# IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE COMPLIANCE - ISO 37301

# CONTENIDO:

1. INTRODUCCIÓN A LA GESTIÓN DE COMPLIANCE.
2. EVOLUCIÓN DE LA NORMA ISO A LA NORMA 19600 A LA NORMA ISO 37301
3. ASPECTOS MAS RELEVANTES DE LA NORMA ISO 37301 – REQUISITOS Y DIRECTRICES. DETERMINACIÓN DEL ALCANCE.
4. ANÁLISIS DETALLADO DE LOS REQUISITOS DE LA NORMA ISO 37301 Y SU RELACIÓN CON LAS DIRECTRICES.
5. IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE ACUERDO A LA NORMA ISO 37301.
6. RELACIÓN DE LA NORMA ISO 37301 CON OTRAS NORMAS DE COMPLIANCE
7. CERTIFICACIÓN DEL SISTEMA DE GESTIÓN DE COMPLIANCE.
8. CASOS PRÁCTICOS.

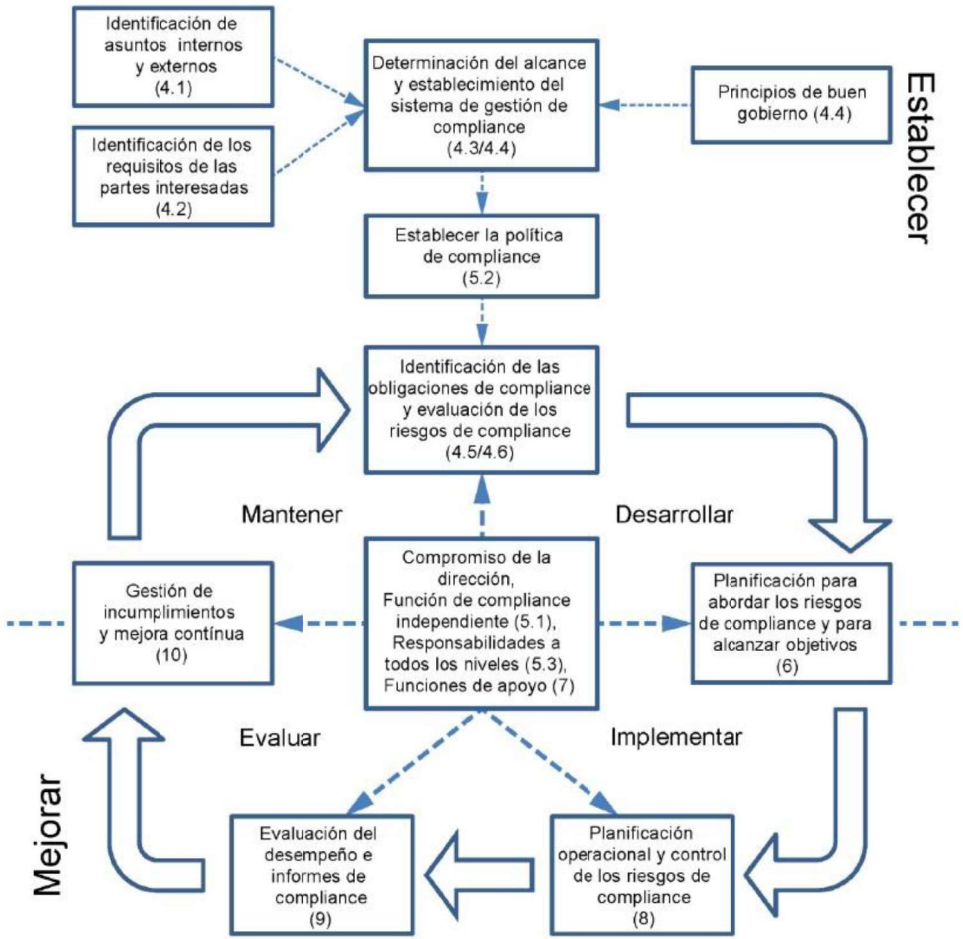
# INTRODUCCIÓN A LA GESTIÓN DE COMPLIANCE.

EL TÉRMINO **COMPLIANCE** (CUMPLIMIENTO) HACE REFERENCIA AL **CUMPLIMIENTO NORMATIVO** (INTERNO Y EXTERNO) A TRAVÉS DE LA GESTIÓN DE **ESTRATEGIAS CORPORATIVAS** QUE PERMITIRÁN, ENTRE OTRAS COSAS, PREVENIR LA MATERIALIZACIÓN DE LOS RIESGOS ASOCIADOS AL INCUMPLIMIENTO.

ES DECIR, LA **GESTIÓN DE COMPLIANCE** VA MÁS ALLÁ DEL PROPIO CUMPLIMIENTO, SINO QUE PARTE DE UNA VOLUNTAD Y DE UNA ESTRATEGIA CORPORATIVA PARA GESTIONAR ESE CUMPLIMIENTO.

LA GESTIÓN DE COMPLIANCE IMPLICA LA **GESTIÓN DILIGENTE** DE LA ORGANIZACIÓN Y ESO GARANTIZA LA **SOSTENIBILIDAD**.

# EVOLUCIÓN DE LA NORMA ISO 19600 A LA NORMA ISO 37301


Identificación de asuntos internos y externos (4.1)
Identificación de los requisitos de las partes interesadas (4.2)
Determinación del alcance y establecimiento del sistema de gestión de compliance (4.3/4.4)
Principios de buen gobierno (4.4)
Establecer
Establecer la política de compliance (5.2)
Identificación de las obligaciones de compliance y evaluación de los riesgos de compliance (4.5/4.6)
Mantener
Desarrollar
Gestión de incumplimientos y mejora contínua (10)
Compromiso de la dirección, Función de compliance independiente (5.1), Responsabilidades a todos los niveles (5.3), Funciones de apoyo (7)
Planificación para abordar los riesgos de compliance y para alcanzar objetivos (6)
Evaluar
Implementar
Mejorar
Evaluación del desempeño e informes de compliance (9)
Planificación operacional y control de los riesgos de compliance (8)


OBJECTIVES
INTEGRITY | CULTURE | CONFORMITY | REPUTATION | VALUE | ETHICS
PRINCIPLES
INTEGRITY | GOOD GOVERNANCE | PROPORTIONALITY | TRANSPARENCY | ACCOUNTABILITY | SUSTAINABILITY
COMMITMENT AT ALL LEVELS DETERMINING THE SCOPE COMPLIANCE POLICY ROLES AND RESPONSIBILITIES OBLIGATIONS AND RISKS
MANAGING NON-COMPLIANCE CONTINUOUS IMPROVEMENT
ACT
PLAN
ESTABLISH
DEVELOP
IMPLEMENT
MAINTAIN
EVALUATE
IMPROVE
LEADERSHIP GOVERNANCE CULTURE
CHECK
DO
INTERNAL AUDIT MANAGEMENT REVIEW MONITORING AND MEASUREMENT RAISING CONCERNS INVESTIGATION PROCESS
SUPPORT COMPETENCE AND AWARENESS COMMUNICATION AND TRAINING OPERATION CONTROLS AND PROCEDURES DOCUMENTATION
ORGANIZATION & ITS CONTEXT
LEGAL | SOCIAL | CULTURAL | DIGITALIZATION | FINANCE | STRUCTURE | ENVIRONMENT | INTERESTED PARTIES

