Asociación Española de Compliance

Cuadernos de Compliance

Sistemas de gestión de Compliance

Alain Casanovas

04

www.asociacioncompliance.com

Instituto de Estudios de Compliance

Alain Casanovas

Abogado y miembro de la Junta Directiva de la Asociación Española de *Compliance* ASCOM, es socio responsable de los servicios de *Legal Compliance* en ***KPMG*** España. Experto acreditado y *Head of Spanish Delegation* en los *Project Committees* 271 y 278 de ISO que produjeron los estándares ISO 19600 sobre *Compliance Management Systems* e ISO 37001 sobre *Anti-Bribery Management Systems*. Coordinador y miembro del grupo de trabajo *ad-hoc* de la Asociación Española de Normalización UNE elaborador de la Norma UNE 19601 sobre sistemas de gestión de *Compliance* penal.

Codirector de los dos primeros Programas de postgrado de *Compliance* en España, en la Universidad Carlos III de Madrid y la Universitat Pompeu Fabra (UPF) de Barcelona. Codirector del Programa Enfocado del IESE sobre *Compliance*, Responsabilidad Social y Buen Gobierno. Director técnico de los congresos nacional e internacional de Compliance organizados por Thomson Reuters y ASCOM.

Presentación

Desde hace tiempo me defino como un estudioso de las normas del "cómo". Aunque no es una clasificación al uso, podemos distinguir entre las normas que indican ***qué*** debemos hacer (normas del "qué") y las que explican ***cómo*** conseguirlo ("normas del cómo"). Podríamos decir que las primeras son ***fáciles de producir***, bastante evidentes y estaríamos mayoritariamente de acuerdo con ellas. Así, por ejemplo, debemos pagar impuestos si deseamos el bienestar común, ser respetuosos con el medio ambiente y con las comunidades donde operamos, evitar conductas incorrectas por parte de las personas de nuestra organización o de quienes se relacionan con ella, y un larguísimo etcétera. ¿Quién se atreve a criticar estos objetivos de sentido común? La dificultad surge cuando nos preguntamos ***cómo*** lograrlos, especialmente en un entorno de negocio complejo, competitivo y globalizado. Es entonces cuando comienza la búsqueda de las normas del "como" y nos damos cuenta de que son escasas.

Conocer ***cómo ser diligente*** en procurar una ***conducta ética y de respeto a la Ley*** no es intrascendente cuando el volumen, complejidad y variabilidad de las normas aumenta a velocidad vertiginosa. En este contexto, son una valiosa ayuda las ***directrices*** y ***requisitos*** que emanan de organismos nacionales e internacionales de reconocido prestigio, señalando el ***modo razonable*** de actuar en un entorno tan difícil como este. Estos textos nos hablaron primero de los ***programas de Compliance***, para referirse después al concepto más moderno de *sistemas de gestión* ("*Compliance Management Systems" o CMS*). Se extraen de ellos los componentes fundamentales que voy a tratar en este Cuaderno, que te serán de utilidad para organizar y desarrollar eficazmente los cometidos de *Compliance*.

Alain Casanovas

Índice

1. Concepto de CMS.

De un tiempo a esta parte, el concepto de "***programa***" de *Compliance* se ha visto superado por el de "***sistema de gestión*** de *Compliance*". Aunque ambos configuran ***modelos*** basados en la concurrencia de una serie de principios y elementos para alcanzar determinados objetivos, los sistemas de gestión ponen énfasis en la ***interacción dinámica*** que debe concurrir entre ellos. Encontrarás más información sobre ello en el Cuaderno número 1 de esta Serie ("*¿Qué es Compliance?*").

Un sistema para la gestión del *Compliance* ("*Compliance Management System – CMS*") permite ***definir*** y ***alcanzar*** los objetivos de *Compliance* de una organización. Desde hace tiempo, ha dejado de ser un concepto ambiguo para estar perfectamente definido en ***estándares internacionales*** como la norma ISO 19600:2014 sobre *Compliance Management Systems* o la norma ISO 37001:2016 sobre *Anti-Bribery Management Systems*.

Quién normaliza los estándares

Normalmente, los Estados delegan la capacidad de ***normalizar*** sobre aspectos técnicos a ciertas entidades, que se encargan de establecer unos ***criterios*** y ***lenguaje de comunicación*** común a través de la producción de estándares. En España, es la *Asociación Española de Normalización* UNE la que tiene atribuidas dichas facultades, como sucede con la *Association Française de Normalisation* AFNOR en Francia, el *Deutsches Institut für Normung* DIN en Alemania, el *Ente Nazionale Italiano di Unificazione* UNI en Italia, el *American National Standards Institute* ANSI en los Estados Unidos, y un largo etcétera. Las entidades de normalización se agrupan en la *International Organization for Standardization* ISO, que es una ***organización no gubernamental independiente*** de la que actualmente forman parte 161 entidades de normalización nacionales.

Practicas reconocidas versus iniciativas no consolidadas

Los estándares de *Compliance*, tanto nacionales como internacionales, no pretenden necesariamente recopilar las prácticas más ***avanzadas***, sino las más ***reconocidas***, esto es, aquellas cuya efectividad esté ampliamente admitida. Puesto que uno de los objetivos de los estándares es procurar ***confianza*** en los mercados, su contenido debe ser ***fiable***. Esto excluye cualquier ensayo o aproximación no consolidadas, susceptibles de ser cuestionadas. De todos modos, las entidades de normalización formulan ***revisiones periódicas*** de sus estándares, para refinar su contenido e incorporar en ellos nuevos elementos de eficacia probada.

