KPMG

Estándares internacionales en *compliance*: ISO 19600 y 37001

Serie *Compliance* avanzado – 7

www.kpmgcumplimientolegal.es

Los documentos de la Serie Compliance avanzado abordan aspectos relacionados con el Compliance cuya adecuada comprensión e interpretación precisa conocimientos previos en esta materia. Salvo que dispongas de ellos, sugiero consultar primero otros materiales sobre Compliance, como son los Cuadernos sobre Cumplimiento Legal, la Serie de Errores sobre Compliance, la Serie de Tests sobre Compliance, los Kits sobre despliegue de Compliance o la Serie de videos Compliance Basics, todo ello de acceso libre en la página web: www.kpmgcumplimientolegal.es

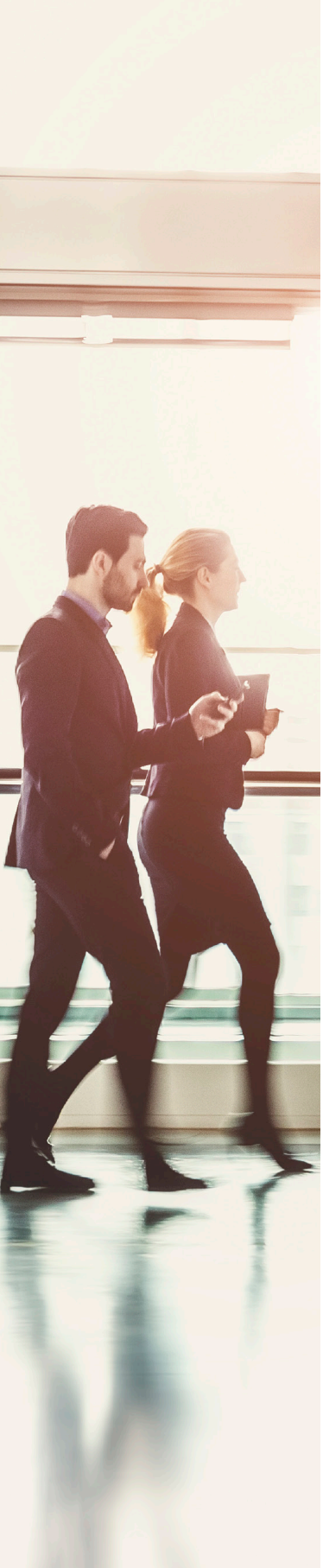
Presentación

Alain Casanovas
Socio de KPMG Abogados
acasanovas@kpmg.es
Perfil en Linkedin

Es en el contexto de los mercados regulados donde encontramos los primeros textos que nos hablan de una función estructurada de *Compliance*. El Comité de Basilea de supervisión bancaria emitió en 2005 un interesante documento sobre la **función de cumplimiento** en los **bancos**, fijando los diez principios esenciales que le eran aplicables. Poco después, la *International Organization of Securities Commissions* (IOSCO) emitió otro documento destinado a ayudar a los intermediarios financieros a incrementar la efectividad de sus funciones de cumplimiento. En estos documentos ya vemos muchos de los elementos reconocibles en los Programas y Sistemas de gestión de *Compliance* modernos. No obstante, aun siendo una fuente de inspiración para cualquier organización, estaban ideados para las que operaban en sus respectivos mercados y su nivel de conocimiento o aplicación analógica fuera de ellos fue limitado.

Aunque el fenómeno de la **proliferación y complejidad normativa** empezó afectando a algunos mercados, rápidamente devino una **situación generalizada** a causa de la creciente complejidad de las actividades empresariales, la irrupción de bloques normativos nuevos (privacidad, prevención penal, etc) y la globalización de la economía. Paralelamente, el incremento de los daños económicos y reputaciones asociados al incumplimiento de las obligaciones de las organizaciones, llevó a plantearse la aplicación de metodologías que permitiesen gestionar esta nueva realidad. Algunas organizaciones recurrieron a conocidos **entornos de control**, como COSO, para definir un entorno de supervisión y gestión de riesgos de naturaleza legal. En los estándares modernos sobre *Compliance*, también se aprecian componentes que derivan de ellos y que forman parte de su ADN actual.

En el año 2006 Australian Standards emitió un texto sobre Programas de *Compliance*, su célebre estándar AS 3806. Recogía una serie de **buenas prácticas**, destinadas a conformar un **Programa de *Compliance*** aplicable a cualquier tipo de organización. Fue la primera norma nacional de esta naturaleza y rápidamente adquirió notoriedad



Presentación (cont.)

y disfrutó de una gran aceptación dentro y fuera de su jurisdicción de origen. Constituyó un eslabón evolutivo significativo, pues hacía ya innecesario recurrir a la interpretación analógica de otros textos para gestionar la realidad del *Compliance*, especialmente cuando éstos parecían más cercanos a otros ámbitos como el control financiero.

