa;

l) supervisar los acuerdos de externalización para asegurar que tienen en cuenta las obligaciones de *compliance*.

5.3.6 Responsabilidad de los empleados

Todos los empleados, incluso los directivos, deberían:

a) observar las obligaciones de *compliance* de la organización que son relevantes a su posición y obligaciones;

b) participar en la formación de acuerdo con el sistema de gestión de *compliance*;

c) usar los recursos de *compliance* disponibles como parte del sistema de gestión de *compliance*;

d) informar sobre preocupaciones, cuestiones o fallos de *compliance*.

6 Planificación

6.1 Acciones para tratar riesgos y oportunidades

Al planificar el sistema de gestión de *compliance*, la organización debería considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, los principios de buen gobierno referidos en el apartado 4.4, las obligaciones de *compliance* identificadas en el apartado 4.5 y los resultados de la apreciación de riesgos de *compliance* referida en el apartado 4.6 para determinar los riesgos y oportunidades que es necesario tratar con el fin de:

– asegurar que el sistema de gestión de *compliance* pueda lograr sus resultados previstos;

– prevenir o reducir efectos indeseados;

– lograr la mejora continua.

La organización debería planificar:

a) las acciones para tratar estos riesgos y oportunidades; y

b) la manera de:

  – integrar e implementar las acciones en sus procesos del sistema de gestión de *compliance*,

  – evaluar la eficacia de estas acciones.

La organización debería conservar información documentada sobre los riesgos de *compliance* y sobre las acciones planificadas para gestionarlos.

6.2 Objetivos de *compliance* y planificación para lograrlos

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

Los objetivos de *compliance* deberían:

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; y

f) actualizarse, según corresponda.

La organización debería conservar información documentada sobre los objetivos de *compliance*.

Cuando se hace la planificación para lograr sus objetivos de *compliance*, la organización debería determinar:

– qué se va a hacer;

– qué recursos se requerirán;

– quién será responsable;

– cuándo se finalizará;

– cómo se evaluarán los resultados, por ejemplo, de conformidad con las medidas y resultados clave de rendimiento de *compliance* identificados.

La organización debería conservar información documentada sobre los objetivos de *compliance* y sobre las acciones planificadas para alcanzarlos.

7 Apoyo

7.1 Recursos

La organización debería determinar y proporcionar los recursos necesarios para el establecimiento, desarrollo, implementación, evaluación, mantenimiento y mejora continua del sistema de gestión de *compliance* de acuerdo con su tamaño, complejidad, estructura y operaciones.

La alta dirección y todos los demás niveles de dirección deberían asegurar que se despliegan los recursos necesarios de forma eficaz para asegurar que el sistema de gestión de *compliance* logra sus objetivos y que se consigue *compliance*.

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

7.2 Competencia y formación

7.2.1 Competencia

La organización debería:

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

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

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

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 Formación

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

El objetivo de un programa de formación es asegurar que todos los empleados son competentes para cumplir con su rol profesional de forma consistente con la cultura de *compliance* de la organización y con el compromiso que tiene con *compliance*.

Una formación diseñada y ejecutada adecuadamente puede proporcionar una manera eficaz para que los empleados comuniquen riesgos de *compliance* que previamente no hubieran sido identificados.

La educación y formación de los empleados deberían:

a) estar hechas a medida de las obligaciones y los riesgos de *compliance* relacionados con los roles y responsabilidades del empleado;

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

c) llevarse a cabo al comienzo de la relación del empleado con la organización y posteriormente de forma continua;

d) estar alineadas con el programa de formación corporativo e incorporadas en los planes anuales de formación;

e) ser prácticas y fácilmente comprensibles para los empleados;

f) ser relevantes para el trabajo diario de los empleados e ilustrativas de la industria, organización o sector de que se trate;

g) ser lo suficientemente flexibles como para que puedan ser impartidas por varias técnicas para acomodarse a las diferentes necesidades de las organizaciones y los empleados;

NOTA La formación interactiva podría ser la mejor forma de impartir formación si los incumplimientos de *compliance* pudieran tener consecuencias serias.

h) ser evaluadas por su eficacia;

i) ser actualizadas siempre que sea necesario;

j) ser registradas y conservadas.