Sistemas de gestión genéricos y sistemas de gestión específicos

Puede hablarse de un sistema de gestión de *Compliance* de manera ***genérica*** (aplicable al conjunto de obligaciones que afectan a una organización), o de forma ***específica***, cuando se proyecta exclusivamente sobre algún tipo de obligaciones de *Compliance* en particular (prevención penal y del soborno, protección de la privacidad y de los datos personales, etc). El estándar ISO 19600:2014 es ***genérico*** (*Compliance* en general), mientras que el ISO 37001:2016 es ***específico*** (*Compliance* anti-soborno). La Norma UNE 19601:2017 es también un estándar ***específico***, ceñido a los modelos de organización y gestión requeridos en el Código penal Español.

El principio de proporcionalidad

La aplicación de los estándares modernos de *Compliance* no conduce a un único modelo de sistema de gestión. Existen múltiples formas de adaptar sus directrices y requisitos, dando lugar a modelos muy variados que se adaptan a las particularidades de cada organización. De hecho, en la mayoría de estándares se reconoce el ***principio de proporcionalidad***: de cada organización cabe esperar un modelo de *Compliance* adecuado a sus ***circunstancias***. Evidentemente, los sistemas de gestión en grandes organizaciones precisarán más recursos y requerirán mayores formalidades que en las pequeñas, pero en ambos casos se cubrirán una serie de ***componentes esenciales***.

Paradójicamente, existen organizaciones pequeñas y medianas que, por la ***naturaleza de sus operaciones*** o por los ***mercados*** en que operan, precisarán modelos de *Compliance* especialmente robustos. Por lo tanto, cuando se habla de las ***circunstancias*** de la

organización no sólo cabe considerar las ***internas*** (cifra de negocios, número de empleados, etc.) sino también las ***externas*** (mercados geográficos o sectores en los que actúa, marco regulatorio, etc.). La aplicación correcta del ***principio de proporcionalidad*** atraviesa por considerar ambos grupos de circunstancias.

Obligación de los administradores

Corresponde a los administradores sociales impulsar un adecuado sistema de gestión de Compliance.

En cualquier caso, siendo los ***administradores*** quienes deben velar por la adecuada gestión de la organización, procurando mantener una conducta ética y de respeto a la Ley, a ellos corresponde ***impulsar*** un adecuado sistema de gestión de *Compliance*. Su ausencia, por lo tanto, puede interpretarse como una ***falta de diligencia*** y reportarles ***responsabilidad personal***, como explico en el Cuaderno número 9 de esta Serie ("*Responsabilidades personales en el ámbito del Compliance*").

2.

Marcos de referencia generalmente aceptados.

El Instituto de Auditores Públicos alemán (IDW) publicó en el año 2011 su estándar AssS 980, regulando el proceso de emisión de una opinión profesional sobre la ***razonabilidad de un sistema de gestión de Compliance*** (CMS). Para identificar los aspectos críticos a tales efectos, el IDW tomó en consideración una serie de textos y estándares aplicables en la esfera del *Compliance*: son los que se relacionan en dos tablas que forman parte de su apéndice 1, titulado "*Marcos CMS generalmente aceptados*". Este estándar alemán es un texto importante no sólo por la novedad que supuso y la calidad técnica de su contenido, sino porque también reconoció y relacionó una serie de documentos sobre *Compliance* con fuerte reconocimiento internacional, emitidos por instituciones de prestigio. Por eso, los calificó como marcos de referencia de *Compliance* "*generalmente aceptados*".

¿Qué es un marco de referencia generalmente aceptado?

En líneas generales, para que un texto sobre *Compliance* se califique como ***marco de referencia***, se precisa que su contenido sea lo suficientemente ***detallado*** para que dos o más profesionales lleguen a conclusiones análogas cuando lo aplican en la práctica (escaso margen de interpretación). El marco de referencia es ***generalmente aceptado*** cuando se ha elaborado por una entidad de prestigio, a través de un procedimiento regulado, transparente y participativo. Los estándares fruto de la ***normalización nacional e internacional*** (ISO) reúnen dichas características.

Estos ***marcos de referencia*** para organizar un CMS tanto pueden ser ***genéricos*** (aplicables a la vigilancia de cualquier bloque normativo o sobre el conjunto de ellos) como haber sido diseñados pensando en alguno en particular. Por eso, existen estándares tanto ***genéricos*** como ***específicos***, como reconocen las dos tablas del citado apéndice 1 del IDW AssS 980.

Los ***marcos de referencia*** o ***entornos*** de *Compliance*, tanto ***genéricos*** como ***específicos***, contienen indicaciones para el diseño y evaluación de sistemas de gestión de ***Compliance***, cuya aplicación práctica dará lugar a modelos muy ***variados*** pero ***coherentes*** en cuanto a directrices o requisitos.

Siete principios de Compliance generalmente aceptados

A través del estudio de los diferentes ***marcos de referencia generalmente aceptados*** en *Compliance*, el IDW observó que compartían muchas de sus aproximaciones y componentes. Es más, en ocasiones su contenido era sumamente parecido, aun siendo textos producidos en jurisdicciones alejadas, por equipos de trabajos diferentes y proyectados sobre sectores distintos. Por ello, puede decirse que existen una serie de ***principios*** de aparición recurrente en estos textos, cuyo conocimiento te ayudará a valorar si el modelo de tu empresa está alineado con ellos y, por lo tanto, si converge con las ***tendencias internacionales*** en materia de *Compliance*.

En los ***siete apartados siguientes*** trataré cada uno de estos principios y finalmente expondré algunas reflexiones acerca del modo de ***documentar*** un modelo de *Compliance* y la posibilidad de ***revisarlo***, ***certificarlo*** o ***auditarlo***. El orden de exposición es parejo a su tratamiento en la norma técnica IDW AssS 980.

3.

El “tone from the top”.

