

UN ANÁLISIS DE LA ISO 37301:2021

Por Carlos Rozen y Amadeo Berdou





1. INTRODUCCIÓN

1.INTRODUCCIÓN

¿Qué pretende este texto?

La lectura y análisis de una norma puede resultar algo tediosa para quienes no tienen práctica en sistemas de gestión normados. Incluso entre expertos en la citada disciplina surgen contrapuntos y controversias respecto del significado de términos, frases e intenciones de los expertos actuantes detrás de cada estándar emitido. Es por ello que hemos efectuado un análisis profundo de la norma **37301:2021**.

Esta norma la podemos calificar como un estándar atípico, dado que su mejor interpretación suele estar dada por expertos en compliance con conocimientos en sistemas de gestión normados, conjuntamente con expertos en estos sistemas de gestión que se hayan introducido en el mundo de la ética, integridad y el compliance. Es por ello que en este texto Carlos Rozen y Amadeo Berdou han reunido sus conocimientos y experiencias para poner profundidad en un tema tan complejo como apasionante.

No obstante, el esfuerzo interpretativo, hemos intentado no apartarnos de los capítulos de la norma original, puesto que el lector podría considerar útil dirigirse al texto original del estándar.

Vamos a arrancar este estudio de la norma con una frase que pretende marcar el tono de todo lo que leeremos a partir de la misma:

Compliance está íntimamente relacionado con la sostenibilidad de la organización, con hacer buenos negocios por el camino correcto y en el largo plazo, generar entusiasmo y confianza en la gente, evitar multas y otras sanciones. Compliance inyecta competitividad. Como sociedad deseamos que todas las organizaciones tengan compliance. Como grupos en una industria, deseamos que todas tengan compliance para que la competencia sea justa. Entonces compliance es un arma de competitividad y la forma en que "ajustemos correctamente las tuercas" marcará la diferencia con nuestros competidores.

¿Por qué puede ser tan importante la ISO 37301:2021?

Las organizaciones que pretenden tener éxito a largo plazo necesitan establecer, mantener y mejorar una **cultura de compliance**, teniendo en cuenta las necesidades y expectativas de las partes interesadas. Por lo tanto, el compliance no es sólo la base para operar en forma adecuada, sino también **una oportunidad**, para que una organización sea 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 si se integra en la cultura de la organización y en el comportamiento y la actitud** de las personas que trabajan en ella. Sin dejar de mantener su independencia, es preferible que **la gestión del compliance se integre en los demás procesos de gestión de la organización**.

Un sistema eficaz de gestión del compliance permite a la organización demostrar su compromiso con el compliance de las leyes pertinentes, las normas de la organización, las mejores prácticas generalmente aceptadas, y las expectativas de la comunidad (además de la propia ISO 37301).

El enfoque que una organización da a Compliance tiene como ingrediente esencial el liderazgo ético en todos los niveles que aplica determinados valores fundamentales que la organización debe definir y comunicar con claridad, y mantener medidas para promover comportamientos consecuentes. Es decir, se busca integrar fundamentalmente el compliance en el comportamiento de las personas que trabajan en una organización.

En algunas jurisdicciones, los tribunales ya han tenido en cuenta el compromiso de una organización con el compliance a través de su sistema de gestión del compliance a la hora de determinar la condena apropiada que debe imponerse por las infracciones de las leyes pertinentes. Por lo tanto, los organismos reguladores y judiciales también pueden beneficiarse de la ISO 37301 como punto de referencia.

Un sistema de gestión de compliance basado en estas premisas, puede salvaguardar la integridad corporativa y evitar o minimizar el incumplimiento de las obligaciones de compliance. La integridad y el cumplimiento efectivo son, por tanto, elementos clave de una gestión buena y diligente. El compliance también contribuye al comportamiento socialmente responsable de las organizaciones.

Objetivos de la norma

Tal como se puede apreciar en el capítulo de introducción a la norma ISO 37301, el objetivo es ayudar a las organizaciones a **desarrollar y difundir una cultura positiva de compliance**, puesto que, si esto se hace en forma consistente, la entidad podría obtener beneficios tales como:

- ▶ mejorar las oportunidades de negocio y la **sostenibilidad**
- ▶ proteger y mejorar la **reputación y la credibilidad** de la organización
- ▶ lograr una mayor responsabilidad social considerando las **expectativas de las partes interesadas**
- ▶ **demostrar** el compromiso de una organización con la gestión de sus riesgos de compliance de forma eficaz y eficiente
- ▶ **aumentar la confianza** de terceros en la capacidad de la organización para lograr un éxito sostenible;
- ▶ **minimizar el riesgo de incumplimientos, con los correspondientes costos y daños a la reputación.**

ISO 37301 entonces **especifica los requisitos**, así como **proporciona orientación** (en el Anexo) sobre los sistemas de gestión de la compliance y las prácticas recomendadas. Tanto los requisitos como las orientaciones de la norma pretenden ser adaptables, y su aplicación puede variar en función del tamaño y el nivel de madurez del sistema de gestión de compliance de una organización y del contexto, la naturaleza y la complejidad de las actividades y los objetivos de la organización.

La norma ayuda a robustecer los requisitos relacionados con el cumplimiento basado en la propia norma y también respecto de otras metodologías implementadas, para ayudar a una organización a mejorar la gestión general de todas sus obligaciones de compliance.

1.1 Alcance

La norma ISO 37301 especifica los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema eficaz de gestión de compliance en una organización. Puesto que plantea tanto requisitos como directrices, usa como las siguientes formas verbales:

- ▶ “deberá” indica un requisito;
- ▶ “debería” indica una recomendación.
- ▶ “puede” indica un permiso, una posibilidad o una capacidad.

ISO 37301 es aplicable a todo tipo de organizaciones, independientemente del tipo, tamaño y naturaleza de la actividad, así como de si la organización es del sector público, privado o sin ánimo de lucro.

1.2 Referencias Normativas

Esta norma no plantea la necesidad de acompañar la lectura de la misma con soporte de otras normas, o la obligatoriedad de cumplir con otras normas ISO al implementarla. Cabe destacar, no obstante, que en su capítulo final, se listan referencias bibliográficas que dan evidencia en qué otras normas ISO u otros documentos de uso público se ha basado el desarrollo del estándar ISO 37301.

1.3 Términos y Definiciones

Con el objetivo de estandarizar el léxico en materia de compliance y garantizar una comprensión de los términos utilizados en la norma, se dan en este capítulo 31 definiciones, que el lector podrá consultar directamente de la norma.



2. CONTEXTO DE LA ORGANIZACIÓN

2. Contexto de la Organización

2.1 Comprensión de la Organización y su Contexto



Puntos donde centrar la atención:

“Contexto” a los efectos de la presente norma, se refiere al conjunto de circunstancias que rodean una organización que podría estar involucrada en un hecho de soborno, y sin las cuales no se podría comprender correctamente.

La organización debe identificar y comprender en profundidad las cuestiones externas e internas a la misma que son relevantes para su propósito y que afectan su capacidad para lograr los resultados que justificaron la implementación de su SGC.

Básicamente el estándar espera que la organización tenga en cuenta ciertos aspectos que definen su contexto, principalmente los siguientes:

- ▶ El modelo de negocio utilizado, su estrategia, su naturaleza, tamaño, complejidad y demás características de las actividades y operaciones
- ▶ la naturaleza y el alcance de las relaciones comerciales con terceros
- ▶ el contexto jurídico, normativo / regulatorio
- ▶ la situación económica
- ▶ el contexto social, cultural y medioambiental
- ▶ las estructuras, políticas, procesos, procedimientos y recursos internos, incluida la tecnología
- ▶ y muy particularmente, su cultura de compliance.

La organización debe poner énfasis en identificar otros aspectos contextuales si es que fueran relevantes a los fines planteados.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

En este punto recomendamos utilizar herramientas tales como “Análisis FODA” (o DAFO) o un análisis basado en la Matriz de las 5 fuerzas de Porter. Y si fuera posible la utilización de ambas herramientas en forma concurrente. Es muy útil que este análisis sea realizando junto con la Dirección de la organización y no un “ejercicio de gabinete o de laboratorio” por parte de Compliance sin contacto con la Dirección de la organización.

Un ejercicio de comprensión del contexto desarrollado a conciencia facilitará notoriamente la identificación y análisis de partes interesadas, de las obligaciones y de los riesgos de compliance.



2.2 Comprensión de las necesidades y expectativas de las partes interesadas



Puntos donde centrar la atención:

La Norma se refiere como parte interesada a persona u organización que puede afectar, ser afectada o percibir que es afectada por una decisión o actividad.

La no identificación de las partes interesadas (problema común en muchos de los programas de compliance que nos ha tocado revisar) se verá reflejada en una identificación de riesgos con limitaciones y, por consiguiente, la gestión de riesgos será incompleta. Esto puede impactar de lleno en la adecuación, proporcionalidad y robustez del modelo implementado. Por otra parte, una pobre identificación de las partes interesadas limitará un requisito posterior, que es el de consultarlas asiduamente.

Básicamente el estándar espera que la organización realice con precisión:

- ▶ un inventario de las partes interesadas que son relevantes para el SGC;
- ▶ la determinación de los requisitos pertinentes de estas partes interesadas;
- ▶ la identificación de requisitos que se abordarán a través del SGC.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para el cumplimiento de este punto nuestro equipo recomienda la utilización de una matriz que al menos tenga 2 dimensiones: x = grado de interés, e y = nivel de influencia. Una vez inventariadas las partes interesadas, y analizadas estas dos variables, se deberán tomar las medidas necesarias de aquí en adelante para relacionarse con esas partes.

A su vez el análisis de riesgos se nutrirá sustancialmente de este análisis.

2.3 Determinación del alcance del sistema de gestión de compliance (SGC)



Puntos donde centrar la atención:

El Alcance constituye un factor clave para realizar una eficaz implementación, y es tal vez uno de los aspectos que fuera más debatido en todo el proceso de creación de la norma.

A fin de establecer con precisión el alcance, la organización debe estudiar con profundidad cuáles son las fronteras del SGC. La importancia de este punto radica en que cada especialidad que compone el abanico de lo que puede llamarse "compliance" abriría la complejidad de manera significativa. No olvidemos que, entre muchas otras cuestiones la organización deberá identificar las obligaciones de compliance (legislación y normas internas),

El alcance del SGC pretende dejar "blanco sobre negro" los principales riesgos de compliance a los que se enfrenta la organización y los límites (geográficos, temáticos, organizativos, o todos, sobre los cuales se aplicará el SGC, especialmente si la organización forma parte de una entidad mayor, ya sea parte de un grupo, sucursal o formato similar).

Para determinar el alcance existe información fundamental a tener en consideración:

- ▶ El contexto interno y externo según se describió más arriba
- ▶ El análisis de partes interesadas, los procesos internos y las obligaciones de compliance



IMPORTANTE:

El alcance es uno de los elementos que **debe estar necesariamente documentado**.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Al definir el Alcance, se debe tener en cuenta también dónde se está implementando el SGC, y si es parte de un grupo, es controlante o controlada. Respecto del control, se debe tener en cuenta si la toma de decisiones sobre el SGC es centralizada (Ej.: desde Casa Matriz) o es descentralizado (Ej.: desde cada Subsidiaria, o posición intermedia, desde centros de responsabilidad o "hubs"). El SGC debería basarse en los principios de buen gobierno, proporcionalidad, integridad, transparencia, responsabilidad y sostenibilidad.

