CURSO DE ESPECIALIZACIÓN

COMPLIANCE OFFICER DE EMPRESA Y CONTROL INTERNO

MANUAL

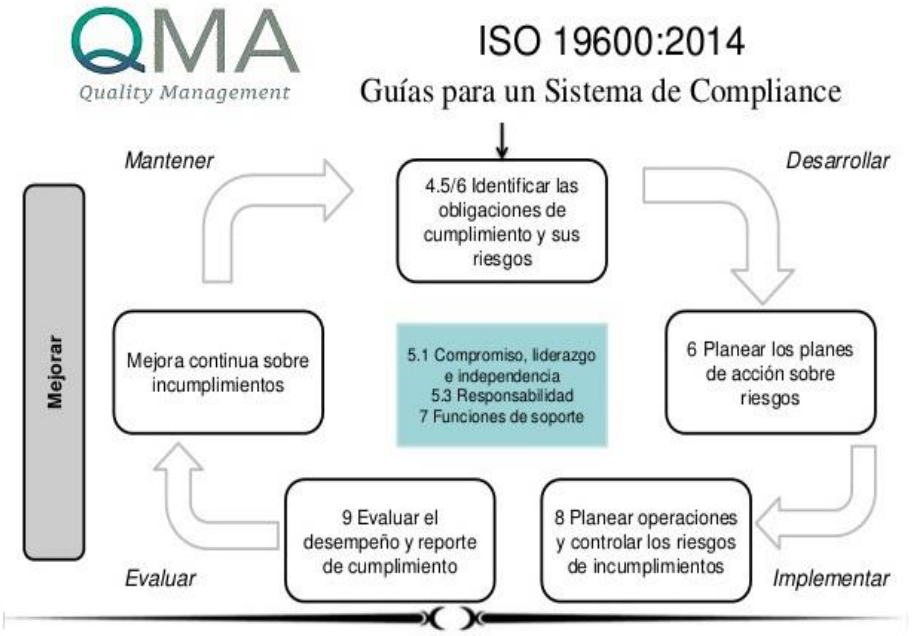
MÓDULO I

INTRODUCTORIO: UNA VISIÓN DEL BOSQUE

INTRODUCCIÓN

«El riesgo de Compliance es el riesgo de que una organización pueda sufrir sanciones, multas, pérdidas financieras o pérdida de su reputación como resultado del incumplimientos de las leyes, regulaciones, normas de autorregulación o códigos de conducta que se apliquen a su actividad» *Compliance and the Compliance function in Banks.* Comité de Supervisión Bancaria de Basilea, 2005.

La responsabilidad penal de las personas jurídicas se introdujo por primera vez en España en diciembre de 2010. Posteriormente, en 2012 se amplió para incluir también a partidos políticos y sindicatos. Y, finalmente, en julio de 2015 entró en vigor el nuevo Código Penal que concretaba más esta figura y recogía la exención de responsabilidad penal para aquellas empresas o entidades en cuyo seno se hubieran adoptado las medidas necesarias para impedir la comisión de delitos.



El Compliance Program o Programa de Cumplimiento Normativo es un dispositivo interno que las empresas implementan para cumplir con la normativa vigente, así como para prevenir y detectar las infracciones legales que se produzcan dentro de las mismas o como parte de las actividades que estas realizan.

A mediados de la década de 1970, diversas empresas estadounidenses y trasnacionales comenzaron a adoptar *Compliance Programs* con la finalidad de evitar y detectar infracciones legales, sobre todo las relacionadas con la libre competencia y antimonopolio (*antitrust*) y actos de corrupción (*bribery laws*). Así, el *Compliance* tiene su origen en la necesidad de las empresas de evitar la comisión de infracciones legales como consecuencia de las actividades que llevan a cabo en el mercado.

Es conocido que con el desarrollo de las distintas actividades económicas, de los avances tecnológicos y científicos, entre otros, se generan nuevos riesgos para la sociedad en su conjunto. Estos riesgos, consecuencia del desarrollo económico y tecnológico, son producidos por la actividad humana, individual o colectiva, por lo que, en principio, son controlables o susceptibles de ser disminuidos.

El derecho, a través de sus diferentes áreas, entra a regular diversas situaciones riesgosas para la sociedad, con la finalidad de mitigar, reducir y prevenir tales situaciones.

La especialización en los trabajos y las tareas, la evolución de las sociedades y los grandes avances económicos son producto de la humanidad, son las personas quienes han creado tales avances. En ese sentido, al tener dentro del ámbito de su control las situaciones riesgosas, se puede decir que son controlables. Por el contrario, aquellos riesgos que escapen del ámbito de control de una persona no podrán ser imputados a esta.

El derecho penal, a lo largo de la historia, se ha encargado de regular diversas actividades riesgosas para los valores que intenta proteger, como tipificar acciones como delictivas por considerarlas nocivas y perjudiciales para el ordenamiento jurídico. Es así que existen riesgos que son tolerados o permitidos y otros, que, debido a un juicio político criminal, constituyen riesgos prohibidos que deben ser evitados o sancionados cuando se producen.

Por otro lado, durante los últimos años, se han originado nuevas formas de criminalidad relacionadas con el sistema económico y el sector empresarial. Ante la aparición de nuevos riesgos y nuevas formas de criminalidad, perjudiciales para la sociedad, el Estado es el encargado de establecer mecanismos para reducir, prevenir y sancionar estas situaciones. Sin embargo, la obligación de prevenir la creación de riesgos prohibidos o el aumento de los riesgos permitidos puede ser, también, trasladada a los privados, en el sentido de exigirles cumplir con ciertos parámetros normativos o reglas al momento de realizar actividades riesgosas o que podrían generar o aumentar un riesgo.

Para controlar y prevenir estos nuevos riesgos que se generan como consecuencia de la actividad del sector empresarial, se ha creado el *Compliance Program* o Programa de Cumplimiento Normativo, que constituye un mecanismo de autorregulación de las empresas para prevenir y/o evitar la comisión de infracciones legales.

El objetivo es que las empresas internalicen o implementen un conjunto de normas o medidas que traten de asegurar la prevención de infracciones que se podrían generar como consecuencia de las actividades que realizan o debido al nivel de complejidad de su estructura organizacional.

El Programa de Cumplimiento Normativo está destinado a velar por el respeto a la normativa penal a fin de prevenir y detectar la comisión de delitos y otras infracciones que podrían desencadenar la comisión de ilícitos.

Como se verá a lo largo del curso, el Compliance es un traje a la medida de cada empresa. El Compliance Officer, a partir de un trabajo de campo, el contacto con todos los directivos y empleados y el conocimiento del ADN de la empresa irá diseñando el sistema con todos los elementos y fases necesarios para su puesta en marcha. Habrá de redactar sus propios protocolos, manuales y plantillas e irá tomando decisiones sobre fases que sea necesario contratar con expertos externos y los programas informáticos que puedan facilitar su tarea como pueden ser los programas ISO. Los modelos, manuales… son una orientación que nunca podrán ser utilizados más allá de orientaciones generales.

Como parte de esta introducción a continuación la conferencia impartida por D. Bernardo del Rosal Blasco, Catedrático de Derecho Penal de la Universidad de Alicante.

https://www.youtube.com/watch?v=umMquSPzNg8

BUEN GOBIERNO Y CÓDIGO ÉTICO

Con el cambio normativo es impostergable el necesario trabajo empresarial para operar bajo un "Buen Gobierno" que se materializa en los Códigos de Conducta Ética a aplicar en la empresa y en su Manual de Prevención de Delitos. Estos conceptos se han incorporado claramente a la cultura empresarial desde la reforma del Código Penal.

Las PYMES, aquellas que puedan presentar cuentas de pérdidas y ganancias abreviadas por tener un volumen neto de cifra de negocios inferior a 22.800.000 euros anuales, la responsabilidad del *Compliance Officer* recae sobre su Órgano de Gobierno que puede ser el consejo de administración o los administradores de la Sociedad.

Son necesarios una serie de requisitos para acreditar el compromiso de la empresa con la prevención de delitos dentro de la misma como es:

1. Compromiso del Órgano de Gobierno firme, real y eficaz, promoviendo una cultura de Compliance que debe estar documentado formalmente. Puede ser a través de un acuerdo que se recoge en acta o mediante la designación del Compliance Officer en un acta del Consejo de Administración de la Sociedad.
2. El Compliance Officer procederá a evaluar los riesgos de comisión de delitos en función de las actividades llevadas a cabo por la empresa. No es, por tanto, un copia y pega, como ha dicho la Fiscalía General del Estado, sino que debe estar personalizado para la realidad de la empresa.
3. Elaborar el Mapa de Riesgos y un Plan de Acción para implementar controles operativos que dificulten la posible comisión de un ilícito penal por parte de los empleados de la compañía.
4. Este programa de compliance se debe recoger en el Manual de Prevención de Delitos de la compañía y en el Código de Conducta Ética que define los comportamientos no permitidos en las tareas de la empresa.
5. El *compliance officer* se ocupará de formar, comunicar y divulgar entre los empleados de la compañía y su entorno operativo: Proveedores, clientes, asesores… el compromiso real de la persona jurídica con el Buen Gobierno y las prácticas mercantiles basadas en un modelo ético.
6. Además, establecerá el canal de denuncias que deberá ser utilizado por los empleados de la compañía al detectar actuaciones que puedan suponer ilícitos penales de los propios compañeros. Ante cualquier denuncia se deberán establecer las medidas correctivas oportunas, inclusive, si la denuncia es probada, puede llevar aparejada el despido y la pertinente denuncia en aplicación del régimen disciplinario que deberá estar perfectamente comunicado a los empleados. También, deberá supervisar y verificar todo el programa de compliance implementado en la compañía proponiendo las mejoras que estime pertinentes para lo cual habrá de contar con los recursos y los medios necesarios para la implantación del programa de compliance si desea gozar de una eximente plena como persona jurídica, para el caso de que fuera necesario.

El Compliance es una manifestación ética. Las presiones comerciales o la trayectoria previa de la persona pueden ser factores vinculados a

incumplimientos éticos o normativos, donde los individuos que los han provocado no llegan a interiorizar su participación y responsabilidad.

Los estándares globales sobre Compliance, la Norma ISO 19600, señala que el cumplimiento puede provenir de “requirements”, obligaciones exigibles por terceros, como de “committments”, compromisos asumidos voluntariamente como puede ser las obligaciones autoimpuestas por la propia empresa, normalmente relacionadas con valores o buenas prácticas, y que suelen cristalizar en los Códigos Éticos o de Conducta. Esto permite ver el compliance con una amplitud de miras que trasciende la literalidad de las leyes.

Por ejemplo, en el año 2009 el Tribunal Federal de Alemania, BGH, sentenció que los cometidos del Compliance Officer no se limitaban a velar por el cumplimiento de las Leyes, sino también a evitar los daños reputacionales de las organizaciones, ámbito estrechamente relacionado con las buenas praxis más allá de la legalidad. Una función de Compliance así entendida dificulta utilizar la literalidad de la Ley como excusa y permite detener iniciativas que, siendo perfectamente legales, serán reprochadas por una amplia mayoría.

El código ético es la ley suprema de la empresa que refleja el marco de lo permitido y lo prohibido por lo que es un traje a la medida. De ahí algunas notas distintivas como es la declaración de compromiso y cumplimiento firmado por el todos los integrantes de la empresa; que refleje los valores de la empresa como es objetivo, misión, visión y valores que le son propios.

El código ético deberá indicar las conductas que se esperan del personal de la empresa por medio de un marco general detallado en las políticas y manuales; establecer un marco general de conductas reprochables y que en ningún caso serán toleradas, tipificando así los supuestos en los que se actuará para sancionar; considerar las distintas obligaciones legales de la empresa y estructurarlas de manera coherente con los valores de la empresa, las conductas esperadas y prohibidas.

El código ético ofrecerá información suficiente sobre las áreas responsables y los procesos existentes para la implementación del programa de Compliance y la canalización de información relativa al cumplimiento normativo, tanto para aclarar dudas como para formular denuncias; incorporar todas las obligaciones que deriven de compromisos voluntarios, derivados de su responsabilidad social corporativa, acuerdos con la comunidad, compromisos con el respeto al medio ambiente o similares.

Se trata de aspectos que serán valorados por los *stakeholders* de la empresa, y cuyo incumplimiento puede generar un impacto relevante para la compañía, no sólo a nivel legal sino a nivel reputacional y financiero.

Regalos de y para la empresa, por ejemplo

Por solo señalar un ejemplo, uno de los temas que puede generar malas prácticas es el relativo al ofrecimiento o recibimiento de obsequios o regalos que puede ser entendido como una forma de cohecho o de corrupción que se castiga en las legislaciones de la mayoría de los países, incluido España, con penas que

van desde los 6 meses a los 6 años de prisión para los autores, estando incluido como uno de los delitos que genera responsabilidad penal de la persona jurídica.

Esto hace necesaria una política de obsequios bien definida y cuyos elementos más importantes podrían ser que esté por escrito; estar comunicada y promovida a lo largo de la organización; prever qué tipo de obsequios pueden ser ofrecidos o aceptados y cuál es su límite económico; estipular cómo deben actuar los empleados en caso de verse en el compromiso de tener que aceptar un regalo u obsequio. Incluir la prohibición de ofrecer, solicitar o aceptar cualquier tipo de regalos u obsequios en los que sea evidente lo que se espera a cambio.