No es ninguna novedad que cualquier proyecto de cambio o mejora en el seno de las organizaciones precisa el ***apoyo*** de su ***órgano de gobierno*** y ***la máxima dirección*** para llegar a buen fin. Establecer, mantener o mejorar una ***cultura ética y de respeto a la Ley*** precisa de este soporte, que ha recibido muchas denominaciones: una de las más actuales es “*tone* ***from*** *the top*”, que se diferencia del tradicional “*tone* ***at*** *the top*”, por enfatizar que el compromiso del órgano de gobierno y de la alta dirección no sólo reside en su propia esfera, sino que desde ella debe también ***permeabilizar*** a toda la organización.

El “*tone from the top*”, es un factor ***clave*** para el desarrollo de una adecuada ***cultura*** empresarial. En el ámbito que nos ocupa, es muy difícil implantar CMS efectivos si la el órgano de gobierno y la máxima dirección no otorgan relevancia y muestran su ***firme compromiso*** con el *Compliance*. Por eso, no es de extrañar que los marcos de referencia generalmente aceptados no sólo reconozcan este elemento, sino que lo consideren ***una de las primeras cuestiones que deben evaluarse***. Sin esta afección, cualquier iniciativa de *Compliance* corre el riesgo de naufragar ante las primeras dificultades. Hallarás más información sobre ello en el Cuaderno número 6 de esta Serie (“*Cultura ética y de respeto a las normas*”).

Podría pensarse que contrastar ese nivel de compromiso con los objetivos de *Compliance* alberga gran subjetividad. Sin embargo, el personal de *Compliance* percibe claramente cuando existe “*tone from the top*” y cuando no. Tú mismo puedes examinar la actitud del órgano de gobierno y equipo directivo, valorando hasta qué punto perciben que es importante tú labor y observan una conducta respetuosa con la ética y la Ley. Un tercero externo también alcanzará una conclusión al respecto observando documentos organizativos que corroboren la importancia que le otorga al cumplimiento de las normas, y su ***soporte explícito*** al equipo de *Compliance*. El *“tone from the top*” deja siempre traza, en forma de hechos y documentos. El ojo educado las detecta fácilmente.

4.

Objetivos de cumplimiento y acciones organizativas.

Cuando concurre un adecuado "*tone from the top*", el compromiso del órgano de gobierno y de la máxima dirección con el *Compliance* se manifestará, entre otros aspectos, en ***objetivos*** a cubrir en esta faceta e impulso de las ***estructuras*** razonables que permitan alcanzarlos.

Objetivos de Compliance

Plantearse cuáles son los ***objetivos*** de *Compliance* es trascendente, porque determinarán las ***estructuras*** (órganos) y otros aspectos (políticas, procedimientos, etc) para lograrlos. Normalmente, los objetivos de *Compliance* atraviesan por una declaración general de ***tolerancia cero a los incumplimientos*** de normas, entendiendo por éstas tanto las que vienen ***impuestas*** ("*requirements*") como las ***asumidas voluntariamente*** ("*committments*"). Podríamos decir que se trata de un objetivo ***estratégico*** general, al que pueden sumarse otros, y que derivarán en objetivos ***tácticos*** u ***operativos***. Todos ellos vendrán condicionados el resultado de la ***evaluación de los riesgos de Compliance***. y las expectativas que tienen depositadas los grupos de interés en la organización. El efecto combinado de ambos factores condiciona la fijación de objetivos ambiciosos en mayor o en menor medida.

Estructuras organizativas

El dimensionado de las ***estructuras organizativas*** vendrá entonces determinado por lo objetivos de *Compliance* que la organización se ha propuesto alcanzar. Las que asumen desarrollar actividades potencialmente expuestas a ***riegos relevantes*** de *Compliance* precisarán medidas orgánicas acordes con ese nivel de exposición, mientras que las que renuncien a ellas podrán volcar menos esfuerzos, comparativamente hablando.

Superestructuras de Compliance

Puesto que pueden coexistir ***diferentes áreas y responsables de cumplimiento*** en una misma organización (responsable de privacidad y protección de datos, responsable de cumplimiento fiscal, responsable de cumplimiento regulatorio, etc), tiene sentido que se coordinen en un foro común, destinado a garantizar la aplicación ***uniforme*** y ***consistente*** de los principios de *Compliance* fijados por la organización en sus políticas: si ésta desea una aplicación ética y prudente de la normativa, los planteamientos fiscales agresivos estarán fuera de lugar, por ejemplo. ***Coordinando*** las diferentes áreas de cumplimiento se evitan este tipo de inconsistencias, se facilita que las iniciativas de alguna de las áreas beneficien también a las restantes, y se brinda una valiosa ***visión de conjunto*** al órgano de gobierno y la máxima dirección.

Por sus beneficios contrastados, cada vez son más frecuentes los modelos transversales de Compliance.

Por sus beneficios contrastados, cada vez son más frecuentes los ***modelos transversales de Compliance*** (también llamados "*superestructuras de Compliance*") dirigidos por "*Compliance Committes*", "*Compliace Steering Groups*" u otros órganos colegiados análogos. Lo que pretenden, en resumen, es ***aglutinar*** y ***coordinar*** las diferentes áreas de cumplimiento para coordinarlas y obtener sinergias. Alguno de sus integrantes adquiere un rol de dirección, constituyéndose en Presidente del órgano o *Chief Compliance Officer* –figura que adquiere sentido cuando ya existen *Compliance Officers* responsables de áreas específicas-.

El ***órgano de Compliance*** establecido al efecto comprobará, entre otras cosas, que existan y se difundan los ***parámetros de conducta*** que deben observar las personas de la organización o incluso los terceros que se vinculan con ella, para ayudarles a prevenir, detectar o gestionar del mejor modo posible los riesgos de *Compliance* que afectan a las diferentes áreas. Esto se construye a través de ***políticas*** y ***procedimientos***, según explico en el Cuaderno número 7 de esta Serie ("*Árbol de políticas de Compliance*").