2.4 Sistema de Gestión de Compliance (SGC)



Puntos donde centrar la atención:

La organización debe establecer, implementar, mantener y mejorar continuamente su SGC, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos estipulados en la 37301. Pero ¿A qué se refiere la Norma con un SGC? Se trata de un marco que integra estructuras, políticas, procesos y procedimientos esenciales para lograr los resultados deseados en la materia que nos convoca (compliance), y actuar para prevenir, detectar y dar respuesta ante incumplimientos.

El SGC requiere de una determinada "infraestructura" para su eficaz desempeño. Es decir, debe estar construido en torno a los valores, objetivos, estrategia y riesgos de compliance de la organización, teniendo en cuenta el contexto interno y externo que se han determinado.

Pero esto no basta para darle completitud. Requiere además de mantenerlo y mejorarlo continuamente, lo cual constituye todo un desafío.

Existen dos tipos de elementos que se diseñan para la adecuada operación de un SGC: a) para apoyar los comportamientos deseados (a estos solemos llamar "aspectos de ética positiva"), y b) para evitar los comportamientos indeseables (los cuales llamamos "aspectos de ética negativa"). Los primeros tienen sus raíces en la cultura oriental y los segundos más arraigados a las costumbres occidentales. Las pautas de comportamiento más usuales de ver hoy en día son de "ética y conducta", utilizando un poco de cada una.

Y todo el andamiaje de elementos organizados requiere de un adecuado monitoreo en materia de compliance que sea capaz de brindar alertas tempranas en caso de que se produzcan incumplimientos.

El SGC deberá reconocer que los errores ocurren y tendrá procesos para garantizar que haya una reacción adecuada que incluya la corrección de los procesos, los sistemas y las partes afectadas.

El SGC estará íntimamente relacionado con los principios de buen gobierno, proporcionalidad, integridad, transparencia, responsabilidad y sostenibilidad.



IMPORTANTE:

Aunque no lo dice el cuerpo principal de la norma, el Anexo recomienda enfáticamente que el SGC esté **necesariamente documentado**. Se refiere a información documentada (y no a un documento), para aportar evidencias en la realización de auditorías y para asegurarnos del correcto desarrollo de dichos procesos



CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Este requisito lo podemos cumplir a través de un “Mapa de Procesos”. Resulta importante además definir adecuadamente las entradas y salidas, la definición de los “responsables de procesos”, la identificación de los riesgos y oportunidades para cada proceso, así como la asignación de los recursos necesarios para cada uno de ellos.

Si la Organización tiene por ejemplo un diagrama de procesos como lo suele pedir ISO 9001, recomendamos basarse en ese, y de lo contrario, confeccionarlo. Sin embargo, en ambas alternativas, la organización deberá buscar identificar y destacar aquellos procesos que son relevantes para compliance, para los bloques de información o temas elegidos. Ej.: para la disciplina de compliance “antilavado de dinero” el procedimiento de “reporte de operaciones sospechosas” y el de “conozca su cliente” deberían ser considerados esenciales, y por ende recomendamos que se hallen documentados.

2.5 Obligaciones de Compliance



Puntos donde centrar la atención:

La organización debe identificar sistemáticamente sus obligaciones de compliance resultantes de sus actividades, productos y servicios, y evaluar su impacto en sus operaciones. Recordemos que “obligaciones de compliance” se conforman con la sumatoria de:

- ▶ **Requisitos obligatorios de compliance:** todo aquello que la organización debe cumplir obligatoriamente por la actividad que desarrolla, los lugares geográficos donde realiza sus actividades y las imposiciones que los entes que regulan su actividad disponen.
- ▶ **Requisitos voluntarios de compliance (Compromisos):** esto se refiere a todo aquello que la organización desea que forme parte de la forma de comportarse de su gente y que no es obligatorio.

De acuerdo con la definición arriba expuesta, requisitos y compromisos, conformando “obligaciones de compliance” son igualmente importantes.

La organización debe contar con procesos y rutinas para:

- a) identificar las obligaciones de compliance nuevas y modificadas para garantizar el cumplimiento continuo;
- b) evaluar el impacto de los cambios identificados y aplicar los cambios necesarios en la gestión de las obligaciones de compliance.

Son ejemplos de “requisitos obligatorios” los siguientes: leyes, regulaciones, reglamentos; permisos, licencias u otras formas de autorización; normas, circulares u orientaciones emitidas por los organismos reguladores; las sentencias de los juzgados y tribunales administrativos; los tratados, convenios y protocolos; entre otros.

Son ejemplos de “requisitos voluntarios” que una organización decide cumplir: acuerdos con grupos comunitarios u organizaciones no gubernamentales; acuerdos con las autoridades públicas y los clientes; un código de comportamiento, las políticas y los procedimientos; compromisos medioambientales; contratos; entre otros.

La organización debe identificar “sistemáticamente” las obligaciones de compliance por departamentos, funciones y diferentes tipos de actividades organizativas para determinar a quiénes afectan estas obligaciones de compliance.



IMPORTANTE:

Las obligaciones de compliance deben conformar un registro que **debe estar necesariamente documentado.**

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Resulta importante que la Alta Dirección haga comprender a los colaboradores que los requisitos obligatorios no están por sobre los voluntarios. Que ambos se hallan en un tono de igualdad y que deben ser cumplidos. Un mensaje de "no tolerancia ante el incumplimiento" a sabiendas, suele ayudar mucho en una implementación de este tipo. La "no tolerancia" se manifiesta a través de la aplicación de una política de sanciones. Sin perjuicio de ello, la norma nada dispone al respecto.

Otro punto de alta relevancia es que la norma pide Identificar "sistemáticamente" las obligaciones de compliance. Y "sistemáticamente" no es lo mismo que hacerlo "periódicamente". La sistematización supone procesos coordinados que persiguen la captura de nuevas obligaciones toda vez que surgen. Respecto de los requisitos es relativamente más sencillo, porque son lanzados por la propia organización. Sin embargo, el seguimiento de requisitos merece una especial coordinación entre todas las áreas de responsabilidad donde el alcance definido lo merezca.

2.6 Evaluación de Riesgos de Compliance



Puntos donde centrar la atención:

En este apartado la norma, basándose siempre en ISO 31000 (Risk Management Systems) pide a la organización que identifique, analice y valore sus riesgos de compliance.

La organización debe identificar los riesgos de compliance y para ello se espera que relacione sus obligaciones de compliance (compromisos y requisitos) con sus actividades, productos, servicios y aspectos relevantes de sus operaciones. La anterior definición del contexto y de las partes interesadas ayudará mucho en esta importante labor.

La organización debe evaluar los riesgos de compliance relacionados con los procesos subcontratados y de terceros.

Los riesgos de cumplimiento se evaluarán periódicamente y, además, toda vez que se produzcan cambios importantes en las circunstancias o en el contexto organizativo.

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

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Teniendo en cuenta que un SGC tiene como "Columba vertebral" el análisis de riesgos, diremos que la Identificación de riesgos se vuelve una instancia crítica, ya que riesgo no identificado, en el peor de los casos emergerá al materializarse y nada habrá podido hacer la organización para mitigarlo.

Para llevar a cabo una buena gestión de estos riesgos de compliance, la norma 31010:2019 propone técnicas herramientas para una eficaz evaluación de riesgos.



A man in a white shirt is looking at a tablet in the foreground. In the background, a group of people is sitting around a table in a meeting, with a blue grid pattern overlaid on the image.

3. LIDERAZGO

3. Liderazgo

3.1 Liderazgo y compromiso

3.1.1 Órgano de gobierno y alta dirección



Puntos donde centrar la atención:

Tal como sucede con cualquier sistema de gestión, independientemente de su foco, la alta dirección tiene un rol fundamental para que el sistema se “viva” en todos los niveles de la organización. En esta norma, además, aparece un escalón aún más alto de la pirámide jerárquica: el órgano de gobierno.

El tan debatido concepto de “Tone from the top” adquiere aquí un protagonismo esencial como es de esperarse. Se identifican algunos aspectos claves que demuestren el involucramiento y compromiso tanto del órgano de gobierno como de la alta dirección, a saber:

- ▶ Existencia de políticas y objetivos compatibles con la estrategia
- ▶ Integración de los procesos de compliance a los procesos del negocio
- ▶ Provisión adecuada de recursos para un correcto funcionamiento y desempeño del SGC
- ▶ Comunicación activa y frecuente de los aspectos más significativos del SGC
- ▶ Seguimiento para verificar que los resultados previstos se cumplen
- ▶ Dirección y apoyo al personal en todos los niveles
- ▶ Promover la mejora del SGC

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Si bien se podría entender que el involucramiento del órgano de gobierno y la alta dirección son intangibles, existen diversos aspectos a través de los cuales el compromiso de la Alta Dirección se puede percibir e incluso medir.

Para implementar estos aspectos de manera eficaz entonces, sugerimos se tomen en consideración algunas de las siguientes acciones:

- la redacción de una política de SGC, firmada tanto por el órgano de gobierno como por la alta dirección
- la existencia de otras políticas y procedimientos de compliance de alto nivel, en el que se evidencie el involucramiento del órgano de gobierno y la alta dirección (por ejemplo, firmando como “aprobadores” las políticas y/o los procedimientos).
- dejar registro a través de minutas de reunión del órgano de gobierno y la alta dirección de todas las veces que se reúnan y traten temas relativos, se tomen decisiones para el correcto funcionamiento (por ejemplo, proveyendo recursos necesarios) o bien se evalúe el desempeño del SGC.
- dejar registro de comunicaciones formales que se emitan en materia de compliance por el órgano de gobierno o la alta dirección (por ejemplo, correos electrónicos institucionales, folletos citando frases relativas a compliance que haya utilizado alguno de los miembros del comité, comunicaciones formales a clientes, proveedores u otras partes interesadas relevantes).
- dejar registro de eventos y/o charlas de inducción provistas por algún miembro del órgano de gobierno o la alta dirección a personal de la organización y otras partes interesadas.
- dejar registro de felicitaciones por sugerencias de mejora y por cumplimientos o sanciones por incumplimientos a políticas y/o procedimientos de la organización.
- registrar formalmente a través de una carta o descripción de puestos firmada, la asignación de un profesional a la Función de Compliance detallando, como mínimo, las responsabilidades establecidas en el apartado 3.3.2 siguiente.

- implementar un sistema formal de planteo de inquietudes, tal lo establecido en 8.3, donde quede en evidencia a través de un procedimiento, cómo será el funcionamiento del sistema, quienes son los responsables y cómo y con qué frecuencia se informará al órgano de gobierno y a la alta dirección acerca de los registros que se obtienen por los canales establecidos.

3.1.2 Cultura de Compliance



Puntos donde centrar la atención:

La cultura de una organización es un activo intangible fundamental en el correcto desarrollo de un SGC.

La cultura está presente en la definición de los valores principalmente, pero también puede encontrarse en las definiciones de misión y visión, así como en la construcción de la estrategia organizacional.

Los antecedentes y la reputación de la organización también son aristas de la cultura, tal como la forma de proceder y hacer negocios que baja desde el órgano de gobierno y la alta dirección.