Se sugiere, además, tener un registro de los obsequios que realiza o recibe la empresa o sus empleados y su valor. Definir el mecanismo para que el empleado informe de posibles vulneraciones de la política de regalos y obsequios, sin miedo a represalias, así como las consecuencias disciplinarias en caso de incumplimiento.

POR QUÉ UN COMPLIANCE

En general, el contenido básico del sistema Compliance deberá incluir las políticas para un buen gobierno y su código ético; identificación de áreas donde puede ocurrir el delito; análisis de riesgos; plan de acciones; procesos de formación; recursos financieros para impedir delitos que pueden ser prevenidos; metodología para informar de incumplimientos, sistema disciplinario; verificación de la implantación; supervisión del modelo por persona independiente con poderes y recursos y cómo se distribuirán las responsabilidades para su funcionamiento.

En relación a la gestión de estas funciones, el artículo 31 bis del Código Penal, en su apartado 2.b, establece que la persona jurídica puede quedar exenta de responsabilidad si: “La supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica”.

Esa persona, debe ser nombrada por la alta dirección; tener autonomía, poderes de control y recursos propios; deberá identificar las obligaciones de cada área y velar por su cumplimiento, realizando seguimientos; definir quiénes son los responsables de qué áreas o sectores; definir indicadores, detectar y realizar la formación necesaria; establecer acciones a ejecutar para dar cumplimiento a la normativa legislativa e interna u otra; será el encargado de la comunicación con organismos regulatorios y de la revisión del sistema, pudiendo intervenir, entre otros, en los ámbitos laboral, compras, comunicación, prevención de riesgos laborales, informática, jurídica, medio ambiente, mantenimiento, relaciones internacionales y de proveedores. Y, en fin, denunciar y comunicar todos los incumplimientos que detecte a la alta dirección dado que en definitiva son los primeros y últimos responsables del Compliance.

Estos esfuerzos de la alta dirección en el establecimiento del Compliance y en el nombramiento de un Compliance Officer, tiene como meta quedar exento de responsabilidad penal dado que una buena implantación puede ayudar a no tener sanciones, ni denuncias y sobre todo una imagen de empresa que refleje la ideología de los dueños.

Para el caso de sentencia firme en la que la persona jurídica es penalmente responsable, la empresa como tal no puede cumplir la sentencia, la empresa no va a la cárcel, por ejemplo. Se entiende que existen responsables que actúan en nombre y beneficio de la organización que son los que cumplirán la pena es decir los Directores o Responsables de las organizaciones con capacidad de decisión, de obrar y de formar la voluntad.

Mapa de riesgos penales

La primera acción a realizar será identificar y analizar los riesgos penales relevantes que afectan a la empresa, distinguiendo los riesgos propios del negocio o actividad que desarrolla la empresa de los riesgos comunes que afectarían a cualquier clase de organización.

En definitiva, identificar riesgos y establecer medidas y pautas de control para poder neutralizarlos.

Hay que tener en cuenta la Circular 1/2016 de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, que considera que no son idóneos los manuales de prevención de delitos o programas de Compliance copiados de otras empresas, extremo que ya puso de manifiesto la Fiscalía General del Estado en su anterior Circular 1/2011, entrando a analizar que dichas prácticas no enervaban la responsabilidad penal de la empresa pudiendo resultar un mero maquillaje que nada tiene que ver con el cambio cultural y ético que supone el Compliance.

Identificar procesos y controles existentes

La segunda acción consistiría en analizar e identificar los mecanismos internos de control con los que cuenta ya la empresa para hacer frente a los riesgos detectados, de acuerdo con el principio de eficiencia en los recursos empresariales.

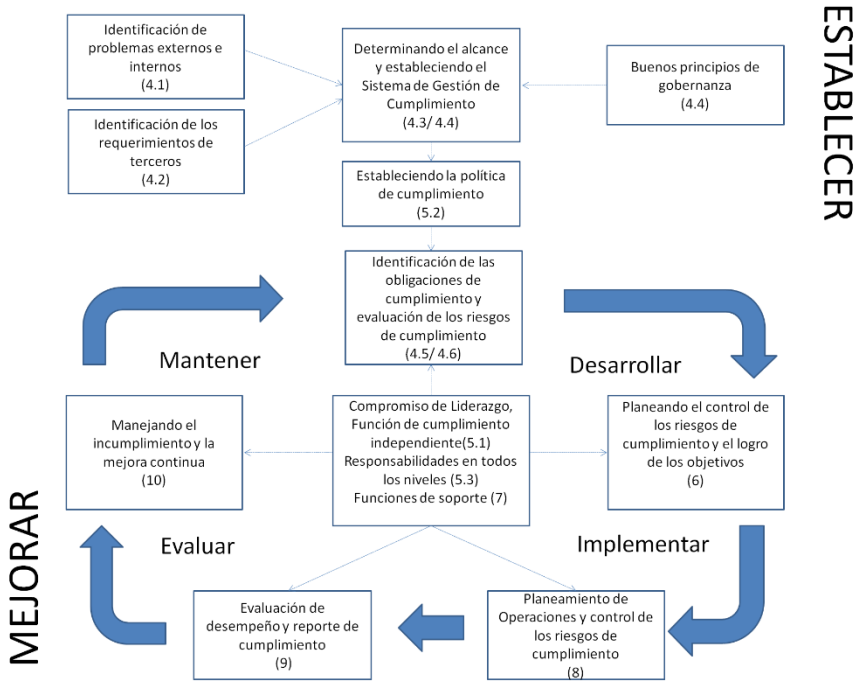
El Modelo de Prevención Penal, MPP, no debe concebirse como algo aislado del resto de áreas de cumplimiento legal de la empresa, es decir, todas aquellas políticas, manuales y procedimientos existentes deben servir para evaluar donde pueden existir riesgos penales: Procesos de gestión de la seguridad de la información y protección de datos, de gestión de RRHH, prevención y blanqueo de capitales, comercial y marketing, *property rights*, etc…

Elaboración del Manual de Prevención Penal

A juicio de la Fiscalía, el modelo ha de ser idóneo para prevenir delitos y para detectarlos. Sin embargo, la comisión de un delito en el futuro no conduciría automáticamente a considerar el programa como ineficaz.

Es necesario contemplar un sistema de sanciones disciplinarias derivado del incumplimiento de MPP conforme a la regulación laboral. Infringir el modelo debe tener consecuencias para Directivos y empleados, de lo contrario resultaría completamente ineficaz.

EL COMPLIANCE ESTANDARIZABLE



Para el caso de un incumplimiento penal, en sede judicial, la carga de la prueba de la idoneidad del modelo correspondería a la empresa que habrá de demostrar que el sistema funciona y todos los mecanismos de supervisión, control y sanción que se hayan establecido a través de los respectivos registros, y que se está ante un incidente aislado y al margen de la política de la empresa, que es lo que en definitiva viene a decir la Circular de la Fiscalía 1/2016,

Dice la circular Fiscalía General del Estado:*"(…) No resulta sencillo conceptuar adecuadamente la naturaleza jurídica de la exclusión de responsabilidad penal de la persona jurídica pues, en los últimos dos siglos, el Derecho Penal ha venido construyendo las referencias dogmáticas a la antijuridicidad, la culpabilidad sobre la base de comportamientos individuales, no colectivos (…) Ahora bien, partiendo de que el art. 31 bis establece un sistema de responsabilidad indirecta o vicarial conforme al cual el fundamento de la responsabilidad penal de la persona jurídica descansa en un hecho ajeno, y no en un hecho propio, la comisión del delito por las correspondientes personas*

físicas en las condiciones que exige el precepto determinará la transferencia de responsabilidad a la persona jurídica. Ello comporta que con el delito de la persona física nace también el delito de la persona jurídica la cual, no obstante, quedará exenta de pena si resulta acreditado que poseía un adecuado modelo de organización y gestión."

La Sentencia del Tribunal Supremo, STS 154/2016, de fecha 29 de febrero y la de 16 de marzo de 2016, sobre la presunción de inocencia de la empresa, y respecto a que "*el juicio de autoría*" de la empresa exigirá a la acusación probar dos extremos: Por un lado, la comisión del hecho delictivo cometido por la persona física y por otro, acreditar que efectivamente había un defecto en el modelo de prevención.

Llegados a este momento, leer la siguiente presentación en PREZI del siguiente enlace:
https://prezi.com/t6cfaistfpfp/introduccion-al-sistema-de-prevencion-de-delitos-compliance-penal/

Ámbito con función propia y distinta de la auditoría interna y la asesoría jurídica

Como venimos señalando, se entiende por "cumplimiento", de acuerdo con la definición que en su momento aplicó Basilea, aquella función que identifica, asesora, alerta y reporta los riesgos de cumplimiento en las organizaciones, es decir, el riesgo de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras o pérdidas de reputación por fallas de cumplimiento con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas.

Esa función de cumplimiento a veces se confunde con otras prácticas profesionales como es la autoría interna y la asesoría jurídica. Si vemos las 3 líneas de defensa, que señalamos mas adelante, tenemos que en una primera línea de defensa nos encontramos a los empleados que llevan a cabo las actividades propias de la empresa; en una segunda línea se encontraría el Compliance, que debe supervisar el correcto funcionamiento de los controles y controlar si la primera línea está aplicando dichos controles y, por último, nos encontramos con la tercera línea de defensa en la que encuadramos la Auditoría Interna, que supervisa a toda la organización, incluyendo el Compliance.

En ese esquema las principales diferencias podrían ser que el Compliance controla la prevención de delitos, mientras que a través de la Auditoría se supervisan todas las áreas de la empresa; el Compliance identifica los problemas de manera mucho más inmediata que a través de Auditoría ya que esta suele detectar los problemas una vez que estos ya se han producido y el Compliance Officer, aun cuando debe ser independiente, debe participar en el diseño de las políticas, procedimientos y controles mientras que los auditores deben estar totalmente al margen del negocio.

Por otra parte, la función del Compliance es proteger los intereses de clientes, accionistas, proveedores y en general toda la sociedad desde dentro de la empresa, mientras que la asesoría jurídica tiene como objetivo la defensa tanto de la empresa como de sus directivos y empleados.

ISO 19600: Sistemas de Gestión de Compliance

La Norma ISO 19600, de Sistemas de Gestión de Compliance, es la referencia internacional que establece las buenas prácticas en materia de gestión de cumplimiento y ayuda a la gestión de, entre otros, el riesgo penal. Su campo de aplicabilidad es extensible a cualquier tipo de empresa y organización, y es compatible con cualquier otra norma que establezca sistemas de gestión.

Además, proporciona orientación para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de compliance eficaz y que genera respuesta por parte de la organización y contiene:

a) Las directrices para implantar, mantener y mejorar un sistema de gestión de compliance eficaz y receptivo.

b) Recomendaciones sobre los elementos con los que una organización debería contar para asegurar que cumple su política de compliance y que tiene capacidad para asumir sus obligaciones en este ámbito.

c) Análisis de nuevas necesidades de formación en materia de compliance para aquellos profesionales involucrados en este campo cuando se produzcan cambios organizativos, legislativos o en los compromisos con los grupos de interés.

d) Recomendaciones sobre la integración del desempeño en Compliance

en la evaluación del desempeño de los empleados, o supervisión de los acuerdos de contratación externa para asegurarse de que recogen obligaciones en materia de compliance.

Circular 1/2016, de la Fiscalía General del Estado

La Circular 1/2016, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas da instrucciones a los fiscales sobre cómo valorar la eficacia de los planes de cumplimiento normativo. Según la circular, los planes de Compliance son una apuesta decidida del legislador por una fórmula de "autorregulación regulada" en la lucha contra la delincuencia de empresa.

La circular destaca la posible conducta delictiva de sus dirigentes y los programas de control: "Si el fundamento de la imputación de la persona jurídica reside en la conducta delictiva de sus dirigentes o en el incumplimiento de sus obligaciones de control sobre los subordinados, esto será lo único que deba probar la acusación. Señala que "los programas de control constituyen una referencia para medir las obligaciones de las personas físicas con mayores responsabilidades en la corporación, como indicaba la Circular 1/2011. Pero será la persona jurídica la que deberá acreditar que tales programas eran eficaces para prevenir el delito, cuestión ésta sobre la que se volverá más adelante al analizar los programas de organización y gestión". Además, que sólo quedarán excluidas de la responsabilidad penal de la persona jurídica "aquellas conductas que, al amparo de la estructura societaria, sean realizadas por la persona física en su exclusivo y propio beneficio o en el de terceros, y resulten inidóneas para reportar a la entidad beneficio alguno, directo o indirecto".

En relación a los programas de cumplimiento normativo señala que "sin duda, muchas empresas se han dotado y se dotarán de completos y costosos programas con la única finalidad de eludir el reproche penal, pero más allá de su adecuación formal a los requisitos que establece el Código Penal, tales programas no pueden enfocarse a conseguir este propósito sino a reafirmar una cultura corporativa de respeto a la Ley, donde la comisión de un delito constituya un acontecimiento accidental y la exención de pena, una consecuencia natural de dicha cultura". De otra manera, advierte el Ministerio Público, "se corre el riesgo de que en el seno de la entidad los programas se perciban como una suerte de seguro frente a la acción penal".

Según explica "los programas deben ser claros, precisos y eficaces y, desde luego, redactados por escrito. No basta la existencia de un programa, por completo que sea, sino que deberá acreditarse su adecuación para prevenir el concreto delito que se ha cometido, debiendo realizarse a tal fin un juicio de idoneidad entre el contenido del programa y la infracción. Por ello, los modelos de organización y gestión deben estar perfectamente adaptados a la empresa y a sus concretos riesgos".