Aquellos cometidos que los principales estándares atribuyen al *Compliance Officer* se hallan resumidos en el conocido *Libro Blanco sobre la función de Compliance*, elaborado por la Asociación Española de *Compliance*.

5.

La evaluación del riesgo.

Por mucho que existan estructuras organizativas de *Compliance*, poca será su eficacia si no se proyectan sobre los ***riegos*** que verdaderamente amenazan a la organización. La puesta en marcha de un sistema de gestión de *Compliance* (CMS) y creación de estructuras organizativas, políticas y procedimientos sólo tiene sentido si se han determinado qué riesgos deben ser prevenidos detectados y gestionados. Por eso, el desarrollo de una ***evaluación de riesgos*** ("*risk assessment*") es un ejercicio clave para orientar y dimensionar el CMS. Sin embargo, no sólo debe realizarse en la etapa inicial de diseño, sino periódicamente para garantizar que el CMS sigue siendo adecuado a las cambiantes ***circunstancias internas*** y ***externas*** de la organización.

Las buenas prácticas abogan por inventariar primero los ***bloques de normas*** que afectan a la organización para, luego, identificar las conductas de riesgo asociadas con cada uno de ellos. En este sentido, la evaluación de riesgos de *Compliance* atraviesa por ***dos etapas***, que transcurren desde una visión ***general*** (bloques de obligaciones de *Compliance*) a una ***específica*** (casuísticas de riesgo en cada bloque). Normalmente, los riesgos de *Compliance* terminan categorizados por ***probabilidad*** de ocurrencia y ***consecuencias*** en tal caso, lo que permite ilustrarlos gráficamente en un esquema de coordenadas cartesianas positivas. En ocasiones, se recurre al concepto de "***gravedad***" o "***severidad***", que es el resultado agregado de los dos factores anteriores, facilitando así priorizar los riesgos evaluados.

Hecho lo anterior, se considera una buena práctica identificar tanto los ***procesos o actividades***, como los ***colectivos*** de personas próximas a los riesgos detectados (incluyendo colaboradores externos), para asegurar que se proyectan sobre ellos medidas de supervisión y control adecuadas.

6. Controles de Compliance.

Es importante que comprendas la necesidad de mantener el ***binomio políticas/controles*** para dotar de ***eficacia*** a tu sistema de gestión de *Compliance* (CMS). Las políticas de empresa, desde la más alta (p.e. el Código Ético) hasta la más específica (p.e. Política sobre uso de los recursos informáticos) determinan ***patrones de conducta*** para quienes se vinculan con la organización. La existencia de estos patrones es ***necesaria*** pero ***no suficiente***: no basta con la difusión interna de estas normas para garantizar su aplicación ***uniforme*** y ***consistente***. Los parámetros de conducta meramente formulados pueden convertirse en papel mojado en ausencia de ***controles*** que velen por su correcta aplicación, y sean capaces de desencadenar ***acciones de remediación*** en aquellos casos que donde se precisen.

Los ***controles***, por sí solos, tampoco están justificados cuando no derivan de ***políticas*** que los amparen. En este sentido, las políticas evitan que los controles se perciban como una supervisión innecesaria o arbitraria. Por ello, el ***binomio políticas-controles*** es algo que deberás tener siempre presente, pues ambos conceptos se dotan de ***sentido recíproco***.

Sobre la base de lo anterior, trata de que tu organización esté ***equilibrada*** en cuanto a ***políticas*** y ***controles***. Es frecuente que las empresas establezcan políticas, las difundan entre sus empleados y socios de negocio, y que incluso pidan una ***declaración de conformidad*** con su contenido. Aunque constituye una buena práctica, sólo con ello no se garantiza su observancia ni supone, *per se*, una medida para detectar desviaciones. Se precisa dar un paso más y establecer ***controles de Compliance***.

No existen los controles infalibles: cuando concurren empleados o socios de negocio resueltos a vulnerarlos, es posible que finalmente lo consigan, eventualidad contra la cual sólo cabrían medidas de prevención más allá de lo razonable en el ámbito empresarial. Además, los controles pueden fallar debido a ***sus propios límites***: por ejemplo, cuando dependen del juicio humano, sujeto a error. Sin embargo, aunque los controles ***no garantizan la seguridad***

absoluta, sí que permiten alcanzar un nivel de ***seguridad razonable*** en cuanto a los parámetros conductuales establecidos, desde luego por encima de la esperable mediante la simple emisión de políticas.

Controles de alto nivel y específicos

Cabe distinguir entre ***controles de alto nivel*** y ***controles específicos***. Los primeros suelen asociarse a políticas de alto nivel (un Código Ético, por ejemplo) y tienen un ***amplio espectro*** en cuanto a cobertura de conductas, mientras que los segundos se vinculan a políticas concretas y vigilan ***ciertas conductas en particular***. Un canal de denuncias vinculado al Código Ético ("*whistleblowing line*") es, por ejemplo, un control de ***alto nivel***, pues a través de él se pueden reportar irregularidades muy variadas. Sin embargo, una revisión periódica del proceso de selección y adjudicación de contrataciones, destinado a vigilar la aplicación razonable de la política de compras, es un ***control específico*** que normalmente centrará su atención en evitar conductas antieconómicas, fraudulentas o corruptas.

Una "whistle-blowing line" es un control de alto nivel, donde se pueden reportar irregularidades muy variadas.

Entre los controles de ***alto nivel*** y los ***específicos*** debería darse cobertura a los bloques normativos y casuísticas de ***riesgo*** surgidas de la ***evaluación de riesgos de Compliance***. Vemos como los elementos que integran el CMS presentan un nivel elevado de interacción.