Pero los antecedentes y las declaraciones de misión, visión, valores y estrategia no son la cultura. La cultura se vive cotidianamente en la organización, el compliance se "respira" en los pasillos, se evidencia en las acciones y las conductas en todos los niveles de la organización.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Tal como en el apartado anterior, la cultura puede ser difícil de medir, pero algunas acciones que pueden implementarse para promover una cultura de compliance adecuada son las siguientes:

- definición clara de los valores y la comunicación efectiva de diversas maneras a toda la organización y partes interesadas pertinentes
- planes de mentoría para roles en formación, dejando registro del progreso.
- predicando con el ejemplo desde el órgano de gobierno, la alta dirección y la gerencia, a la hora de establecer bonos, reconocimientos, gratificaciones, sanciones y/o penalidades independientemente de la función que ocupe el / los involucrado/s.
- procesos transparentes de contratación de personal y promociones internas, con registros / evidencias de debida diligencia para empleados con cargos claves dentro del sistema de gestión.
- programas de inducción y planes de capacitación documentados para garantizar un grado de conciencia consistente con el sistema de gestión, adecuado a lo que se desea alcanzar como valores y objetivos organizacionales.
- comunicación transparente de casos de incumplimiento y no conformidades, para tomar como ejemplo y mejora, con evidencia de acciones tomadas para corregir los desvíos.
- valorización y jerarquización del rol de la Función de Compliance.
- motivación al personal para que registre las inquietudes a través de los canales establecidos.
- establecimiento y mejora de indicadores de desempeño de la cultura (midiendo varias de las acciones descritas arriba)
- recopilación de opiniones de partes interesadas acerca de su percepción de la cultura de compliance de la organización (por ejemplo, mediante encuestas anónimas a proveedores y clientes)

3.1.3 Gobernanza de Compliance



Puntos donde centrar la atención:

Algunos principios de buen gobierno corporativo son fundamentales para el correcto desarrollo y funcionamiento de un SGC. Garantizar la implementación de estos principios aumentará drásticamente la probabilidad de un desempeño eficaz de las funciones clave tanto como del SGC.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Los principios a observar e implementar son los siguientes:

- acceso directo de la Función de Compliance al órgano de gobierno. Es decir, que en el organigrama se detalle a la función de compliance como dependiente directo del órgano de gobierno o bien con una línea de trazos en caso de que su dependencia no sea directa. Por otro lado, en la práctica dar evidencia de que ese canal de comunicación existe, por ejemplo, a través de reuniones y/o informes directos periódicos.

- independencia de la función de compliance, es decir que sea prevista de recursos necesarios y libertad de acción tanto para apoyar y fomentar una cultura de compliance, como para dar seguimiento y control a temas específicos independientemente de la jerarquía de los roles, funciones o procesos a controlar. Se debe garantizar que no existan presiones infundadas a la función de compliance ni adulteración de la información y/o reportes emitidos por ésta.

- autoridad y competencia adecuadas, entendiendo que la función de compliance es de relevancia fundamental en este sistema y que no puede ser cubierta por cualquier persona que "quede cómoda" sino que debe ser una designación premeditada y estratégica. En caso se decida por una persona sin la competencia suficiente, se debe garantizar el desarrollo e implementación un plan de capacitación y mentoría adecuado para alcanzar los resultados deseados de esta función. Además, se la debe proveer de recursos necesarios y equipo de profesionales interno y/o externo suficiente para poder lidiar con todos los asuntos relativos a sus responsabilidades.

3.2 Política de compliance



Puntos donde centrar la atención:

Se debe desarrollar, emitir y aprobar por parte del órgano de gobierno y la alta dirección una política de compliance que oficiará de "acta constitutiva" del SGC.

La política debe ser un documento escrito y la norma establece claramente los aspectos a incluir en ella.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Leer atentamente los aspectos a incluir en la política y desarrollar una política documentada que contenga lo determinado en la norma.

Puesto que una de las premisas a cumplir por la política es que "proporcione un marco para establecer objetivos de la organización" se puede redactar la política como una serie de "viñetas" o "numerar" su contenido para que luego pueda vincularse un objetivo a cada uno de sus numerales o párrafos.

En la práctica, la política suele tener una extensión de 1 (una) página, aunque esto no constituye una regla general.

Se debe comunicar y estar disponible para partes interesadas relevantes por lo que es útil dejar evidencias de esa comunicación y también publicar, en los idiomas adecuados, y es muy recomendable exteriorizarla en el sitio web de la organización.



IMPORTANTE:

La política de compliance **debe estar necesariamente documentada.**

3.3 Funciones, responsabilidades y autoridades

3.3.1 Órgano de gobierno y alta dirección



Puntos donde centrar la atención:

Para un correcto funcionamiento del SGC deben definirse y comunicarse claramente las funciones y responsabilidades clave.

Por otro lado, la alta dirección debe informar al órgano de gobierno acerca del desempeño del SGC, a la vez que debe mantenerse obligada a rendir cuentas en caso no se alcancen los resultados previstos.

En la operación del sistema de gestión, la alta dirección debe asegurar una adecuada provisión de recursos y no debería, en consecuencia, excusarse en la falta de estos si no se alcanzan los objetivos planteados. Al respecto es importante destacar que en la mayoría de los países donde la responsabilidad penal de las personas jurídicas está más desarrollada, a la Justicia no le importa mucho la eficiencia de la función y actividades de compliance, sino su eficacia.

Adicionalmente, entre las acciones más importantes del ejercicio de autoridad de la alta dirección, en su rol ejecutivo dentro de la organización, se destacan la necesidad de establecer sistemas de reporte eficaces en todos los niveles, establecer mecanismos de autoridad incluyendo acciones disciplinarias y de asegurar que las evaluaciones de desempeño del personal incluyen aspectos relativos a compliance.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Aquí recomendamos la revisión del organigrama donde queden claramente identificadas las diferentes funciones claves del SGC, dentro de la estructura jerárquica de la organización.

Para cada una de las funciones determinadas en el organigrama, se deberá revisar los descriptivos de puestos para agregar un apartado donde se detallen los requerimientos relativos a competencias y responsabilidades de compliance.

Dentro de las responsabilidades de compliance en el descriptivo de puestos se puede establecer la necesidad de reportar ciertos resultados a ciertas partes interesadas; o bien establecer un "Procedimiento de Reportes" en el que se establezcan reportes por función, detallando contenidos mínimos y periodicidad.

En los procedimientos y formatos existentes de Recursos Humanos para evaluación de desempeño, se debe agregar la necesidad de evaluar el grado de cumplimiento de los aspectos de compliance establecidos en el descriptivo de puestos de cada función, incluyendo reportes de la alta dirección al órgano de gobierno.

Por último, el establecimiento de una política de bonos o beneficios adicionales para funciones claves del negocio, debería velar por la alineación de los resultados con conductas adecuadas de cumplimiento, sin exigir resultados inalcanzables que promuevan conductas indeseadas.

3.3.2 Función de Compliance



Puntos donde centrar la atención:

Al leer la norma, queda en evidencia que este rol dentro del SGC es el más protagónico, dadas las responsabilidades asignadas.

No se debe mal interpretar como que la función de compliance debe ser cubierta por una única persona, sino que podrían dividirse las responsabilidades en diferentes responsables mediante una "superestructura de compliance" con un máximo responsable a cargo, teniendo incluso la posibilidad de tercerizar en externos, parte de esta función.

En línea con la tercerización de algunas responsabilidades, es importante tener en cuenta que esta norma plantea sistemas de gestión de compliance de carácter amplio, debiendo cada organización definir el alcance como ya vimos en el apartado 2.3. Es por este motivo, que se hace importante también que la función de compliance reciba asesoramiento necesario de expertos sobre las leyes, reglamentos, códigos, normas aplicables y buenas prácticas en la materia.

La Función de Compliance tiene como rol principal velar por el adecuado funcionamiento del SGC, responsabilizándose de impulsar operativamente el SGC, mediante las actividades específicas detalladas por la norma, entre las que se destacan las siguientes:

- ▶ facilitar la identificación de las obligaciones de compliance y documentar la evaluación del riesgo de compliance según 2.5 (Obligaciones de Compliance) y 2.6 (Gestión de Riesgos de Compliance) respectivamente;
- ▶ monitorear los resultados del sistema para verificar cumplimiento de objetivos, estableciendo indicadores de desempeño;
- ▶ evaluar el desempeño para identificar la necesidad de implementar acciones correctivas;
- ▶ establecer un sistema de información y garantizar que el SGC se revisa según 7.2 (Auditoría Interna) y 7.3 (Revisión por la Dirección);
- ▶ establecer un sistema para planteo de inquietudes y garantizar que todo el personal recibe la formación pertinente en este y otros temas;

Es importante tener presente que las obligaciones específicas de la función de compliance no exigen al resto del personal de sus responsabilidades en materia de compliance.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para la asignación de las responsabilidades pertinentes a la función de compliance, es importante tener en cuenta:

- el alcance del SGC definido en 2.3, las obligaciones de compliance definidas en 2.5 y los riesgos definidos en 2.6
- la estructura que se le dará a la función, es decir, si se delegarán todas las responsabilidades en una única persona o se constituirá un comité de compliance
- si se tercerizarán algunas de las responsabilidades establecidas

Una vez definido esto, se debería formalizar en un documento (como ser el o los perfiles de puesto firmados incorporando las responsabilidades determinadas por la norma) la asignación de esta función a una o varias personas internas o externas de la organización.



IMPORTANTE:

alinear el alcance y los aspectos de compliance a incluir en el SGC junto con la designación de esta función a uno o varios responsables de la organización, **es un aspecto fundamental en la planificación y construcción del sistema.**

3.3.3 Dirección



Puntos donde centrar la atención:

Si consideramos que compliance "es tarea de todos" no es extraño encontrar en esta norma, un apartado dedicado también a la dirección o gerencia y al personal. Lo común en otras normas ISO es que exijan compromisos y obligaciones únicamente de la alta dirección. Aquí ya vimos que llega aún más alto, exigiendo involucramiento y compromiso del órgano de gobierno (como también sucede en la ISO 37001 de Sistemas de Gestión Antisoborno) pero también más abajo, exigiendo compromiso e imponiendo obligaciones tanto a la dirección o gerencia como al resto de los empleados.

Cada director o gerente debe ser responsable en su área de influencia, de que el SGC alcance los resultados previstos. Esto implica que deben ser conscientes y conocer cada una de sus obligaciones de compliance así también como los riesgos a los que están expuestos tanto personalmente como los equipos que tenga a su cargo.

Es decir que la norma nos insta a demostrar liderazgo y cumplimiento en todos los niveles de la organización.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Revisar los procedimientos de negocios en cada área, identificando riesgos y obligaciones de cumplimiento para establecer puntos de control sobre los cuales debería quedar un registro cada vez que se ejecute una tarea, como evidencia de cumplimiento del control y por ende cumplimiento de la obligación.

Dejar evidencias de comunicaciones (por ejemplo, con minutas de reunión, sesiones de concientización y/o capacitación) de directores a sus equipos de trabajo en los que se traten obligaciones y/o riesgos de compliance, así como el uso de los canales para planteo de inquietudes.

Involucrar a los directores de cada área alcanzada por el SGC, en el registro (no conformidades) y resolución de desvíos, incidentes, dudas y/o mejoras planteadas (acciones correctivas).

