



**ISO 37301**  
**GUÍA PRÁCTICA PARA EL**  
**ESTABLECIMIENTO DE UN SISTEMA**  
**DE GESTIÓN DE *COMPLIANCE***

Risk Advisory Services

# INTRODUCCIÓN Y ANTECEDENTES

## CONTEXTO

La concienciación sobre la relevancia de un comportamiento ético y adecuado en el mundo empresarial es cada vez mayor, lo que ha derivado en una tendencia global focalizada en la puesta en marcha de iniciativas que fomenten determinados principios y valores en la forma de hacer negocios.

Dicha tendencia se ha visto acompañada por nuevos marcos y estándares normativos, que instan a las organizaciones a disponer de modelos de gobierno corporativo y cumplimiento que velen por el correcto comportamiento de sus empleados y socios de negocio en el ámbito empresarial.

En este contexto, la ISO 37301 supone, con respecto al anterior estándar internacional de sistemas de *compliance*, ISO 19600, una actualización y reemplazo de la normativa anterior que iremos desglosando a lo largo del presente documento, permitiendo a las organizaciones obtener una certificación a nivel internacional.

## OBJETIVO Y ÁMBITO DE APLICACIÓN

La Organización Internacional de Normalización (ISO) en su labor de revisión, actualización y mejora continua en la revisión de los estándares normativos, con el objetivo de mejorarlos y adaptarlos a los nuevos tiempos, ha publicado la nueva norma ISO 37301.

Esta nueva norma proporcionará los requisitos para el establecimiento, desarrollo, implementación, evaluación y mejora de un sistema de *compliance* efectivo y apropiado dentro de una organización.

El sistema de *compliance*, en adelante SC, que propone la ISO 37301 es aplicable a cualquier organización, independientemente de sus características.

Esta norma internacional se basa en los principios de buen gobierno, proporcionalidad, transparencia y sostenibilidad. Una novedad muy importante en la nueva ISO 37301 con respecto a la actual ISO 19600 es que será certificable por cualquier organización.



### PUBLICACIÓN

La fecha de publicación de la ISO fue el **13 de abril 2021**.



### CERTIFICACIÓN

El estándar será certificable por un externo independiente, en los mismos términos que el resto de estándares ISO.



### ALCANCE

La ISO 37301 es aplicable a cualquier tipo de organización independientemente de su tamaño, sector y naturaleza de la actividad.

# REQUERIMIENTOS DEL MODELO

EL ESTÁNDAR **ISO 37301** ESTABLECE DISTINTOS REQUISITOS Y ELEMENTOS PIVOTADOS EN TORNO A 7 ÁMBITOS:

## CONTEXTO DE LA ORGANIZACIÓN

# 1

Identificar factores externos e internos con incidencia en la actividad de la organización, alcance del SC y sus riesgos y de las necesidades y expectativas de las partes interesadas.

## LIDERAZGO

# 2

Compromiso de la organización con el cumplimiento normativo, establecimiento de la política de *compliance* y delimitación de responsabilidades en el SC de los distintos órganos de la compañía.

## PLANIFICACIÓN

# 3

Acciones para la planificación del sistema de *compliance*, incluyendo el establecimiento de los objetivos, obligaciones y método de evaluación del SC.

## APOYO

# 4

Garantizar la disponibilidad de los recursos para el correcto funcionamiento del SC, incluyendo personal competente, adecuada comunicación y conservación de documentación.

## OPERACIONES

# 5

Incluye la planificación e implantación de controles y sus procedimientos para garantizar el cumplimiento normativo, la implantación de un sistema de denuncias y el proceso de su investigación.

## EVALUACIÓN DEL RENDIMIENTO

# 6

Vigilancia, medición, análisis y evaluación del SC y del grado de cumplimiento de sus objetivos.

## MEJORA CONTINUA

# 7

Gestión de disconformidades, incumplimientos y acciones correctivas, así como medidas para garantizar una cultura de mejora continua.

# 1\_ CONTEXTO DE LA ORGANIZACIÓN

## COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO

La organización debe determinar factores externos e internos relevantes para sus objetivos y que afectan a su capacidad de gestión.