Controles financieros y no financieros

Muchos marcos de referencia en *Compliance* distinguen también entre los ***controles financieros*** y los ***no financieros***. Los primeros se proyectan sobre ***flujos económicos*** y dotan de seguridad a la información financiera (la segregación de funciones, por ejemplo), mientras que los segundos se aplican a otros procesos (política de compras a través de una mesa debidamente estructurada, por ejemplo).

Controles preventivos y detectivos

Es también común la distinción entre ***controles preventivos*** y ***detectivos***. Los primeros previenen la materialización del riesgo de *Compliance*, mientras que los segundos la detectan. Son habituales, por ejemplo, los ***manuales de instrucciones*** que ayudan al personal a comportarse dentro de unos parámetros de conducta deseados. En este sentido, por ejemplo, un ***manual*** de actuación ante solicitudes de datos personales constituye un ***control preventivo***. El desarrollo de "revisiones internas de *Compliance*", donde la función comprueba directamente la aplicación uniforme y consistente de sus directrices es, sin embargo, un ***control detectivo***.

Controles automatizados y manuales

También es muy frecuente la distinción entre controles ***automatizados*** y ***manuales***, normalmente para otorgar un mayor grado de fiabilidad a los primeros, especialmente cuando su ***frecuencia*** de aplicación es también mayor.

7.

Reportes de Compliance.

Puesto que la organización ha establecido sus ***objetivos de Compliance***, es razonable esperar que se interese por conocer si se están alcanzando y las incidencias que surgen en dicho camino. Por ello, es difícil justificar la ausencia de reportes internos de *Compliance* en aquellas organizaciones verdaderamente comprometidas con la ética y el cumplimiento de la Ley.

Aunque dedico el Cuaderno número 8 de esta Serie ("*La cadena de reporte en Compliance*") a explicar el modo en que se monitorizan los objetivos de *Compliance*, sí interesa ahora anticipar el sentido de los ***flujos de la información relevante*** y cómo pueden terminar impactando en los grupos de interés de la organización.

Información de uso interno, y de uso externo

Existen informaciones relacionadas con el *Compliance* que son ***trascendentes*** para terceros, dado que pueden fundamentar sus decisiones atendiendo a datos que constan en los reportes públicos. Es el caso de inversores, bancos o las propias autoridades públicas. Por lo tanto, posiblemente manejarás informaciones con capacidad no sólo de afectar a la organización sino también a estos y otros terceros. Por eso, no es en absoluto prudente minusvalorar la información de *Compliance*, que deberá estar sujeta a unos ***flujos controlados*** y adecuadamente ***supervisados***, que eviten ***perjudicar*** a la ***propia organización*** y también a ***terceros***.

Obtención de información de calidad

Maneja siempre ***información de calidad***. Es la información que se obtiene a través de los diferentes procedimientos y que se reporta periódicamente, como explico en el Cuaderno número 8 de esta

Serie ("*La cadena de reporte en Compliance*"). Aunque se puede escribir mucho acerca de lo que es "información de calidad", aplica un criterio análogo al que esperarías respecto de la información financiera: ¿sería información financiera de calidad la obtenida a través de conversaciones de café con los responsables de las operaciones? Del mismo modo que existen ***procedimientos*** y ***herramientas*** para capturar la información económica que ridiculizan el enunciado de la pregunta, también deben concurrir respecto de la información de *Compliance*.

Un reporte de *Compliance* no basado en procedimientos y herramientas definidas al efecto corre el riesgo de ***degradarse*** con el transcurso del tiempo, ***erosionando*** su ***objetividad*** y ***perjudicando*** su ***eficacia***. Tales circunstancias son especialmente peligrosas cuando terminan afectando no solo a la organización sino también a sus grupos de interés.

8.

Planes de acción.

Consecuencia lógica de los reportes de *Compliance* son los ***planes de acción***: no se concibe que se detecten ***irregularidades*** o ***aspectos susceptibles de mejora*** sin que inmediatamente se planifiquen y ejecuten las medidas apropiadas.

Los planes de acción suelen adjuntarse o referirse en los ***reportes*** de *Compliance*, de forma que no sólo se exponen los incidentes detectados sino también las acciones sugeridas para tratarlos, incluyendo hitos a cubrir, responsables de su ejecución y plazos. Encontrarás más información al respecto en el Cuaderno nº 8 de esta Serie ("*La cadena de reporte en Compliance*").

Los planes de acción no sólo deben contemplar las actividades adecuadas para evitar o mitigar irregularidades, sino también (i) las medidas que se adoptarán para ***evitar que se reproduzcan***, y (ii) las ***consecuencias*** que de derivarán para las personas de la organización o sus colaboradores que las han ocasionado.

Evidentemente, forma parte de las competencias de *Compliance* y del contenido de los reportes en su ámbito, ***monitorizar*** la correcta ***ejecución*** de los planes de acción y proponer las correcciones oportunas cuando no logren su propósito.

9. La monitorización.

El término "*monitoring*" se suele traducir con los anglicismos "monitorizar" (Español) o "monitorear" (Español internacional). Son términos muy extendidos en la literatura y marcos de referencia de control interno y de *Compliance*.

En el contexto que ahora nos ocupa, monitorizar significa, en esencia, ***vigilar*** que las capacidades del modelo de *Compliance* no mermen por el transcurso del tiempo o debido al cambio de las circunstancias de la organización, tanto de internas como externas. Es más, a través de la monitorización del modelo de *Compliance* se intenta que ***mejore*** según la experiencia acumulada, y vaya así cubriendo las fisuras que se identifiquen sucesivamente en búsqueda de la excelencia.