3.3.4 Personal



Puntos donde centrar la atención:

Como mencionamos en el apartado precedente, el personal no está exento de sumar su aporte a compliance.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Demostrar que el personal conoce los riesgos y las obligaciones de compliance y por lo tanto conoce los procedimientos y políticas que forman parte de su labor cotidiana para controlar cumplimiento y mitigación de riesgos, dejando registro de charlas de concientización o sesiones de capacitación.

Además, resulta muy importante dejar registro de sesiones de concientización y/o capacitación en el uso de las herramientas y políticas del SGC (consecuencias de incumplimiento, no conformidades, canales para registro de inquietudes, acciones correctivas, análisis y gestión de riesgos, identificación de obligaciones de compliance, auditoría interna, etc.).





4. PLANIFICACIÓN

4. Planificación

4.1 Acciones para tratar riesgos y oportunidades



Puntos donde centrar la atención:

Para planificar el SGC, la organización debe tener en cuenta el análisis que efectuó del contexto interno y externo, de las partes interesadas y de las obligaciones de compliance. Entonces deberá garantizar lo siguiente, respecto del mismo:

- ▶ Que pueda alcanzar los resultados previstos;
- ▶ Que logre prevenir o reducir los efectos no deseados;
- ▶ Que consiga la mejora continua.

¿Qué debe tener en cuenta al planificar el SGC la organización? Básicamente:

- ▶ los objetivos de compliance según lo mencionado al tratar el punto siguiente (4.2.).
- ▶ las obligaciones de compliance identificadas
- ▶ los resultados de la evaluación del riesgo de compliance según se explicó arriba también

¿Y qué debe planificar la organización? Se trata de:

- a) acciones para abordar estos riesgos y oportunidades (que principalmente se trata de controles, aunque pueden ser planes de tratamiento u otras acciones);
- b) definir cómo integrar y aplicar las acciones en los procesos de su SGC;
- c) evaluar la eficacia de estas acciones.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

El propósito de la planificación es anticiparse a los posibles escenarios y consecuencias; por lo tanto, es una actividad preventiva. Necesariamente este ejercicio debe basarse en los resultados de la evaluación de riesgos de compliance. Y en esencia se trata de que la organización planifique cómo hacer frente a los efectos no deseados antes de que se produzcan y cómo beneficiarse de las condiciones o circunstancias favorables que puedan derivarse del SGC.

Es necesario incorporar la gestión de compliance en las actividades y procesos de la organización. Para hacerlo, recomendamos acciones tales como: la fijación de objetivos, el control operativo u otras cláusulas específicas (por ejemplo, disposiciones sobre recursos, competencia). También deben planificarse las medidas para evaluar la eficacia del SGC. Esto suele incluir el monitoreo, las técnicas de medición, la auditoría interna o la revisión por parte de la dirección.

4.2 Objetivos de compliance y planificación para lograrlos



Puntos donde centrar la atención:

La organización debe establecer objetivos de compliance en las funciones y niveles pertinentes. Nos referimos a planteos de metas o propósitos a alcanzar. Los objetivos de compliance deberán tener determinadas características que describimos a continuación:

- a) ser consistentes con la política de compliance;
- b) ser medibles (siempre que fuera posible) y en su caso en qué período de tiempo (en general anual); Al respecto Lord Kelvin bien afirmó: *"Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre"*.
- c) ser monitoreados a fin de identificar desvíos; esto es a intervalos definidos, pero también toda vez que se exceda de límites de tolerancia o umbrales;

- d) ser comunicados a los niveles que corresponda; incluyendo revisiones por la dirección, auditoría interna y auditoría de certificación.
- e) estar actualizados toda vez que lo merezcan, a fin de que su definición no se degrade por cambios en el contexto o en los procesos.

Al planificar cómo alcanzar los objetivos de compliance, la organización debe determinar:

- ▶ qué se hará específicamente;
- ▶ qué recursos se necesitarán;
- ▶ quién será responsable;
- ▶ cuando se completará;
- ▶ cómo se evaluarán los resultados.



IMPORTANTE:
Los objetivos de compliance y los detalles de responsabilidad frente a los mismos deben formar parte de la **documentación** disponible.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

En general se debería tender a que los responsables de procesos (también llamados “process owners”) sean quienes mantengan la responsabilidad por estos objetivos, independientemente de quiénes colaboren en su producción. Se debe tener en cuenta que los objetivos pueden referirse a diferentes disciplinas o “bloques de conocimiento de compliance” (como anticorrupción, antilavado, medio ambiente, de reporte financiero, etc.). Pueden además referirse a toda la organización, o específicos de un proyecto, producto, servicio o proceso

Sin perjuicio de ellos el entorno tecnológico actual supone la utilización de tecnologías analíticas que puedan mejorar la capacidad de generación de información confiable y de sencilla lectura para un eficaz monitoreo por parte de la organización.

4.3 Planificación de los cambios



Puntos donde centrar la atención:

El requisito Planificación de los cambios, que aparece con alta relevancia en la ISO 9001:2015, ya existía en la versión 2008, pero disgregado a lo largo de la norma. Ahora, está destacado en un requisito específico y, por lo tanto, ha ganado más importancia en los sistemas de gestión. La norma ISO 37301 toma este requerimiento en el mismo sentido.

Cuando la organización determine la necesidad de realizar cambios en el SGC, los cambios se llevarán a cabo de forma planificada, lo que supone la utilización del enfoque PDCA (Planificar, Hacer, Verificar, Actuar). Y cada cambio que pueda impactar sobre los objetivos de compliance merecerá un abordaje particular.

La planificación de los cambios es un punto que puede tener cierta complejidad de comprensión para quienes no vienen del mundo de los sistemas de gestión normados. Cuando usted trata una No Conformidad “NC”, por ejemplo, seguramente analice las causas, traza planes de acción, define responsables y monitorea los resultados de ese trabajo. Al hacer esto, está analizando críticamente el SGC y cambiando lo que se necesita. Todas estas rutinas (análisis de causas, planificación, ejecución y monitoreo) son la “planificación de cambios de su organización” al que se refiere la norma.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

La sumatoria de cambios planeados suponen la utilización de alguna herramienta de gestión de proyecto mediante el cual no solo se puedan abordar cada uno de los cambios que lo merezcan, sino, además, mantener actualizado el porfolio de proyectos que engloban la mejora continua de sistema. A dichos fines el área de Compliance podría ser una eficaz oficina de gestión de proyectos (“PMO”), siempre que disponga los recursos, aunque sin asumir la responsabilidad por la adecuada concreción de los mismos en los casos en que sea responsabilidad de las diferentes áreas.



5. APOYO

5. Apoyo

5.1 Recursos



Puntos donde centrar la atención:

En este capítulo ingresamos en la etapa del ciclo de Deming de "hacer". Es decir que saliendo de los capítulos de planificación (2, 3, 4) debemos comenzar a implementar el SGC. En línea con este hecho, lo primero que debemos incorporar son los recursos necesarios para que el sistema funcione.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Se deberá contar ahora con los recursos planificados en capítulos anteriores, tal lo que se le ha exigido al órgano de gobierno y a la alta dirección: garantizar provisión de recursos suficientes.

Estos recursos pueden ser (independientemente de los recursos humanos que serán abordados en 5.2 y 5.3 específicamente), pero sin limitarse a: infraestructura de TI, apoyo de consultores externos, proveedores específicos (asesores técnicos, canales de denuncia o línea ética, software para debida diligencia, bases de datos, fuentes de información, etc.), equipos de computación, bibliografía de referencia, etc.

5.2 Competencia

5.2.1 Generalidades



Puntos donde centrar la atención:

El personal que esté alcanzado por el sistema de gestión debe ser competente para las tareas que le toca desarrollar en vínculo con compliance. Para garantizar competencias, se deberá analizar el "perfil ideal" de puestos construido según lo recomendado en 3.3.1 con el "perfil real" de cada empleado, para luego determinar las acciones de capacitación necesarias para cerrar la brecha existente como resultado de ese análisis.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Desarrollar perfiles de puesto completos según lo especificado ya en 3.3.1 y desarrollar un plan de capacitación específico por función (especialmente para aquellas funciones claves del sistema).

A medida que se va ejecutando el plan de capacitación, se debe guardar registro de las capacitaciones tomadas por cada empleado.

Notar que las capacitaciones pueden ser impartidas por personal interno o externo, a la vez que pueden usarse otras formas para aumentar competencias como ser: tutoría, mentorías, coaching, capacitaciones en puesto de trabajo, etc.



IMPORTANTE:

Los **registros** que den evidencias de las **competencias se deben conservar como información documentada** que dé evidencia objetiva de cumplimiento de este requisito.

5.2.2 Proceso de Contratación



Puntos donde centrar la atención:

Si quisiéramos, como organización, jactarnos de ser “transparentes” debemos tener en cuenta que los procesos de contratación de personal deben de hecho, ser transparentes.

Por este motivo, la norma nos invita a estructurar específicamente el proceso de contratación y promociones internas para garantizar que la selección está libre de conflictos de intereses.

Dependiendo del grado de exposición a los riesgos identificados para una determinada función, se deberá llevar a cabo un proceso de debida diligencia sobre el personal.

Por último, debemos tener en cuenta la necesidad de revisar los objetivos de desempeño, las bonificaciones por desempeño y otros incentivos, para verificar que existen medidas adecuadas para evitar que se fomente el incumplimiento.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Desarrollar un procedimiento de contratación, traslado y/o promoción de personal, donde se detallen los pasos a llevar a cabo en cada caso, así como los controles a implementar incluyendo procesos de debida diligencia si correspondiera.

Especificar en ese procedimiento, la necesidad de entregar una copia de la política de compliance (y otros documentos importantes) que el nuevo empleado debe leer y firmar que la ha recibido y comprendido. En ese mismo acto de entrega y firma, recomendamos que firme que también que ha leído y comprende las políticas, procedimientos y obligaciones de compliance acorde al alcance de sus funciones / responsabilidades, así como las consecuencias y/o posibles sanciones en casos de incumplimiento.

En otro procedimiento, se deberán especificar las condiciones a través de las cuales se planifican, evalúan resultados y otorgan pagos de bonos por desempeño y otros incentivos para evitar que promuevan comportamientos de incumplimiento.

5.2.3 Formación



Puntos donde centrar la atención:

Más allá de la generalidad planteada en 5.2.1 precedente, refuerza aquí la norma la necesidad de proveer formación específica al personal implicado en el sistema. Menciona que la formación debe ser impartida de manera regular desde el inicio de la contratación y luego a intervalos planificados según la organización determine.

Tiene sentido este hecho, si consideramos que el contexto es cambiante y consecuentemente se actualizan obligaciones de compliance, riesgos, herramientas de gestión, controles, procesos, procedimientos, políticas, sistemas informáticos, requisitos de partes interesadas, etc.

Claro está que para ciertas funciones claves dentro del sistema, esta formación deberá ser especialmente planificada, supervisada y revisada para garantizar que ha sido eficaz.

Por otro lado, en caso existan terceros que actúen en nombre de nuestra organización, debemos también tenerlos en cuenta en los planes de formación periódicos para evitar incumplimientos por parte de ellos que puedan afectar a la organización.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Tal lo recomendado en 5.2.1, se debe garantizar que se proveen las capacitaciones para garantizar que el personal es competente, entendiendo que es competente aquel que tiene la capacidad de aplicar los conocimientos y las habilidades para lograr los resultados previstos.

Sugerimos construir un plan de capacitación e ir guardando registro a medida que se imparten las capacitaciones.