Advierte que no se realicen *copia y pega* de los programas de cumplimiento, asumiendo que con eso la empresa ya cumple. "No es infrecuente

en la práctica de otros países que, para reducir costes y evitar que el programa se aleje de los estándares de la industria de los *compliance*, las compañías se limiten a copiar los programas elaborados por otras, incluso pertenecientes a sectores industriales o comerciales diferentes. Esta práctica suscita serias reservas sobre la propia idoneidad del modelo adoptado y el verdadero compromiso de la empresa en la prevención de conductas delictivas".

En relación al *Compliance Officer,* la Circular señala que "debe necesariamente ser un órgano de la persona jurídica, lo que facilitará el contacto diario con el funcionamiento de la propia corporación. Ello no implica que este órgano deba desempeñar por sí todas las tareas que configuran la función de cumplimiento normativo, que pueden ser realizadas por otros órganos o unidades distintos al específico de cumplimiento normativo, como la unidad de riesgos, la unidad de control interno, el servicio de prevención de riesgos laborales o el de prevención del blanqueo". Y añade que "lo esencial será que exista un órgano supervisor del funcionamiento general del modelo, que deberá establecer claramente el responsable de las distintas funciones y tareas".

Agrega que "tampoco existe inconveniente alguno en que una gran compañía pueda recurrir a la contratación externa de las distintas actividades que la función de cumplimiento normativo implica". Y explica que "carecería de sentido y restaría eficacia al modelo imponer a una multinacional la realización y control interno de todas las tareas que integran la función de cumplimiento normativo". Lo verdaderamente relevante, apunta, es "que la persona jurídica tenga un órgano responsable de la función de cumplimiento normativo, no que todas y cada una de las tareas que integran dicha función sean desempeñadas por ese órgano".

Puntualiza que "muchas de ellas incluso resultarán tanto más eficaces cuanto mayor sea su nivel de externalización, como ocurre por ejemplo con la formación de directivos y empleados o con los canales de denuncias, más utilizados y efectivos cuando son gestionados por una empresa externa, que puede garantizar mayores niveles de independencia y confidencialidad".

Entiende la Fiscalía que "el oficial de cumplimiento normativo puede con su actuación delictiva transferir la responsabilidad penal a la persona jurídica puesto que está incluido entre las personas que ostentan facultades de organización y control dentro de la misma". Además, "puede ser una de las personas que al omitir gravemente el control del subordinado permite la transferencia de responsabilidad a la persona jurídica. En este supuesto, la omisión puede llevarle a ser él mismo penalmente responsable del delito cometido por el subordinado". Recuerda que "si el oficial de cumplimiento omite sus obligaciones de control, la persona jurídica en ningún caso quedará exenta de responsabilidad penal".

Sobre las pequeñas empresas, la Fiscalía dice que "extremarán la prudencia en su imputación", ya que su estructura organizativa no puede compararse con la de las empresas dotadas de una organización de cierta complejidad. Podrán demostrar su compromiso ético mediante una razonable

adaptación a su propia dimensión de los requisitos formales, que les permita acreditar su cultura de cumplimiento normativo, más allá de la literalidad del precepto y en coherencia con las menores exigencias que estas sociedades tienen también desde el punto de vista contable, mercantil y fiscal".

El TRIBUNAL SUPREMO INDICA EL CAMINO

El Tribunal Supremo dictó una sentencia en la que abordó por primera vez, y en profundidad, la responsabilidad penal de las personas jurídicas. Este fallo, supone un hito importante en el ámbito del Derecho Penal y para los profesionales especializados en cumplimiento normativo, ya que marca las pautas que el alto tribunal tendrá en cuenta a la hora de abordar cuestiones de esta naturaleza.

En su sentencia, el Pleno de la Sala de lo Penal confirma las condenas impuestas por la Audiencia Nacional a tres empresas por su participación en delitos contra la salud pública, en concreto en el tráfico de más de 6.000 kilos de cocaína escondida en maquinaria objeto de importación y exportación entre España y Venezuela.

No obstante, el tribunal modifica la pena de las empresas excluyendo la disolución de la misma debido a que cuenta con una plantilla de más de cien personas que no tienen que sufrir los graves perjuicios de dicha medida, pero confirma que la sociedad debe pagar una multa de 775 millones de euros.

La sentencia, de la que ha sido ponente el magistrado José Manuel Maza, explica los requisitos que se tendrán en cuenta para apreciar la responsabilidad de las empresas de acuerdo con el artículo 31 bis del Código Penal:

En primer lugar, la Suprema señala que, como presupuesto inicial, debe constatarse la comisión de un delito por una persona física que sea integrante de la persona jurídica. En este caso eran administradores de hecho o de derecho.

En segundo lugar, que las empresas hayan incumplido su obligación de establecer medidas de vigilancia y control para evitar la comisión de delitos. La sentencia señala: "La determinación del actuar de la persona jurídica, relevante a efectos de la afirmación de su responsabilidad penal, ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquélla, ha sido posible o facilitado por la ausencia de una cultura de respeto al derecho como fuente de inspiración de la actuación de su estructura organizativa e independiente de la de cada una de las personas jurídicas que la integran, que habría de manifestarse en alguna clase de formas concretas de vigilancia y control del comportamiento de sus directivos y subordinados jerárquicos tendentes a la evitación de la comisión por éstos de los delitos".

Aunque lo descartan en este caso, los magistrados advierten de situaciones futuras donde puedan producirse conflictos de intereses procesales entre las personas físicas acusadas del delito y las personas jurídicas que sean representadas por esas mismas personas físicas, lo que podría originar una conculcación efectiva del derecho de defensa de la empresa. En ese sentido, pide a los jueces y tribunales que intenten evitar riesgos de ese tipo para proteger

el derecho de defensa de la persona jurídica. Asimismo, sugiere al legislador que "remedie normativamente" este tipo de situaciones.

La sentencia hace la diferencia entre la empresa con actividad real y las que califica como sociedades "pantalla", carentes de cualquier actividad lícita y creadas exclusivamente para la comisión de hechos delictivos. Según apunta la sentencia, estas últimas han de ser consideradas al margen del régimen de responsabilidad penal del artículo 31 bis del Código Penal, sin perjuicio de que en el caso de autos se considere de utilidad mantener las penas de disolución y multa impuestas.

En opinión de estos magistrados, "no procede constituir a las personas jurídicas en un modelo privilegiado de excepción en materia probatoria", sino que corresponde a la persona jurídica alegar la concurrencia de dichos instrumentos, y aportar una base racional para que pueda ser constatada la disposición de los mismos.

Esta sentencia del Tribunal Supremo supone un paso importante en materia de *Compliance* o cumplimiento normativo, ya que permite a las empresas y a los asesores en este ámbito conocer cuáles van a ser los criterios de interpretación a partir de ahora. Además, como hemos señalado, estas pautas se suman a las ya ofrecidas por la Circular que emitió la Fiscalía General del Estado el pasado 22 de enero, en la que el Ministerio Público concretaba cuáles serán las pautas que se seguirán para perseguir este tipo de delitos.

DELITOS Y PENAS PREVISTOS EN EL CÓDIGO PENAL

Se exigirá responsabilidad penal a una persona jurídica respecto a un catálogo de delitos que son formulados expresamente en las disposiciones del libro II del Código Penal y que son:

1. Art. 156 bis: C.P.Tráfico ilegal de órganos.
2. Art.177 bis: Trata de seres humanos.
3. Art. 189 bis: Delitos relativos a la prostitución y a la corrupción de menores.
4. Art.197 quinquies CP (reforma 2015): Delito contra la intimidad y allanamiento informático.
5. Art. 251.bis: Estafas propias e impropias.
6. Art.264 quáter (reforma 2015): Delitos informáticos y hacking.
7. Arts.270-277: Delitos contra la propiedad intelectual e industrial.
8. Arts.278-286 quáter (reforma 2015): Delitos relativos al mercado y a los consumidores.
9. Arts.304 bis (reforma 2015): Delito de financiación ilegal de los partidos políticos.
10. Arts.305-310 bis: Delitos contra la Hacienda Pública y la Seguridad Social.
11. Arts. 318 bis: Delitos contra los derechos de los ciudadanos extranjeros.
12. Art.319-320: Delitos sobre la ordenación del territorio y el urbanismo.
13. Art.325-328 (reforma 2015): Delitos contra los recursos naturales y el medio ambiente.
14. Art.343: Delitos relativos a la energía nuclear y a las radiaciones ionizantes.
15. Art.348: Delitos de riesgo provocados por explosivos y otros agentes.
16. Art.366 (reforma 2015): Delitos contra la salud pública.

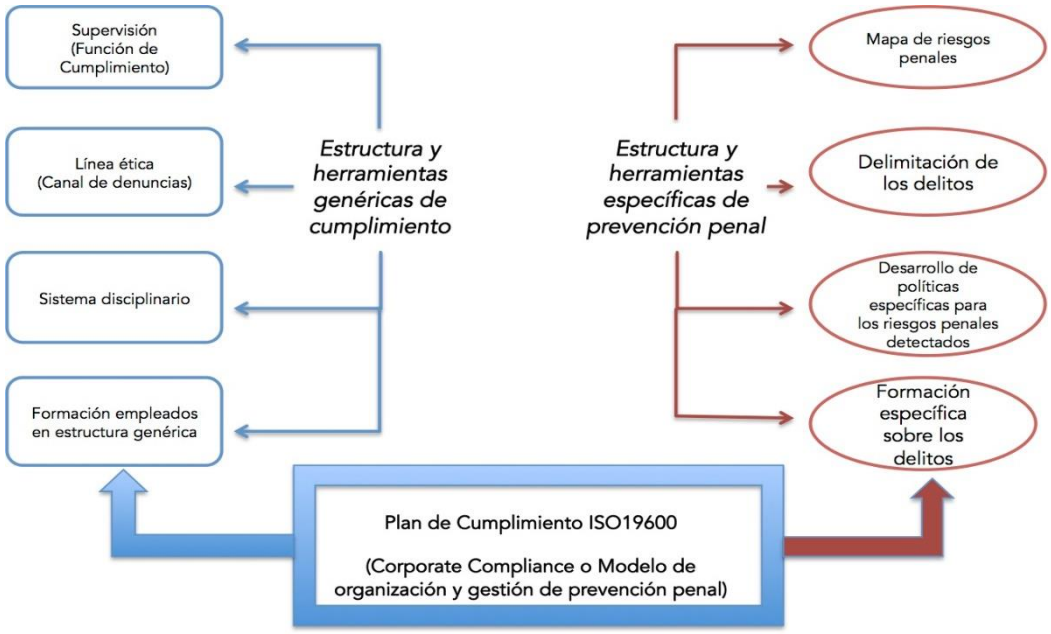
17. Art.369 bis: Tráfico de drogas.
18. Art.386 (reforma 2015): Delito de falsificación de moneda y efectos timbrados.
19. Art.399 bis: Falsificación de tarjetas de crédito y débito y cheques de viaje.
20. Art.427 bis (reforma 2015) y Art. 430: Cohecho y tráfico de influencias.
21. Art.510.bis (reforma 2015): Delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución.
22. Art.576: Delitos de terrorismo.
23. Art.445 Corrupción de funcionario extranjero.
24. Art.302: Blanqueo de capitales.
25. Arts. 258 ter y 261 bis (reforma 2015): Insolvencias punibles. Alzamientos y concursos punibles.

En relación a las penas aplicables a las personas jurídicas, estas se establecen en el apartado 7 de Art. 33 del Código Penal que asigna siete tipos de penas:

1. Multa por cuotas o proporcional.
2. Disolución de la persona jurídica.
3. Suspensión de las actividades.
4. Clausura de los locales y establecimientos.
5. Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito.
6. Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social.
7. Intervención judicial.

Además, hay otras consecuencias para las empresas que pueden resultar igualmente graves y perjudiciales para la marcha del negocio, tales como:

1. Repercusión con los clientes y proveedores.
2. Entidades financieras que dificulten o nieguen la concesión o renovación de créditos u otras operaciones financieras.
3. Disminución del valor de la sociedad.
4. Desprestigio social y empresarial en los medios de comunicación, web, etc.



UN POCO DE HISTORIA DEL COMPLIANCE

Las primeras noticias sobre el Compliance las encontramos en EE.UU. Entre los años 30, con la llegada al poder del presidente Roosevelt y hasta los años 60, la regulación jurídica de las empresas se ceñía a cuestiones relativas fundamentalmente a la prohibición de los monopolios, el establecimiento de impuestos y a las condiciones de trabajo. En la década de los 60, se entró más en regulaciones de carácter social y de vigilancia medio ambiental.

En los años 70 y 80, con la aparición de algunos escándalos de corrupción y financieros que afectaron a grandes compañías como el *Escándalo Lockheed Corporation, sobre soborno a altos funcionarios extranjeros,* se dictó la *Foreign Corrupt Practices Act o FCPA (19.12.1977) con* disposiciones anti-soborno y requerimientos y prohibiciones en materia de libros y registros.

A mediados de la década de 1970, diversas empresas estadounidenses y trasnacionales comenzaron a adoptar Compliance Programs con la finalidad de evitar y detectar infracciones legales, sobre todo las relacionadas con la libre competencia y antimonopolio (antitrust) y actos de corrupción (bribery laws).