Monitorización programada y sobrevenida

La monitorización se puede desarrollar de manera ***programada*** o ***sobrevenida***. La ***programada*** supone una revisión periódica que se desarrolla aunque no concurran situaciones excepcionales: simplemente para verificar que el modelo sigue siendo adecuado a las circunstancias de la organización y estado del arte en su ámbito. La ***sobrevenida*** concurre ante un cambio de circunstancias, tanto internas como externas, o frente a la materialización de un incidente de *Compliance* que obliga a replantearse el modelo. Ambos tipos de revisiones deben estar previstas y reguladas en el CMS.

Monitorización continua

Las buenas prácticas abogan por la ***monitorización continua***, de forma que las capacidades del modelo se evalúen constantemente sin esperar hitos específicos, actualizando y reforzando el sistema de gestión tan pronto se tiene ocasión. En este sentido, los reportes

operativos de *Compliance* constituyen una buena oportunidad para desarrollar ese "*monitoring*", en el sentido de corroborar la robustez de los ***controles*** que han permitido prevenir o detectar un incidente, o valorar aquellos otros ***que deben implantarse*** o que ***no han funcionado correctamente***, aflorando, en ambos casos, debilidades del modelo que inducen a la reflexión sobre cómo erradicarlas.

Monitorización interna, externa y mixta

Salvo que exista mandato legal al respecto, la monitorización del modelo de *Compliance* no tiene por qué desarrollarse externamente, pudiendo ejecutarse internamente, siempre que se dispongan de recursos para ello y se salvaguarde la ***independencia*** del revisor. Cabe también la posibilidad de que sea encomendada a profesionales externos (igualmente desvinculados del diseño y operación del modelo) o constituir un equipo mixto (interno/externo) a tales efectos.

10.

Documentación del modelo.

Documentar adecuadamente el sistema de gestión de *Compliance* no es una mera cuestión formal, sino algo necesario para evitar que se degrade, demostrar su existencia y poder llegar a certificarlo o auditarlo.

Todos los elementos que hemos tratado en este Cuaderno deberían hallarse soportados documentalmente. Los estándares ISO sobre *Compliance* recurren para ello al concepto de "información documentada" que no sólo cubre aquella que guarda relación con la ***descripción del sistema de gestión***, sino también con su ***implementación*** y ***ejecución*** práctica. De ahí la importancia de no sólo documentar el modelo, sino también las diferentes actividades y decisiones que de él se derivan.

Documentar el modelo y el resultado de su aplicación permite constatar su existencia, aunque cuestión distinta será valorar su ***razonabilidad*** y ***eficacia***.

Puesto que la aplicación de principios de *Compliance* generalmente aceptados puede producir modelos muy variados, adecuados a cada perfil de organización, se darán también ***múltiples formas de documentarlos***, sin que exista un único patrón al respecto. Ahora bien, al elaborar o analizar dicha documentación deberá ponerse especial cuidado en que refleje tanto los principios relacionados en este Cuaderno, como evidencias inequívocas de su aplicación práctica.

En cualquier caso, la documentación del modelo y de su implementación real son ***condiciones necesarias*** si deseamos revisarlo, certificarlo o auditarlo por un tercero independiente, que aplicará el ***principio de escepticismo profesional*** y cuestionará toda manifestación carente de soporte documental.

11.

Certificación o auditoría del modelo.

Puesto que tanto la inexistencia, la inadecuación o la defectuosa ejecución de un sistema de gestión de *Compliance* puede reportar daños a la organización y terceros, es lógico que se busque cierto confort a través de la ***opinión de un tercero independiente*** sobre la razonabilidad de su ***diseño***, el adecuado ***nivel de implementación*** y su ***eficacia***. Además, la revisión del modelo de *Compliance* por un externo ***cualificado*** constituye una valiosa palanca de mejora.

Desde otra perspectiva, el ***órgano de gobierno*** también tendrá interés en acreditar su ***diligencia*** en la implantación y ejecución de un modelo de *Compliance* a través de la opinión de un tercero independiente. Encontrarás más comentarios acerca de la ***responsabilidad personal*** tanto de los administradores como del propio *Compliance Officer* el Cuaderno número 9 de esta Serie (“*Responsabilidades personales en el ámbito del Compliance*”).

A efectos de dicha revisión, comprueba si se realizará por comparación con algún ***estándar reconocido internacionalmente***, así como los ***criterios y metodología de revisión*** que el tercero independiente aplicará en su trabajo (estándar de revisión). Ambos aspectos son ***muy importantes*** para poner en valor la revisión efectuada y dotarla de la ***mayor robustez posible***.

Evita las revisiones realizadas sin referencia a un patrón claro de CMS y/o utilizando metodologías de verificación singulares, pues su valor puede ser ***fácilmente cuestionado*** por terceros.

12.

Preguntas frecuentes.

¿Figuran relacionados en algún lugar los textos que se consideran marcos de referencia generalmente aceptados en Compliance?

Podemos encontrar una relación de marcos de referencia generalmente aceptados en el ámbito del *Compliance* en el estándar de auditoría AssS 980 emitido por el Instituto alemán de Auditores públicos (IDW) en el año 2011. Su apéndice 1 incluye dos tablas enunciativas pero no limitativas: una de marcos ***genéricos*** y otra de marcos ***específicos***, a los que considera generalmente aceptados. Aunque esta relación inicial no está actualizada, son textos de conocimiento obligado para cualquier profesional vinculado con el *Compliance*.

¿Qué puedo hacer si no percibo el "tone from the top" en mi organización?