IMPORTANTE:

Los **registros** que den evidencias de las **competencias se deben conservar como información documentada** que dé evidencia objetiva de cumplimiento de este requisito.

5.3 Concientización



Puntos donde centrar la atención:

Más allá de las competencias adquiridas atendiendo lo planteado en el apartado 5.2 precedente, es importante que el personal alcanzado por el sistema de gestión sea consciente de diversos aspectos constitutivos de compliance, como ser: la política, obligaciones, riesgos, consecuencias de incumplimiento para la organización.

Construir cultura mediante procesos adecuados de concientización, contribuirá a la mejora del sistema por cumplimiento por voluntad propia en lugar de por aplicación de sanciones (que ya se sabe que no es tan eficaz en el largo plazo).

Las metodologías propuestas por expertos en "gestión del cambio" ("change management") suelen ser muy efectivas para este tipo de desafíos relacionados con la cultura.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

El proceso de brindar conciencia a los empleados y terceros actuando dentro del sistema de gestión, puede reducirse a sesiones de concientización o charlas planificadas (presenciales o remotas).

Además, si se utilizaran metodologías adicionales y más modernas, se aumentan las probabilidades de conseguir que se entiendan e incorporen culturalmente los aspectos principales de compliance y una mejor percepción de los riesgos que trae aparejado su incumplimiento.

Existen numerosos métodos y herramientas que promueven la interacción sincrónica y asincrónica entre formadores y miembros de la organización, tanto en formatos presenciales, a distancia o híbridos. Técnicas de basadas en "aprender haciendo", de gamificación e inteligencia lúdica pueden ser muy efectivas a la hora de lograr cambios de mirada respecto de determinadas situaciones relevantes para la organización. Otras formas de lograr concientización pueden basarse en el desarrollo de folletos digitales interactivos, infografías, videos, y un sinnúmero de alternativas solo limitadas por la creatividad de los expertos y proveedores de soluciones existentes en el mercado.

Tomar como base los valores y propósito de la organización suele ser una forma muy eficaz para arraigar comportamientos positivos que faciliten luego el mejor cumplimiento de políticas, normas y procedimientos de compliance.

5.4 Comunicación



Puntos donde centrar la atención:

Una comunicación eficaz con partes interesadas (tanto internas como externas) es fundamental para garantizar que haya un entendimiento suficiente de los aspectos relevantes de compliance.

Para que sea eficaz la comunicación, se deben tener en cuenta aspectos que podrían contraponerse en caso de ser desatendidos, a saber: diversidad cultural, idiomas y opiniones de otras partes interesadas.

El contenido mínimo a comunicar debería incluir: la política y objetivos del sistema, la cultura, las obligaciones de compliance y los riesgos, políticas y procedimientos para internos y externos, canales para planteo de inquietudes, resultados de auditorías y/o revisiones, resultados de medición de procesos e indicadores de desempeño.

A la hora de definir a quiénes comunicar, se pueden tomar como ejemplos las siguientes partes interesadas: organismos reguladores, clientes, contratistas, proveedores, inversores, servicios de emergencia, organizaciones no gubernamentales y vecinos.

Por último, al definir los métodos de comunicación, se puede tomar como ejemplos los siguientes: sitios web y correos electrónicos, comunicados de prensa, anuncios y boletines periódicos, informes anuales, debates informales, jornadas de puertas abiertas, grupos de discusión, diálogo con la comunidad, participación en eventos comunitarios y líneas telefónicas de ayuda.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para dar soporte al área de comunicaciones de la organización, se puede desarrollar en este caso una matriz de comunicación que plantee en columnas la siguiente información: tema, cuando, a quién, cómo (a través de que medios), quién.

Luego en filas se van desarrollando los temas a comunicar y se completan las columnas indicadas en el párrafo precedente.

Esto será una buena base para estandarizar los temas a comunicar, definiendo claramente las responsabilidades y a quienes va dirigido cada tema.



IMPORTANTE:

Los registros que den evidencias de las comunicaciones realizadas se deben conservar como información documentada que dé evidencia objetiva de cumplimiento de este requisito.

5.5 Información documentada

5.5.1 Generalidades



Puntos donde centrar la atención:

Si contamos las veces que la norma nos exige la emisión de un documento escrito (información documentada), omitiendo aquellas veces que menciona "información documentada" como evidencia de cumplimiento (registros), encontramos: alcance (2.3), obligaciones de compliance (2.5), evaluación de riesgos (2.6), política (3.2), objetivos (4.2).

Claro está que con esos 6 documentos únicamente, un SGC no podrá operar de manera eficaz. Es por tal motivo, que la norma nos invita a desarrollar tantos documentos (adicionales a los exigidos) como la organización necesite para operar para la eficacia del SGC.

Estos documentos pueden ser: políticas, procedimientos, asignación de funciones, asignación de responsabilidades, formularios, planes, programas, etc.

Dependiendo del tamaño de la organización, la competencia del personal y la complejidad de sus procesos será tanto más extensa la estructura documental del sistema de cada organización.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Se deberán crear entonces, tantos documentos (políticas, procedimientos, matrices, manuales, planes, códigos, etc.) como sea necesario para un correcto funcionamiento del SGC.

Como premisa, se puede considerar los siguientes motivos para determinar la necesidad de desarrollar un documento: lo exige la norma ISO 37301, lo exige una regulación, lo exige una parte interesada, es un compromiso u obligación de compliance, es necesario para garantizar un control interno, es necesario para que el resultado de un proceso sea idéntico independientemente de quién lo opere.

5.5.2 Creación y actualización de la información documentada



Puntos donde centrar la atención:

Una vez definida la estructura documental necesaria para la correcta operación del SGC, debemos tener en cuenta que dichos documentos y su distribución deben cumplir con ciertos requisitos vinculados tanto a forma como a la manera de gestionarlos. Es evidente que, **si un documento específico y necesario para operar un proceso en una determinada área, no se encuentra disponible para el personal que lo necesita, lo más probable es que no se cumplan los pasos allí establecidos**. Por tal motivo, se debe establecer una metodología para garantizar que la información documentada está disponible en cada lugar de uso; es decir, que sea accesible a todo el personal alcanzado en cada caso, independientemente de su formato (físico, digital, etc.).

Además, para garantizar que ciertos requerimientos de forma se establezcan con el objetivo de identificar unívocamente cada documento, debemos tener en cuenta algunos de los siguientes elementos mínimos en cada uno que construyamos: identificación, descripción, título, fecha, autor o código de referencia, revisión, aprobación.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Los documentos de los sistemas de gestión normalmente respetan formatos establecidos, agregando los elementos descriptos en el párrafo precedente (usualmente en encabezado y pie de página).

Por otro lado, para garantizar que están disponibles en cada puesto de trabajo o para cada responsable de implementarlos o usarlos, suelen compartirse en redes locales o en la nube, de modo que, con un nombre de usuario y contraseña, cada colaborador tiene acceso a los documentos que necesita.

5.5.3 Control de la información documentada



Puntos donde centrar la atención:

Luego de definir la documentación necesaria y la manera en que se crea y actualiza, tal como vimos en los dos apartados precedentes, **debemos garantizar que la estructura documental de la organización se controla de manera adecuada**.

Algunos de los aspectos a tener en cuenta a la hora de controlar la documentación son: garantizar disponibilidad según necesidad; velar por la confidencialidad de la información; evitar pérdida de integridad de la información; evitar usos inadecuados; garantizar una adecuada distribución, acceso, uso y recuperación; garantizar un adecuado almacenamiento, preservación y legibilidad; controlar los cambios que se realicen; disponerlos adecuadamente en caso ya no sean necesarios.

Por último, la norma nos insta a identificar también la información de origen externo (es decir, documentos que no son creados por la organización) que pueda ser necesaria para el correcto funcionamiento del SGC. Entre otros documentos, podemos identificar los siguientes: reglamentos, regulaciones, leyes, decretos, políticas corporativas y reglas o buenas prácticas a los que la organización adhiera.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para garantizar que el acceso sea adecuado, se deberían establecer diferentes tipos de acceso o perfiles, a las redes o nubes en los que se comparte la información. Lo más usual es compartir documentos por área o departamento a la vez que se limita la acción posible sobre los mismos, según la jerarquía del usuario (por ej.: acceso de solo lectura, acceso para edición o modificación, acceso para borrado individual, acceso irrestricto para borrar de manera masiva, etc.).

Además, para conocer en detalle cuál es la estructura documental, recomendamos construir un listado o matriz de documentos en los que se detalla la siguiente información de cada documento: nombre, código, fecha y/o número de revisión, para quién debe estar disponible, ruta en servidor para llegar a él, etc. Por último, de manera similar al párrafo precedente, se puede construir un listado o matriz de documentos "de origen externo" para todos los documentos que quedan fuera de nuestro alcance, pero son necesarios para operar el sistema de gestión en cumplimiento con los requisitos y obligaciones establecidos y/o identificados.



6. OPERACIÓN

6. Operación

6.1 Planificación y control operacional



Puntos donde centrar la atención:

Al igual que otros sistemas de gestión normalizados, la organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos, y para implementar las acciones determinadas en la cláusula referida a planificación. Para ello deberá:

- ▶ establecer criterios para los procesos de forma tal de poder establecer si lo entregado estará conforme con los requisitos;
- ▶ implementar controles de los procesos de acuerdo con esos criterios.

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

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios involuntarios, tomando medidas para mitigar cualquier efecto adverso, según sea necesario.

Cuando los controles operativos fallan, será necesario tomar medidas para hacer frente a los resultados o efectos no deseados.

Si se recurre a terceros o a procesos subcontratados en las actividades de la organización, ésta debe llevar a cabo una debida diligencia efectiva para garantizar que sus normas y su compromiso con el cumplimiento no se vean erosionados. La organización debe asegurarse de que se celebren acuerdos de nivel de servicio (SLA) adecuados que especifiquen las obligaciones de compliance para el proveedor de servicios.

Además, debe asegurarse de que los procesos, productos o servicios suministrados externamente, que sean relevantes para el SGC, sean controlados y supervisados, ya que la tercerización de las operaciones no exime a la organización contratante de sus responsabilidades legales ni de sus obligaciones de compliance.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Un SGC bien diseñado comprende medidas (por ejemplo, políticas, procesos, procedimientos) que dan contenido y efecto a una cultura de compliance. Se ocupan de los riesgos identificados y tienen como objetivo reducirlos.

Resulta importante comprender que los controles son consecuencia de los riesgos identificados. Si la identificación de riesgos arriba descrita no resulta amplia y participativa, es más que probable que el set de controles implementado no sea el más adecuado para gestionar el SGC.

Respecto de los terceros, es frecuente, mientras más clientes relevantes posean, que dispongan las medidas para demostrar la adecuación de sus controles y mecanismos de supervisión. La certificación de su SGC bajo esta norma podría ser una eficaz herramienta.

Si bien la ISO 37001 nada mencionaba, la presente norma explica que un código de conducta que establezca, entre otras cosas, el pleno compromiso de la organización con las obligaciones de compliance pertinentes constituye un elemento básico del control operativo. Un código de conducta debe ser aplicable a todo el personal y ser accesible de manera rápida y sencilla. Basadas en el código de conducta, las medidas de compliance deben incorporarse a las operaciones cotidianas de la organización para fomentar una cultura de compliance

¿Qué elementos deberían considerarse al contratar un tercero?