 FACTORES EXTERNOS	 FACTORES INTERNOS
Marco legal y regulatorio	Estructuras, políticas, procedimientos, procesos y recursos internos
Contexto sociocultural y medioambiental	Modelo de negocio (estrategia, naturaleza, tamaño, escala de complejidad y sostenibilidad de la actividad de la organización)
Tecnología	Naturaleza y alcance de las relaciones de negocio
Situación económica	Cultura del <i>compliance</i> actual

## NECESIDADES Y EXPECTATIVAS DEL PERSONAL CLAVE DE LA ORGANIZACIÓN

La organización debe identificar las expectativas del personal clave de la compañía en relación al SC.

## ALCANCE DEL SISTEMA

Se deberán definir los límites y ámbito de aplicación del SC, en base al contexto anteriormente analizado y los objetivos en cumplimiento definidos.

## IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS DE COMPLIANCE

Por último, se deberá identificar los riesgos de cumplimiento normativo en base a las actividades, productos y servicios que integran su negocio y definir un sistema de evaluación y monitorización de dichos riesgos.

## 2\_ LIDERAZGO

### LIDERAZGO Y COMPROMISO

La normativa ISO 37301 exige a la organización y al personal clave liderazgo y compromiso con respecto al SC. La norma requiere definir las funciones principales que deben asumir tanto por los órganos de gobierno (Consejo de Administración y *top management*), como el resto de personal de la organización.

A continuación, se resumen algunos de los roles y responsabilidades del personal involucrado:



#### ÓRGANO DE GOBIERNO

- Garantizar el cumplimiento de los objetivos de *compliance* y promover la mejora continua.
- Establecer mecanismos de control a la alta dirección fijando posibles objetivos para medir el cumplimiento.



#### COMITÉ DE COMPLIANCE

- Como órgano responsable del modelo, deberá evaluar periódicamente la adecuación de los riesgos y el SC.
- Integrar las políticas y obligaciones de *compliance*.
- Formación periódica al personal para crear y promover una cultura de *compliance*, ofreciendo asesoramiento en caso de dudas o cuestiones al respecto.



#### GERENTES

- Cooperar y apoyar a la función del *compliance*.
- Asegurar el cumplimiento del personal con sus obligaciones de *compliance*, así como concienciar a todo el personal bajo su responsabilidad.
- Alentar denuncias de incumplimientos e implementar acciones correctivas cuando sea necesario.



#### ALTA DIRECCIÓN

- Colaborar con el comité de *compliance* garantizando los sistemas de presentación de resultado de *compliance*.
- Dada su visión general y profunda de la organización, determinará y alineará los objetivos estratégicos y operacionales con los establecidos en materia de *compliance*.
- Integrar el *compliance* en las evaluaciones de desempeño



#### PERSONAL

- Adhesión a obligaciones, políticas, procedimientos y procesos de *compliance* de la organización.
- Informar de fallos de *compliance*.
- Participar en las formaciones.

Por último, se detalla la importancia de que la organización cumpla con las siguientes acciones:

- Fomentar y desarrollar una cultura de *compliance* en todos los niveles de la compañía. Para ello, los órganos de gobierno deben definir los principios y valores que alienten esta cultura de cumplimiento a sus profesionales.
- Elaborar, publicar y comunicar la política de *compliance* proporcionando un marco de referencia con los objetivos de cumplimiento y los principales elementos que constituyen el SC implementado.

## 3\_ PLANIFICACIÓN

ES CLAVE DEFINIR UNA PLANIFICACIÓN CONTEMPLANDO, ENTRE OTRAS, LAS SIGUIENTES ACCIONES:

### ACCIONES PARA GESTIONAR RIESGOS Y OPORTUNIDADES

Fijar una periodicidad para la correcta monitorización de la efectividad de las medidas implementadas en los SC.

### EVALUACIÓN DEL RIESGO DE CUMPLIMIENTO

Identificar y evaluar periódicamente los riesgos de *compliance*, especialmente ante cambios internos o externos significativos.

### OBLIGACIONES DE COMPLIANCE

Establecer mecanismos para identificar nuevos requerimientos, novedades normativas u obligaciones a considerar en el SC.

### OBJETIVOS DE COMPLIANCE

Incluir en la planificación cuáles son los objetivos en materia de *compliance*. Dichos objetivos deben ser:

- Coherentes y alineados con la política de *compliance* de la organización.
- Medibles para facilitar la monitorización de los mismos.
- Alineados con las expectativas de sus grupos de Interés.
- Conocidos por todos los miembros de la organización

## 4\_ APOYO

PARA ALCANZAR LOS OBJETIVOS Y DESARROLLAR LAS ACCIONES MARCADAS EN LA PLANIFICACIÓN, LA NORMA DESTACA ALGUNOS ASPECTOS RELEVANTES A CONSIDERAR POR LA ORGANIZACIÓN:

### RECURSOS ADECUADOS

Asignar los recursos financieros y humanos necesarios conforme a los objetivos marcados, y en base a la planificación prevista.