El ***compromiso*** del órgano de gobierno y la máxima dirección en cuanto a los objetivos de *Compliance* es un factor esencial no sólo para alcanzarlos sino también para tu ***evolución profesional***. Puedes tratar de transmitir su importancia directamente o a través de terceros expertos, que, seguramente, aportarán argumentos y experiencias comparativas de utilidad. Pero si no vislumbras que adquirir conciencia de la importancia del *Compliance* es una eventualidad remota, tendrás que plantearte seriamente si te encuentras en la ***organización adecuada*** para tu ***desarrollo profesional***.

Para asegurar el cumplimiento de las normas en la organización, ¿es mejor designar un órgano individual o colegiado?

Si estas en una organización con cierta diversidad en cuanto a ***bloques normativos aplicables***, lo más efectivo será pensar en un órgano colegiado que integre a sus diferentes responsables, coordinado por un Presidente o por el *Chief Compliance Officer* (CCO). Pero en organizaciones medianas y pequeñas, tal vez no tengas esta posibilidad ni sea necesaria, especialmente en casos de poca complejidad del entorno normativo de aplicación.

¿Puedo desarrollar yo mismo la evaluación de riesgos de Compliance?

En ningún lugar consta que dicha tarea deba necesariamente encomendarse a profesionales externos. Ahora bien, en modelos de *Compliance* ***transversales***, es importante que el "*risk assesment*" cubra ***todos los bloques de normas*** que afectan a la organización, y es difícil que una sola persona o un equipo reducido disponga de los conocimientos precisos para ello. Por eso, normalmente, este ejercicio lo realizarán equipos mixtos integrados por personal cualificado de la organización junto con expertos externos de algunas áreas específicas. Si en tu organización dispones de personas con los conocimientos y experiencia necesarios, podrás desarrollar este cometido junto con ellos. En caso contrario, mejor auxíliate con profesionales externos.

¿Se necesita que los empleados firmen todas las políticas de la empresa?

La organización debe cuidarse de difundir sus políticas, de manera que sean conocidas por todos aquellos a quienes afectan (sean o no empleados). Es una buena práctica no sólo difundirlas sino ***dejar constancia de su conocimiento e incluso aceptación***, mediante su firma física o a través de otras evidencias digitales. Algunas normas y estándares exigen este procedimiento para ***personas que ocupan posiciones especialmente expuestas*** (vinculadas a procesos que entrañan riesgos de *Compliance* superiores a bajo). Para el resto de supuestos, suele ser suficiente su entrega y puesta a disposición. Es frecuente establecer "*welcome packs*" para nuevos empleados, que contienen el conjunto de documentos esenciales que aquellos precisan conocer, y que normalmente suscriben con su incorporación.

Los reportes informales suelen degradarse con el transcurso del tiempo.

¿Se puede considerar adecuado el reporte verbal periódico en materia de Compliance?

Los inconvenientes de los ***procedimientos informales***, como un reporte verbal periódico, es que suelen degradarse con el transcurso del tiempo, y resulta difícil tanto su consulta como verificar su correcto desarrollo. Desde luego, un tercero independiente verá con ojos críticos este tipo de reportes, de los que puede cuestionarse no sólo su ***utilidad*** sino su ***propia existencia***. Además, si las materias así tratadas pueden afectar significativamente a la organización o a sus *stakeholders*, la ausencia de soporte documental adquiere tintes de negligencia grave.

Los planes de acción frente incumplimientos, ¿deben reportar medidas disciplinarias a los empleados que los ocasionaron?

No es admisible la ***pasividad*** frente al incumplimiento. Además de los corregir este tipo de situaciones, se deben estudiar medidas en el orden ***laboral*** (empleados) y ***mercantil*** (externos) ***proporcionales*** a la magnitud de la irregularidad, y amparadas por la normativa que resulte de aplicación. En cualquier caso, es una buena práctica prever medidas en el ámbito de los Recursos Humanos que no sólo ***penalicen*** las conductas de incumplimiento sino que ***premien*** las conductas correctas.

El hecho de que se produzca un incumplimiento, ¿es prueba de la inadecuación del CMS?

Un incumplimiento lo único que evidencia es lo obvio: que el sistema de gestión ha fallado ante unas circunstancias concretas. Pero esto no significa necesariamente que el CMS sea inadecuado en su conjunto. De hecho, los marcos de referencia sobre *Compliance* suelen recurrir al principio de ***seguridad razonable***, en contraposición al de ***seguridad absoluta***, partiendo de la base de ***que no existen sistemas de gestión infalibles***. Ahora bien, ante un incumplimiento se tendrán que evaluar ***sus causas*** y determinar por qué no pudo prevenirse, detectarse o gestionarse a tiempo, modificando el CMS para que la situación no se reproduzca. No puede admitirse esta ausencia de análisis o que se ***repitan*** irregularidades de la misma naturaleza, pues todo ello sí delata a la inadecuación del CMS o ***negligencia*** en su gestión.

¿Se salvaguarda la responsabilidad de la organización y sus responsables disponiendo de un documento descriptivo del CMS?

El calificativo "*effective*", de aparición recurrente en bastantes textos internacionales sobre *Compliance*, no es en absoluto casual. Y es que un sistema de gestión de Compliance ***no supone un mero planteamiento formal***, sino un conjunto de elementos que deben funcionar para disminuir la probabilidad de incumplimientos o reducir sus consecuencias, y que ***dejan traza de su puesta en práctica***. Se equivocan completamente las organizaciones que disponen de un CMS ***puramente formal***, pues es relativamente fácil demostrar que es una medida cosmética, que poco o nada contribuye a prevenir, detectar o gestionar los riesgos de *Compliance*. En estos casos, no cabrá esperar que mitigue la responsabilidad de la organización y de sus administradores, sino más bien lo contrario.

Serie de Cuadernos Compliance

Cuaderno 1

¿Qué es *Compliance*?