- diligencia debida inicial y continua;
- aplicar los controles adecuados;
- realizar un monitoreo continuo;
- una revisión adecuada de los acuerdos legales/contractuales;
- consideración de los SLA;
- utilizando terceras partes certificadas en este documento.

6.2 Establecimiento de controles y procedimientos



Puntos donde centrar la atención:

Se pide que la organización implemente controles para gestionar sus obligaciones de compliance y los riesgos de compliance asociados. Básicamente se busca que estos controles prevengan, detecten y corrijan los incumplimientos.

Estos controles se mantendrán, se revisarán periódicamente en cuanto a la vigencia de su diseño, y se probarán para garantizar su eficacia continua.

Probar los controles significa llevar a cabo un ejercicio diseñado para comprender si el control hace lo que se pretendía en el momento de haber sido diseñado, si es posible eludirlo, o es realmente eficaz para reducir el impacto o la probabilidad del riesgo.

¿A qué controles se refiere la Norma? Los siguientes son ejemplos, entre muchos otros:

- ▶ Existencia de políticas, procedimientos e instrucciones de trabajo documentados, claros, prácticos y fáciles de seguir; con la identificación clara de las actividades de control. Al respecto resulta esencial integrar las obligaciones de compliance en los mismos, como así también dentro de los formularios utilizados, los sistemas de información, los contratos, entre otros.
- ▶ Informes de excepción;
- ▶ Aprobaciones; autorizaciones (se recomienda que exista un esquema documentado)
- ▶ Adecuada segregación de funciones incompatibles (no solo teóricas sino también dentro de los sistemas informáticos); Si esto no fuera viable por un tema de tamaño de la organización o elevados costos, se deberían implementar "controles compensatorios".
- ▶ Planes anuales de compliance;
- ▶ Autoevaluaciones y auditorías de compliance;
- ▶ El compromiso de la dirección con adecuadas evidencias, así como otras medidas para fomentar el comportamiento conforme con el Código de Ética / Conducta;
- ▶ Comunicación activa, abierta y frecuente sobre el comportamiento esperado de los empleados (normas y valores, códigos de conducta). Formación y, concientización sobre estos temas.



CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Es importante comprender en materia de compliance que un control jamás puede tener un costo mayor que el beneficio que produce. Por ello es importante que la organización pueda valerse de recursos internos o asesores externos que lo puedan asistir en materia de control interno.

para poder realizar un buen análisis del diseño y probar su efectividad, tener en cuenta que existen distintos tipos de controles (a nivel entidad, a nivel procesos | preventivos, detectivos | manuales, automáticos, semiautomáticos | automáticos inherentes, automáticos configurables | entre otros. Es importante clasificarlos en forma adecuada puesto que en muchas oportunidades los equipos de testeo de controles tienen diferente especialización.

Toda vez que existan muchas funciones de supervisión (Ej. auditorías de muchos sistemas de gestión normados, auditorías internas y de procesos, etc.), se debe procurar coherencia y eficiencia, integrando las mismas siempre que fuera posible; de esta forma se optimizará el esfuerzo de los colaboradores sin estresarlos).

Se recomienda que existan disposiciones específicas para identificar, notificar y elevar los casos de incumplimiento y los riesgos de incumplimiento.

6.3 Planteamiento de inquietudes



Puntos donde centrar la atención:

La organización debe establecer, implementar y mantener un proceso para fomentar y permitir reportar (de buena fe) intentos, sospechas o violaciones reales a las pautas de comportamiento definidas en la política de compliance o de las obligaciones de compliance en general (requisitos y compromisos).

Si bien la mayoría de los lectores de la norma consultados relacionan este punto en forma directa con el canal o línea de denuncias, y aunque este dispositivo es muy importante, la organización debería comunicar que existen otros canales preferibles para agotar si fuera esto posible (conversarlo con un superior o con el área de Compliance, por ejemplo)

El proceso para plantear inquietudes deberá:

- ▶ Estar claramente explicado, visible y de fácil accesibilidad en toda la organización;
- ▶ Tratar los reportes de forma confidencial;
- ▶ Permitir como alternativa el reporte anónimo; incluso cuando no sea exigido por la legislación de determinados países.
- ▶ Garantizar a los denunciantes (de buena fe) de cualquier tipo de represalias como producto de su denuncia;
- ▶ Permitir o propiciar que el personal reciba asesoramiento.

La organización debe ocuparse de que todo el personal conozca los procedimientos de reporte de inquietudes y sus derechos y protecciones.

Destacamos el lanzamiento de la norma ISO 37002, que se ocupa de este apartado específico ("Whistleblowing Management System").

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Muchas organizaciones plantean en forma directa el canal de denuncias para cumplir con este apartado. No sería este el espíritu de la ISO 37301, como tampoco lo fue el de su antecesora ISO 19600.

La organización tiene que generar confianza para que el canal de deporte sea utilizado toda vez que se requiera.

Respecto de la posibilidad de efectuar un reporte, el personal debería entender que no solo es un derecho denunciar el incumplimiento, sino que las buenas prácticas recomiendan plantearlo además como un deber.

La atención por parte de un tercero es una buena práctica utilizada por la mayor cantidad de organizaciones a nivel global.

6.4 Proceso de investigación



Puntos donde centrar la atención:

La organización debe desarrollar, establecer, aplicar y mantener procesos para valorar, evaluar, investigar y cerrar informes sobre casos de incumplimiento presuntos o reales. Estos procesos deben garantizar una toma de decisiones justa e imparcial. Es importante no solo que esto ocurra, sino que los colaboradores sean conscientes de ello porque influirá en su comportamiento.

Los procesos de investigación se deben llevar a cabo de forma independiente y sin conflicto de intereses por personal competente.

La organización debe utilizar el resultado de las investigaciones para mejorar el SGC, según corresponda (ver apartado de mejora continua).

La organización debe informar periódicamente sobre el número y los resultados de las investigaciones al órgano de gobierno o a la alta dirección.

Cualquier denuncia o sospecha de conducta indebida por parte de la organización, su personal o terceros pertinentes debería disparar acciones claras al respecto. Como respuesta a estos hechos o sospechas, la organización deberá mantener la documentación de la respuesta, incluidas las medidas disciplinarias y/o de corrección adoptadas, y las revisiones del sistema de gestión del cumplimiento teniendo en cuenta las lecciones aprendidas. No olvidemos que esto tiene ligación con posibles hechos que puedan tratarse en la justicia penal o administrativa (según cada país).



IMPORTANTE:
La organización debe mantener información documentada de las investigaciones.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

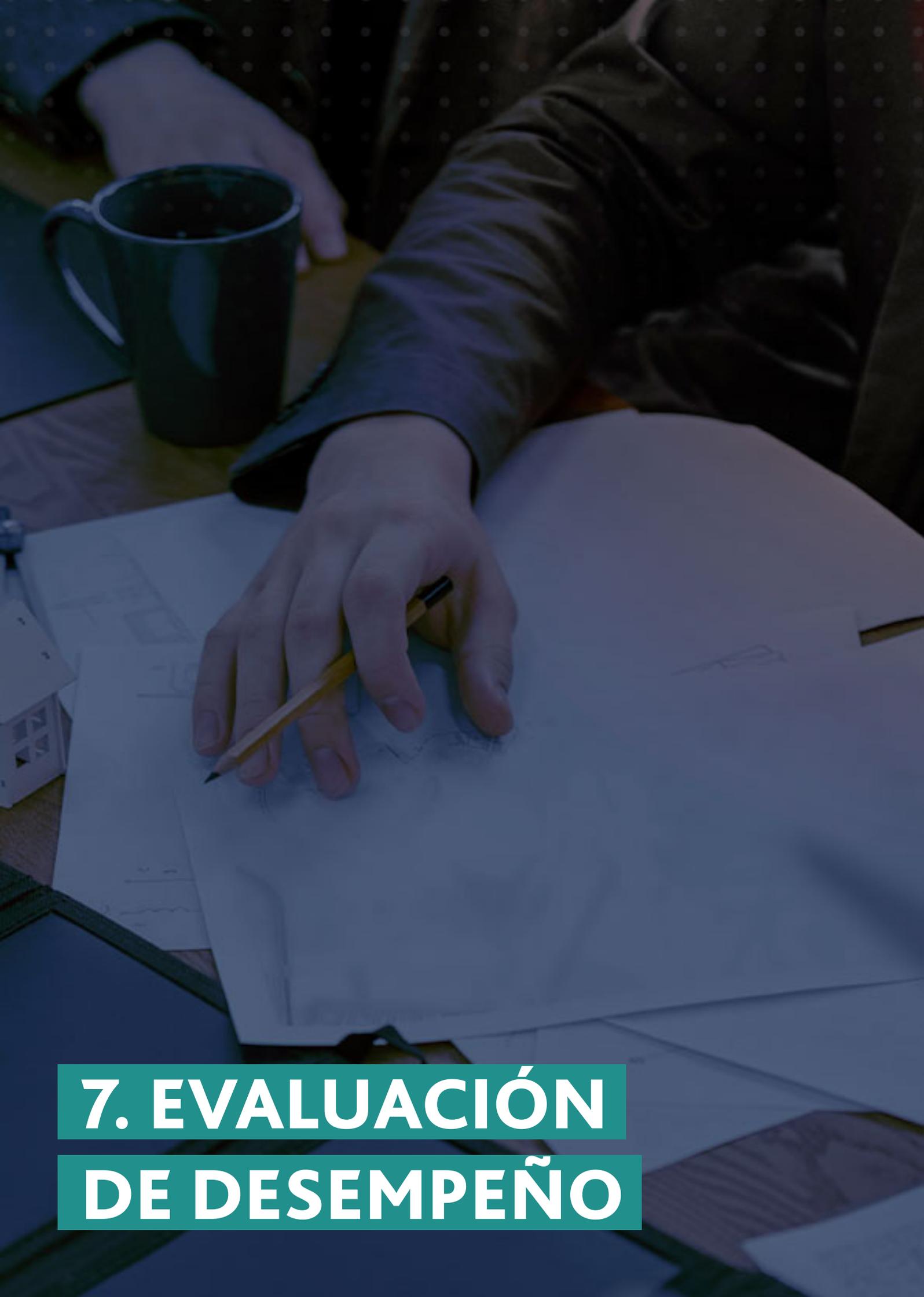
Muchas veces el establecimiento de procesos para investigar se denomina "protocolos" dado que contemplan un conjunto de pasos que deben cumplirse cuidadosamente, bajo riesgo de dañar la investigación o recibir una denuncia del personal y/o terceros investigados.

La investigación desarrollada por personal experto en la materia, y externo a la organización otorga en la mayoría de los casos más garantías de que se podrá llegar a los objetivos planteados en el objetivo de la investigación.

La creación de un comité independiente para supervisar la investigación y garantizar su exhaustividad e independencia es una práctica muy recomendable.

La organización debe establecer un mecanismo de información sobre las investigaciones, que incluya el nivel hasta el que se deben comunicar las conclusiones de las investigaciones.

En ocasiones, las organizaciones están obligadas por ley a informar de los incumplimientos. En estos casos, se informa a las autoridades reguladoras de acuerdo con la normativa aplicable, o según se acuerde. Si no estuvieran obligadas por la ley a informar sobre el incumplimiento, pueden considerar la posibilidad de revelar voluntariamente el incumplimiento a las autoridades reguladoras para mitigar las consecuencias del incumplimiento.