| | CAMBIOS MÁS RELEVANTES RESPECTO A LA UNE-ISO 19600 |
|---|---|
| **DEFINICIONES** | En la UNE-ISO 37301 ya solo se habla de “obligación de Compliance” uniendo lo que, en la anterior norma, era “requisito de Compliance” (obligatorio) y “compromiso de Compliance” (voluntario).<br><br>Definición más sencilla de la función de Compliance en la UNE-ISO 19600. |
| **CONTEXTO** | Se contienen los mismos apartados, algo más sencillo el contexto y las partes interesadas en la UNE-ISO 19600.<br><br>El resto de apartados contenían gran parte de las actuales directrices. |
| **LIDERAZGO** | En la UNE-ISO 19600 no se contenía tanta referencia al órgano de gobierno, más a la alta dirección.<br><br>En la UNE-ISO 19600 no se incluye en este bloque la cultura de Compliance, aparece en el bloque de apoyo. |
| **APOYO** | En la UNE-ISO 19600 se recoge aquí la cultura de Compliance.<br><br>No se contenían referencia a los procesos de empleo (selección y contratación de personal). |
| **OPERACIÓN** | La UNE-ISO 19600 tenía un apartado de procesos externalizados que no está en la norma vigente.<br><br>No contenía referencia alguna al canal de comunicaciones. |

# ASPECTOS MÁS RELEVANTES DE LA NORMA UNE-ISO 37301. REQUISITOS Y DIRECTRICES. DETERMINACIÓN DEL ALCANCE.

**CUESTIONES MAS RELEVANTES QUE SE GENERAN CON LA PUBLICACIÓN DE ESTA NORMA**:

LAAPARICIÓN DE UNA NORMA DE COMPLIANCE EN SENTIDO AMPLIO (SIN APELLIDO)

NORMA INTERNACIONAL

ESTRUCTURA DE ALTO NIVEL

APORTAASPECTOS RELEVANTES SOBRE LA FUNCIÓN DE COMPLIANCE

PARTE DE LA IDENTIFICACIÓN DE OBLIGACIONES Y DE LA EVALUACIÓN DE RIESGOS

IDENTIFICACIÓN DE OBLIGACIONES: DIAGRAMA DE PARETO



## ESTRUCTURA DE LA NORMA:

TIENE UNA PRIMERA PARTE EN LA QUE SE DEFINEN LOS **REQUISITOS** (DEBES).

TIENE UNA SEGUNDA PARTE QUE ES UNA GUÍA QUE CONTIENE **DIRECTRICES**: ESTAS DIRECTRICES **NO SON OBLIGATORIAS.**

LAS DIRECTRICES AYUDAN AAMPLIAR LA INFORMACIÓN DE LOS REQUISITOS Y SU INTERPRETACIÓN, POR LO QUE ES MUY ACONSEJABLE TENERLAS EN CONSIDERACIÓN.



**ESTRUCTURA DE ALTO NIVEL:**

LOS REQUISITOS SE RECOGEN EN LOS CAPÍTULOS 4 AL 10:

**CONTEXTO**
**LIDERAZGO**
**PLANIFICACIÓN**
**APOYO**
**OPERACIÓN**
**EVALUACIÓN DEL DESEMPEÑO**
**MEJORA**

ESO PERMITE SU FÁCIL INTEGRACIÓN CON OTROS SISTEMAS DE GESTIÓN Y ESPECIALMENTE CON LOS SISTEMAS DE COMPLIANCE YA EXISTENTES.



# CICLO PDCA


OBJECTIVES
INTEGRITY | CULTURE | CONFORMITY | REPUTATION | VALUE | ETHICS
PRINCIPLES
INTEGRITY | GOOD GOVERNANCE | PROPORTIONALITY | TRANSPARENCY | ACCOUNTABILITY | SUSTAINABILITY
COMMITMENT AT ALL LEVELS DETERMINING THE SCOPE COMPLIANCE POLICY ROLES AND RESPONSIBILITIES OBLIGATIONS AND RISKS
MANAGING NON-COMPLIANCE CONTINUOUS IMPROVEMENT
ACT
PLAN
CHECK
DO
ESTABLISH
DEVELOP
IMPLEMENT
MAINTAIN
EVALUATE
IMPROVE
LEADERSHIP
GOVERNANCE
CULTURE
INTERNAL AUDIT
MANAGEMENT REVIEW
MONITORING AND MEASUREMENT
RAISING CONCERNS
INVESTIGATION PROCESS
SUPPORT
COMPETENCE AND AWARENESS
COMMUNICATION AND TRAINING
OPERATION
CONTROLS AND PROCEDURES
DOCUMENTATION
ORGANIZATION & ITS CONTEXT
LEGAL | SOCIAL | CULTURAL | DIGITALIZATION | FINANCE | STRUCTURE | ENVIRONMENT | INTERESTED PARTIES

**DEFINICIONES**:
LA DIFERENCIA QUE REALIZA ENTRE "**NO CONFORMIDAD**" E "**INCUMPLIMIENTO DE COMPLIANCE**", LA PRIMERA PARA REFERIRSE AL INCUMPLIMIENTO DE UN REQUISITO Y LA SEGUNDA PARA REFERIRSE AL NO CUMPLIMIENTO DE LAS OBLIGACIONES DE COMPLIANCE.

"**FUNCIÓN DE COMPLIANCE**", PERSONA O GRUPO DE PERSONAS CON RESPONSABILIDAD Y AUTORIDAD PARA LA OPERACIÓN DEL SISTEMA DE GESTIÓN DE COMPLIANCE.

"**OBLIGACIÓN DE COMPLIANCE**", REQUISITO QUE UNA ORGANIZACIÓN TIENE OBLIGATORIAMENTE QUE CUMPLIR ASÍ COMO AQUELLOS QUE UNA ORGANIZACIÓN ELIGE VOLUNTARIAMENTE CUMPLIR.

"**CULTURA DE COMPLIANCE**", VALORES, ÉTICA, CREENCIAS Y CONDUCTAS QUE EXISTEN E INTERACTÚAN EN LA ORGANIZACIÓN CON LAS ESTRUCTURAS Y SISTEMAS DE CONTROL.

## ALCANCE

Para el alcance de la certificación habrá que delimitar si se abarca toda la organización, una unidad específica o una función específica dentro de la organización.

También es relevante determinar el ámbito geográfico.

El alcance ha de ser razonable y proporcionado teniendo en cuenta la naturaleza y los riesgos de Compliance a los que se enfrenta la organización.

# ANÁLISIS DETALLADO DE LOS REQUISITOS DE LA NORMA ISO 37301 Y SU RELACIÓN CON LAS DIRECTRICES

## REQUISITOS

Los “debes” de la norma





## DIRECTRICES

Las recomendaciones, no obligatorias

# 4.1 CONTEXTO

# 4. CONTEXTO

1. COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO

2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE COMPLIANCE

4. SISTEMA DE GESTIÓN DE COMPLIANCE

5. OBLIGACIONES DE COMPLIANCE

6. EVALUACIÓN DE LOS RIESGOS DE COMPLIANCE

## 4.1.COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO



La norma nos requiere la realización de un análisis de contexto, para lo que debemos tener en cuenta:

**Debe** determinar las cuestiones internas y externas relevantes (para el propósito y para alcanzar los objetivos).

**Debe** tener en cuenta una serie de cuestiones que propone la norma (no limitativas):

Modelo de negocio (estrategia, naturaleza, tamaño, complejidad, sostenibilidad)

Contexto legal y regulatorio
Situación económica
Contexto social, cultural y ambiental
Estructuras, políticas, procesos, procedimientos y recursos internos, tecnología
Cultura de Compliance

## 4.1.COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO



Relevancia del alto grado de comprensión de la organización de las cuestiones que realmente son relevantes y que pueden afectar al sistema de gestión de Compliance.