El estándar australiano se convirtió en el texto de partida del primer estándar internacional sobre *Compliance*, la norma ISO 19600, desembocando así en la **nueva generación de estándares** sobre esta materia, que determinan el estado actual del arte sobre ella. Conocer estos textos es indispensable para cualquier profesional de *Compliance*, de modo que en este documento comentaré sus fundamentos y contenido básico.

Índice

La actividad internacional de normalización

Las actividades de normalización son la respuesta a la inquietud social de dar un tratamiento homogéneo a determinados aspectos técnicos. En la esfera del *Compliance*, la proliferación de normas que afectan a las actividades empresariales ha justificado impulsar directrices sobre el modo de gestionar esta complejidad. Además, la **irrupción del Derecho penal** en la esfera económica ha incrementado tal necesidad, contribuyendo a agravar las consecuencias adversas en los campos económicos y de reputación que se pueden derivar de los incumplimientos.

Tal como expliqué en el Documento número 1 de esta Serie ("*Certificaciones y auditorías de Compliance*"), los poderes públicos pueden otorgar la capacidad de emitir **normas técnicas** a ciertas entidades en su respectiva jurisdicción, con la finalidad de producir estándares que determinen un lenguaje de comunicación común en las materias que lo precisen. En España es la **Asociación Española de Normalización UNE**, del mismo modo que lo es ANSI en los Estados Unidos, BSI en el Reino Unido, DIN en Alemania, AFNOR en Francia, UNI en Italia, etc. Estos organismos se agrupan a nivel internacional en la Organización Internacional de Normalización ISO. Fundada en 1947, es una organización independiente y no-gubernamental que aglutina a las entidades nacionales de normalización. Promueve la creación de estándares internacionales a través de un procedimiento **regulado, transparente y participativo**. En bastantes ocasiones, los procesos de normalización internacional toman, como punto de partida, estándares nacionales que han disfrutado de gran reconocimiento en la comunidad internacional. Adoptando estos textos como base del primer "*Working Draft*" (WD), se perfila progresivamente el contenido del documento hasta obtener un nivel adecuado de consenso entre los países que participan en él, momento a partir del cual se publica como estándar.

El primer estándar nacional sobre **programas** de *Compliance* fue el normalizado por *Australian Standards*, organización independiente sin ánimo

de lucro, reconocida por el Gobierno de Australia e integrante de ISO. Fue el conocido AS 3806, publicado el año 2006. A pesar de ser un estándar **nacional**, la norma adquirió una notable difusión internacional por la practicidad de sus contenidos. Se convirtió en la base de trabajo para la elaboración del primer estándar internacional sobre *Compliance*, la norma ISO 19600 sobre *Compliance* Management Systems (CMS). No obstante, conviene recordar que este estándar, a diferencia de su antecesor, establece directrices que definen un **sistema de gestión** y no un simple **programa** de *Compliance*, cuyas diferencias conceptuales expliqué en el Documento número 6 de esta Serie ("Claves sistémicas en *Compliance*").

No obstante lo anterior, la sociedad había venido mostrando interés por modelos de *Compliance* que contribuyesen a la lucha contra la **corrupción**, en general, y el **soborno**, en particular. Aunque se habían emitido recomendaciones por diferentes plataformas tanto nacionales como internacionales sobre este particular, la entidad de normalización británica *British Standards Institution* publicó la norma de especificaciones BS 10500 para *Anti-Bribery Management Systems* (ABMS) en el año 2011, al hilo de la conocida *UK Bribery Act* publicada en el año 2010. Siendo considerado el estándar anti soborno más avanzado, conformó la base para la elaboración del estándar ISO 37001 sobre *Anti-Bribery Management Systems* (ABMS).

Ni las **entidades** de normalización nacionales ni ISO a nivel internacional, disponen de capacidad para emitir certificados de conformidad con sus normas. Estas actividades las desarrollan otras entidades, que pueden **acreditarse** ante el organismo nacional que tiene atribuida tal función, según expliqué en el Documento número 1 de esta Serie ("*Certificaciones y auditorías de Compliance*").

La estructura de alto nivel de los sistemas de gestión

ISO ideó la llamada **estructura de alto nivel** (High Level Structure, HLS) aplicable a los estándares sobre sistemas de gestión (*Management System Standard, MSS*) elaborados por dicha organización. La HLS permite que todos los sistemas de gestión tengan una estructura y definiciones básicas comunes, facilitando su interpretación e integración.