7. EVALUACIÓN DE DESEMPEÑO

7. Evaluación de desempeño

7.1 Seguimiento, medición, análisis y evaluación

7.1.1 Generalidades



Puntos donde centrar la atención:

En este capítulo ingresamos a la etapa de “verificar” en el Ciclo de Deming. Esto implica que debemos evaluar el desempeño del SGC como un todo.

Para ello, la organización debe definir qué va a medir y/o monitorear, estableciendo metodologías sistemáticas en las que se definan: periodicidades y responsables de la medición, periodicidades y responsables del análisis y evaluación de resultados.

En particular se debe medir algunos aspectos esenciales como son:

- ▶ los objetivos establecidos para el sistema de gestión
- ▶ grado de cumplimiento de las obligaciones de compliance (ver 2.5)
- ▶ eficacia de las formaciones
- ▶ eficacia de los controles (por ej.: mediante pruebas por muestreo)
- ▶ asignación efectiva de responsabilidades para cumplir con las obligaciones de compliance
- ▶ eficacia en la resolución de desvíos de compliance previamente identificados
- ▶ revisión de estrategia organizacional para promover una actualización adecuada de las obligaciones y riesgos de compliance

Notar que, para dar evidencia de cumplimiento de este requisito, se debe dejar registro de las mediciones y evaluaciones realizadas como información documentada.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Mediante la creación de un procedimiento de medición del desempeño global, se puede dejar claramente establecida la metodología a utilizar, los responsables y plazos en cada aspecto que se desee seguir, monitorear o medir.

Otra alternativa es agregar un apartado en cada procedimiento, en el que se establezcan los puntos de control y/o indicadores que se establecen para garantizar el correcto funcionamiento del proceso descrito en dicho procedimiento.

Por supuesto, se puede considerar una combinación de las dos propuestas precedentes, es decir:

- considerar un procedimiento macro para medición y seguimiento de aspectos generales (relativos a contexto, partes interesadas, etc.); y
- adoptar la segunda práctica recomendada, para los procedimientos más operativos.



IMPORTANTE:

La organización debe mantener información documentada de las mediciones y evaluaciones realizadas.

7.1.2 Fuentes de retroalimentación sobre el desempeño de compliance



Puntos donde centrar la atención:

La norma ISO 9001 (casualmente también en el apartado 7.1.2 "Satisfacción del Cliente") indica que se debe establecer una metodología para recopilar información acerca del grado en que se han cumplido las expectativas y necesidades de nuestros Clientes (parte interesada fundamental dentro del sistema de gestión de calidad).

En este caso, **la norma ISO 37301 de manera análoga a la ISO 9001, nos invita a implementar una metodología para poder recibir retroalimentación de diversas partes interesadas** (no solo de los clientes) para evaluar, desde su punto de vista, el grado en que hemos cumplido las obligaciones de compliance, o bien en general, que tan bueno fue nuestro desempeño en materia de compliance.

En caso de que la retroalimentación deje en evidencia algún incumplimiento, debemos analizar la información de manera crítica para identificar las causas fundamentales (causa raíz) del incumplimiento y tomar medidas adecuadas para evitar que vuelva a suceder. Notar que esto debe retroalimentar la evaluación de riesgos de 2.6.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Dependiendo el alcance del SGC definido en 2.3, las partes interesadas identificadas en 2.2 y el tipo de actividad de cada organización (producto o servicio ofrecido) se podrán implementar diversas metodologías para recopilar información de las partes interesadas pertinentes.

Algunas pueden ser: línea de ética o denuncia, línea de ayuda, buzones de sugerencias, encuestas de percepción, sondeos o consultas por diversos medios (correo electrónico, teléfono, redes sociales, página web, cursos de capacitación y/o concientización, debates, auditorías, focus groups, etc.).

7.1.3 Desarrollo de indicadores



Puntos donde centrar la atención:

De acuerdo con este apartado, **se deberán establecer metodologías de medición mediante la implementación de indicadores para poder evaluar el desempeño de compliance y el grado de cumplimiento de los objetivos planteados** para el sistema de gestión.

En algunos casos puede resultar complejo decidir qué aspectos medir en compliance, y por tal motivo sugerimos que se analicen los riesgos identificados para establecer los indicadores en vínculo con éstos.

De inicio, durante la implementación del sistema de gestión, seguramente sea útil evaluar aspectos más superficiales (incluso de aspectos del proyecto de implementación en curso; como ser: cuántos procedimientos están en creación, cuántos ya aprobados, cantidad de horas de concientización inicial dictadas, etc.) y a medida que vaya madurando el sistema, se podrá desarrollar indicadores más precisos que midan aspectos más críticos del funcionamiento del sistema (como ser: cantidad de capacitaciones eficaces, cantidad de investigaciones atendidas en plazo, tiempo que se tarda en informar y tomar medidas ante incumplimientos, tasa de incumplimiento real versus la esperada en función a mediciones de periodos pasados, etc.).

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

En este apartado se refuerza la necesidad planteada ya en el apartado 7.1.1, detallando específicamente la necesidad de construir indicadores.

Para el caso, existen diversos sistemas informáticos de inteligencia de negocios que presentan tableros de control o dashboards, de manera gráfica y con actualización de información en línea (instantánea).

Claro está que también pueden construirse tableros de indicadores de actualización manual, por medio de planillas de cálculo.

7.1.4 Informes de Compliance



Puntos donde centrar la atención:

Tal como se planteó ya en 3.1 y 3.3, es fundamental determinar un proceso de reporte adecuado para poder garantizar que el funcionamiento del sistema de gestión es informado a las partes interesadas pertinentes.

En el proceso de reporte entonces, se deberá definir:

- ▶ los criterios para la emisión de informes
- ▶ los plazos para la presentación de informes
- ▶ situaciones en las cuales es necesario notificar ad hoc (es decir, es tan importante la notificación de situaciones cotidianas a periodos determinados como la notificación puntual de un incumplimiento grave o también leve pero que denota una grave falla en un control específico)
- ▶ criterios para que la información sea exacta, íntegra y no sufra adulteraciones (en particular los informes emitidos por la función de compliance al órgano de gobierno y/o a la alta dirección)

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Desarrollar una política de reportes de compliance ad hoc, así como procedimientos de reportes periódicos es fundamental para garantizar que se entienda la forma y contenidos a informar.

A la hora de establecer la metodología, tener en cuenta los aspectos detallados en lo descrito en este apartado 7.1.4.

A continuación, mostramos como ejemplo, aspectos a tener en cuenta al definir el contenido y/o alcance de cada reporte:

- notificaciones a, reuniones, citas y/o contactos con autoridades reguladoras
- cambios en obligaciones de compliance y/o riesgos
- resultados de mediciones según 7.1.1, 7.1.2 y 7.1.3
- cantidad y detalles de incumplimientos, investigaciones o análisis posteriores, acciones implementadas y su eficacia
- desempeño y tendencias del SGC
- resultados de auditorías

7.1.5 Registro de datos



Puntos donde centrar la atención:

Este es un aspecto fundamental a la hora de gestionar la información documentada. Los registros poseen carácter probatorio, es decir que, **ante un incumplimiento, podremos demostrar los procesos y controles existentes mediante la presentación de registros documentados**, incluso ante autoridades en la Justicia (si fuera el caso).

Estos registros, para garantizar la integridad del sistema, deben estar protegidos contra cualquier adición, supresión, modificación, uso no autorizado u ocultación.

Si bien este aspecto ya se trató en el apartado 5.5, aparece nuevamente en este capítulo dado que una adecuada conservación de registros ayudará en los procesos de seguimiento y revisión para demostrar la conformidad con el SGC y los objetivos planteados.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Tal como sugerimos en el apartado 5.5, para garantizar una adecuada gestión de los registros, recomendamos construir un listado o matriz de documentos en los que se detalla la siguiente información de cada documento: nombre, código, fecha y/o número de revisión, para quién debe estar disponible, ruta en servidor para llegar a él, etc.

Adicionalmente, se debe tener consideración respecto a los permisos de acceso, visualización, modificación, eliminación, etc. de cada usuario, ya sea que la información documentada esté en formato físico o digital.

7.2 Auditoría Interna

7.2.1 Generalidades



Puntos donde centrar la atención:

Este es un aspecto diferencial si contrastamos los sistemas de gestión de compliance con los programas de compliance.

El hecho de que realizar una auditoría interna sea obligatorio, le otorga robustez la gestión y es un pilar fundamental de la mejora continua.

Pasar por procesos de auditoría siempre deja resultados positivos para modificar metodologías en pos de mitigar riesgos de incumplimiento y mejorar la forma en que se consigue cumplir con las obligaciones de compliance.

El objetivo de realizar auditorías internas a intervalos planificados es verificar si el sistema de gestión cumple con los requisitos de la norma y los requisitos propios que la organización ha determinado para su compliance.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para que el resultado de la auditoría tenga validez, debemos contar con auditores internos (que pueden ser externos a la organización) con adecuada competencia e independencia.

Dependiendo de la madurez del SGC será la cantidad de veces al año que se audite la organización. En términos generales, recomendamos que las auditorías internas (completas de todo el sistema) sean al menos anualmente cuando el sistema ya tenga un tiempo de corrida y cada 6 meses cuando sea nuevo. De todos modos, es una recomendación general y la frecuencia podría variar según la situación de cada organización.

La competencia de los auditores se consigue mediante cursos de capacitación, pero, sobre todo, mediante la experiencia práctica. Es decir, que un plan de formación de auditores debe contemplar la participación de auditores en entrenamiento en todos los procesos de auditoría que se lleven a cabo en la organización.

El principio de independencia es fundamental para garantizar resultados eficaces, por lo que debemos cuidar siempre que el auditor no audite los procesos en los que está involucrado en su área de responsabilidad. Para el caso, se debe contar siempre al menos con 2 auditores internos, que sean de áreas o departamentos diferentes, de manera que auditen de forma cruzada mutuamente, los procesos de los que son responsables.

7.2.2 Programa de auditoría interna



Puntos donde centrar la atención:

Para gestionar de manera adecuada las auditorías planificadas, la norma invita a desarrollar e implementar un programa de auditoría en el que se especificará la siguiente información: el objetivo de la auditoría, los criterios, el alcance, la frecuencia, los métodos, las responsabilidades, los requisitos de presentación de informes y la competencia de los auditores.

Al programar las auditorías, se deberá tener en cuenta también la relevancia de los procesos y los resultados de las auditorías anteriores.

Se deberá dejar un registro como información documentada que demuestre la implementación y puesta en práctica del programa de auditoría y los resultados de la misma.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Tal como recomienda la norma, hacer uso de la norma ISO 19011 de "Directrices para auditoría de sistemas de gestión" es una muy buena práctica.

La lectura e interpretación de la norma ISO 19011 es relativamente sencilla por ser una norma de directrices o lineamientos. Es un compendio de recomendaciones o buenas prácticas probadas, a la hora de auditar sistemas de gestión.

En la práctica, existen soluciones digitales para programar y planificar auditorías; dependiendo de la complejidad de la organización y sus procesos, sin embargo, el desarrollo de un plan de auditorías puede limitarse a una matriz en una planilla de cálculo, donde se especifiquen los aspectos listados en la explicación de este apartado 7.2.2.