Factores externos: no considerar sólo los contextos legales y regulatorios y tener en cuenta las tendencias futuras relevantes que podrían generar impacto.

Factores internos: importancia de tomarlos en consideración.

Ni los requisitos ni las directrices apuntan metodología alguna pero si destacan la importancia de realizar este análisis como punto de partida del sistema de gestión.

## 4.2.COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LA PARTES INTERESADAS



La organización **debe** determinar:

Las partes interesadas pertinentes al sistema de gestión de Compliance

Los requisitos pertinentes de estas partes interesadas

Cuáles de estos requisitos se abordarán en el sistema de gestión de Compliance

## 4.2.COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS



Es necesario identificar las partes interesadas que:

Pueden afectar
Verse afectadas
Percibirse como afectadas

por el sistema de gestión de Compliance

Tener en consideración que hay necesidades y expectativas que se convierten en obligaciones.

Ejemplos de partes interesadas: gobiernos y agencias gubernamentales, organismos reguladores, dirección, empleados, clientes, proveedores, socios comerciales, sociedad, propietarios, accionistas, inversores…

## 4.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE COMPLIANCE



La organización **debe** determinar:

Los límites y la aplicabilidad del sistema de gestión de Compliance para determinar su alcance.

Para determinar el alcance la organización **debe** considerar: las cuestiones externas e internas, los requisitos de los apartados 4.2, 4.4 y 4.5.

El alcance **debe** estar disponible como información documentada.

Nota: el alcance pretende aclarar los principales riesgos de Compliance a los que se enfrenta la organización y los límites geográficos y/u organizativos a los que se aplicará el sistema, especialmente si es parte de una entidad más amplia.

## 4.3.DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE COMPLIANCE



La determinación del alcance es el proceso por el que la organización ha de establecer los límites físicos y organizativos a los que se aplica el sistema de gestión.

La organización tiene la libertad y la flexibilidad de elegir implementar el sistema de gestión en toda la organización o en una unidad específica.

Lo más habitual será que se implante en toda la organización.

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

Este alcance tiene que estar alineado con el análisis de contexto y de partes interesadas.

## 4.4. SISTEMA DE GESTIÓN DEL COMPLIANCE



La organización **debe** establecer, implementar, mantener y mejorar continuamente un sistema de gestión de Compliance.

El sistema de gestión **debe** reflejar los valores, objetivos, estrategia y riesgos de Compliance de la organización teniendo en cuenta el contexto de la organización.

## 4.4. SISTEMA DE GESTIÓN DEL COMPLIANCE



Un sistema de gestión de Compliance es un marco que integra estructuras, políticas, procesos y procedimientos esenciales para conseguir los resultados de Compliance y actuar para prevenir, detectar y reaccionar ante un incumplimiento de Compliance.

Es una cuestión estructural, la infraestructura necesaria sobre la que construir el sistema.

El sistema puede disponer de muchos elementos, y es necesario que integre elementos para detectar y para reaccionar ante los incumplimientos.

El sistema debe basarse en los principios de buen gobierno, proporcionalidad, integridad, transparencia, responsabilidad y sostenibilidad.

## 4.5. OBLIGACIONES DE COMPLIANCE



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

**Debe** disponer de procesos para:

Identificar novedades y modificaciones en las obligaciones de Compliance para asegurar un cumplimiento continuo.

Evaluar el impacto de los cambios identificados e implementar cualquier cambio necesario en la gestión de las obligaciones de Compliance.

**Debe** conservar información documentada de las obligaciones de Compliance.

## 4.5. OBLIGACIONES DE COMPLIANCE



Las obligaciones de Compliance deberían ser la base para establecer, desarrollar e implementar un sistema de gestión de Compliance así como para mantenerlo.

Las obligaciones pueden provenir de diferentes fuentes. Se puede diferenciar entre las que la organización tiene que cumplir obligatoriamente (normalmente las que provienen de leyes, reglamentos, reguladores, sentencias…) de las que ha elegido cumplir voluntariamente (acuerdos con terceros, políticas y procedimientos internos…)

Es importante relacionar las obligaciones con las funciones y departamentos afectados.

Importancia de los procesos por los que se obtiene información sobre la actualización de las obligaciones.

Principio de orientación al riesgo, principio de Pareto. Identificar obligaciones, establecer el impacto, gestionar las obligaciones, los controles vinculados, la evaluación de riesgos.

## 4.6. EVALUACIÓN DE LOS RIESGOS DE COMPLIANCE



La organización **debe** identificar, analizar y evaluar sus riesgos de Compliance basándose en una evaluación.

**Debe** identificar los riesgos de Compliance relacionando las obligaciones con las actividades, productos y servicios y aspectos relevantes de sus operaciones.

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

La organización **debe** conservar información documentada sobre la evaluación de riesgos de Compliance y sobre las acciones para abordar estos riesgos.

## 4.6. EVALUACIÓN DE LOS RIESGOS DE COMPLIANCE



La evaluación de riesgos constituye la base del sistema de Compliance porque debe permitir la adecuada asignación de recursos y de los procesos adecuados.

Se apuntan cuestiones que pueden ayudar para establecer la metodología de evaluación:

- Tener en cuenta criterios de probabilidad e impacto
- Incluir la diferencia entre riesgo inherente y riesgo residual
- Definir las situaciones concretas de riesgo de Compliance
- Nivel de riesgo aceptable
- Reevaluación periódica y ante determinadas situaciones

El resultado de la evaluación de riesgos sirve para establecer donde hay que centrar la atención y los recursos.
Todos los riesgos deben ser objeto de seguimiento y tratamiento.

# 5. LIDERZGO

# 5. LIDERAZGO

1. LIDERAZGO Y COMPROMISO
2. POLÍTICA DE COMPLIANCE
3. ROLES, RESPONSABILIDADES Y AUTORIDADES

## 5. LIDERAZGO Y COMPROMISO



### 5.1.1 ÓRGANO DE GOBIERNO Y ALTA DIRECCIÓN

Se hace referencia a ambos órganos indistintamente.

El órgano de gobierno y la alta dirección **deben** demostrar liderazgo y compromiso con respecto al sistema de gestión de Compliance. La norma detalla como materializar estas obligaciones (asegurando que se establezca la política, asegurando la disponibilidad de recursos, comunicando la importancia del sistema…)

Se indican aquellas funciones principales entre las que cabe destacar “designar o nominar una función de Compliance”

### 5.1.2 CULTURA DE COMPLIANCE

La organización **debe** desarrollar, mantener y promover una cultura de Compliance. El órgano de gobierno, la alta dirección y la dirección **deben** demostrar un compromiso activo, visible, consistente y sostenido.