### CONCIENCIACIÓN

Concienciar al personal sobre:

- Principios y valores recogidos en la política de *compliance*.
- Su rol y responsabilidades en el sistema.
- Consecuencias derivadas del incumplimiento de las obligaciones asumidas.

### COMUNICACIÓN Y FORMACIÓN

Fomentar la comunicación y formación en el ámbito de *compliance*, y en concreto:

- Comunicaciones internas y externas relacionadas con el SC.
- Diseño e impartición de formaciones periódicas y personalizadas en función de los colectivos existentes y su exposición al riesgo.

### COMPETENCIA DEL PERSONAL

- Determinar el nivel de competencia necesario del personal involucrado en los SC.
- Implantar las medidas necesarias para que todo el personal de la organización cumpla con las obligaciones del SC (asistencia a las formaciones, denunciar cualquier sospecha, etc.).

### INFORMACIÓN DOCUMENTADA

Toda la información del SC deberá estar siempre disponible, protegida y revisada periódicamente, focalizándose en su completitud e integridad. El alcance de dicha información puede diferir de una organización a otra en función del tamaño, actividad, complejidad de los procesos, etc.

## 5\_ OPERACIONES

PARA CUMPLIR CON LOS DIFERENTES ELEMENTOS REQUERIDOS POR LA ISO 37301 EN UN SC, ES IMPORTANTE QUE LA ORGANIZACIÓN DESARROLLE LAS SIGUIENTES ACTIVIDADES:

### PLANIFICACIÓN Y CONTROL DE LOS PROCESOS

Priorizar las acciones a acometer, en función de los objetivos, y establecer mecanismos de medición y seguimiento.

### ESTABLECIMIENTO DE CONTROLES Y PROCEDIMIENTOS

Identificar y actualizar de manera periódica los controles que previenen y mitigan los riesgos identificados en el ámbito de *compliance*. Éstos deben ser revisados/testeados periódicamente para garantizar su eficacia.

### PLANTEAMIENTO DE DENUNCIAS

Habilitar canales de comunicación que permitan informar sobre cualquier circunstancia que pueda suponer un intento, sospecha o violación real de las obligaciones de cumplimiento.

Los canales deben cumplir con la normativa vigente, garantizando la confidencialidad de la identidad de las personas que realicen la comunicación y cerciorarse de que el personal es consciente de los procedimientos de reporte.

### PROCESOS DE INVESTIGACIÓN

Implementación de procesos para evaluar, e investigar sobre casos sospechosos o reales de incumplimiento, informando regularmente del número y resultado de las investigaciones. Toda la información sobre la investigación debe ser conservada y protegida.



# 6\_ EVALUACIÓN DEL RENDIMIENTO

LA ORGANIZACIÓN SUPERVISARÁ EL SC PARA ASEGURAR QUE SE LOGREN LOS OBJETIVOS DEFINIDOS A TRAVÉS DE LAS SIGUIENTES ACTIVIDADES:

## VIGILANCIA, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

- Definición de qué vigilar y medir, métodos de evaluación a aplicar, periodicidad de la medición y reporte de resultados.
- Desarrollo de indicadores (KPI's) para la evaluación de los objetivos y medición de los niveles de desempeño en el ámbito de *compliance*.
- Validación de resultados por la alta dirección.

## AUDITORÍA INTERNA

Planificación, definición, implementación y mantenimiento de programas de auditoría interna focalizados en el SC con una periodicidad definida.

## REVISIÓN DE LA GESTIÓN

Revisión del sistema, incluyendo, entre otros:

- Estado de las acciones correctivas identificadas durante la evaluación del SC e información y seguimiento sobre los resultados de las auditorías.
- Cambios en factores internos y externos relevantes que pudieran afectar al SC.

## 7\_ MEJORA CONTINUA

POR ÚLTIMO, EL SISTEMA DE COMPLIANCE DEBE ESTAR EN CONTINUA MEJORA Y ACTUALIZACIÓN.

### ACCIONES CORRECTIVAS

Tras las revisiones o auditorías llevadas a cabo por las organización, se pueden detectar incumplimientos o puntos de mejora del SC, determinando la organización las acciones a llevar a cabo e implantar las medidas correctivas necesarias, causas, revisar la eficacia de cualquier acción correctora, seguimiento de las mismas, etc.