ISO también distingue entre los MSS de **tipo A** y los de **tipo B**. Los primeros proporcionan **especificaciones** y admiten certificar la conformidad con sus contenidos, mientras que los segundos facilitan **líneas directrices** y no son certificables. La HLS debe siembre emplearse en los MSS ISO de tipo A, y cuando sea posible también en los de tipo B. Por eso, una de las primeras labores que se desarrolló en los procesos de normalización internacional sobre *Compliance* consistió en adaptar los contenidos de los estándares nacionales AS 3806 y BS 10500 a la HLS de ISO. Así, comparten estructura (índice principal) y también una buena parte de sus definiciones (no las añadidas por motivo de especialidad). No obstante, el estándar ISO 19600 es un MSS de Tipo B (**no certificable**), mientras que el estándar ISO 37001 es de Tipo A (**certificable**).

La HLS está organizada en 10 capítulos:

Introducción

Consiste en una breve **exposición de los motivos** que justifican el estándar. Es el lugar donde se encuentran algunas explicaciones acerca de su contenido y argumentos sobre su utilidad. Es interesante para comprender el estándar y ayuda a interpretar su articulado en el sentido adecuado.

Objeto y campo de aplicación

Determina el **objeto** del estándar y quienes pueden ser sus **destinatarios**. En los estándares de *Compliance* se clarifica que pueden aplicar a cualquier tipo de organización, tanto del sector privado como del público, así como a las organizaciones sin ánimo de lucro.

Normas para consulta

Se relacionan aquellos otros estándares que son **necesarios** para la correcta aplicación del que se regula. Ni los estándares ISO 19600 e ISO 37001, ni la norma UNE 19601, contienen referencias normativas. Aunque en otros apartados se citan algunos estándares ISO, emplearlos no constituye un requisito para dichos textos.

Términos y definiciones

Se relacionan definiciones que son **comunes** a todos los sistemas de gestión. Estos pueden añadir **definiciones adicionales** por motivo de materia, o complementar el contenido de las existentes. Es importante prestar atención a las definiciones, dado que condicionan de manera significativa la interpretación de los apartados donde se emplean.

Contexto de la organización

Aparecen los aspectos que pueden influir en la organización, tanto **internos** como **externos**. Son, por lo tanto, factores a considerar tanto en el diseño y como en la operación del sistema de gestión. Por ejemplo, las expectativas o requisitos de los grupos de interés son uno de los aspectos que aparecen tratados.

Liderazgo

Figuran los **roles** y **responsabilidades** de aquellas figuras que encarnan el **liderazgo** en el sistema de gestión. En los estándares sobre *Compliance* no sólo constan el órgano de gobierno y la alta dirección sino también la propia función de *Compliance*.

Planificación

Las actividades de planificación permiten calibrar de manera continua el sistema de gestión para que se adapte tanto a las circunstancias internas como externas de la organización. En materia de *Compliance* se contempla tanto la **fijación de objetivos** como la de **indicadores** para valorar su grado de consecución y que permitan, por lo tanto, adoptar las decisiones que contribuyan a su consecución.

Elementos de apoyo

Los elementos de apoyo incluyen una serie de aspectos sin los cuales **difícilmente puede operar correctamente un sistema de gestión**. Además de aspectos de capacitación vinculados a las actividades formativas y de concienciación, también se contempla la necesidad de recursos o de información documentada. Los estándares de *Compliance* inciden en aspectos relacionados con la generación y mantenimiento de una adecuada cultura.

Operación

Se abordan cuestiones relacionadas con la **operatividad** del sistema de gestión, que lleva al establecimiento de determinados **procesos y procedimientos** clave para cumplir con sus requisitos. En el ámbito de *Compliance* se regulan ciertos procedimientos y controles típicos en su ámbito, como son los de **diligencia debida** o los controles tanto financieros como no financieros así como las salvaguardas contractuales.

Evaluación del desempeño

Este capítulo regula cómo medir el desempeño del sistema de gestión. En el ámbito del *Compliance*, cabe prestar especial atención a los órganos a los que se debe **reportar** el **desempeño** del sistema de gestión y el modo de hacerlo adecuadamente.

Mejora

Como estructura viva, el sistema de gestión debe contener los elementos que no sólo le permitan adaptarse a las circunstancias sino mejorar de manera continua. Esto lleva a reglar cómo proceder ante **no conformidades** para evitar que se reproduzcan, así como las revisiones del sistema de gestión en su conjunto.

Algunos principios esenciales

Los estándares ISO 19600 y 37001 comparten algunos **fundamentos** esenciales que es preciso conocer para interpretar correctamente su contenido. Aunque estos textos no se refieren expresamente a ellos, incorporan contenidos claramente vinculados con su esencia.

Subordinación a Ley

Ningún estándar resultante de la normalización privada puede **contravenir el Derecho positivo**. Aunque los estándares nacionales se producen por entidades nacionales con capacidades de normalización reconocidas por los poderes públicos, sus normas forman parte de la esfera privada y **no son equiparables a Leyes**. Lo mismo sucede con las normas que se producen en el ámbito de ISO, que, como he explicado, es una organización independiente y no-gubernamental. Por lo tanto, la aplicación del contenido de los estándares ISO 19600 e ISO 37001 no puede conculcar las exigencias de **Derecho positivo** en la jurisdicción donde se apliquen. Si alguna **directriz** o **requisito** colisionara con la normativa local, se entendería que no procede su aplicación, sin que sea necesario que así venga reiterado continuamente en el cuerpo de los estándares.