## 5.1.LIDERAZGO Y COMPROMISO



### 5.1.2 CULTURA DE COMPLIANCE

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

### 5.1.3 GOBIERNO DE COMPLIANCE

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

- Acceso directo de la función de Compliance al órgano de gobierno
- Independencia de la función de Compliance (ausencia de interferencia/presión)
- Autoridad y competencia adecuada de la función de Compliance

## 5.1.LIDERAZGO Y COMPROMISO



### 5.1.1 ÓRGANO DE GOBIERNO Y ALTA DIRECCIÓN

Importancia de que ambos órganos muestren su compromiso. Propone la aprobación de la política por el órgano de gobierno.
Se detalla algo más como se puede concretar este compromiso.

### 5.1.2. CULTURA DE COMPLIANCE

Indica factores que apoyan el desarrollo de esta cultura (conjunto de valores publicados, dirección que implementa y respeta, predicar con el ejemplo, comunicación continúa, formación, reconocimiento de los logros de Compliance, medidas disciplinarias ante incumplimientos…)

Se debería medir la cultura de Compliance, recabar aportaciones de los empleados y establecer planes de acción.

## 5.1.LIDERAZGO Y COMPROMISO



### 5.1.3. GOBIERNO DE COMPLIANCE

La gobernanza de Compliance se basa en los siguientes principios:

El acceso directo de la función de Compliance al órgano de gobierno.

La independencia de la función de Compliance.

La autoridad de la función de Compliance.

Recursos adecuados para la función de Compliance.

## 5.2.POLÍTICA DE COMPLIANCE



El órgano de gobierno y la alta dirección **deben** establecer una política de Compliance. Esta debe ser adecuada al propósito de la organización, proporcionar marco para los objetivos, incluir el compromiso de cumplir los requisitos aplicables e incluir el compromiso de la mejora continua.

La política **debe**:

- Estar alineada con los valores, objetivos y estrategia de la organización.
- Requerir el cumplimiento de las obligaciones de Compliance.
- Apoyar los principios de gobierno de Compliance.
- Hacer referencia a la función de Compliance y describirla.
- Resumir las consecuencias de no cumplir con las obligaciones de Compliance, políticas…
- Fomentar el planteamiento de inquietudes y prohibir cualquier tipo de represalia.
- Estar escrita en lenguaje sencillo.
- Implementarse y hacerse cumplir de forma adecuada.
- Estar disponible como información documentada.
- Comunicarse dentro de la organización.
- Estar disponible para las partes interesadas, según corresponda.

## 5.2. POLÍTICA DE COMPLIANCE



El documento de política establece los principios generales y el compromiso de acción de una organización en relación con el Compliance.

Aprobación por el órgano de gobierno.

No debería ser un documento único, sino apoyarse por otros documentos.

Traducida a los idiomas necesarios.

Adecuada para las obligaciones de Compliance que derivan del alcance y sus actividades.

Se indican consideraciones para su desarrollo.

## 5.3. ROLES, RESPONSABILIDADES Y AUTORIDADES



### 5.3.1 ÓRGANO DE GOBIERNO Y ALTA DIRECCIÓN

**Deben** asegurarse que se asignen y comuniquen las responsabilidades y autoridades.
**Deben** asignar las responsabilidades y autoridad para:

- Asegurar que el sistema de Compliance cumpla con los requisitos de esta norma.
- Informar al órgano de gobierno y alta dirección sobre el desempeño del sistema.

El órgano de gobierno **debe**:
Garantizar que a la alta dirección se la mide en función del logro de objetivos de Compliance
Ejercer la supervisión de la alta dirección en relación con la operación del sistema

La alta dirección **debe**:
Asignar recursos adecuados, asegurar que existen sistemas eficaces para informar sobre el desempeño del sistema, asegurar el alineamiento entre las metas estratégicas y las operativas y las obligaciones, establecer y mantener los mecanismos de rendición de cuentas, asegurar la integración del desempeño de Compliance en las evaluaciones de desempeño del personal.

## 5.3.ROLES, RESPONSABILIDADES Y AUTORIDADES



### 5.3.2. FUNCIÓN DE COMPLIANCE

**Debe** responsabilizarse de la operación del sistema de gestión de Compliance; facilitando las obligaciones de Compliance, la evaluación de riesgos de Compliance, la alineación de los objetivos, medir el desempeño y hacer el seguimiento, analizar y evaluar el desempeño del sistema, establecer un sistema de información y documentación de Compliance, asegurarse que el sistema se revise a intervalos planificados y establecer un sistema para plantear inquietudes y garantizar que estas se aborden.

**Debe** responsabilizarse de vigilar: asignación de obligaciones en los puestos, integrar las obligaciones de Compliance en procesos y procedimientos, que todo el personal esté formado y que se establezcan indicadores.

**Debe** responsabilizarse de realizar seguimiento y medir el desempeño, analizar y evaluar el desempeño, asegurar que el sistema se revisa a intervalos planificados.

**Debe** proporcionar acceso al personal a los recursos y asesoramiento a la organización.

## 5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES



### 5.3.3 DIRECCIÓN

**Debe** ser responsable de Compliance dentro de su área de responsabilidad.

(cooperando y apoyando a la función de Compliance, integrando las obligaciones de Compliance, desarrollando la concienciación del personal, animando al personal a plantear inquietudes…)

### 5.3.4 PERSONAL

Todo el personal **debe:**

Observar las obligaciones, políticas, procedimientos y procesos de Compliance.

Informar sobre inquietudes, cuestiones o fallos de Compliance.

Participar en la formación cuando corresponda.

## 5.3. ROLES, RESPONSABILIDADES Y AUTORIDADES



Se insiste en la relevancia del **órgano de gobierno y la alta dirección**.
Órgano de gobierno: su involucración activa es fundamental y contribuye a asegurar que los empleados comprenden plenamente la política y los procedimientos.
Es necesario que órgano de gobierno y alta dirección prediquen con el ejemplo.
La alta dirección ha de fomentar comportamientos que crean en el Compliance y no debería tolerar comportamientos que comprometan el Compliance.

Sobre la **función de Compliance**, se habla de las posibles formas que puede adoptar (unipersonal o colegiado), que no siempre puede ser una función exclusiva y que se puede contratar externamente.
Se hace referencia a las consideraciones en relación con la función de Compliance: integridad y compromiso, habilidades, capacidad y prestigio, competencia pertinente, firmeza, enfoque estratégico.
Se refuerza que la independencia es mantenerse alejado de actividades expuestas a obligaciones de Compliance.

## 5.3. ROLES, RESPONSABILIDADES Y AUTORIDADES



En relación con **la Dirección** se refuerza el papel de todos los directivos, no solo de la alta dirección, en relación con el sistema. Por eso es importante que se describan estas responsabilidades y se incluyan en la descripción de sus puestos.

En relación con **el personal** se espera que cumplan con las obligaciones de Compliance y que mediante la formación, las políticas y los procedimientos conoce sus responsabilidades. Además debería ser proactivo y contribuir al conocimiento y las mejoras.

# 6. PLANIFICACIÓN

## 6. PLANIFICACIÓN

1. ACCIONES PARAABORDAR RIESGOS Y OPORTUNIDADES
2. OBJETIVOS DE COMPLIANCE Y PLANIFICACIÓN PARA LOGRARLOS
3. PLANIFICACIÓN DE LOS CAMBIOS

## 6.1.ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES



Teniendo en cuenta el contexto y los requisitos de las partes interesadas, la organización **debe** determinar los riesgos y oportunidades que necesitar abordarse para:

- Asegurar que el sistema de Compliance puede lograr los resultados previstos.
- Evitar o reducir los efectos no deseados.
- Lograr la mejora continua.