El Derecho Penal tiene la función de proteger bienes jurídicos que pueden verse afectados o puestos en peligro como consecuencia de las actividades que realizan las empresas. En tal sentido, el Estado busca prevenir los nuevos y ya existentes riesgos de la actividad empresarial a través del Derecho Penal de diversas maneras, entre ellas, la regulación de programas de prevención de riesgos de cumplimiento obligatorio por parte de las empresas. En esa misma línea, resulta necesario señalar que desde la década de 1990, con la aparición de las «Sentencing Guidelines», se habla de la creación de incentivos para que sean las empresas mismas quienes se autorregulen, de allí el concepto de autorregulación regulada.

Un ejemplo son las investigaciones oficiales que sucedieron al famoso escándalo Watergate, que tuvieron como resultado que unas 400 empresas norteamericanas reconocieran haber hecho pagos irregulares a funcionarios gubernamentales, políticos y partidos políticos extranjeros por más de 300 millones de dólares, para asegurarse algún tipo de acción o conducta en su beneficio o para asegurarse que los funcionarios realizaban acciones más diligentemente o de la forma más rápida.

En los años ochenta, y a raíz de escándalos financieros relativos a "abusos de información privilegiada" (*insider trading*) y de otras figuras delictivas, se produjo un cambio sustancial en el ámbito y el formato de estos programas, que comenzaron a incluir códigos de conducta, programas de entrenamiento para empleados, medidas disciplinarias para quienes hubieran actuado incorrectamente, así como la implantación de medidas específicas para el tipo de negocio concreto.

En el año 1909 el administrador de una operadora ferroviaria ofreció descuentos a varias empresas refinadoras de azúcar, infringiendo la ley que, en aquel sector regulado prohibía cualquier discriminación en los precios. En la resolución de este asunto el Tribunal Supremo afirmó que los hechos delictivos cometidos por cualquier tipo de empleado, podían ser imputados a la empresa, siempre que estos actuaran en el ejercicio de sus funciones y con el ánimo de beneficiar a la propia empresa. El argumento básico que empleó el Tribunal es el hecho de que la conducta se lleva a cabo en beneficio de la empresa. Debido a ello y por razones de interés público, se extiende a partir de aquí la doctrina de la responsabilidad penal a las corporaciones.

Así, la empresa, que actúa como principal, y todos sus empleados, independientemente del rango que puedan tener, se configuran como sus agentes, debiendo, por tanto, la empresa responder por sus actos ilícitos, del mismo modo en que se beneficia de los actos ventajosos realizados por sus agentes. A continuación, ante cualquier inspección y propuesta de sanción por parte de la Administración, se defendían con el argumento de la "buena fe", solicitaban la exención de la imputación penal por la imposibilidad del control de todos los empleados, solicitando la restricción de la responsabilidad vicaria de la empresa. Las empresas también reclamaron derechos constitucionales propios, independientes de los derechos constitucionales de los individuos que la conforman o que trabajan para ellos. A raíz de todas estas opiniones, el Tribunal Supremo a finales de siglo afirmó que las personas jurídicas eran personas a los efectos de la protección otorgada por la Décimo Cuarta Enmienda.

La Décimo Cuarta Enmienda es una de las enmiendas posteriores a la Guerra Civil, e incluye, entre otras, la Cláusula del Debido Proceso y la Cláusula de Protección Igualitaria. Fue propuesta el 13 de junio de 1866, y ratificada el 9 de julio de 1868. Provee una amplia definición de ciudadanía nacional, que anula la decisión de *Dred Scott v. Sandford* (1857), que había excluido a los esclavos y sus descendientes, de poseer derechos constitucionales. Requiere que los estados provean de una protección igualitaria ante la ley a todas las *personas* (no solo a los *ciudadanos*) dentro de sus jurisdicciones. La

importancia de la Decimocuarta Enmienda fue ejemplificada cuando se interpretó para prohibir la segregación racial en los colegios públicos en el caso *Brown v. Board of Education*. Las otras dos enmiendas post-guerra son la Decimotercera Enmienda (prohibiendo la esclavitud) y la Decimoquinta Enmienda (prohíbe las cualificaciones respecto al voto determinadas por la raza). De acuerdo con el Juez de la Corte Suprema Noah Swayne, «construida con justicia, podría decirse de estas enmiendas que se elevan a la dignidad de una nueva Carta Magna».

Por otro lado, las investigaciones llevadas a cabo por la Comisión de Seguridad en el Cambio, *Securuty Exchange Comission,* SEC, revelaron que los sobornos eran una práctica habitual en el ámbito empresarial. Esta comisión ofreció un "programa de divulgación voluntaria", *voluntary disclosure program* para las sociedades públicas (que finalmente acabó expandiéndose al ámbito privado), en el que se les animó a realizar investigaciones internas y a revelar su contenido a cambio de "clemencia" (*leniency*) por las posibles infracciones cometidas.

Además, debemos señalar la creación del *Committee of Sponsoring Organizations of the Treadway Commission* cuyo objetivo era proporcionar liderazgo y orientación sobre el control interno, la gestión de riesgos empresariales y la disuasión del fraude, que se encargó de la redacción de reseñados informes sobre la materia (COSO I y COSO II).

Estados Unidos también modificó su sistema judicial, aprobando la *Sentencing Reform Act,* dando paso a las *Organizational Guidelines*, que establecen una atenuación de la pena para aquellas empresas que incorporen los programas de Compliance. La *última reforma es del 2004 e incluye normas de Effective Compliance and Ethics Program.*

Estados Unidos también promovió que los países miembros de la OCDE firmaran en el año 1997 el *Convenio de Lucha contra la Corrupción de Agentes Públicos Extranjeros en las Transacciones Comerciales e Internacionales* lo que permitió modificar la FCPA, incluyendo cláusulas de extra-territorialidad que implicaban el enjuiciamiento de cualquier persona física o jurídica, nacional o extranjera, vinculada al país, que infrinja la ley.

Con la investigación y detección de algunos escándalos como Enron, Tyco International, WorldCom o Peregrine Systems, en el año 2002 se promulgó la *Sabanes-Oxley Act, para* mejorar la protección de los inversores a través del establecimiento de condiciones legales exigentes en relación con la exactitud y veracidad de la información que divulgan las empresas.

La Sarbanes-Oxley Act fue un punto de inflexión en los programas de Compliance ya que, a partir de ella, las exigencias en esta materia se hicieron más estrictas y extensas, tanto en EE.UU. como en Europa.

Entre los referentes más cercanos tenemos a Italia. El Decreto Legislativo número 231, de 8/6/2001, *Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica* estableció la responsabilidad administrativa, no penal, de las personas

jurídicas, por infracciones cometidas por sus administrativos y personal dependiente. Los eventuales procesos derivados de estas situaciones se siguen ante un juez penal y bajo las normas del proceso penal.

En Chile, tras su ingreso a la OCDE, fue aprobada la Ley 20.393 de 2009, que establece la *Responsabilidad Penal de las Personas Jurídicas en los Delitos de Cohecho, Lavado de Activos y Financiamiento del Terrorismo.*

Reino Unido, que fue criticado por la OCDE por tener una normativa obsoleta en materia de corrupción, y tras el escándalo de la empresa *BAE Systems PLC*, aprobó en el 2010 la *Bribery Act,* considerada la más dura en todo el mundo.

En España se introduce el Compliance con la normativa relativa a protección de datos y blanqueo de capitales.

Como se ha indicado antes, el Estado tiene la obligación de la vigilancia que evite la comisión delictiva y precisamente por ello posee la exclusiva de la investigación en el ámbito penal. Al darse cuenta de que no podía controlar a las grandes corporaciones por falta de medios y de conocimiento, les ha obligado a establecer un sistema de cumplimiento normativo que, en caso de ser violentado, tendrá que tener los registros y pruebas suficientes que demuestren que hizo todo lo que debía para que no sucediera. De ahí el nacimiento del Chef Compliance Officer que da seguimiento a un sistema de gestión y prevención de delitos penales y reputacionales.

BUEN GOBIERNO CORPORATIVO

No obstante, la introducción de programas de compliance por la legislación penal es novedoso en nuestro ordenamiento. Los sistemas de enforcement autónomos han existido desde mucho antes, sobre todo en empresas de mayores dimensiones, multinacionales y cotizadas de gran tamaño. Estas corporaciones ya contaban con normas internas y medidas de control sectoriales que han terminado integrando los programas de cumplimiento, estando también condicionadas por la existencia de normativa sectorial de carácter sancionador, elemento coercitivo ante la posible actuación antijurídica de la empresa que ya le imponía obligaciones de muy diversa índole: Legislación tributaria, prevención de riesgos laborales, blanqueo de capitales, etc.

La introducción del Derecho Penal ha supuesto que junto con el tradicional riesgo económico de la empresa, provocado por la existencia del derecho sancionador, surja el riesgo de responsabilidades penales, que puede tener las mismas o mayores consecuencias negativas que el riesgo económico precisamente por el carácter de último ratio del Derecho Penal y el riesgo reputacional que supone someterse a un proceso de esta índole.

La idea de que la empresa debe tomar el control sobre sí misma antes de que se produzca la intervención del derecho administrativo sancionador y el derecho penal, con la creación de códigos de buen gobierno corporativo, códigos éticos y Programas de Compliance Penal que fomenten de una manera autómata y naturalizada las buenas prácticas empresariales, surge antes, como se ha dicho, principalmente en países anglosajones y en numerosas recomendaciones internacionales donde se insiste en la necesidad de entender la estrecha relación entre un sistema ético y la prevención como base fundamental para el buen funcionamiento de la empresa.

Con el establecimiento del liberalismo económico cada vez se hace más presente la enorme influencia de las grandes corporaciones sobre los poderes públicos, y con ello, se inicia el debate sobre la necesidad de intervención estatal sobre las empresas a fin de ejercer un mayor control de legalidad sobre sus actuaciones, o si, por el contrario, se debe promover una intervención mínima del Estado favoreciendo la capacidad de autorregulación de las propias empresas, intervención versus autorregulación.

La balanza se ha inclinado hacia el favorecimiento de la autorregulación junto a cuerpos legislativos anti fraude, junto a una serie de escándalos financieros que producen un aumento de la preocupación sobre cómo se estaban gestionando las empresas y sus relaciones con los gobiernos, en el caso de Estados Unidos con el gobierno de Reagan y posteriormente con la aprobación de la Ley Sarbannes Oxley, que establece procedimientos de auditoría interna, y paralelamente, con el Gobierno de Margaret de Thatcher en Reino Unido.

Europa proseguirá también estas tendencias, desarrollándose durante las últimas décadas un modelo de intervencionismo estatal cuyo eje central es la capacidad de autorregulación de las corporaciones. La Unión Europea ha reconocido expresamente estas nuevas técnicas de producción normativa de marcado carácter soft law, configuradas como mecanismos alternativos a las imposiciones legales realizadas mediante directivas o reglamentos, como las recomendaciones de la Unión Europea, autorregulación y corregulación.

En 1999, los miembros de la OECD, entre ellos España, que lo es desde su creación en 1961, aprueban los Principios de Buen Gobierno Corporativo, que constituyen un instrumento internacional que ofrece normas no vinculantes y buenas prácticas internacionales, con una guía para su implantación que incluye 12 recomendaciones sobre los derechos de los accionistas, revelación de datos, o funciones de los consejos de administración, entre otros.

Estos modelos se basan en la cooperación entre distintos agentes sociales, económicos y gobiernos, convirtiendo además a la empresa en responsable no sólo de fomentar ciertas prácticas a través de códigos de buen gobierno corporativo o códigos éticos, junto a la acción de la propia legislación, sino de auténtico garante de cumplimiento de esos códigos creando sus propios sistemas de enforcement, que a su vez favorecen el cumplimiento de la ley en la medida en que los miembros de las empresas comiencen a asumir valores éticos como propios, valores en los que también descansa el propio Derecho Penal.

Las ventajas de estas herramientas de autorregulación no son pocas; principalmente, resultan en muchos casos más eficaces las propias regulaciones internas de las empresas en la medida en que se acercan más a su realidad al haberse creado en su ámbito y con medios y conocimientos técnicos específicos para cada actividad. De forma contraria, se corre el riesgo de que las empresas terminen usando estas herramientas de manera negativa, precisamente para crear estructuras criminales con aparente cumplimiento normativo.

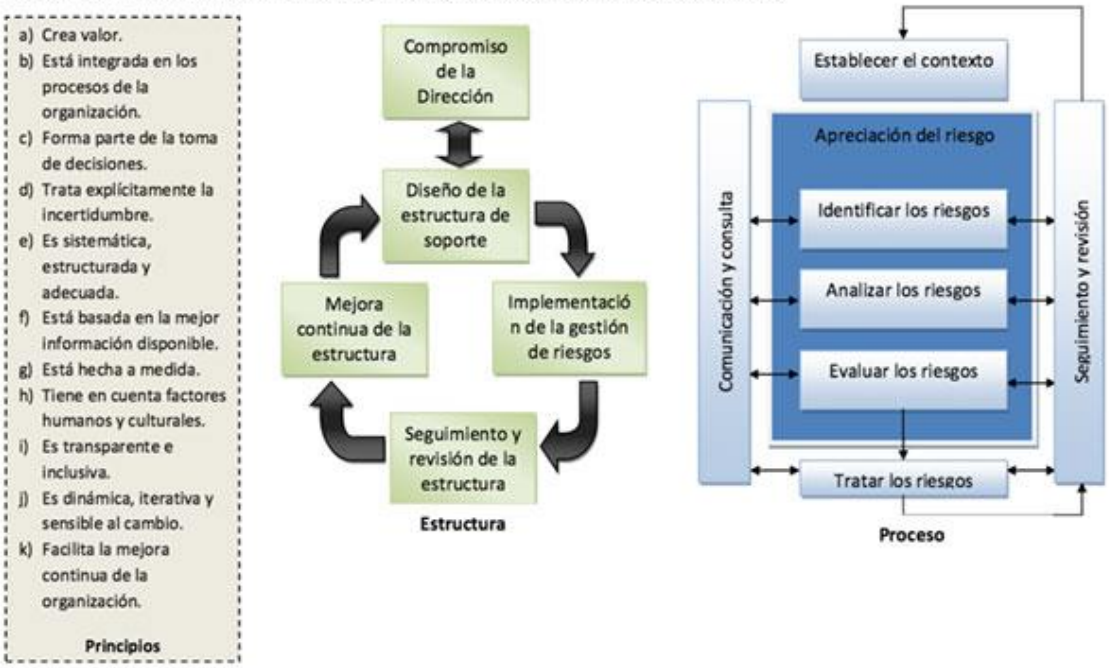
La autorregulación se configura como un mecanismo que sirve a las empresas para la propia valoración de los riesgos, creación de normas de conducta y sistemas de control interno sobre esos posibles riesgos, aumentando los niveles de diligencia dentro de la empresa y conformándose como una parte significativa de los programas de cumplimiento normativo, lo que contribuye a mitigar la posible responsabilidad penal de la empresa.