Proporcionalidad

Las referencias al principio de **proporcionalidad** son muy comunes en los textos sobre *Compliance*, aunque en ocasiones se cite con nombres diferentes ("flexibilidad") o incluso de forma implícita. En cualquier caso, la aplicación proporcional de las buenas prácticas de *Compliance* pretende favorecer modelos adaptados a las circunstancias, tanto internas como externas, de cada organización. Aunque la cifra de negocios y otras **magnitudes económicas** son relevantes a la hora de aplicar este principio, es erróneo basarse sólo en ellas sin considerar **otros factores** clave como el tipo de operaciones de la organización o los países donde se realizan, por ejemplo.

Ahora bien, la aplicación del principio de proporcionalidad no puede interpretarse como la capacidad de **no aplicar** algunos requisitos de los estándares ISO por considerarlos gravosos. Se aplicarán **todos ellos**, de forma proporcional a las circunstancias de cada organización.

Aproximación basada en el riesgo

Aplicar una **aproximación basada en el riesgo** a un sistema de gestión de *Compliance* significa priorizarlo hacia la prevención, detección y reacción frente a los riesgos que exponen a la organización. Esto implica conocer cuáles son tales riesgos (**identificación**), examinarlos (**análisis**) y finalmente otorgarles una calificación (**valoración**). Estas tres actividades se conocen, en su conjunto, como **evaluación de los riesgos**, y es la que permite orientar adecuadamente una gran parte de los elementos que conforman el sistema de gestión de *Compliance*. Así, por ejemplo, los objetivos de *Compliance* de una organización serán coherentes con los riesgos a que le exponen, debiendo ser más ambiciosos cuando aquellos sean mayores. Desde esta perspectiva, la aproximación basada en el riesgo permite conocer cuándo se está aplicando adecuadamente el **principio de proporcionalidad**.

La aproximación basada en el riesgo afecta a actividades tan importantes como la determinación de los **objetivos** de *Compliance*, los **recursos** que se precisarán para su consecución, las **actividades formativas**, y un largo etcétera.

Seguridad razonable

Todo mecanismo de control tiene **limitaciones** que le impiden prevenir o detectar vulneraciones. Bajo este entendimiento, un entorno de control no puede brindar **garantía absoluta** de ausencia de irregularidades, pero puede contribuir a reducir la exposición de ese riesgo. Los textos modernos de *Compliance* acogen este razonamiento, heredado de los **entornos de control maduros**, de manera que no garantizan que no hayan existido irregularidades o que no vayan a producirse. Lo contrario significaría exigir un estándar de **perfección** imposible.

La materialización de una contingencia de *Compliance* no invalida necesariamente el modelo establecido para su prevención, detección y gestión; ahora bien, la reiteración de incidentes de la misma tipología sí cuestiona seriamente su diseño y/o eficacia.

Mejora continua

Un sistema de gestión de *Compliance* mantendrá su **eficacia** si es capaz de adaptarse a las cambiantes circunstancias de la organización y mejorar continuamente. Esta mejora no sólo se traduce en reducir progresivamente los riesgos residuales de *Compliance* en la organización, sino también en **incrementar su nivel de exigencia**, fijando incluso objetivos por encima de los mínimos legales exigidos.

Los estándares ISO de *Compliance* evitan referirse a la eficiencia como palanca de mejora, entendida como la consecución de los objetivos pretendidos con el menor número de recursos posible. Dado que esto

conduce a dinámicas peligrosas, se destierra este enfoque y la mejora continua sólo tiene sentido en términos de incrementar la capacidad de lograr los objetivos de *Compliance*, esto es, la eficacia del sistema de gestión.

Transparencia

Una **gestión ética** se asocia con la **transparencia**, dado que las prácticas irregulares suelen desarrollarse en la opacidad.

Aunque rara vez aparece citado explícitamente en los estándares ISO, el **principio de transparencia** inviste muchos de sus componentes y se relaciona especialmente con algunos en concreto, como la difusión de valores o las comunicaciones de *Compliance* tanto internas como externas.

La Norma ISO 19600

El estándar ISO 19600 sobre *Compliance* Management Systems (CMS) es el resultado de un proyecto de normalización que se inició en el año 2013 y concluyó en diciembre de 2014. Partió del reconocido estándar australiano AS 3806:2006, adaptándolo a la HLS y mejorando su contenido no sólo para incorporar **buenas prácticas** adicionales sino para convertirlo en un **sistema de gestión**.