Al planificar el sistema de Compliance, la organización **debe** considerar:

- Sus objetivos de Compliance
- Las obligaciones de Compliance identificadas
- Los resultados de la evaluación de los riesgos de Compliance

La organización **debe** planificar:

- Acciones para abordar riesgos y oportunidades
- La forma de integrar e implementar las acciones y evaluar la eficacia de estas acciones

## 6.1. ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES



La planificación del sistema de Compliance se ha de realizar tanto a nivel estratégico como a nivel operativo.

El principal propósito de planificar es anticipar escenarios y consecuencias potenciales, carácter preventivo. La organización ha de planificar en base al resultado de la evaluación de riesgos.

Esta planificación ha de incluir como incorporar las acciones en las actividades o procesos operativos.

También se deberían planificar las medidas para evaluar la eficacia del sistema (seguimiento, técnicas de medición, auditoria interna o revisión por la dirección)

## 6.2.OBJETIVOS DE COMPLIANCE Y PLANIFICACIÓN PARA LOGRARLOS



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

Los objetivos **deben**:

- Ser coherentes con la política de Compliance
- Ser medibles, si es posible
- Tener en cuenta los requisitos aplicables
- Ser objeto de seguimiento
- Comunicarse
- Actualizarse cuando corresponda
- Estar disponible como información documentada

Cuando se planifican, la organización **debe** determinar: que se va a hacer, que recursos son necesarios, quien será responsable, cuando se finalizará, como se evaluarán los resultados.

## 6.2. OBJETIVOS DE COMPLIANCE Y PLANIFICACIÓN PARA LOGRARLOS



Se insiste en que los objetivos se especifiquen de manera que puedan medirse.

La importancia de indicar el “qué”, el “cuándo” y el “quién”.

La importancia de realizar el seguimiento de los objetivos y su actualización cuando sea necesario.

## 6.3. PLANIFICACIÓN DE LOS CAMBIOS



Cuando la organización determine que es preciso realizar cambios en el sistema de gestión, estos **deben** llevarse a cabo de forma planificada.

No hay directrices en la segunda parte de la norma sobre este apartado.

# 7. APOYO

## 7. APOYO

1. RECURSOS
2. COMPETENCIA
3. TOMA DE CONCIENCIA
4. COMUNICACIÓN
5. INFORMACIÓN DOCUMENTADA

## 7.1. RECURSOS



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

## 7.1. RECURSOS



Cuando se habla de recursos se incluyen:

- Los financieros
- Los humanos
- Los técnicos
- Acceso a asesoramiento externo
- Infraestructura organizativa
- Material de referencia sobre gestión de Compliance y obligaciones legales
- Desarrollo profesional y tecnología

## 7.2. COMPETENCIA



7.2.1 GENERALIDADES

La organización **debe:**

Determinar la competencia necesaria de las personas que realizan trabajos que afectan al desempeño de Compliance

Asegurarse que estas personas son competentes, en base a la educación, formación o experiencia adecuado

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

7.2.2 PROCESO DE EMPLEO

En relación con todo el personal, la organización debe:

Establecer que las condiciones de empleo requieran que el personal cumpla con el sistema

En un periodo razonable desde la incorporación el empleo, que el personal reciba copia o acceso a la política y formación relacionada con esta

Se tomen las acciones disciplinarias adecuadas contra el personal que infrinja las obligaciones

## 7.2. COMPETENCIA



Como parte del proceso de empleo la organización **debe** considerar los riesgos de Compliance, aplicando los procedimientos de diligencia debida que correspondan antes de cualquier contratación, cambio de puesto o promoción.

La organización **debe** implementar un proceso que permita la revisión periódica de las metas de desempeño, las bonificaciones de desempeño y demás incentivos para verificar que se aplican las medidas adecuadas para evitar que se fomente el incumplimiento.

### 7.2.3. FORMACIÓN

La organización **debe** proporcionar formación al personal pertinente de forma regular desde su incorporación y a intervalos planificados. La formación **debe**:

Ser adecuada a los roles del personal y a los riesgos de Compliance a los que se expone el personal

Evaluarse en términos de eficacia

Revisarse regularmente

**Debe** conservarse información documentada.



## 7.2 COMPETENCIA

### 7.2.1 GENERALIDADES

Recuerda que la competencia requiere de conocimientos, experiencia y habilidades para que una persona pueda realizar sus funciones de manera eficaz.
Es necesario definir la competencia de todo el personal pero, en este caso, especialmente las del personal con funciones de Compliance y conservar la evidencia documentada que acredite esa competencia.
Las competencias se han de adaptar para garantizar que pueden mantenerse y adquirirse nuevas, en función de las necesidades.

### 7.2.2 PROCESO DE EMPLEO

Se hace referencia a la necesidad de establecer los procedimientos de diligencia debida adecuados previos a la contratación o a la promoción interna. Estos procedimientos podrían conllevar la comprobación de referencias o de antecedentes.

## 7.2. COMPETENCIA



### 7.2.3. FORMACIÓN

Un programa de formación adecuado puede asegurar que el personal es competente para cumplir con su rol profesional y puede proporcionar una manera eficaz de que el personal comunique riesgos de Compliance.

Se refuerza la importancia de los programas de formación adecuados a las necesidades, que la formación puede ser una de las mejores reacciones ante los incumplimientos y detalla que circunstancias pueden aconsejar impartir formación adicional (cambios en procedimientos, cambios en roles, cambios en la estructura, cambios en las obligaciones, cambios en las actividades…).

## 7.3. TOMA DE CONCIENCIA



Las personas que trabajan en la organización **deben** tomar conciencia de:

- La política de Compliance
- Su contribución a la eficacia del sistema de Compliance
- Las implicaciones de no cumplir los requisitos del sistema
- Los medios y procedimientos para plantear inquietudes
- La relación entre la política de Compliance y las obligaciones pertinentes en sus roles
- La importancia de apoyar la cultura de Compliance

## 7.3. TOMA DE CONCIENCIA



Por un lado, la toma de conciencia requiere poner a disposición y asegurar que son accesibles tanto la política o los procedimientos, facilitar la formación, la comunicación o los materiales de referencia y sus actualizaciones.

Pero, además, implica sensibilizar al personal para que adopten el sistema y animar al personal para que haga sus sugerencias que faciliten la mejora continua.

## 7.4. COMUNICACIÓN



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

Contenido de la comunicación
Cuando comunicar
A quién comunicar
Como comunicar

La organización **debe** considerar los obstáculos potenciales y la diversidad, asegurar que se tienen en cuenta las opiniones de las partes interesadas, responder a las comunicaciones pertinentes, conservar información documentada de las comunicaciones, comunicar internamente la información pertinente del sistema, asegurar que los procesos de comunicación permiten al personal su contribución y asegurar que pueden plantear inquietudes, comunicar externamente la información pertinente.

## 7.4. COMUNICACIÓN



El enfoque de la comunicación externa ha de ser práctico y teniendo en cuenta todas las partes interesadas.

Refuerza la importancia de la comunicación interna.

Se pueden usar distintos medios para la comunicación, lo importante es que se adapten a la diversidad y a las necesidades de los grupos a los que se quiere comunicar.