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

– cambios en la posición o en las responsabilidades;

– cambios en las políticas, procedimientos y procesos internos;

– cambios en la estructura organizativa;

– cambios en las obligaciones de *compliance*, en especial las relativas a requisitos legales o de las partes interesadas;

– cambios en las actividades, productos y servicios;

– cuestiones identificadas en el seguimiento, auditorías, revisiones, reclamaciones e incumplimientos, incluyendo las opiniones de los accionistas.

7.3 Toma de conciencia

7.3.1 Generalidades

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

a) la política de *compliance*;

b) su contribución a la eficacia del sistema de gestión de *compliance*, incluyendo los beneficios de una mejora del desempeño de *compliance*;

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

7.3.2 Comportamientos

7.3.2.1 Generalidades

Se deberían fomentar los comportamientos que generan y apoyan a *compliance* y no se deberían tolerar comportamientos que comprometen a *compliance*.

7.3.2.2 Rol de la alta dirección en el apoyo a *compliance*

La alta dirección tiene una responsabilidad crucial para:

a) alinear los compromisos de *compliance* de una organización con sus valores, objetivos y estrategia para posicionar a *compliance* de forma adecuada;

b) comunicar su compromiso con *compliance* para sensibilizar y motivar a los empleados para que adopten el sistema de gestión de *compliance*;

c) animar a todos los empleados para que acepten la importancia de alcanzar los objetivos de *compliance* de los que son responsables;

d) crear un entorno en el que se fomenta que se informe sobre los incumplimientos y en el que se protege de represalias al empleado que informe;

e) animar a los empleados a que hagan sugerencias que faciliten la mejora continua del desempeño de *compliance*;

f) asegurar que *compliance* se incorpora en la cultura amplia de la organización y en las iniciativas de cambio cultural;

g) identificar los incumplimientos de *compliance* y actuar de forma inmediata para corregirlos o gestionarlos;

h) asegurar que las políticas, procedimientos y procesos de la organización apoyan y alientan a *compliance*;

i) asegurar que los objetivos y metas operacionales no comprometen un comportamiento adecuado.

7.3.2.3 Cultura de *compliance*

El desarrollo de una cultura de *compliance* exige que el órgano de gobierno, la alta dirección y la dirección tengan un compromiso visible, consistente y sostenido con un estándar común y publicado de comportamiento que se requiere en todas y cada una de las áreas de la organización.

EJEMPLO Algunos ejemplos de factores que apoyarán el desarrollo de una cultura de *compliance* son:

- un conjunto claro de valores publicados,
- que se vea a la dirección implementando activamente y respetando los valores,
- consistencia en el tratamiento de acciones similares, con independencia de la posición,
- guiar, entrenar y predicar con el ejemplo,
- realizar evaluaciones adecuadas a los potenciales empleados antes de su contratación,
- un programa de iniciación u orientación adecuado que enfatice *compliance* y los valores de la organización,
- formación continua de *compliance*, incluyendo actualizaciones de la formación,
- comunicación continua de las cuestiones de *compliance*,
- 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*,

– reconocimiento visible de los logros en la gestión de *compliance* y en sus resultados,

– 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 reflejen *compliance* como esencial para alcanzar los resultados de la organización,

– una comunicación abierta y adecuada sobre *compliance*.

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

– se implementan los puntos señalados arriba;

– las partes interesadas (especialmente los empleados) creen que se han implementado los puntos señalados arriba;

– los empleados entienden la relevancia de las obligaciones de *compliance* relativas a sus propias actividades y a las de sus unidades de negocio;

– la remediación de los incumplimientos se asumen y se gestionan en todos los niveles de la organización cuando sea necesario;

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

– se permite y se anima a los empleados a que comuniquen sus preocupaciones de *compliance* al nivel adecuado de la dirección.

7.4 Comunicación

7.4.1 Generalidades

La organización debería determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de *compliance*, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) cómo comunicar.

NOTA En 9.1.7 y 9.1.8 se da orientación sobre información interna y externa de *compliance*.

7.4.2 Comunicación interna

La organización debería adoptar métodos adecuados de comunicación para asegurar que el mensaje de *compliance* es escuchado y comprendido por todos los empleados de forma continua. La comunicación debería indicar claramente cuáles son las expectativas de la organización sobre los empleados y cuáles son los incumplimientos que se espera que sean escalados, en qué circunstancias y a quién.

7.4.3 Comunicación externa

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, pero no están limitadas a, organismos reguladores, clientes, contratistas, proveedores, inversores, servicios de emergencia, organizaciones no gubernamentales y vecinos.