Se considera un estándar adecuado para definir sistemas de gestión sobre campos específicos de *Compliance* que carezcan de un texto adaptado a sus particularidades, y también para construir **superestructuras** de vocación transversal, capaces de coordinar diferentes bloques técnicos (privacidad, competencia, prevención penal, etc.).

Como estándar internacional, rehúye la utilización de conceptos jurídicos que pudieran vincularlo con Leyes u ordenamientos específicos. En cualquier caso, las definiciones que incorpora no son jurídicas sino **organizativas**: así, por ejemplo, el concepto de "organización" no es equivalente al de "persona jurídica".

Es el primer texto en aclarar que las obligaciones de *Compliance* tanto pueden provenir de obligaciones **impuestas** o **exigidas**, como de aquellas otras asumidas **voluntariamente**. Por consiguiente, un sistema de gestión de *Compliance* alineado con ISO 19600 contemplará ambos tipos con un mismo nivel de exigencia. La necesaria **evaluación de riesgos** tendrá en cuenta ese perímetro.

Es un MSS de Tipo B, es decir, de **directrices** o **recomendaciones**, por lo cual no puede emplearse en trabajos de evaluación de la conformidad en sentido estricto, aunque si pueden desarrollarse análisis de proximidad con su contenido. No obstante, en algunas jurisdicciones se emiten **certificaciones no acreditadas**. Sobre esta materia, puedes consultar el Documento número 1 de esta Serie ("*Certificaciones y auditorías de Compliance*").

El sistema de gestión que define el estándar estará operado por una función de *Compliance*. Se abandona el concepto de "Oficial de cumplimiento" empleado en textos anteriores, apostando por el concepto de "**función**" que brinda una mayor flexibilidad:

órgano individual, colegiado, función asignada a un órgano pre-existente, etc. Así, la **función de *Compliance*** puede revestir la forma que mejor se adapte a las circunstancias de cada organización para desplegar mayor eficacia.

Uno de los requisitos del sistema de gestión es la ***Política de Compliance***. A tal requisito se le otorga una importancia notable, muy propia de los entornos de *Compliance*, donde el establecimiento de la voluntad de la organización en esta materia y los parámetros de conducta esperados constituyen elementos de capital relevancia.

No es un estándar sectorial, siendo de aplicación a diferentes **sectores** y perfiles de organización, incluyendo las del ámbito privado, público o incluso las organizaciones sin ánimo de lucro.

Es el primer estándar internacional sobre *Compliance*, utilizado como baremo general del estado del arte en su materia. Sus contenidos han condicionado los del estándar ISO 37001 sobre sistemas de gestión anti soborno, así como los de la norma española UNE 19601 sobre sistemas de gestión de *Compliance* penal.

La Norma ISO 37001

El estándar ISO 37001 sobre *Anti-Bribery Management Systems* (ABMS) es el resultado de un proyecto de normalización que se inició en el año 2013 -muy poco después de haberse iniciado el proyecto referente al estándar ISO 19600-, concluyendo en octubre de 2016. Su punto de partida fue el estándar británico BS 10500:2010, coetáneo de la *UK Bribery Act*, adaptado a la HLS de ISO.

Este estándar ayuda a establecer y verificar sistemas de gestión de *Compliance* para la prevención, detección y gestión de **riesgos de soborno**, tanto en el ámbito de la corrupción **pública** como **privada**. Incorpora un anexo (no normativo) que recoge una interesante taxonomía de **transacciones conflictivas** susceptibles de encubrir sobornos (regalos, hospitalidad, donaciones, etc). También contempla la necesidad de controles **no financieros**, junto con los **financieros** que vienen siendo tradicionales en este tipo de textos.

Evita recurrir a conceptos vinculados con la normativa anti-soborno de determinadas jurisdicciones. Al igual que sucede con otros estándares ISO, sus definiciones no son jurídicas sino **organizativas**.