Las comunicaciones han de respetar los principios de transparencia, adecuación, credibilidad, capacidad de respuesta, accesibilidad y claridad.

## 7.5 INFORMACIÓN DOCUMENTADA



### 7.5.1 GENERALIDADES

El sistema de gestión de Compliance **debe** incluir:

- La información documentada que requiere la norma
- La información documentada que la organización ha determinado como necesaria

### 7.5.2 CREACIÓN Y ACTUALIZACIÓN DE LA INFORMACIÓN DOCUMENTADA

La información documentada **debe**:

- Tener la identificación y descripción adecuada
- Tener el formato y los medios de soporte adecuados
- La revisión y aprobación con respecto a la idoneidad y adecuación

### 7.5.3 CONTROL DE LA INFORMACIÓN DOCUMENTADA

La información documentada **debe** estar disponible y adecuada para su uso, estar protegida adecuadamente.

Para el control **debe** tratar las actividades de distribución, acceso, almacenamiento, control cambios, retención y disposición…

## 7.5. INFORMACIÓN DOCUMENTADA



La información documentada puede incluir:

política y procedimientos
objetivos y metas
asignación de roles y responsabilidades
registro de obligaciones de Compliance
registro de riesgos de Compliance y su priorización basado en el resultado de la evaluación
registro de incumplimientos
planes anuales de Compliance
registros de personal
registros de auditoria interna

# 8. OPERACIÓN

## 8. OPERACIÓN

1. PLANIFICACIÓN Y CONTROL OPERACIONAL
2. ESTABLECIMIENTO DE CONTROLES Y PROCEDIMIENTOS
3. PLANTEAMIENTO DE INQUIETUDES
4. PROCESOS DE INVESTIGACIÓN

## 8.1. PLANIFICACIÓN Y CONTROL OPERACIONAL



La organización **debe** planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas mediante:

- El establecimiento de criterios para los procesos
- La implementación del control de los procesos de acuerdo con los criterios

La organización **debe** controlar los cambios planificados y revisar las consecuencias de los cambios no previstos.

La organización **debe** asegurar que los procesos, productos o servicios que se proporcionan externamente se controlan y realiza el seguimiento de los mismos.

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

## 8.1. PLANIFICACIÓN Y CONTROL OPERACIONAL



Los controles operacionales se requieren para situaciones relacionadas con los procesos de negocio cuando la falta de tales controles podría llevar a desviaciones de la política de Compliance o a una infracción de las obligaciones de Compliance.

El grado de control puede variar dependiendo de:

- Importancia o complejidad de las funciones
- Consecuencias potenciales de incumplimiento
- Apoyo técnico involucrado o disponible

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

En caso de uso de procesos de terceras partes, se recomienda usar procedimientos de diligencia debida eficaz.

## 8.2. ESTABLECIMIENTO DE CONTROLES Y PROCEDIMIENTOS



La organización **debe** implementar controles para gestionar sus obligaciones de Compliance y los riesgos de Compliance asociados.

Estos controles se **deben** mantener, evaluar y probar periódicamente para asegurarse de que continúan siendo eficaces.

## 8.2. ESTABLECIMIENTO DE CONTROLES Y PROCEDIMIENTOS



Los controles han de diseñarse con el rigor suficiente para facilitar el logro de las obligaciones de Compliance y siempre que se pueda esos controles deben estar integrados en los procesos organizativos normales.

Los controles pueden incluir; políticas, procedimientos, instrucciones de trabajo, autorizaciones, sistemas e informes, segregación de roles, procesos automatizados, planes anuales de Compliance, planes de desempeño de empleados, evaluaciones de Compliance y auditorias…

Los procedimientos que apoyan la gestión de Compliance han de integrarse con los procedimientos organizativos, ser consistentes con las funciones de revisión y control, realizar seguimiento y medición continuos y evaluar e informar de su cumplimiento.

## 8.3. PLANTEAMIENTO DE INQUIETUDES



La organización **debe** establecer, implementar y mantener un proceso para animar y permitir que se informe sobre los intentos de infracción, las infracciones supuestas o reales de la política o de las obligaciones de Compliance.

Este proceso **debe**:

- Ser visible y accesible en toda la organización
- Tratar los informes de forma confidencial
- Aceptar los informes anónimos
- Proteger a aquellos que realizan los informes de las represalias
- Permitir al personal que reciba asesoramiento

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

## 8.3. PLANTEAMIENTO DE INQUIETUDES



Se indica que, incluso en aquellos casos en que no lo requiera la reglamentación local, se tendrían que desarrollar mecanismos de denuncias que admiten el anonimato, lo que contribuya a generar confianza en los empleados para el uso de estos canales sin miedo a represalias.

## 8.4. PROCESOS DE INVESTIGACIÓN



La organización **debe** desarrollar, establecer, implementar y mantener los procesos para valorar, evaluar, investigar y cerrar los informes sobre casos supuestos o reales de incumplimientos. Estos procesos **deben** asegurar que la toma de decisiones es justa e imparcial.

Los procesos de investigación **deben** realizarse de forma independiente y sin conflicto de interés por el personal competente.

La organización **debe** usar el resultado de las investigaciones para la mejora del sistema.

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

La organización **debe** conservar la información documentada sobre la investigación.

## 8.4. PROCESOS DE INVESTIGACIÓN



Un mecanismo eficaz para las investigaciones es una característica de un sistema de gestión de Compliance.

Con el se han de identificar las causas raíz de las malas prácticas, las vulnerabilidades del sistema de gestión y los fallos de responsabilidad.

Importancia de las investigaciones justas e independientes.

Importancia del mecanismo de información de las investigaciones.

# 9. EVALUACIÓN DE DESEMPEÑO

## 9. EVALUACIÓN DEL DESEMPEÑO

1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN
2. AUDITORIA INTERNA
3. REVISIÓN POR LA DIRECCIÓN

## 9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN



### 9.1.1 GENERALIDADES

La organización **debe** revisar el sistema de gestión de Compliance para garantizar que se alcanzan los objetivos de Compliance.

La organización **debe** determinar:

- Que debe ser objeto de seguimiento y que es necesario medir
- Los métodos de seguimiento, medición, análisis y evaluación para asegurar resultados válidos
- Cuando se deberían llevar a cabo el seguimiento y la medición
- Cuando se debería analizar, evaluar y comunicar los resultados del seguimiento y la medición

Se **debe** conservar la información documentada.

## 9.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN



### 9.1.2 FUENTES DE OPINIÓN SOBRE EL DESEMPEÑO DE COMPLIANCE

La organización debe establecer, implementar, evaluar y mantener procedimientos para buscar y recibir opiniones de su desempeño de Compliance de una serie de fuentes.

La información debe analizarse y evaluarse críticamente para identificar las causas fundamentales de incumplimiento, garantizar que se toman las acciones adecuadas y reflejar esta información en la evaluación periódica de riesgos.

### 9.1.3 DESARROLLO DE INDICADORES

La organización debe definir, implementar y mantener un conjunto de indicadores adecuados que ayuden a la organización a evaluar el logro de sus objetivos y a cuantificar el desempeño.