El contenido de la función de *Compliance* ha evolucionado en los últimos años, de la mano de estándares internacionales y textos emitidos por reputadas autoridades nacionales. En la actualidad, se encuentran claramente definidas las expectativas que la sociedad deposita en la función de *Compliance* y en los responsables que la representan.

Cuaderno 2

Conoce tu organización

La función de *Compliance* no actúa en paralelo a los procesos de negocio sino que forma parte de ellos. Por lo tanto, conocer la organización, no sólo desde la perspectiva societaria sino especialmente en cuanto a sus estructuras, roles, responsabilidades y procesos de negocio, es fundamental para desarrollar razonablemente labores de prevención, detección y gestión de riesgos de incumplimiento. Conocer funciones sinérgicas y tender puentes con ellas es clave en todo modelo eficaz de *Compliance*.

Cuaderno 3

Relación de *Compliance* con Gobernanza y Gestión de riesgo

La función de *Compliance* está condicionada por aspectos relacionados con la Gobernanza y la Gestión del riesgo. Sus interacciones son tan importantes, que los modelos de gestión empresarial modernos establece su gestión coordinada: son las fórmulas GRC (*Governance, Risk Management and Compliance*). Su interrelación es tal, que incluso se utilizan aplicativos diseñados para asegurar la consistencia en su tratamiento.

Cuaderno 4

Sistemas de gestión de *Compliance*

En los últimos años, los denominados “Programas de *Compliance*” se han visto sobrepasados por los “Sistemas de Gestión de *Compliance*”, que suponen un salto evolutivo en la prevención, detección y gestión de riesgos de incumplimiento. Los exponentes más conocidos son los estándares ISO 19600:2014 sobe *Compliance Management Systems* (CMS) e ISO 37001:2016 sobre *Anti Bribery Management Systems* (ABMS). En España destaca la Norma UNE 19601:2017 sobre sistemas de gestión de *Compliance* penal. Estos modelos descansan en una serie de componentes clave que se retroalimentan, mejorando notablemente la efectividad del modelo.

Cuaderno 5

Autonomía e independencia en *Compliance*

Autonomía e independencia no son términos sinónimos en *Compliance*, y su concurrencia es clave para la eficacia de la función. Ambos conceptos se traducen en una serie de buenas prácticas que impulsan las organizaciones comprometidas con una gestión responsable. El perfil profesional del propio *Compliance Officer* es igualmente importante para que pueda sacar el máximo partido a ambos factores.

Cuaderno 6

Cultura ética y de respeto a las normas

El objetivo último de la función de *Compliance* es establecer o mejorar la cultura ética y de respeto hacia las normas. La vinculación entre ética y *Compliance* es indisociable, hasta el punto de engendrar una figura híbrida en pujanza: el *Chief Ehics & Compliance Officer*. Los estándares avanzados en *Compliance* incluyen dentro de su perímetro de supervisión las normas asumidas voluntariamente por las organizaciones, dando entrada por esa vía al control sobre los compromisos éticos.

Cuaderno 7

Árbol de políticas de *Compliance*

El establecimiento o mejora de la cultura ética y de respeto a las normas precisa facilitar directrices de conducta a los miembros de la organización. Este cometido se logra a través de las políticas internas, que conforman un entramado complejo de patrones de conducta y procedimientos para encauzarlos adecuadamente. Esta red obedece a una estructura jerárquica –de árbol- que comienza con valores públicamente asumidos por la organización, y que debe conocerse y gestionarse correctamente (*policy management*).

Cuaderno 8

La cadena de reporte en *Compliance*

Dentro de los cometidos que desarrolla la función de *Compliance* se cuenta informar a los órganos correspondientes del resultado de sus labores de supervisión, tanto en términos de actividad desarrollada como de resultados obtenidos. Esta dinámica da lugar a reportes operativos y memorias anuales de *Compliance*, susceptibles de condicionar la información que hace pública la organización. Para nutrir estos reportes se precisa obtener y gestionar información interna de calidad, canalizada a través de procedimientos diseñados con tal propósito.

Cuaderno 9

Responsabilidades personales en el ámbito del *Compliance*

La falta de impulso o desarrollo inadecuado de labores de *Compliance* puede acarrear consecuencias relevantes en términos de responsabilidad personal de los administradores sociales, pero también del propio *Compliance Officer*, como han puesto de manifiesto pronunciamientos jurisprudenciales pioneros en esta materia.

Cuaderno 10

Compliance en el ámbito de la prevención de delitos

Existen determinadas conductas irregulares que pueden adquirir dimensión penal, siendo la actividad empresarial un entorno propicio de ocurrencia. El caso más habitual son las prácticas de soborno, ampliamente proscritas a nivel internacional. Tanto los Estados como las principales plataformas internacionales impulsan modelos de *Compliance* en los ámbitos de la prevención de los delitos, en general, o del soborno, en particular.

Cuaderno 11

Resistencia al cambio y conductas obstructivas

Impulsar modelos de *Compliance* efectivos puede suponer introducir en las organizaciones una serie de cambios que no siempre serán bien acogidos por quienes se ven afectados por ellos. La psicología social ha estudiado el comportamiento humano, determinando factores que corrompen la conducta de las personas en las organizaciones, así como su resistencia al cambio y desarrollo de conductas obstructivas.

Cuaderno 12

Compliance en pequeñas organizaciones

Las pequeñas y medianas organizaciones (*Small and Medium Enterprises*, SME) disponen una cantidad limitada de recursos para impulsar modelos efectivos de *Compliance*. Esto se traduce en la necesidad de adaptar las buenas prácticas a sus circunstancias específicas, lo cual no implica limitarse a observar sólo una parte de ellas, sino el conjunto aplicando correctamente el principio de proporcionalidad.

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

Asociación
Española
de Compliance