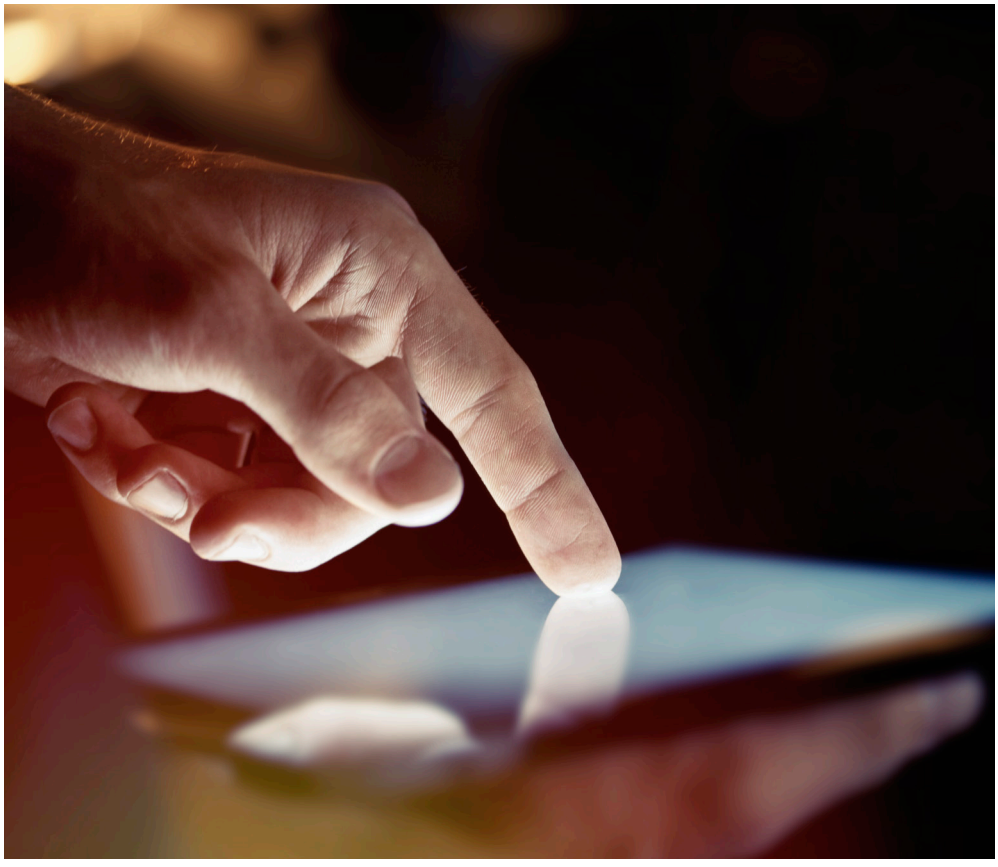
El **alcance objetivo** del estándar no coincide con las necesidades de prevención en algunos ordenamientos (el español, por ejemplo), donde los ilícitos penales vinculados con el soborno sólo son **una pequeña parte** de los que aplican a la persona jurídica y que deben ser objeto de cobertura. Al seguir una aproximación basada en el riesgo, la **evaluación de riesgos de soborno** se convierte en un ejercicio condicionante de buena parte de los elementos y actividades derivadas del sistema de gestión.

Es un MSS de Tipo A, es decir, de **requisitos**, pudiéndose emplear en trabajos de evaluación de la conformidad desarrollados por entidades independientes. No obstante, también recoge algunas **recomendaciones** que ayudan a interpretar y aplicar el estándar. Sobre esta materia, consulta el Documento número 1 de esta Serie (“*Certificaciones y auditorías de*

Compliance"). Puede operar de manera autónoma, o integrado en un sistema de gestión de mayor alcance (establecido sobre la base del estándar ISO 19600). Sobre este particular, puedes leer el Documento número 10 de esta Serie ("*Integraciones horizontales y verticales en Compliance*"). El estándar se puede aplicar a diferentes **sectores** y **perfiles** de organización, incluyendo las del ámbito privado, público o incluso las organizaciones sin ánimo de lucro.

El sistema de gestión que define el estándar está operado por una función de *Compliance* anti soborno, en la misma línea que el estándar ISO 19600. Igualmente, regula una ***Política de Compliance Anti-Bribery*** como pieza relevante en el sistema de gestión.

Por el número de países e instituciones que participaron activamente en su elaboración, el estándar ISO 37001 se ha convertido en un referente ampliamente aceptado y reconocido a nivel internacional. Está contribuyendo a la **generación de confianza** en operaciones internacionales que implican regiones o transacciones de riesgo.



Diligencia debida frente a socios de negocio

Cuando hablamos de *Compliance*, los procedimientos de **diligencia debida** sobre **socios de negocio** suponen **evaluarlos** para conocer el nivel de riesgo que entraña vincularse con ellos. A partir de ahí, es posible decidir sobre la conveniencia de tal relación y establecer, en su caso, las **salvaguardas** oportunas.

Este proceso normalmente pasa por definir unos parámetros objetivos de riesgo y desarrollar trabajos de evaluación de diferente calado según su resultado. Así, frente a entidades y/o transacciones de **riesgo bajo**, tal vez no proceda indagar más ni adoptar cautelas de *Compliance* especiales, más allá de las genéricas.

En otros casos, es frecuente que la función de *Compliance* busque satisfacerse de la **compatibilidad** del socio de negocio con los valores de la organización y sus políticas, procurándose información que le facilite este análisis. En este contexto, no son infrecuentes los **cuestionarios de *Compliance***, destinados a capturar información y documentación sobre las medidas de que dispone el potencial socio de negocio en materia de *Compliance*. Estos análisis requieren tiempo y entrañan cierto riesgo: formular preguntas incorrectas, no pedir documentos relevantes o interpretar erróneamente la información facilitada puede comprometer a quien ejecuta el proceso.