## 9.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN



### 9.1.4 INFORMES DE COMPLIANCE

La organización **debe** establecer, implementar y mantener procesos para lo informes de Compliance para asegurar que se definen los criterios para su presentación, se establecen plazos, se implementa un sistema de informes de excepciones, se implementan sistemas y procesos que aseguran la exactitud de los informes y que su contenido es completo, se facilita una información exacta y completa a las funciones o áreas apropiadas

### 9.5.1 MANTENIMIENTO DE REGISTROS

Se **deben** mantener registros actualizados de las actividades de la organización con objeto de ayudar en los procesos de seguimiento y revisión y para determinar la conformidad con el sistema de Compliance.

## 9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN



9.1 GENERALIDADES

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

Este seguimiento del sistema incluye: eficacia de la formación, eficacia de los controles, asignación eficaz de las responsabilidades, actualización de las obligaciones, eficacia de la gestión de fallos, revisiones de la estrategia frente a fallos…

El seguimiento del desempeño incluye: incumplimientos y conatos, casos en que no se cumplen las obligaciones, casos en que no se alcanzan los objetivos, estado de la cultura, indicadores predictivos y reactivos.

9.2 FUENTES DE OPINIÓN SOBRE EL DESEMPEÑO DE COMPLIANCE

Se incluyen ejemplos de fuentes (empleados, clientes, proveedores, reguladores…), de métodos para recoger información y de que cuestiones se pueden incluir.



## 9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

9.1.3. DESARROLLO DE INDICADORES

Los indicadores han de tener relación con las principales características de los riesgos de Compliance.

Los indicadores son relevantes para medir la eficacia del sistema y estos indicadores variarán a medida que la organización y el sistema maduren.

Se incluyen ejemplos de indicadores reactivos y de indicadores predictivos.

9.1.4 INFORMES DE COMPLIANCE

Se incluyen sugerencias sobre el contenido de los informes de Compliance.

9.1.5 MANTENIMIENTO DE REGISTROS

Se incluyen ejemplos de registros del desempeño y se recuerdan las cautelas con los registros.

## 9.2. AUDITORIA INTERNA



### 9.2.1. GENERALIDADES

La organización **debe** llevar a cabo auditorias internas a intervalos planificados para proporcionar información de que el sistema:

Cumple; tanto con los requisitos de la norma como con los requisitos propios

Se implementa y se mantiene eficazmente

### 9.2.2 PROGRAMA DE AUDITORIA INTERNA

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

**Debe** considerar la importancia de los procesos y los resultados de auditorias previas.

**Debe** definir para cada auditoria los criterios, objetivos y alcance, seleccionar los auditores y asegurar la objetividad e imparcialidad, asegurar que los resultados se comunican a los directivos pertinentes y a la dirección.

## 9.2. AUDITORIA INTERNA



Las funciones de auditoria interna han de estar libres de conflicto de intereses y ser independientes para cumplir con su rol. Tanto si estas funciones son internas como si son externas.

Se hace referencia a la norma UNE 19011:2018 que recoge los requisitos sobre como realizar una auditoria interna de un sistema de gestión.

## 9.3 REVISIÓN POR LA DIRECCIÓN



### 9.3.1 GENERALIDADES

El órgano de gobierno y la alta dirección **deben** revisar el sistema de gestic
intervalos planificados, para asegurar su idoneidad, adecuación y eficacia.

### 9.3.2 ENTRADAS PARA LA REVISIÓN DEL SISTEMA

La revisión **debe** incluir:

Estado de las acciones desde anteriores revisiones

Cambios en las cuestiones internas y externas

Cambios en las necesidades y expectativas de las partes interesadas y que son relevantes

Información sobre el desempeño (no conformidades, seguimiento y resultado de las mediciones, resultados auditorias)

Oportunidades de mejora continua

La revisión **debe** tener en cuenta:

Adecuación de la política, independencia de la función, grado de cumplimiento de objetivos, adecuación de los recursos, adecuación de evaluación de riesgos, eficacia controles e indicadores, comunicaciones, investigaciones, eficacia sistema de informes.



## 9.3. REVISIÓN POR LA DIRECCIÓN

### 9.3.3. RESULTADOS DE LA REVISIÓN POR LA DIRECCIÓN

Los resultados de la revisión **deben** incluir las decisiones relacionadas con:

- Las oportunidades de mejora
- Cualquier necesidad de cambio en el sistema

Se **debe** conservar información documentada.

## 9.3. REVISIÓN POR LA DIRECCIÓN



Se recogen otras cuestiones que también podrían ser incluidas en la revisión por la dirección:

- Necesidad de cambio en la política y en sus objetivos
- Cambios en los procesos de Compliance
- Áreas sobre las que hacer seguimiento de incumplimientos
- Acciones correctivas frente a incumplimientos
- Lagunas o carencias en el sistema e iniciativas al respecto
- Reconocimiento de un comportamiento ejemplar

# 10. MEJORA

## 10. MEJORA

1. MEJORA CONTINUA
2. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

## 10.1. MEJORA CONTINUA



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

Cuando la organización determina la necesidad de hacer cambios, **deben** realizarse de manera planificada.

La organización **debe** considerar:

- El propósito de los cambios y sus potenciales consecuencias
- El diseño y la eficacia operacional del sistema de gestión de Compliance
- La disponibilidad de recursos adecuados
- La asignación o reasignación de las responsabilidades y autoridades

## 10.2. NO CONFORMIDADES Y ACCIONES CORRECTIVAS



Cuando ocurra una no conformidad o un incumplimiento de Compliance, la organización **debe:**

Reaccionar ante la no conformidad o incumplimiento y tomar acciones o gestionar las consecuencias

Evaluar la necesidad de acciones para eliminar las causas de la no conformidad y/o incumplimiento con el fin de que no vuelva a ocurrir

Implementar cualquier acción necesaria

Revisar la eficacia de las acciones correctivas tomadas

Si es necesario, hacer cambios en el sistema de gestión de Compliance

## 10.1 MEJORA CONTINUA



La eficacia del sistema de gestión se caracteriza por tener la capacidad de tener la capacidad de mejorar y evolucionar continuamente.

La adecuación y eficacia del sistema se ha de evaluar de manera continuada y regular mediante varios métodos.

## 10.2 NO CONFORMIDADES Y ACCIONES CORRECTIVAS

La detección de no conformidades no implica que el sistema de gestión de Compliance no sea eficaz, lo importante es analizar las causas raíz y aprovechar las lecciones aprendidas.

# IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN ISO 37301

## IMPLANTACIÓN

Primer paso: el compromiso y la voluntad del órgano de gobierno y la implicación de la alta dirección.

Segundo paso: tras el análisis de contexto y las partes interesadas, el adecuado establecimiento del alcance del sistema.

Tercer paso: identificación de las obligaciones y análisis de los riesgos.

De manera continuada se debe trabajar la implantación de la cultura de Compliance.