En el ámbito de las sociedades cotizadas y grandes corporaciones, en España, se pretende en 1998 por vez primera concretar y especificar una serie de principios de referencia para las empresas, publicándose el Informe de la Comisión Especial para el Estudio de un Código Ético de los Consejos de Administración de las Sociedades, que se materializa en un Código de Buen Gobierno denominado Código Olivenza, con 23 reglas en forma de recomendaciones de voluntario cumplimiento. En el 2002, se encargó a la Comisión Aldama una visión más completa del gobierno corporativo y en la que se estudiasen algunas medidas de necesario cumplimiento derivadas de diversa normativa, para finalmente, en el año 2006, aprobarse el Código Unificado de Buen Gobierno Corporativo dirigido a las sociedades cotizadas en consonancia con las recomendaciones de la Unión Europea y la legislación internacional.

La auditoría interna también resulta un elemento esencial en la formación de los programas de cumplimiento o compliance, siendo uno de sus elementos primarios. La posibilidad de detección de irregularidades y fraude en el seno de los procedimientos de la empresa supone una importante responsabilidad para las personas encargadas de velar porque la actividad se desarrolle dentro de legalidad, confiriendo a los auditores la función de denunciar e investigar dichas regularidades. Junto a ello, que las empresas se sometan además a controles externos tanto de índole financiero cómo de otro tipo como puede ser de sostenibilidad, laboral, etc., garantiza que un órgano externo supervise su actuación de manera objetiva.

Se trata de un verdadero ecosistema en el que cohabitan elementos de autorregulación y de coerción estatal, configurado por los códigos éticos y de buen gobierno y las normativas sectoriales y administrativas, por lo que la imposición de sistemas de cumplimiento normativo entendidos como un único bloque va a propiciar el correcto funcionamiento de las organizaciones empresariales en el tráfico jurídico, fomentando las buenas prácticas e imponiendo medidas penales gravosas para aquellas que decidan no seguir los procesos establecidos.

Relaciones entre los principios de gestión del riesgo, la estructura organizacional y el proceso.



MODELO DE COMPLIANCE PENAL

Los requisitos de la ley para que el Compliance implique eximente de la responsabilidad penal, implican que el plan debe contener y promover:

1. Un modelo de control, prevención y reacción penal de la empresa, de sus directivos y de sus empleados. Una parte esencial en la implementación de un modelo de Compliance es la definición de un protocolo de toma de decisiones que garantice que las mismas se tomen de un modo ético y transparente, tanto por los dirigentes como por los empleados.

2. Un mapa de riesgos de comisión de delitos en función de las distintas áreas o departamentos de la empresa.

3. Nombramiento de un responsable de Compliance o un Comité de Compliance, en función del tamaño de la empresa, garantizando su independencia y dotándolo de mecanismos de control descentralizados.

4. Al responsable o los responsables de cumplimiento normativo deberá asignársele una partida presupuestaria: Por ello, es necesario adoptar un modelo de financiación que debe quedar correctamente reflejado en la política de cumplimiento normativo.

5. Definición de un modelo de gestión de los recursos financieros de una compañía aplicado al Compliance adecuado para impedir la comisión de los delitos identificados en el mapa de riesgos.

6. Creación de canales o medios internos de denuncia de delitos. Deben implementarse canales de denuncias para que cualquier empleado, o incluso un cliente o un proveedor, puedan transmitir de manera confidencial al responsable o responsables del cumplimiento normativo cualquier incumplimiento de las normas internas de la empresa o bien conductas ilegales. La Circular de la Fiscalía ha aclarado el especial valor del descubrimiento de delitos por la propia empresa, de manera que esta sea la que los pone en conocimiento de la autoridad competente.

7. Establecimiento de un sistema disciplinario eficaz y suficiente. Sin un sistema que castigue aquellas conductas contrarias a la ética de la empresa el programa de Compliance carecería de eficacia. Es recomendable establecer un sistema de incentivos para el comportamiento ético de empleados.

8. Redacción de un código ético que establezca las bases de comportamiento de la empresa, como la integridad, la prohibición de corrupción, tráfico de influencias e infracciones de propiedad intelectual, etc. Dicho código ético debe ser obligatorio para todos los miembros de la empresa, y su incumplimiento debe ser comunicado al responsable del cumplimiento normativo y este a la más alta dirección para la adopción de medidas y la puesta en marcha del sistema disciplinario establecido, dejando siempre los correspondientes registros de lo detectado, actuado y decidido.

DERECHO PENAL Y NUEVAS FORMAS DE CRIMINALIDAD ECONÓMICA

El Derecho Penal representa una forma de control social formal. A través del poder punitivo del Estado, específicamente, de la criminalización de conductas (función preventiva) y de la sanción de las infracciones cometidas (función represiva), se busca controlar el comportamiento de las personas a fin de evitar la vulneración del ordenamiento jurídico.

Es necesario mencionar que el Derecho Penal, al ejercer poder punitivo y coacción sobre las personas, se rige bajo el principio de última ratio y de mínima intervención, es decir, solo se ejercerá cuando otras formas de control social, informales o formales, fracasen. En tal sentido, queda claro que el derecho penal no interviene en todas las situaciones que generan algún daño al orden jurídico, sino que limita su actuación a aquellas situaciones más graves, más

reprochables. De modo que la sobre criminalización de conductas, es decir, la creación indiscriminada de delitos, constituye una injerencia inconstitucional en la esfera jurídica de las personas y es contraria a los principios básicos del Derecho Penal.

Durante las últimas décadas, la sociedad ha sido testigo del desarrollo y crecimiento exponencial de diversas corporaciones como consecuencia de la liberalización del mercado, de la globalización, de las múltiples operaciones económicas que se realizan día a día y del avance científico y tecnológico. Estas distintas y nuevas actividades empresariales constituyen una fuente de riesgos y han dado lugar a la generación de nuevas formas de criminalidad, en especial, la criminalidad empresarial.

Sumado a esto, es necesario recordar los grandes escándalos económicos en Estados Unidos de América, como consecuencia de la quiebra de grandes corporaciones como Enron o Lehman Brothers Holdings, Inc. Estos casos permiten percibir la relevancia de las corporaciones en la sociedad, en tanto generan un alto impacto, en algunas ocasiones negativo, provocando riesgos para los bienes jurídicos que el derecho penal busca proteger.

Por ejemplo, de acuerdo con una encuesta realizada por PricewaterhouseCoopers (PwC)2 en 90 países, resulta que el 6,3% de las empresas consultadas experimentó un episodio de delito económico, originados tanto interna como externamente. En el caso peruano, el 19,5% de las empresas ha sufrido un delito económico en los últimos 24 meses. Si bien la cifra no es alta, lo preocupante es que del 73,2% de las empresas peruanas que participaron de la encuesta y aseguraron no haber sido víctimas de un delito económico en los últimos 24 meses, el 41,4% no realizó una evaluación de riesgos de fraude en dicho periodo. Es decir, un gran porcentaje de las empresas peruanas no cuenta con mecanismos para la prevención y detección de delitos económicos que se cometan al interior o exterior de la empresa o como consecuencia de las actividades que esta realiza.

Frente a esta situación de creación de nuevos riesgos, el Estado, como parte de su deber de protección de la sociedad, ha decidido tomar acciones conducentes a controlar y prevenir tales situaciones de riesgo. Por ejemplo, en el caso de los Estados Unidos de América, si bien en 1991 la United States Sentencing Commission promulgó las «Sentencing Guidelines» para incentivar a las corporaciones a adoptar programas de *Compliance*, a fin de prevenir las infracciones legales, los casos recientes de grandes fraudes, estafas y evasión de impuestos por parte de las empresas han obligado al Estado a iniciar una acción preponderante con la finalidad de controlar los riesgos empresariales.

Como se ve, existe consenso en que la actividad empresarial y el desarrollo económico, tecnológico y científico generan nuevos riesgos que ponen en peligro los bienes jurídicos que el derecho penal busca proteger.

EL RIESGO REPUTACIONAL

Aparece cuando la empresa no es capaz de cumplir con las expectativas de sus grupos de interés, stakeholders, y principalmente, de sus clientes. Al tratarse de ideas que se encuentran en la mente de los clientes, es algo externo sobre lo que la empresa puede influir pero no puede controlar. La buena reputación es el activo intangible más valioso de una empresa y por todos es conocido que una buena reputación puede tardar años en forjarse y unas pocas horas en perderse.

En los años 80 se calculaba que el 70% del valor de un negocio dependía de sus activos tangibles y un 30% de lo que aportaban sus activos intangibles, este paradigma ha dado un giro de 180 grados, ya que actualmente se calcula que un 70% del valor de un negocio depende de la calidad y gestión de los activos intangibles siendo la reputación el que tiene más peso.

Los daños a la reputación traen consigo no sólo un daño a la imagen de marca sino también, una reducción significativa de los ingresos debido al descenso de las ventas, en la mayoría de las ocasiones también tiene aparejado un aumento de la litigiosidad de la empresa y, dependiendo de la gravedad del caso, puede llegar incluso a la desaparición de la empresa.

Ejemplos como los casos Bankia o Volkswagen nos traen a la mente los efectos devastadores de una mala reputación y de una mala gestión por parte de su directiva.

Aquellos que piensan que este tipo de daños son propios de las empresas del IBEX35 están equivocados, ya que afectan a todas y cada una de las empresas por el solo hecho de estar activas y de tener clientes u otros grupos de interés como los casos de Fagor y Panrico.

Consideremos también un enfoque positivo sobre la reputación ¿Qué aporta a una organización cuidar y proteger activamente su reputación? Mayores ventas, mejor imagen corporativa, ser referente en el mercado, una mayor atracción y retención del talento en procesos de selección.

Para saber cómo protegerla debemos tener en cuenta cómo se originan estos riesgos. En primer lugar, encontramos los conflictos propiciados por la ética y la integridad de terceros incluyendo fraude, soborno y corrupción, seguidos muy de cerca por los riesgos de seguridad corporativa, los ataques provenientes de la competencia y por decisiones estratégicas tomadas sin la información necesaria.

Las organizaciones tienen más confianza cuando tienen que tratar riesgos que pueden afrontar bajo su control directo, como los relacionados con el cumplimiento de las normativas, los empleados y la mala conducta ejecutiva.

Ante estas situaciones las organizaciones necesitan disponer de modelos de gestión ágiles que permitan reducir los daños cuando un posible Riesgo Reputacional se convierte en realidad.

Una vez identificados los posibles riesgos de la empresa a través del mapa de riesgos, se deben desarrollar sistemas para el seguimiento, control y reporting. Sistemas en los que debe compaginar un enfoque proactivo con un enfoque reactivo. El enfoque proactivo se centra en la prevención, siendo su objetivo principal que los potenciales riesgos de reputación a los que está expuesta la organización no se materialicen, definiendo procedimientos de control para los principales Riesgos Reputacionales que hayan sido identificados en el mapa de riesgos.

La parte reactiva se centra en la minimización del daño una vez se haya convertido en realidad. Es necesario realizar tareas de investigación de lo sucedido, así como una eficaz tarea de comunicación y de control de daños.

Las empresas más avanzadas, están creando Comisiones que contemplan la reputación corporativa como un aspecto de enorme importancia, junto con otras áreas como la responsabilidad social corporativa y los recursos humanos.

De un estudio sobre Reputación Corporativa realizado en 2014 se desprenden los siguientes datos:

a) Un 87% de los directivos encuestados valora el Riesgo Reputacional como un riesgo más o mucho más importante que otros riesgos estratégicos.

b) La responsabilidad en la gestión de la reputación corporativa residirá en los niveles más altos de la organización: El CEO (36%), el Chief Risk Officer (21%), los directores de la Junta (14%) y el Chief Financial Officer (11%).

c) Las compañías encuestadas que habían tenido previamente experiencias negativas con su imagen, afirmaron que las áreas que se vieron más afectadas fueron los ingresos (41%), el valor de la marca (41%) y las investigaciones de los reguladores (37%).

La reputación corporativa está considerada actualmente como uno de los pilares de la supervivencia, el crecimiento de las empresas y de su diferenciación con respecto a su competencia. Por lo tanto es fundamental establecer procedimientos encaminados a su protección, es imprescindible la implicación de toda la empresa y el impulso decidido por parte del Management para implantar una cultura ética, basada en el Compliance y en el cuidado de la reputación.

