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