La reciente aparición de estándares **certificables** de *Compliance* abre la posibilidad de que la razonabilidad de un sistema de gestión de *Compliance* de **socios de negocio** pueda soportarse a través de la opinión de un **tercero independiente** cualificado. La solicitud de este tipo de opiniones o certificados se enmarca en lo que se conoce como "procesos de generación de confianza". Por lo tanto, dentro del proceso de contratación se puede solicitar este tipo de opiniones, valorando **positivamente** su existencia y supliendo con ellas algunos procesos de verificación adicionales. Esto no significa que vayan a terminar los cuestionarios de *Compliance* y el análisis de documentos e informaciones, pero contribuye a limitar su empleo en los casos indispensables.

Serie Compliance avanzado

1. Certificaciones y auditorías de *Compliance*

La existencia de reconocidos estándares nacionales e internacionales sobre *Compliance* ha permitido desarrollar trabajos tanto de diseño como de evaluación de programas y sistemas de gestión sobre la base de sus contenidos. En relación con estas evaluaciones de conformidad, existen diferentes enfoques y alcances de revisión que brindan diferentes niveles de confort a las organizaciones. Este documento aborda las dudas más frecuentes sobre esta materia.

2. Psicología social y cognitiva en *Compliance*

Las organizaciones aglutinan a un volumen cada vez mayor de personas. En estos contextos, conocer aspectos que afectan tanto al comportamiento individual como al colectivo de las personas es clave para una gestión exitosa de *Compliance*. En este documento se tratan algunos sesgos relevantes a tales efectos, identificados a lo largo de estudios y experimentos desarrollados en los ámbitos de la psicología cognitiva y de la psicología social.

3. Corrupción: taxonomía moderna de actividades conflictivas

Los estándares modernos de *Compliance* han ido perfilando actividades aparentemente normales que, sin embargo, son propicias para encubrir comportamientos ilícitos. Normalmente, no se trata de actividades necesariamente prohibidas, aunque su desarrollo inadecuado puede llegar a canalizar actos de corrupción. Este documento trata la taxonomía más moderna de este tipo de actividades, de gran utilidad para la definición de políticas anti-soborno y establecimiento de controles tanto preventivos como detectivos.

4. Carreras profesionales en *Compliance*

La madurez de los cometidos asociados al *Compliance* abren la posibilidad de diferentes carreras profesionales en este ámbito, que van desde el *Compliance* en ámbitos específicos por motivo de materia (prevención penal general, prevención de la corrupción, prevención del blanqueo de capitales y financiación del terrorismo, protección de la privacidad y los datos personales, prevención medioambiental, etc) o

de sector (financiero, farmacéutico, energía, etc), hasta la coordinación de diferentes bloques de normas mediante superestructuras de *Compliance*. Surge igualmente la posibilidad de desarrollar actividades de asesoramiento, defensa jurídica o auditoría de modelos de *Compliance*, por citar algunos ejemplos. Este documento comenta el abanico de oportunidades de desarrollo profesional que brindan los entornos de *Compliance*.

5. Detectando el paper *Compliance*

Los modelos de *Compliance* no constituyen una mera formalidad, sino que deben ser adecuados para cubrir una serie de objetivos. Puntualmente, pueden darse casos de programas "sobre el papel", sin la menor intención de que desarrollen su cometido realmente. Son modelos de "*fake Compliance*" o "*paper Compliance*" y se pueden detectar fácilmente desde el primer momento de su impulso. En este documento expondré una serie de medidores objetivos que facilitan identificar modelos de *Compliance* generados para defraudar y que deben reprobarse.

6. Claves sistémicas en *Compliance*

Los "Programas" de *Compliance* han dado paso a los "Sistemas de gestión" de *Compliance*, cuya naturaleza y forma de operar es particular, exigiendo una interacción entre sus elementos que no es indispensable en los modelos lineales que se han venido utilizando hasta la fecha. En este documento se analizarán las principales diferencias entre un "programa" y un "sistema de gestión", así como algunos de los elementos más importantes que permiten revestir de funcionamiento sistémico a las actividades de *Compliance*, a través de interrelaciones, que es necesario definir.

7. Estándares internacionales en *Compliance*: ISO 19600 y 37001

Los primeros estándares internacionales sobre *Compliance* surgen de sendas iniciativas de normalización en el seno de ISO durante año 2013: la primera, ISO 19600, sobre sistemas de gestión de *Compliance* (*Compliance Management Systems*, CMS), que adopta como referente de partida la norma australiana AS 3806; la segunda, ISO 37001, sobre sistemas de gestión anti-soborno (*Anti-Bribery Management Systems*, ABMS), que toma como base la norma británica BS 10500. Beneficiándose de estos antecedentes, se redactan los estándares internacionales con la participación de múltiples países e instituciones, conformándose en los referentes actuales en materia de *Compliance*. Este documento analiza los aspectos clave de su contenido.