EL RIESGO PENAL

El marco normativo de la Responsabilidad penal de las personas jurídicas en España, lo encontramos fundamentalmente:

-Por supuesto, el Código Penal, artículos 31 bis a 31 quinquies.

-La Circular de la Fiscalía General del Estado de 22 de enero de 2016.

-La Sentencia del Tribunal Supremo Nº 154/2016, de fecha 29/02/2016.

Ambas, Circular y Sentencia, insisten en el concepto de *"cultura de cumplimiento"* y "*cultura ética empresarial*". Se debe basar en la identificación y gestión de los riegos legales, en una actualización constante del panorama normativo y jurisprudencial que es fuente de tales riesgos y en un modelo de trabajo basado en que los comportamientos de los miembros de una organización estén orientados al cumplimiento, como vía para aumentar el valor de la organización, de sus productos y/o de sus servicios.

La RAE, define cultura como el *"Conjunto de modos de vida y costumbres, conocimientos y grado de desarrollo artístico, científico, industrial, en una época, grupo social, etc."*

La cultura de Compliance es un concepto desarrollado, por ejemplo, en la mencionada *Norma UNE-ISO 19600, Sistemas de gestión de compliance-Directrices (2014),* en cuyo apartado 7.3.2.3 se indican los parámetros por los que se puede medir el grado de cultura de Compliance de una organización.

En cualquier organización, el compromiso de la alta dirección y la implantación de cultura de Compliance deberían contemplar, como mínimo, lo siguiente:

-Una declaración formal, documentada y formulada por los administradores, en la que se manifieste su firme compromiso en favor de los objetivos de Compliance. Esta declaración debería hacerse pública, tanto dentro como fuera de la empresa incluyéndose, por ejemplo, en el Código de Conducta de la organización, debería ser comunicada periódicamente a todas las personas afectadas y podría estar disponible en la intranet y en la web pública de la empresa. Cada organización debe elaborar esta declaración en función de sus valores, objetivos y estrategia.

-Un compromiso real de la alta dirección en el desarrollo del Programa de Compliance, que deberá ser proporcional al tamaño y a las circunstancias de la organización. En organizaciones muy pequeñas, por ejemplo, el compromiso de los administradores será total, mientras que en grandes organizaciones la implicación de los administradores se reducirá a aprobar las políticas y a supervisar su correcta implantación, delegando en los equipos ejecutivos el diseño, la ejecución y la gestión de los procedimientos. Pero, en todo caso,

existen facultades indelegables que deben ser necesariamente ejercidas por los administradores

En Compliance, el cambio de cultura corporativa es una exigencia, y una consecuencia, sabiendo que el cambio es un camino que conlleva un proceso de interiorización, el empleo de recursos y de tiempo, y que debe articularse a través de los siguientes elementos esenciales como es un marco normativo, encabezado por un Código de conducta / ético, Canal de denuncias interno, la figura del Chief Compliance Officer autónomo y con recursos propios, formación y concienciación junto a un régimen disciplinario.

El Compliance es una realidad y una necesidad. El FC Barcelona está siendo investigado y acaba de nombrar una Compliance Officer. Telefónica está siendo investigada, lo mismo que Lazard Asesores Financieros, con relación a uno de los procedimientos contra Rodrigo Rato.

Por tanto, las empresas pueden adoptar dos posiciones: Esperar a que las *"innovaciones llevadas a cabo en otros grupos humanos"* les sean de interés cuando se vean incorporadas a procedimientos penales, en los que cambiar su cultura de Corporate Compliance sirva, a lo sumo, para reducir la pena; o adoptar un modelo de Corporate Compliance que responda a su propia realidad, tamaño, actividad, ubicación, enfoque de riesgo, precedentes, etc.

Exención penal a través del Compliance

Un Compliance es una oportunidad de negocio con la que lograr tanto eliminar los riesgos penales por la comisión de delitos en el seno de la compañía, como consolidar su buena reputación en el mercado y obtener ventajas competitivas frente a otros.

El Compliance mejorará la percepción de terceros sobre la empresa y le permitirá acceder a la eximente de responsabilidad penal de la persona jurídica del Código Penal, siempre que pueda acreditar, a través de sus registros, el haber implementado correctamente un buen sistema de prevención de delitos.

El itinerario viene marcado por la Circular de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas**,** que ha permitido definir los pasos que una empresa debe dar en la implementación de su modelo de Compliance. La obtención de la exoneración completa de responsabilidad o bien de tan solo una exoneración parcial dependerá del correcto desarrollo de dicho modelo.

Como indica la Circular de la Fiscalía, no es suficiente establecer un modelo de organización y gestión a través del programa de Compliance, sino que el mismo debe implementarse correctamente en la práctica. Se trata de que se traduzca en el día a día de la empresa en una verdadera cultura ética

corporativa**,** de modo que influya en la toma de decisiones tanto de empleados como de directivos.

Para lograr esto, es fundamental establecer vías de control y hacer un seguimiento escrupuloso del cumplimiento del programa de Compliance. Es importante también trasladar la ética del programa de Compliance a todos los trabajadores, de modo que conozcan la política de la empresa; un modo eficaz de lograr esto es a través de la realización de ciclos didácticos por parte de profesionales de Compliance para formar a los empleados.

A lo largo de la vida de una empresa los delitos con riesgo de ser cometidos y las necesidades de control de las áreas o departamentos no permanecerán inalterados, de ahí la necesidad de hacer un seguimiento continuo y de adaptar el plan de Compliance a la realidad de la misma como elementos claves a la hora de lograr una eximente total de responsabilidad en caso de que se cometa un delito en el seno de la compañía. Realizar una auditoría y una readaptación periódica del plan de la política de Compliance se convierte en un aspecto esencial de dicha política.

Eximentes, agravantes y atenuantes

Una circunstancia eximente de la responsabilidad penal es aquella que exonera o libera de la responsabilidad penal a aquel que ha cometido un delito. Aunque en el Código Penal vienen enumeradas, el juez puede en atención al caso concreto, decidir sobre la aplicación y alcance finales de la eximente.

En concreto nuestra normativa contempla como causas eximentes:

a) Cualquier anomalía o alteración psíquica**,** que impida comprender la ilicitud del hecho.
b) Hallarse bajo Intoxicación plena o un síndrome de abstinencia**.**
c) Sufrir graves alteraciones en la percepción de la realidad.
d) El que obre en defensa de la persona o derechos propios o ajenos.
e) Evitar un mal propio o ajeno.
f) El que actúa impulsado por miedo insuperable.
g) Obrar en cumplimiento de un deber**.**

Un ejemplo de exención de responsabilidad penal es la adecuada adopción y ejecución de un programa de *Compliance* por parte de la empresa. De esta forma, en caso de producirse un delito en el seno y en beneficio de la compañía, aunque fuese indirecto, el plan de prevención de delitos implantado previamente de forma correcta, actuaría como circunstancia eximente de la responsabilidad penal derivada de la comisión de ese delito.

Es atenuante la circunstancia que reduce o aminora la responsabilidad penal. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas físicas o jurídicas haber realizado, con posterioridad a la comisión del delito, alguna o varias de las siguientes actividades:

a) Confesar la infracción a las autoridades.
b) Reparar o disminuir el daño causado por el delito.
c) Haber colaborado en la investigación del hecho.

d) Haber establecido antes del comienzo del juicio oral medidas eficaces para prevenir y descubrir los delitos**.**

Es agravante la circunstancia modificativa que aumenta el grado de responsabilidad de aquel que comete el delito. A efectos penales supone la aplicación de penas más duras para el infractor por considerarse mayor su grado de culpa o intencionalidad. Puede ser:

a) Ejecutar el hecho con alevosía.
b) Ejecutar el hecho con abuso de superioridad o aprovechando las circunstancias.
c) Ejecutar el hecho mediante precio, recompensa o promesa.
d) Cometer el delito por motivos racistas, antisemitas o discriminatorios.
e) Aumentar deliberada e inhumanamente el sufrimiento de la víctima.
f) Obrar con abuso de confianza.
g) Prevalerse del carácter público que tenga el culpable.
h) Ser reincidente.

CANAL DE DENUNCIAS INTERNO, WHISTLEBLOWERS

Su objetivo es prevenir el fraude interno, resguardando los intereses de la compañía, mitigar el riesgo de conflictos legales y contribuir a la transparencia en la gestión del negocio. En algunas empresas se utiliza una línea telefónica, un correo electrónico o ambos. A través de Whistleblowing, los trabajadores de la empresa, podrán denunciar hechos irregulares, contrarios a la norma y al código ético de la empresa, siendo los puntos esenciales los siguientes:

a) Carácter confidencial de la denuncia.
b) Carácter independiente al *Management d*e la empresa.
c) Necesidad de soporte probatorio.
d) Valoración técnico-jurídica de la denuncia.
e) Actuación, autoridad y control del proceso.
f) Respuesta inmediata.
g) Protección frente a represalias.

Un canal de denuncias ofrece a las empresas una alternativa para convertir a su personal, proveedores, clientes en guardianes del patrimonio empresarial y la reputación de la marca. Según cifras de la ACFE, Association of Certified Fraud Examiners, en su estudio anual sobre Fraude Ocupacional de 2016, el 39.1% de los fraudes internos cometidos por personal de una empresa, son detectados inicialmente por una denuncia.

Dos de cada cinco fraudes a empresas son descubiertos porque un empleado es quien lo comunica, y es por ello que las empresas están implementando canales de denuncia formales, a través de mecanismos que garanticen la confidencialidad y protejan al denunciante frente a cualquier tipo de represalias.

La denuncia es el principal método de detección de fraude tanto en PyMES como en grandes empresas, lo cual rompe el paradigma de que los sistemas éticos y líneas éticas sólo son útiles en grandes empresas.

En el caso de organizaciones con una línea de denuncias, se detectó el fraude en 47.3% de los casos, mientras que en organizaciones sin línea de denuncias se detectó en apenas 28.2% de los casos.

La detección a tiempo de incidencias y posibles infracciones legales, permite a la empresa planificar su reacción, iniciar las investigaciones pertinentes, subsanar los daños y notificar a las autoridades cuando corresponda. La ejecución de estas medidas puede suponer pérdidas en multas, transacciones, gestión de la crisis, además del posible lucro cesante y daño emergente, y de la inversión en recursos humanos y tiempo que debe dedicar la empresa a atender el asunto.

No obstante, el canal de denuncias debe enfocarse como una vía efectiva para generar eficacias, ahorrar costes y tiempos a la empresa, en lugar de ser considerado como un requisito o exigencia formal para cumplir con el programa de Compliance.

Para las PyMES, la implementación de un canal de denuncias es también un aval frente a los proveedores, aliados y clientes de la empresa, quienes tendrán la garantía de que podrán informar a su stakeholder de cualquier situación irregular o incidencia para que ésta sea atendida.

Algunos perciben los canales de denuncias como una carga para la empresa porque la obliga a investigar denuncias que en ocasiones pueden ser falsas o pudieran ser utilizadas para difamar el buen nombre de algún trabajador o la reputación de la empresa. Se trata de un medio necesario para conocer lo que ocurre dentro de la empresa de una manera objetiva, segura y confiable, de una fuente que tiene acceso a información que de otra forma no podría conocerse por los responsables del cumplimiento normativo.

Lo viable no es omitir el canal de denuncias, sino implementar mecanismos efectivos de investigación que permitan filtrar la información, descartando aquella que no sea relevante ni pertinente, y procediendo a investigar formalmente aquellas denuncias que enciendan los niveles de alarma.

No escuchar al trabajador que tiene intención de denunciar una irregularidad es uno de los mayores errores que puede cometer una empresa hoy en día, no sólo porque atenta contra una cultura de ética corporativa transparente, sino porque aquellos trabajadores que no son escuchados por sus empresas, suelen recurrir a las autoridades, como ha sido el caso de grandes empresas como Enron, quiebra; GlaxoSmithKline, 750 millones de dólares en multas o Pfizer, 2.300 millones de dólares.

FORMAR LA VOLUNTAD, FORMACIÓN Y COMUNICACIÓN

En relación a la toma de decisiones, los modelos de organización y gestión de las empresas deben establecer los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas. El esquema básico de un proceso de toma de decisiones críticas o de alto riesgo, que debería formar parte del reglamento del Consejo de Administración y del modelo de prevención y control de una empresa, podría tener: solicitud de informes internos y externos; asesoramiento jurídico especializado en los riesgos a prevenir; evaluación objetiva de los riesgos: Laboral, fiscal, medioambiental, penal, etc.; análisis de advertencias y mensajes de alerta recibidos; análisis de escenarios posibles; análisis de alternativas; análisis de costes y nivel de endeudamiento; balance de prioridades entre intereses individuales y colectivos y mayoría reforzada en el proceso de votación.

La prevención del delito depende de la formación de la voluntad que es posible en buena medida a través de programas de formación, comunicación y procesos democráticos y transparentes de toma de decisiones.

El objetivo es instaurar una cultura de cumplimiento empresarial por medio de sensibilizar y concienciar de la necesidad de unirse a la cultura de cumplimiento y de esta manera diseñar y disponer de las herramientas adecuadas.