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, involucración en eventos de la comunidad y líneas telefónicas directas. Estos enfoques pueden apoyar el entendimiento y la aceptación del compromiso con *compliance* de una organización.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión de *compliance* de la organización debería incluir:

a) la información documentada requerida por esta norma internacional;

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

EJEMPLO Ejemplos de información documentada incluyen:

- la política de *compliance* de la organización,
- los objetivos, fines, estructura y contenido del sistema de gestión de *compliance*,
- la asignación de roles y responsabilidades de *compliance*,
- el registro de las obligaciones de *compliance* relevantes,
- los registros de los riesgos de *compliance* y la priorización del tratamiento basada en el proceso de apreciación de riesgos de *compliance*,
- el registro de los incumplimientos y de los conatos de incumplimientos,
- los planes anuales de *compliance*,
- los registros personales, incluyendo, pero no limitado a, los registros de formación.

NOTA 1 La información documentada puede incluir materias relacionadas con requisitos de información regulatorios.

NOTA 2 El extensión de la información documentada para un sistema de gestión de *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, y
- la competencia de las personas.
- la madurez del sistema de gestión de *compliance*.

7.5.2 Creación y actualización

Al crear y actualizar información documentada, la organización debería 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 de *compliance* y por esta norma internacional se debería controlar para asegurarse de que:

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

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

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

– distribución, acceso, recuperación y uso;

– almacenamiento y preservación, incluida la preservación de la legibilidad;

– control de cambios (por ejemplo, control de versión);

– retención y disposición final;

– el papel de terceras partes en la creación y el control de la información documentada.

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

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

NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

8 Operación

8.1 Planificación y control operacional

La organización debería planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el apartado 6.1 mediante:

– la definición de los objetivos de los procesos;

– el establecimiento de criterios para los procesos;

– la implementación del control de los procesos de acuerdo con los criterios;

– el mantenimiento de información documentada en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.

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

8.2 Establecimiento de controles y procedimientos

Se deberían implantar controles para gestionar las obligaciones de *compliance* identificadas y los riesgos de *compliance* asociados y para alcanzar el comportamiento deseado.

Se necesitan controles eficaces para asegurar que se cumplen las obligaciones de *compliance* y que se previenen, o se detectan y corrigen, los incumplimientos. Los tipos y niveles de 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 embebidos en los procesos organizativos normales.

EJEMPLO Ejemplos de controles incluyen:

– políticas operativas, procedimientos, procesos e instrucciones de trabajo documentados, claros, prácticos y fáciles de seguir,

– sistemas e informes de excepciones,

– autorizaciones,

– segregación de roles y responsabilidades incompatibles,

– procesos automatizados,

– planes anuales de *compliance*,

– planes de desempeño de empleados,

– evaluaciones de *compliance* y auditorías,

– compromiso de la dirección demostrado y comportamiento ejemplarizante y otras medidas para promover un comportamiento cumplidor,

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

Estos controles se deberían mantener, ser evaluados y probados periódicamente para asegurarse de que continúan siendo eficaces.

Se deberían establecer, documentar, implementar y mantener procedimientos para apoyar la política de *compliance* y traducir las obligaciones de *compliance* a la práctica.

Al desarrollar estos procedimientos, se debería considerar lo siguiente:

a) integración de las obligaciones de *compliance* en procedimientos, incluyendo sistemas informáticos, formularios, sistemas de información, contratos y otra documentación legal;

b) consistencia con otras funciones de revisión y control de la organización;

c) seguimiento y medición continuos;

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

e) disposiciones específicas para identificar, informar y escalar casos de incumplimientos y riesgos de incumplimientos.

8.3 Procesos externalizados

La organización se debería asegurar que los procesos externalizados son controlados y se realiza seguimiento de los mismos.

Normalmente, la externalización de las operaciones de una organización no le libera de sus responsabilidades legales o sus responsabilidades de *compliance*. Si existe alguna externalización de las actividades de la organización, la organización necesita llevar a cabo una diligencia debida eficaz para asegurar que sus estándares y compromisos con *compliance* no son rebajados. También debería haber controles sobre los contratistas para asegurar que se cumple con el contrato de forma eficaz (por ejemplo, evaluaciones del desempeño de terceras partes).

La organización debería considerar los riesgos de *compliance* relacionados con otros procesos relacionados con terceras partes, tales como el suministro de bienes y servicios y la distribución de productos, y establecer controles según sea necesario (por ejemplo, introducir las obligaciones de *compliance* en cláusulas contractuales).