IMPORTANTE:

La organización debe mantener información documentada de los programas y de los resultados de las auditorías.

7.3 Revisión por la dirección

7.3.1 Generalidades



Puntos donde centrar la atención:

En el mismo nivel de importancia de la auditoría interna se encuentra este proceso de revisión de la gestión, por parte del órgano de gobierno y la alta dirección, es decir, la más alta jerarquía de la organización.

Esta revisión debe realizarse también a periodos planificados de manera de asegurar su eficacia y, como veremos en el apartado siguiente, uno de los datos que se debe evaluar es el resultado de auditorías, motivo por el cual se debe vincular la periodicidad de ambos procesos (auditoría y revisión).

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

La revisión por la dirección debe entenderse como un proceso: existe información de entrada y acciones o decisiones de salida.

Normalmente, se desarrolla la información pertinente en cada área o departamento de la organización y se la comparte con el área de compliance quien se ocupa de compaginar la información recibida y prepararla para la revisión, que se realiza mediante una reunión del órgano de gobierno y la alta dirección.

Es usual que en la revisión participen otras direcciones o gerencias además de compliance, de manera de poder explicar y presentar resultados, así como las acciones tomadas frente a desvíos o incumplimientos.

7.3.2 Entradas a la revisión por la dirección



Puntos donde centrar la atención:

Queda claramente especificado en la norma cuales son todos los datos a tener en cuenta como información de entrada al proceso de revisión.

Estos son:

- ▶ el estado de las acciones de revisiones anteriores;
- ▶ los cambios en cuestiones externas e internas que sean relevantes;
- ▶ los cambios en las necesidades y expectativas de las partes interesadas relevantes;
- ▶ información sobre los resultados de cumplimiento, incluyendo:
 - ▶ no conformidades, incumplimientos y acciones correctivas;
 - ▶ resultados del seguimiento y mediciones;
 - ▶ resultados de auditorías;
 - ▶ oportunidades de mejora.

También se deberá tener en cuenta:

- ▶ la adecuación de la política de compliance;
- ▶ la independencia de la función de compliance;
- ▶ el grado de cumplimiento de los objetivos;
- ▶ la adecuación de los recursos;
- ▶ la adecuación de la gestión de riesgos de compliance;
- ▶ la eficacia de los controles e indicadores de desempeño;
- ▶ la comunicación de las personas que plantean inquietudes, las partes interesadas, incluida la retroalimentación (7.1.2) y las denuncias;
- ▶ investigaciones (6.4);
- ▶ la eficacia del sistema de reporte (7.1.4).

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Siguiendo los aspectos indicados por la norma, se deberá realizar una reunión de revisión por la dirección y dejar un registro de: los participantes en la reunión, la fecha, la duración, los aspectos evaluados y la información analizada.

7.3.3 Revisión por la dirección



Puntos donde centrar la atención:

La salida del proceso de revisión por la dirección debe incluir las decisiones que se han tomado como resultado de la información analizada.

Las decisiones pueden incluir: acciones a implementar sobre oportunidades de mejora identificadas (con responsables, plazos, etc.), la necesidad de asignar recursos o presupuesto para implementar las acciones o mejorar el desempeño de un área o proceso, otras necesidades de cambios en el sistema.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

La salida de la revisión por la dirección es un informe documentado en el que se detallan las decisiones tomadas.

La extensión del informe puede ser de unas pocas páginas resumiendo los temas tratados (como ser un acta o minuta de la reunión) y la atención debe estar puesta en una adecuada definición de acciones, responsables, plazos y recursos necesarios.



IMPORTANTE:

La organización debe mantener información documentada de las revisiones por la dirección realizadas.





8. MEJORA

8. Mejora

8.1 Mejora continua



Puntos donde centrar la atención:

Es tal vez uno de los aspectos más determinantes a la hora de explicar la eficacia de un SGC frente a otras alternativas para implementar programas o planes de compliance.

La norma pide a la organización que mejore continuamente tres puntos esenciales de su SGC:

- ▶ la idoneidad: que el sistema sea pertinente para gestionar las obligaciones y los riesgos de compliance.
- ▶ la adecuación: que significa que el sistema sea "proporcional", contemplando los aspectos relevantes del contexto interno y externo, observando y dialogando con las partes interesadas, identificando las obligaciones de compliance y gestionando los riesgos.
- ▶ la eficacia del SGC: que luego de definidos los indicadores críticos de éxito, se monitoree su cumplimiento, se audite el sistema de gestión, se revise por la Dirección, se capturen las no conformidades, incumplimientos y oportunidades de mejora y se mejore consecuentemente el sistema en forma continuada.

Cuando la organización determine la necesidad de realizar cambios en el SGC, producto de la mejora continua requerida por la norma, estos cambios se llevarán a cabo de forma planificada, tal como se ha mencionado. A dichos fines la organización deberá considerar:

- ▶ el objetivo de los cambios y sus posibles impactos en el sistema de gestión, tanto en el diseño, como en su eficacia operativa
- ▶ la disponibilidad de recursos adecuados;
- ▶ los ajustes de estructura organizativa que resulten necesarios (asignación o reasignación de responsabilidades y autoridades).

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Para que el sistema sea considerado eficaz debe ser sostenible en el tiempo. La forma válida para lograrlo es que tenga la capacidad de mejorar y evolucionar continuamente, ya que existirán cambios en el entorno interno y externo de la organización, en su actividad, en sus partes interesadas y en las obligaciones de compliance que le sean aplicables.

Para lograr esto la función de Auditoría Interna adquiere alta relevancia por su capacidad de evaluar en forma periódica el sistema de gestión y la solidez de sus controles. Pero este no es el único método. La autoevaluación por parte de cada una de las áreas de la organización es un método muy válido también.

Otra forma para evaluar la efectividad de compliance es midiendo su cultura de cumplimiento mediante entrevistas y/o incluyendo preguntas relevantes a compliance en las encuestas de clima organizacional.

Se espera además que las revisiones por la dirección sean una fuente de oportunidades de mejora del SGC.

Sería esperable que de estas revisiones y análisis se planifiquen cambios en el SGC, se lleven a cabo, se verifique la eficacia de la acción emprendida y se normalice. Aquí se resume lo que llamamos "mejora continua".

8.2 No conformidades y acciones correctivas



Puntos donde centrar la atención:

Las no conformidades (NC) o incumplimientos merecen especial atención para el SGC. Toda vez que existan, la organización debe articular una rutina diligente que contenga como mínimo estos pasos:

- a) reaccionar inmediatamente ante la NC o el incumplimiento, y según sea aplicable:
 - 1) tomar las acciones adecuadas para controlarla y corregirla;
 - 2) hacer frente a las consecuencias;
- b) evaluar la necesidad de acciones para eliminar las causas de la NC o el incumplimiento, con el fin de que no vuelva a ocurrir, mediante:
 - 1) revisión, comprensión y definición clara de la NC o del incumplimiento, o de ambos;
 - 2) determinación de las causas que produjeron la NC o del incumplimiento, o de ambos;
 - 3) determinación de la factibilidad de que puedan producirse no conformidades o incumplimientos similares;
- c) implementar cualquier acción necesaria;
- d) revisar la eficacia de cualquier acción correctiva tomada;
- e) si fuera necesario, hacer cambios al SGC, lo que implicaría su mejora en los términos planteados en el apartado anterior.

Entonces nuevamente podemos apreciar con claridad que esto no es otra cosa que el necesario "ciclo PDCA" de la mejora continua.

Las acciones correctivas serán adecuadas a los efectos de las no conformidades o incumplimientos, o ambos, encontrados, esto significa, que deben ser diseñadas para producir un cambio positivo en los hallazgos que han surgido y, en consecuencia, en el SGC como un todo.



IMPORTANTE:

La organización debe mantener en forma documentada, como evidencia:

- la naturaleza de las no conformidades y cualquier acción tomada respecto de la misma;
- los resultados de cualquier acción correctiva, producto del chequeo planeado que corresponda.

CONSEJOS PARA UNA EFICAZ IMPLEMENTACIÓN:

Es importante tener en consideración que el hecho de no prevenir o detectar un incumplimiento puntual no significa necesariamente que el SGC no sea eficaz, en general, para prevenir y/o detectar un incumplimiento. No obstante, un SGC que no sea capaz de accionar un esquema de mejora continua como actividad recurrente para mejorar el desempeño con resultados medibles, en función de lo mencionado en el punto anterior, podrá ser catalogado como ineficaz.

También debemos comprender que cuando la norma se refiere a una "NC", quiere significar el incumplimiento de un requisito del SGC (esté especificado o no), mientras que un "Incumplimiento" se refiere al no cumplimiento de una obligación de compliance, la que debería estar definida como tal en los términos de la presente norma. Entendemos entonces que se podrían identificar NC que no representen incumplimientos de compliance.

Cuando la norma se refiere a "reaccionar" inmediatamente, esto podría implicar una investigación en los términos del apartado 6.4. Nótese que, según los procedimientos administrativos o penales en algunos países, una presentación espontánea o autodenuncia ante la Justicia podría interrumpir o bloquear consecuencias altamente gravosas para las personas jurídicas. Pero ello es prácticamente inviable sin que exista un proceso investigativo.



Amadeo Berdou

Director de
TÜV NORD México

aberdou@tuv-nord.com



- ▶ Ingeniero Mecánico de la Universidad de Buenos Aires
- ▶ Auditor Líder de las Normas ISO 37001, 9001, 14001, 45001
- ▶ Entrenador en las mencionadas normas en organizaciones públicas y privadas
- ▶ Presidente de TÜV NORD México S.A. de C.V. desde 2020 al presente
- ▶ Presidente de TÜV NORD Argentina S.A. desde 2012 al 2020
- ▶ Auditorias de Sistemas de Gestión para diversas industrias en numerosos países de la Región Latinoamérica
- ▶ Inspecciones de soldadura y de equipos en instalaciones nucleares e industria en general
- ▶ Posgrado en estrategia, globalización de negocios y gestión del cambio
- ▶ Padre de Astor (5) y Ceferino (3), hinchas de River Plate



Carlos Rozen

Socio BDO

crozen@bdoargentina.com



- ▶ Socio de BDO (GRC – Governance, Risk & Compliance) y FID (Fraude, Investigaciones & Disputas) y Gestión del Cambio Cultural.
- ▶ Integrante del Comité de Innovación de BDO Internacional
- ▶ Emprendedor, creador de herramientas de compliance que son utilizadas en diferentes partes del mundo.
- ▶ Contador Público (U.B.A.) - Auditor Líder de la Norma ISO 9001 - Consultor certificado en Risk Management PCEB – Auditor certificado en ISO 37001.
- ▶ Director de Empresas Profesional (DEP) – IGEP
- ▶ Director de la Certificación Internacional en Ética y Compliance (AAEC – Universidad del CEMA – IFCA International Federation Of Compliance Associations)
- ▶ Docente en Compliance en 5 universidades argentinas y profesor invitado en 4 universidades del exterior. Integrante del Consejo Asesor de Maestrías en UADE.
- ▶ Especialista en gamificación aplicado al Compliance – Profesor invitado en la Certificación Internacional en Inteligencia Lúdica (Ludic Intelligence Institute Latam-Spain)
- ▶ Ha dirigido la implementación de más de 100 programas de compliance.
- ▶ Hinchista de River. Esposo de Claudia. Padre de Rafaela (7) y Elena (3), ambas de Boca.