Se sugiere una formación básica común a todo el personal, pero no es necesario que el personal del área de ventas y el personal del almacén de la empresa reciban la misma formación, ni que se realice a través del mismo medio. Debe adaptarse a las necesidades empresariales para que los empleados entiendan sus obligaciones y los riesgos de incumplimiento. No sólo será formación inicial sino que debe repetirse con regularidad para profundizar en los conocimientos adquiridos, informar sobre las novedades, modificaciones y nuevos riesgos.

Por su parte, la comunicación tiene una doble dimensión, la de dar a conocer las posibles irregularidades que puedan producirse en el seno de la compañía, canal de denuncias y la de extender el mensaje de conducta ética empresarial. Con el correcto uso de la comunicación interna para informar a los trabajadores y orientar acerca de las mejores prácticas y procesos se conseguirá una adhesión mayor.

La estrategia de comunicación debe englobar todas las áreas de la empresa y así convertirse en un rasgo diferenciador de la cultura empresarial.

Para que la implantación del Programa de Compliance sea eficiente y efectivo es necesario que sea bien entendido tanto por los altos cargos de la organización como por el resto de empleados. Además depende del conocimiento que los miembros de la compañía tengan sobre el mismo, por lo que la formación y la comunicación interna son factores decisivos, que están muy

conectados ya que los empleados solo podrán detectar posibles irregularidades, y por tanto comunicarlas, si las han conocido a través de la formación.

Para que esto sea posible la Alta Dirección de la empresa debe estar especialmente sensibilizada y debe apoyar al Compliance Officer en el desempeño de sus funciones. El éxito del programa de Corporate Compliance se basa en establecer acciones de formación que garanticen que los empleados entienden qué se espera de ellos. Asimismo, la comunicación adecuada del mensaje de conducta ética profesional y su cumplimiento debe ser permanente, hasta convertirse en un rasgo diferenciador de la cultura empresarial.

De acuerdo con las mejores prácticas internacionales así como las federal sentencing guidelines (FSG), la formación de los empleados en ética y compliance es un elemento esencial de cualquier programa de compliance. La ISO 19600 y las FSG van más allá al recordar que la organización deberá adoptar los pasos apropiados para comunicar de forma periódica y práctica sus políticas y procedimientos en compliance así como todos los aspectos relevantes del programa de ética y compliance mediante programas de formación efectivos e informar a los empleados en función de sus puestos y responsabilidades.

La formación en ética y compliance permite adquirir las competencias necesarias para tratar y decidir correctamente ante conflictos éticos en el trabajo. De esta forma los empleados pueden actuar con la seguridad necesaria y evitar dilemas insalvables. Por un lado, la formación adaptada a cada área o departamento y trabajo es más útil para los empleados y por tanto más efectiva en términos de compliance. Por el otro, recientes estudios muestran que los empleados que han participado en formación en ética y compliance tienen una percepción e imagen mejor de la propia empresa. Cuanta más comunicación menos incumplimientos. De esta forma la actitud de la empresa debe ser proactiva y salir de la formación tradicional y frontal y aprovechar una buena política de comunicación interna, externa y formación para inculcar los valores y principios éticos recogidos en su Código Ético.

MODELO DE LAS TRES LÍNEAS DE DEFENSA

La mayoría de las organizaciones cuentan con áreas y personal especializado para la gestión del riesgo y control interno. A veces pueden existir brechas o espacios en la cobertura de los controles internos y hasta generar duplicación o creación de actividades innecesarias. El modelo de las Tres Líneas de Defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

El modelo clasifica las áreas funcionales y de responsabilidad de la empresa y brinda una visión de las operaciones, garantizando una adecuada supervisión y gestión del riesgo, además de ser apropiado para cualquier organización independientemente de su tamaño o complejidad.

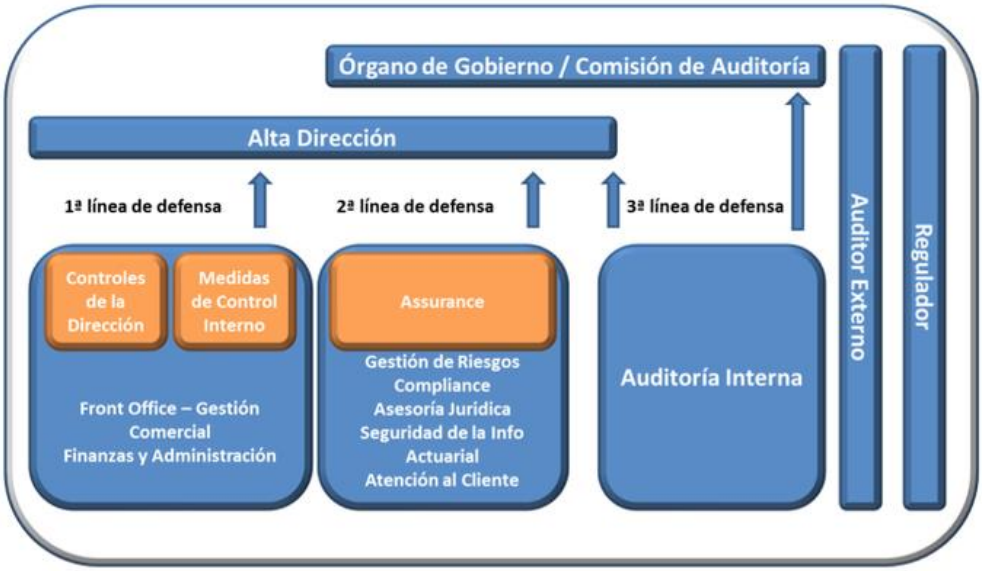
El modelo distingue tres líneas de actividades que participan en una efectiva gestión y supervisión de riesgos. La alineación de las tres líneas de defensa permite mitigar de una forma integral los riesgos.

La primera línea está compuesta por el control de la gerencia, donde cada área operativa de la organización pone en práctica la gestión de sus propios riesgos y controles, para asegurar el cumplimiento de los objetivos de la organización a través de un adecuado sistema de control interno.

La segunda línea contempla las funciones de supervisión de riesgos, controles y cumplimiento de políticas y estándares establecidas por la administración, abordando riesgos transversales, complejos y específicos; ambas, primera y segunda línea, reportan a la Alta Dirección.

En la tercera línea está el aseguramiento independiente, la Auditoria Interna, la cual aporta supervisión objetiva sobre las dos primeras líneas de defensa, evalúa el sistema de control interno de la organización en su conjunto para identificar debilidades y recomendar mejoras. La Auditoría Interna debe reportar a la Alta Dirección y a la Junta Directiva.

Finalmente, y fuera del marco de la organización, se encuentran la Auditoría Externa y Organismos Reguladores, que no integran el sistema de control interno sino que lo examinan independiente y externamente.



Cada una de las tres líneas juega un papel distinto dentro del marco de gobernabilidad de la organización, considerando primero las funciones esenciales de los organismos de gobierno corporativo.

Las tres líneas de defensa deben contar con un nivel de separación e independencia suficiente para no comprometer la efectividad del esquema general, y actuar coordinadamente con el fin de maximizar su eficiencia y potenciar su efectividad.

El Instituto Internacional de Auditores, IIA, establece ciertos principios orientativos para determinar si el grado de madurez de la organización permite avanzar hacia un modelo de tres líneas de defensa, o no, como son:

a) Existencia de un comité de auditoría idóneo, capaz de monitorear el accionar de las diferentes funciones de aseguramiento y su integración.
b) Formalización de las responsabilidades por el mantenimiento de un sistema de control interno y la gestión de riesgos.
c) La auditoría interna debe ser profesional y eficaz, habiendo logrado demostrar su adhesión a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, y el Director Ejecutivo de Auditoría Interna debe contar con la necesaria independencia para ejercer sus funciones

Si se intenta avanzar en un modelo de tres líneas de defensa sin haber asegurado previamente estas condiciones, es posible que el control interno de la organización no mejore sino que incluso se perjudique, al intentar confiar funciones más importantes a áreas que no son idóneas ni confiables

Ventajas del modelo de tres líneas de defensa:

- **Sólido:** Sólido significa que no presenta grietas. Está explícito el alcance de las labores de cada una de las funciones de segunda línea de defensa, hasta dónde llega cada una de ellas. Para evitar solapamientos en las tareas y contradicciones entre las opiniones de diversas áreas.
- **Robusto:** Esta característica se percibe al advertir que la fuerza de las distintas funciones de aseguramiento es mayor cuando actúan coordinadamente que cuando cada una de ellas lo hace por separado.
- **Resistente:** La resistencia deriva de su integralidad y de la confianza que provee a la Dirección Superior el saber que una diversidad de especialistas están actuando coordinadamente a su servicio. Esto reduce sustancialmente la probabilidad de que alguna o algunas de las tareas de aseguramiento resulten eliminadas o debilitadas por no percibirse claramente su contribución al éxito de la organización.
- **Genera crecimiento dentro de la organización**: El rol de evaluación de un marco de control interno amplio que salvaguarde el cumplimiento de las metas operativas y atienda a sus riesgos estratégicos puede, colocar a la Auditoría Interna en un nivel alto.
- **Las operaciones se hacen más eficientes:** Al integrarse y fluir la operación y el control como parte del mismo engranaje y sin oponerse el uno a la otra.
- **La información mejora y se integra.** Los diversos informes producidos por cada sector de la organización podrán ser consultados por el resto en forma oportuna para sus necesidades.
- **Se reducen los inconvenientes operacionales por riesgos imprevistos**: Dado que cada función atiende su responsabilidad sin omisiones, duplicidades ni contradicciones

Desventajas del modelo de tres líneas de defensa:

1. Es un modelo tan sofisticado y complejo que involucra diversas erogaciones:

    a) En personal, debe existir personal idóneo para atender las diversas funciones de la segunda línea de defensa.
    b) En capacitación, este personal debe mantenerse constantemente entrenado y motivado.
    c) En desarrollo de normativa, el desarrollo de las políticas y procedimientos para coordinar a este equipo suponen un esfuerzo económico considerable.
    d) En software, no necesaria, pero idealmente, podría contarse con un software que integre una base de datos de conocimiento compartido por todas las áreas, de modo que cada quien disponga de información adecuada para el desarrollo de sus funciones, en primer lugar, y para supervisión del nivel superior, en segundo término.

2. Para lograr las sinergias entre las áreas de segunda línea de defensa, y una adecuada interrelación entre éstas y la gerencia de primera línea, se requiere un importante esfuerzo de coordinación y buena comunicación interdepartamental.

En caso contrario, surge una burocracia que traba la operación y resta eficiencia a la organización.

El COMPLIANCE OFFICER

El *Compliance Officer* es considerado dentro del entorno corporativo como una pieza vital en la dirección de las empresas. Su rol como garante del cumplimiento normativo lo ha convertido en una figura ya no consultiva o reactiva, sino un verdadero partícipe en la toma de decisiones empresariales.

La figura del *Compliance Officer*, Oficial de Cumplimiento, apareció originalmente en los mercados financieros altamente regulados y en el sector farmacéutico, como una función encargada de vigilar el debido cumplimiento de la extensa normativa que debían cumplir las empresas en esos sectores.

A raíz de los escándalos financieros corporativos de principios de los 2000 y posteriormente la promulgación de la *Sarbanes-Oxley Act* en 2002 en los Estados Unidos de América, se comenzó a designar a esta figura como una especie de intendente para garantizar el cumplimiento normativo dentro de la empresa, con cada vez mayor injerencia en las decisiones del negocio. En países como Inglaterra, Italia o Alemania, incluso existen precedentes de sanciones por incumplimiento de la responsabilidad del *Compliance Officer*.

En las grandes empresas ya no se habla sólo de un *Compliance Officer*, sino de un *Chief Compliance Officer* (CCO), figura de mayor autoridad y responsabilidad dentro de la empresa que goza de independencia operativa y financiera, con la capacidad para promover y ejecutar medidas específicas de prevención de riesgos legales, comunicar los planes y llevar a cabo las formaciones del personal, realizar investigaciones y recomendar sanciones.

A España, la figura del *Compliance Officer* llega de los países de habla inglesa, como una función de las empresas internacionales que se veían obligadas a cumplir con regulaciones extranjeras o políticas internas donde ya se exigía esta función.

Ni la reforma al Código Penal del año 2010 ni la modificación que entró en vigor el 1 de julio de 2015, se refieren específicamente al *Compliance Officer*. Sin embargo, sí establece esta última la obligación de cumplir con un deber de supervisión o vigilancia que tácitamente se resume en el cargo en cuestión; ello como condición *sine qua non* para hacer valer la exención de la responsabilidad penal de la empresa en el supuesto en que se concrete un delito que la genere.

Se trata entonces de un cargo que no está regulado expresamente en el marco jurídico español, pero que ejerce unas funciones que son de obligatorio cumplimiento para la prevención de riesgos penales. Es por ello que las empresas deben definir claramente cuál es el rol que jugará el *Compliance Officer*, estableciendo sus responsabilidades y por encima de todo dotándole de las atribuciones suficientes para que pueda ejercer la función encomendada que no es otra que la supervisión o vigilancia respecto al cumplimiento normativo de la empresa.

Marco Legal del *Compliance Officer*

Las obligaciones relativas a la supervisión y vigilancia derivan del artículo 31 del Código Penal que dice: "S*i el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones…..:*

2.ª La supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica…;

4.ª No se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª

Adicionalmente, es de obligado cumplimiento el cuarto punto del párrafo 5 del mismo artículo 31 bis, que encomienda al órgano encargado de vigilar el funcionamiento y observancia del modelo de prevención, *la obligación de informar de posibles riesgos e incumplimientos*.