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

9.1.1 Generalidades

La organización debería determinar:

a) a qué es necesario hacer seguimiento y qué es necesario medir;

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

c) cuándo se deberían llevar a cabo el seguimiento y la medición;

d) cuándo se deberían analizar y evaluar los resultados del seguimiento y la medición.

La organización debería conservar la información documentada adecuada como evidencia de los resultados.

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

9.1.2 Seguimiento

Se debería hacer seguimiento del sistema de gestión de *compliance* para asegurar que se alcanza el desempeño de *compliance*. Se debería establecer un plan de seguimiento continuo, definiendo los procesos, programas y recursos del seguimiento y la información que se debe recoger.

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

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

– eficacia de la formación;

– eficacia de los controles, por ejemplo, a través de los resultados de análisis sobre una muestra;

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

– actualización de las obligaciones de *compliance*;

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

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

El seguimiento del desempeño de *compliance* típicamente incluye:

– incumplimientos y conatos (es decir, incidentes sin efectos adversos);

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

– casos en los que no se alcanzan los objetivos;

– estado de la cultura de *compliance*;

– indicadores predictivos y reactivos establecidos en 9.1.6.

9.1.3 Fuentes de opinión sobre el desempeño de *compliance*

La organización debería establecer, implementar, evaluar y mantener procedimientos para buscar y recibir opiniones de su desempeño de *compliance* de una serie de fuentes, incluyendo:

– empleados, por ejemplo, a través de canales de denuncias, líneas de ayuda, buzones de opinión y de sugerencias;

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

– proveedores;

– reguladores;

– registros de control de procesos y registros de actividad (incluyendo tanto electrónicos como en papel).

EJEMPLO Ejemplos de opiniones sobre el desempeño de *compliance* incluyen:

– cuestiones de *compliance*,

– incumplimientos y preocupaciones relativas a *compliance*,

– cuestiones de *compliance* emergentes,

– cambios continuos regulatorios y organizativos,

– comentarios sobre la eficacia y el desempeño de *compliance*.

Las opiniones deberían servir como una fuente clave de mejora continua del sistema de gestión de *compliance*.

9.1.4 Métodos de recogida de información

Existen muchos métodos para recoger información. Cada método que se relaciona más abajo es relevante 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.

EJEMPLO Ejemplos de recogida de información incluyen:

– informes ad hoc de incumplimientos cuando aparecen o son identificados,

– información obtenida en líneas directas, reclamaciones y otras fuentes, incluyendo el canal de denuncias,

– discusiones informales, talleres de trabajo y grupos temáticos,

– pruebas integrales y por muestreo, tales como *mystery shopping*,

– resultados de encuestas de percepción,

– observaciones directas, entrevistas formales, visitas a las instalaciones e inspecciones,

– auditorías y revisiones,

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

9.1.5 Análisis y clasificación de la información

Es fundamental hacer una clasificación y gestión eficaz de la información.

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

EJEMPLO Ejemplos de criterios de clasificación de información incluyen:

– fuente,

– departamento,

– descripción del incumplimiento,

– referencias de la obligación,

– indicadores,

– severidad,

– impacto real o potencial.

Los sistemas de gestión de la información deberían capturar tanto problemas como reclamaciones y permitir la clasificación y el análisis de aquellos que estén relacionados con *compliance*.

Una vez que la información ha sido recogida, necesita analizarse y evaluarse de forma crítica para identificar el origen y las acciones adecuadas que es necesario tomar. 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.

9.1.6 Desarrollo de indicadores

Es importante que las organizaciones desarrollen un conjunto de indicadores medibles que ayuden a la organización a medir el logro de sus objetivos (véase 6.2) y a cuantificar su desempeño de *compliance*. Este proceso debería tener en cuenta los resultados de la apreciación de los riesgos de *compliance* (véase 4.6) para asegurar que los indicadores estén relacionados con las principales características de los riesgos de *compliance* de la organización. La cuestión de qué y cómo medir el desempeño de *compliance* puede ser complejo en ocasiones, pero sin embargo es un factor vital para demostrar la eficacia del sistema de gestión de *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.

EJEMPLO 1 Ejemplos de indicadores de actividad incluyen:

– porcentaje de empleados a los que se haya impartido formación de forma eficaz,

– frecuencia de los contactos con los reguladores,

– utilización de mecanismos para obtener opiniones (incluyendo comentarios sobre el valor de dichos mecanismos por parte de sus usuarios),

– qué tipo de acción correctiva se tomó para cada incumplimiento.