### MEJORA CONTINUA

- Definición de las acciones que permitan solventar debilidades o ineficiencias identificadas a partir de las evaluaciones de rendimiento periódicas.
- Adaptación del sistema a los factores cambiantes tanto externos como internos.

# COMPARATIVA CON OTROS ESTÁNDARES EN MATERIA DE COMPLIANCE

En la siguiente tabla se plantean diversas cuestiones que pueden ser relevantes en comparación con otros estándares actualmente vigentes en materia de *compliance*, como son la actual ISO 19600 de sistemas de gestión de *compliance*, y la ISO 37001 de sistemas de gestión antisoborno:

ASPECTOS GENERALES	ISO 37301	ISO 19600	ISO 37001
¿Se trata de un estándar válido para cualquier ámbito de cumplimiento?	SÍ	SÍ	<b>NO</b> Alcance limitado al ámbito anticorrupción y antisoborno
¿Son aplicables a todo tipo de organizaciones con independencia de tamaño, actividad, etc.?	SÍ	SÍ	SÍ
¿Su alcance es internacional?	SÍ	SÍ	SÍ
¿Su cumplimiento es certificable por parte de un tercero independiente?	SÍ	<b>NO</b>	SÍ
<b>ASPECTOS TÉCNICOS</b>			
¿Se requiere de una función específica u órgano de <i>compliance</i> , autónomo e independiente dentro de la organización, como responsable del sistema?	SÍ	SÍ	SÍ
¿Define y otorga responsabilidades específicas al órgano de gobierno y <i>top management</i> ?	SÍ	SÍ	SÍ
¿Requiere de una evaluación de riesgos e identificación de medidas mitigadoras existentes en la organización?	SÍ Aplicable a riesgos de <i>compliance</i> en su conjunto	SÍ Aplicable a riesgos de <i>compliance</i> en su conjunto	SÍ Aplicable a riesgos de corrupción y soborno
¿Se incluye algún apartado relativo a diligencia debida de los procesos, controles de filiales y socios de negocio y condiciones contractuales?	<b>NO</b>	<b>NO</b>	SÍ

# CONCLUSIONES

Teniendo en cuenta el contexto regulatorio actual, en clara fase de crecimiento y cuya característica más acentuada es el dinamismo, cobra vital importancia disponer de un modelo de *compliance* completo y eficaz que permita a las organizaciones identificar y gestionar los principales riesgos de carácter normativo y regulatorio a los que se encuentran expuestos por su actividad, localización geográfica, etc.

Desde BDO, basándonos en nuestra experiencia, entendemos que la ISO 37301, da respuesta a las necesidades del mercado en materia de *compliance* (en lo que respecta a la estandarización y homogeneización de la gestión del cumplimiento normativo), definiendo una serie de ámbitos y requisitos sobre los que un modelo de *Compliance* robusto y eficiente ha de cambiar.

## PARA MÁS INFORMACIÓN:

### **LUIS BOLÍVAR CASTILLO**

Socio | Risk Advisory Services  
lcastillo@bdo.ec

Esta publicación ha sido redactada en términos generales y debe ser contemplada únicamente como una referencia general. Esta publicación no puede utilizarse como base para amparar situaciones específicas y usted no debe actuar, o abstenerse de actuar, de conformidad con la información contenida en este documento sin obtener asesoramiento profesional específico. Póngase en contacto con BDO en cualquiera de nuestras oficinas para tratar estos asuntos en el marco de sus circunstancias particulares. BDO, sus socios y empleados, no aceptan ni asumen cualquier responsabilidad ante cualquier pérdida derivada de cualquier acción realizada o no por cualquier individuo al amparo de la información contenida en esta publicación o ante cualquier decisión basada en ella.

BDO Auditores, S.L.P. es una sociedad limitada española independiente y miembro de la red internacional de BDO, constituida por empresas independientes asociadas de todo el mundo, y creada por BDO International Limited, una compañía limitada por garantía del Reino Unido.

BDO es la marca comercial utilizada por toda la red BDO y para todas sus firmas miembro.

Copyright © 2020. Todos los derechos reservados. Publicado en España.

**bdo.ec**  
**bdo.global**  
**bdo.es/blogs/blog-coordenadas-bdo**



Auditoría & Assurance | Advisory | Fiscal y Legal | Outsourcing