8. El estándar nacional sobre *Compliance* penal: UNE 19601

La participación activa de España en la elaboración de los estándares internacionales ISO 19600 e ISO 37001 brindó acceso a conocimientos de primer nivel sobre sistemas de gestión de *Compliance*. Fruto de aquella experiencia, se creó un grupo *ad-hoc* en el seno de la Asociación Española de Normalización UNE para elaborar un estándar nacional que diese cobertura a los requisitos establecidos en el Código

penal sobre sistemas de organización y gestión para la prevención de delitos. En este documento se aborda de manera sistemática aspectos clave del estándar oficial español sobre *Compliance* penal.

9. Elementos representativos de la cultura de *Compliance*

La generación, mantenimiento o mejora de una cultura ética y de respeto a la Ley es el objetivo último de un programa o sistema de gestión de *Compliance*. Aunque hay quien considera que la cultura ética es un elemento difícilmente constatable y medible, existen multitud de aspectos que muestran su existencia. Vemos estos elementos en las diferentes etapas de creación, operación y mejora del sistema de gestión de *Compliance*, dejando en su mayor parte evidencias que son constatables por terceros independientes. Este documento señala algunos de estos elementos, vinculando algunos de ellos a magnitudes económicas perfectamente trazables.

10. Integraciones horizontales y verticales en *Compliance*

La eventual existencia de sistemas de gestión de *Compliance* sobre ámbitos específicos permite su integración en superestructuras de *Compliance*. No obstante, la proliferación de sistemas de gestión puede derivar en modelos difíciles de establecer y operar en entornos de recursos limitados. En estos contextos, procede analizar la posibilidad de integrar ámbitos de *Compliance* bajo un mismo sistema de gestión de manera tanto horizontal (por bloques de normas o dominios) como vertical (a través de la coordinación de diferentes bloques o dominios). En este documento se tratan diferentes experiencias al respecto, de especial interés para PYMES.

11. Factores de independencia de la función de *Compliance*

La efectividad de los modelos de *Compliance* se asocia a la autonomía e independencia de la función de *Compliance*. La autonomía guarda relación con la capacidad de operar por iniciativa propia, sin necesidad de ser mandatada y con capacidad para acceder a las personas e información relevante para sus cometidos. La independencia se vincula a la neutralidad en la toma de decisiones, estando en disposición de sugerir las acciones más adecuadas para la organización, sin miedo a represalias. Este documento analiza diferentes maneras de procurar esa independencia así como de amenazarla, comprometiendo en tal caso el recto proceder de la función de *Compliance*.

12. Key *Compliance* Indicators (KCIs)

Los KCIs son el resultado de aplicar KPIs (*Key Performance Indicators)* y KRIs (*Key Risk Indicators*), ya que ambos deben concurrir en un sistema de gestión de *Compliance*. Este documento abarca los diferentes KPIs, vinculados a las actividades planificadas de *Compliance*, así como los KRIs relacionados con la materialización de riesgos de *Compliance*; distinguiendo así entre elementos de medición de actividad y de eficacia.

Bibliografía del autor

Compliance Penal Normalizado – El estándar UNE 19601

Alain Casanovas

*Prólogo de **José Manuel Maza Martín***

Coedición: Thomson Reuters Aranzadi, AENOR Publicaciones.

Madrid 2017

Legal _Compliance_ - Principios de Cumplimiento Generalmente Aceptados

Alain Casanovas

*Prólogo de **José Manuel Maza**, Magistrado del Tribunal Supremo*

Editor, Grupo Difusión

Difusión Jurídica y Temas de Actualidad, S.A.

Madrid 2013

Control Legal Interno

Alain Casanovas

*Prólogo de **Pedro Mirosa**, Catedrático de Derecho Mercantil, ESADE, Factultad de Derecho*

Editor, Grupo Wolters Wluwer

Editorial La Ley, S.A.

Madrid 2012

Control de Riesgos Legales en la empresa

Alain Casanovas

*Prólogo de **Lord Daniel Brennan** Q.C., former President of the Bar of England and Wales*

Editor, Grupo Difusión

Difusión Jurídica y Temas de Actualidad, S.A.

Madrid 2008

Obra digital del autor

Cuadernos sobre Cumplimiento Legal
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2013

Casos sobre errores de *Compliance*
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2014

Tests de *Compliance*
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2015

Kits de despliegue de *Compliance*
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2016

Videos *Compliance* basics
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2017

Contacto

Alain Casanovas
Socio de KPMG Abogados
T: +34 93 253 29 22
E: acasanovas@kpmg.es

Perfil en
LinkedIn