EJEMPLO 2 Ejemplos de indicadores reactivos incluyen:

- cuestiones e incumplimientos identificados y comunicados, por tipo, área y frecuencia,
- consecuencias de los incumplimientos, que pueden incluir 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 adoptar acciones correctivas.

EJEMPLO 3 Ejemplos de indicadores predictivos incluyen:

- riesgos de incumplimientos, medidos como la pérdida/ganancia potencial de los objetivos (ingresos, salud y seguridad, reputación, etc.) a lo largo del tiempo,
- tendencias de incumplimientos (tasa de *compliance* esperada basada en tendencias pasadas).

9.1.7 Informes de *compliance*

El órgano de gobierno, la dirección y la función de *compliance* deberían asegurarse de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión de *compliance* de la organización y de su adecuación continua, incluyendo todos los incumplimientos relevantes, y promover activamente el principio de que la organización anima y apoya una cultura de información completa y franca. Las disposiciones relativas a la información interna deberían asegurar que:

a) se establecen criterios adecuados y obligaciones de información;

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

c) existe un sistema de informes de excepciones que facilita información ad hoc sobre incumplimientos emergentes;

d) existen sistemas y procesos que aseguren la exactitud y completitud de los informes;

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 remediadoras;

f) hay un proceso de firmas que confirmen la exactitud de los informes que se remiten al órgano de gobierno, incluyendo la firma de la función de *compliance*.

Una organización debería elegir un formato, contenido y periodicidad de sus informes internos de *compliance* que sean adecuados a sus circunstancias, a no ser que haya alguna especificidad legal en otro sentido.

Los informes de *compliance* deberían incorporarse en los informes normales de la organización.

Sólo se deberían preparar informes separados en caso de que hubiera incumplimientos graves y para cuestiones emergentes.

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

Se debería animar a los empleados a que respondan e informen sobre incumplimientos de las leyes y otros incidentes de incumplimientos de *compliance* y para que vean dichos informes como una acción positiva y no amenazante, sin ningún temor a sufrir represalias.

Las obligaciones de informar deberían establecerse de forma clara en la política y procedimientos de *compliance* de la organización y reforzarse por otros métodos, tales como refuerzos informales de la dirección durante su trabajo del día a día con los empleados.

9.1.8 Contenido de los informes de *compliance*

Los informes de *compliance* pueden incluir:

a) cualquier materia sobre la que la organización deba notificar a cualquier regulador o autoridad;

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

c) medidas del desempeño de *compliance*, incluyendo los incumplimientos y la mejora continua;

d) número y detalles de posible(s) incumplimiento(s) y su análisis subsiguiente;

e) acciones correctivas adoptadas;

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

g) contactos, y desarrollo de las relaciones, con los reguladores;

h) resultados de las auditorías, así como de las actividades de seguimiento.

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

9.1.9 Mantenimiento de registros

Se deberían 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 de *compliance*.

El mantenimiento de registros debería incluir el registro y clasificación de las reclamaciones, los conflictos y los presuntos incumplimientos 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 de *compliance* de la organización pueden incluir:

a) información sobre el desempeño de *compliance*, incluyendo los informes de *compliance*;

b) reclamaciones, su resolución y comunicaciones de las partes interesadas;

c) detalles de los incumplimientos y acciones correctivas y preventivas;

d) resultados de los seguimientos y de las auditorías de los sistemas de gestión de *compliance* y las acciones adoptadas.

9.2 Auditoría interna

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

a) cumple:

   1) los requisitos propios de la organización para su sistema de gestión de *compliance*,

   2) los requisitos de esta norma internacional,

b) se implementa y mantiene eficazmente.

Se pueden realizar auditorías adicionales en caso de que sea necesario.

La organización debería:

– planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deberían tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

– para cada auditoría, definir los criterios y el alcance de ésta;

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

– asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y

– conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

9.3 Revisión por la dirección

La alta dirección debería revisar el sistema de gestión de *compliance* de la organización a intervalos planificados, para asegurarse de su idoneidad, adecuación y eficacia continuas.