# RELACIÓN DE LA ISO 37301 CON OTRAS NORMAS DE COMPLIANCE

## ¿CON QUE NORMAS DE COMPLIANCE VA A CONVIVIR LA UNE-ISO 37301?

UNE 19601, SISTEMAS DE GESTIÓN DE COMPLIANCE PENAL

UNE-ISO 37001, SISTEMAS DE GESTIÓN ANTISOBORNO

UNE 19602, SISTEMAS DE GESTIÓN DE COMPLIANCE TRIBUTARIO

**¿VIENE ESTA NORMA A SUSTITUIR A LAS YA EXISTENTES?**

**NO**

**PRINCIPALES DIFERENCIAS:**

PUNTO DE PARTIDA DE LOS SISTEMAS DE GESTIÓN DE COMPLIANCE PENAL, ANTISOBORNO Y TRIBUTARIO

LA IDENTIFICACIÓN DE POTENCIALES SITUACIONES DE RIESGO

PUNTO DE PARTIDA DEL SISTEMA DE GESTIÓN DE COMPLIANCE

LA IDENTIFICACIÓN DE OBLIGACIONES RELEVANTES PARA LA ORGANIZACIÓN EN RELACIÓN CON SUS ACTIVIDADES, SERVICIOS, PRODUCTOS, OPERACIONES

ESCENARIO INCIERTO/ESCENARIO CIERTO

EVALUACIÓN DE RIESGOS

## PRINCIPALES COINCIDENCIAS:

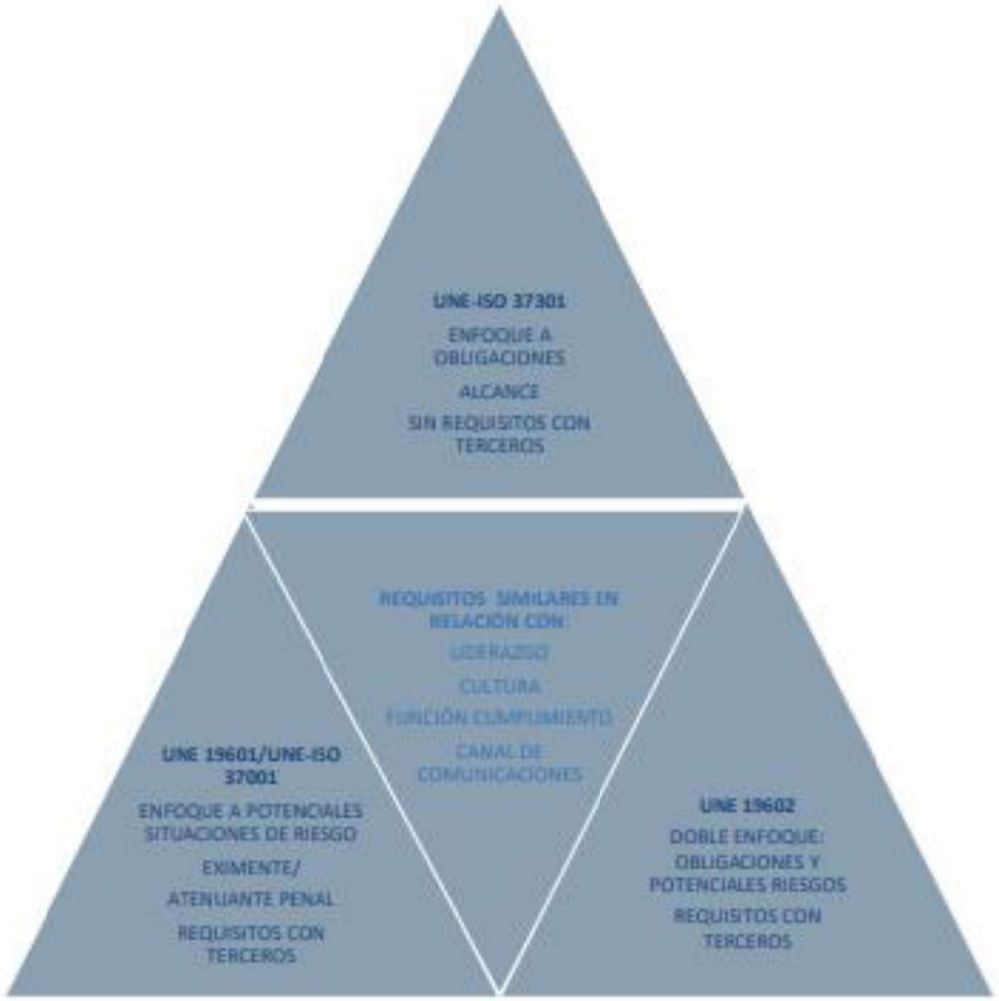
LIDERAZGO

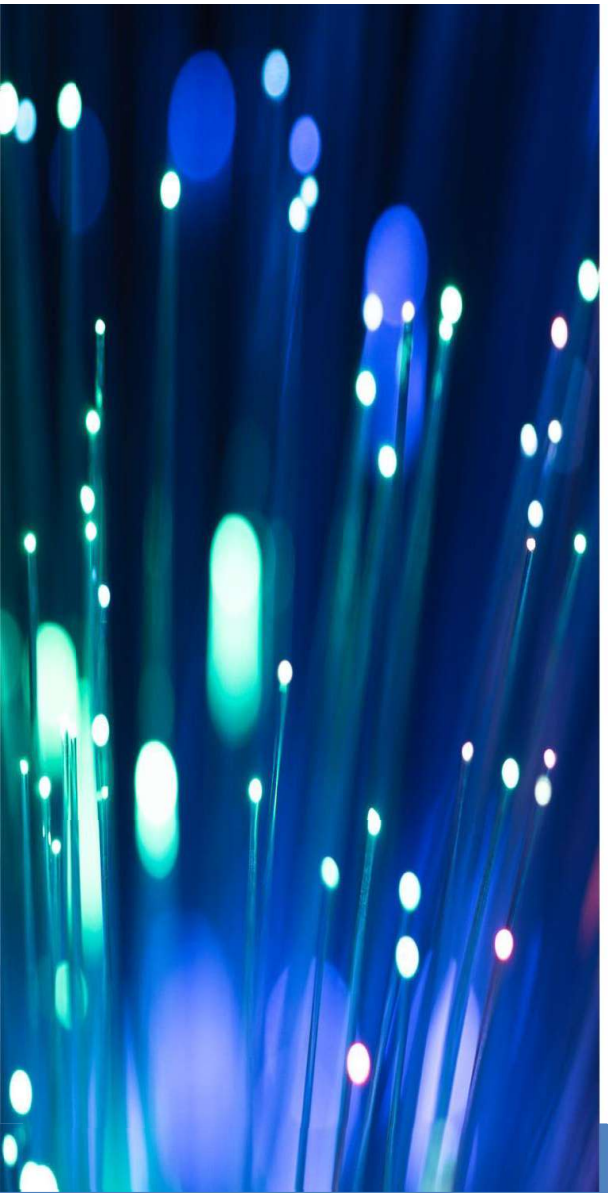
FUNCIÓN DE COMPLIANCE

CULTURA DE COMPLIANCE

MECANISMOS DE CONTROL

CANAL DE DENUNCIAS


UNE-ISO 37301
ENFOQUE A OBLIGACIONES
ALCANCE
SIN REQUISITOS CON TERCEROS
REQUISITOS SIMILARES EN RELACIÓN CON:
LIDERAZGO
CULTURA
FUNCIÓN CUMPLIMIENTO
CANAL DE COMUNICACIONES
UNE 19601/UNE-ISO 37001
ENFOQUE A POTENCIALES SITUACIONES DE RIESGO
EXIMENTE/
ATENUANTE PENAL
REQUISITOS CON TERCEROS
UNE 19602
DOBLE ENFOQUE: OBLIGACIONES Y POTENCIALES RIESGOS
REQUISITOS CON TERCEROS



# PREGUNTAS.