La revisión por la dirección debería considerar:

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

b) la adecuación de la política de *compliance*;

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

d) la adecuación de los recursos;

e) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de *compliance*;

f) la información sobre el desempeño de *compliance*, incluidas las tendencias relativas a:

   – no conformidades, acciones correctivas y tiempos para su resolución,

   – seguimiento y resultados de las mediciones,

   – comunicación de las partes interesadas, incluyendo las reclamaciones,

   – resultados de la auditoría,

g) las oportunidades de mejora continua.

Las salidas de la revisión por la dirección deberían incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de *compliance*.

Debería incluir también recomendaciones sobre:

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

b) cambios de los procesos de *compliance* para asegurar una integración eficaz con las prácticas operacionales y sistemas;

c) áreas sobre las que hacer seguimiento de incumplimientos futuros potenciales;

d) acciones correctivas respecto a los incumplimientos;

e) lagunas o carencias en los sistemas de *compliance* existentes e iniciativas de mejora continua a más largo plazo;

f) reconocimiento de un comportamiento de *compliance* ejemplar dentro de la organización.

La organización debería conservar información documentada como evidencia de los resultados de las revisiones por la dirección y se debería entregar una copia al órgano de gobierno.

10 Mejora

10.1 No conformidades y acciones correctivas

10.1.1 Generalidades

Cuando ocurra una no conformidad, la organización debería:

a) reaccionar ante la no conformidad, y según sea aplicable:

   – tomar acciones para controlarla y corregirla, y

   – hacer frente a las consecuencias;

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

   – la revisión de la no conformidad;

   – la determinación de las causas de la no conformidad; y,

   – la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas; y

e) si es necesario, hacer cambios al sistema de gestión de *compliance*.

La falta de prevención o detección de un incumplimiento puntual no significa necesariamente que el sistema de gestión de *compliance* no sea eficaz para prevenir y detectar los incumplimientos en general.

Las acciones correctivas deberían ser adecuadas a los efectos de las no conformidades encontradas. La organización debería conservar información documentada, como evidencia de:

– la naturaleza de las no conformidades y cualquier acción tomada posteriormente; y

– los resultados de cualquier acción correctiva.

La información obtenida del análisis de las no conformidades y/o de los incumplimientos puede usarse para considerar si:

– evaluar el rendimiento del producto y servicio;

– mejorar y/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 de potenciales incumplimientos;

– rediseñar o revisar los controles;

– mejorar las etapas de notificación e información a niveles superiores (internos y externos).

10.1.2 Escalado de información

Se debería adoptar y comunicar un proceso claro y puntual de información a niveles superiores, para asegurar que todos los incumplimientos se ponen de manifiesto, se reportan y eventualmente se escalan a niveles relevantes de la dirección, y que se informa a la función de *compliance* y ésta es capaz de apoyar esta información a niveles superiores. Cuando sea necesario, la información a niveles superiores se debería hacer a la alta dirección y al órgano de gobierno, incluyendo los comités relevantes. El proceso debería especificar a quién, cómo y cuándo se deben reportar los asuntos y los plazos para reportar interna y externamente.

Cuando se requiere por ley que las organizaciones informen sobre los incumplimientos, las autoridades regulatorias deben ser informadas de acuerdo con la legislación aplicable o según lo convenido.

Aun cuando la legislación no requiera que las organizaciones informen sobre los incumplimientos, deberían considerar hacer declaraciones voluntarias de los incumplimientos a las autoridades regulatorias para mitigar las consecuencias de los incumplimientos.

Un sistema de gestión de compliance eficaz debería incluir un mecanismo para que los empleados de la organización y/u otras personas informen sobre malas prácticas reales o sospechosas, o sobre violaciones de las obligaciones de *compliance* de la organización, de forma confidencial y sin temor a represalias.

10.2 Mejora continua

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

La información recogida, analizada y evaluada consecuentemente, e incluida en los informes de *compliance*, debería usarse como base para identificar las oportunidades de mejora del desempeño de *compliance* en la organización.

Bibliografía

[1] ISO 9001, *Quality management systems. Requirements.*

[2] ISO 10002, *Quality management. Customer satisfaction. Guidelines for complaints handling in organizations.*

[3] ISO 14001, *Environmental management systems. Requirements with guidance for use.*

[4] ISO 19011, *Guidelines for auditing management systems.*

[5] ISO 22000, *Food safety management systems. Requirements for any organization in the food chain.*

[6] ISO 26000, *Guidance on social responsibility.*

[7] ISO 31000, *Risk management. Principles and guidelines.*

[8] ISO Guide 73:2009, *Risk management. Vocabulary.*

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032