En consecuencia, es posible concluir que la supervisión, vigilancia y control deben ser encomendados a una persona u órgano que deberá cumplir con las siguientes premisas:

– Disponer de poderes autónomos de iniciativa y de control, o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos: Una de las características de la función debe ser su capacidad para tomar decisiones por cuenta propia y sin depender de la autorización de otros órganos, teniendo autonomía operativa y presupuestaria para llevar a cabo las investigaciones y ejecutar las medidas que considere apropiadas para garantizar el cumplimiento normativo.

– Que no se produzca una omisión o ejercicio insuficiente de sus funciones: El *Compliance Officer* será en muchas ocasiones el último filtro ante la prevención del delito. La determinación del límite que demarca el cumplimiento y la omisión en el ejercicio de sus funciones es una cuestión no exenta de dificultad, no existiendo todavía en nuestro país jurisprudencia sobre la materia. Es por ello que se exigirá al *Compliance Officer* la máxima diligencia, esto es, diligencia debida, en el desarrollo de sus funciones.

– Cumplir con el deber de informar los posibles riesgos e incumplimientos: Constituye la piedra angular de la función de supervisión y vigilancia, pues de su habilidad para detectar y notificar los riesgos se desprenderá la capacidad de la empresa para prevenir los delitos y tomar las medidas adecuadas para garantizar el cumplimiento normativo. Esta obligación está en consonancia con la posición de garante del *Compliance Officer*, tanto frente a la empresa como a terceros.

ESTRUCTURA INTERNA DE COMPLIANCE

Si bien el Código Penal enuncia las obligaciones de la función de supervisión, vigilancia y control, siendo su principal característica desde el punto de vista subjetivo la autonomía, no establece sino una limitación en cuanto al diseño de la estructura, y es que en las personas jurídicas de pequeñas dimensiones, las funciones de supervisión podrán ser asumidas directamente por el órgano de administración. Todas aquellas empresas que no sean consideradas personas jurídicas de pequeñas dimensiones deberán designar a una persona o un órgano para ejercer las funciones de supervisión, vigilancia y control.

Aquellas personas jurídicas de pequeñas dimensiones que consideren atribuir las funciones de supervisión al órgano de administración deberán tener en cuenta las dificultades que ello implicará para deslindar la responsabilidad de los Administradores de aquella que correspondería al *Compliance Officer*.

Para que la función vigilancia por parte del Compliance Officer sea considerada adecuada, es necesario:

– **Acceso directo al órgano de gobierno**: Si bien hasta hace algunos años era aceptable que la figura del *Compliance Officer* fuese un cargo intermedio que reportase al área legal o a un gerente o director financiero, hoy en día el estándar deseable es que la persona encargada o uno de los miembros del Comité (el CCO) tenga acceso no sólo al órgano de Administración, sino a quienes ejerzan el control del mismo o ante quienes rinde cuentas el órgano de Administración por ostentar la soberanía de la persona jurídica (Junta General).

– **Independencia**: Aunque ya señalamos la excepción para los casos de las personas jurídicas de pequeñas dimensiones, una de las características, y así está reflejado en la Norma ISO 19600, de un modelo de gestión de Compliance eficaz es la independencia de la función de supervisión y vigilancia, que deberá tener libertad de criterio y la garantía de que no sufrirá represalias por las decisiones que pueda tomar.

– **Nivel de autoridad apropiada y recursos adecuados**: Esto incidirá directamente en la eficacia del modelo de Compliance, puesto que un *Compliance Officer* sin la autoridad y recursos para implementar medidas, no sólo estará limitado en sus funciones sino que denotará falta de voluntad de la empresa en implementar el programa de Prevención de Riesgos Penales. Es clave para la empresa dotar a su *Compliance Officer* de suficiente autoridad y recursos, de manera que pueda llevar a cabo la gestión del modelo, realizar las investigaciones, la formación al personal, consultar a expertos, atender las crisis y mitigar adecuadamente los riesgos, pues no hacerlo puede tener como consecuencia el fracaso de todo el modelo. Todo ello sin perjuicio de que reporte y someta sus recomendaciones al órgano de Administración de la empresa.

Las mejores prácticas internacionales recomiendan que el Compliance Officer dependa directamente del órgano de administración, del Comité de Auditoría o del Comité de Compliance (en caso de que existan), dotándole

también de cierto grado de independencia presupuestaria. Alternativamente, puede establecerse una dependencia dual, reportando, por ejemplo, jerárquicamente al Consejo de Administración o al Comité de Auditoría y funcionalmente a un ejecutivo, como puede ser el Consejero Delegado o el Secretario General.

Qué se espera del Compliance Officer

Las responsabilidades del *Compliance Officer* en España parten del deber de informar los posibles riesgos e incumplimientos, pero no se limitan a ello. Se trata de una función que para poder cumplir cabalmente con ese deber y ser eficaz en su gestión, requiere ejecutar una serie de tareas de seguimiento, control, implementación, capacitación y notificación a los órganos de gobierno de la empresa.

No existe consenso en relación a sus responsabilidades, ya que varían de acuerdo al tamaño, sector y forma de organización de la empresa. Hay unas líneas generales de actuación comunes que vienen recogidas en la Norma ISO 19600:

1. Identificar las obligaciones a que están sujetas las empresas, tanto desde el punto de vista legal como también aquellas directrices que deriven de Códigos Sectoriales o de sus propias políticas o de Códigos Éticos. La doctrina refiere estos dos tipos de obligaciones como *Hard Law* y *Soft Law*, siendo las primeras aquellas que derivan de un mandato jurídico cuyo incumplimiento representa una infracción, mientras que las últimas son aquellas que voluntariamente decide cumplir la empresa como buenas prácticas sectoriales o de desarrollo de buen gobierno.

2. Comprender los procesos y procedimientos de la empresa, de manera que pueda integrar el desarrollo de los mismos con las obligaciones en materia de cumplimiento normativo.

3. Proveer o coordinar la formación continua en materia de cumplimiento normativo y dar soporte en el caso de dudas sobre cómo proceder o si cierta conducta constituye o no una infracción al Compliance de la empresa.

4. Responderá por la adecuada comunicación del programa de Compliance a los empleados, debiendo divulgar cualquier información relevante en materia de cumplimiento a las empresas y hacer entrega del Código de Conducta y las políticas a que estará sujeto el personal.

5. Contribuir en la descripción de las obligaciones de Compliance que sean inherentes a cada área o cargo dentro de la empresa, como parámetro objetivo en la evaluación de desempeño del personal.

6. Uno de los sectores que puede generar riesgos para las empresas son sus relaciones con terceras partes, deberá identificar y atender los riesgos derivados de sus relaciones con clientes, proveedores, distribuidores y

comerciales externos, así como con cualquier colaborador que pudiese ser considerado representante de la empresa.

7. Monitorear el funcionamiento del sistema de prevención de riesgos y tomar las medidas preventivas y correctivas que garanticen su eficacia y asegurar la revisión en los intervalos planificados.

8. Asesorar a la organización en materia de Compliance, bien sea directamente o a través de expertos externos.

9. Informar sobre cualquier incumplimiento, e implementar las medidas y controles que le permitan conocer oportunamente los riesgos e incidencias, bien sea a través del personal o inferidas de la propia documentación que recaba a través de procesos internos como puede ser:
   a) Sistema de denuncias, quejas y soporte telefónico o mediante correos electrónicos.
   b) Reuniones periódicas con los responsables de procesos.
   c) Informes periódicos de reporte de incidencias.
   d) Mecanismos de soporte directo a los empleados que tengan dudas sobre si una conducta representa un riesgo, antes de ejecutarla.
   e) Checkpoints y controles de procesos en los casos en que se exceda de los parámetros normales de operación en los cuales se requiera la aprobación del *Compliance Officer* , por ejemplo firma de contratos que excedan determinado monto, autorización de obsequios corporativos…
   f) Indicadores de desempeño y de cumplimiento de las medidas establecidas para garantizar el cumplimiento normativo y que reflejen la evolución del sistema de prevención de riesgos.

En relación al perfil del profesional del Compliance, quien asuma funciones de *Compliance Officer* o conforme un Comité a tales fines, se espera que demuestre valores como integridad, compromiso, liderazgo, comunicación efectiva, la habilidad para insistir y convencer sobre la aceptación de sus recomendaciones y un conocimiento profundo, o el acceso a expertos en la materia en temas de cumplimiento normativo.

Cabe destacar que el incumplimiento de estas responsabilidades puede acarrear no sólo las sanciones penales que establece el Código Penal para la empresa, sino también responsabilidades personales para el *Compliance Officer* que no haya ejercido su deber de vigilancia diligentemente.

Por ejemplo, un Tribunal Federal en Alemania condenó a la *Compliance Officer* de una empresa de basura de Berlín en el año 2009 por haber incurrido en omisiones respecto a su deber de supervisión y vigilancia a pesar de haber notificado el incumplimiento. Caso que, desde luego, será el espejo en el que se mirarán nuestros tribunales en breve como viene sucediendo en materia de Derecho Comunitario de la Unión Europea.

Además, en relación a sectores regulados, en España existen distintos organismos supervisores como es la Comisión Nacional del Mercado de Valores (CNMV), el Banco de España, la Comisión Nacional de los Mercados y de la

Competencia (CNMC), el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) o la Agencia Española de Protección de Datos (AEPD). En empresas de sectores regulados, sometidos a la supervisión de uno o varios organismos, es importante que exista una coordinación interna de las relaciones que se mantienen con ellos, con objeto de asegurar que se mantiene un diálogo abierto y transparente y de garantizar que se cumple con todos los compromisos adquiridos. Esta labor de coordinación generalmente es ejercida por el Compliance Officer.

Finalmente, solo señalar que las tareas del Compliance Officer implican relacionarse con un conjunto de *stakeholders*, tanto internos como externos a la organización. La necesidad de obtener información, asesorar y formar, realizar recomendaciones y supervisar al resto de departamentos de la organización, así como de relacionarse en ocasiones con personas ajenas a la organización (organismos supervisores, clientes, proveedores, etc.) para tratar de cuestiones en ocasiones delicadas, obliga a que el Compliance Officer deba tener una serie de aptitudes personales, tales como saber escuchar, capacidad de influencia o aptitudes de comunicación verbal y escrita, que le permitan hacerlo sin causar conflictos innecesarios.

El perfil del Compliance Officer

Dado la característica multidisciplinar del trabajo a desarrollar y lo que se espera de sus funciones, la titulación de origen es muy diversa.

En ocasiones puede ser un licenciado en derecho, en cuyo caso se tendrá que rodear de un equipo que cubra los aspectos relacionados con la monitorización, o por el contrario ser una persona con experiencia en gestión de riesgos, en cuyo caso deberá apoyarse en un equipo experto en el asesoramiento legal.

Independientemente de su formación académica, deberá conocer bien el negocio en el que opera la organización y tener la suficiente cualificación y experiencia profesional para ejercer la dirección de la función de Compliance. Capacidad, competencia y prestigio profesional son las cualidades necesarias para que las opiniones y recomendaciones del Compliance Officer sean aceptadas.

El jurista conoce las normas y obligaciones legales, sabiendo cómo interpretarlas y diseñar estrategias en torno a las mismas. Esa base de formación académica hace propicia la función del jurista para ejercer cargos de supervisión y vigilancia.

Sin embargo, debe distinguirse del rol del abogado defensor. El Compliance Officer velará por el cumplimiento de las leyes, pero es recomendable que la representación y defensa legal de la empresa dependa de otro profesional del Derecho para evitar una confusión en los roles. Es por ello que muchas grandes empresas han optado por separar su Departamento Legal de su Departamento de Compliance.

La función de Compliance Officer deberá velar por que cada quien dentro de la empresa cumpla con sus funciones, en lugar de interpretar las normas, ejercer o implementar estrategias defensivas en el caso de incumplimiento.

Al tener la responsabilidad de ejercer el control, supervisión y vigilancia dentro de la empresa, puede existir la percepción de que el Compliance Officer tendría que ser un experto en todas las materias. Sin embargo, esto no sólo es extremadamente improbable en la práctica sino que diluiría toda su capacidad de detectar incidencias al tener que abarcar áreas muy extensas.

El Compliance como disciplina involucra un conjunto de bloques normativos, que dependiendo del país pueden estar agrupados de distintas maneras. El Compliance Officer no tiene que ser un técnico especializado en cada una de ellas, pero sí debe poder supervisar las áreas, detectar los puntos débiles dentro de la organización, tener la capacidad de desarrollar mecanismos de control y controlar su evolución.

Algunas empresas farmacéuticas optan por designar a ingenieros químicos como Compliance Officers, o que las TIC se inclinen por un experto en seguridad informática; las empresas de la construcción, seguros, seguridad, etc. un ingeniero, arquitecto; las financieras un economista; los hospitales, un médico… En la medida en que las empresas tienen estructuras más amplias, se dará siempre el caso de un Chief Compliance Officer que aun siendo experto en alguna de las ramas, deberá confiar en otros profesionales para aquellas que no maneja directamente.

Como hemos señalado, en España el Compliance como obligación legal se generaliza a través del Código Penal, creando un catálogo cerrado de delitos que generan responsabilidad penal a la persona jurídica. La transversalidad de la legislación penal, que puede afectar delitos de los distintos bloques normativos, le da al penalista un perfil adecuado para atender los requerimientos de la función de un Compliance Officer integral, siempre trabajando de la mano de profesionales de otras disciplinas que lo asistan en la gestión de otros bloques normativos específicos.

A veces, se plantea que el rol del Compliance Officer es el de un policía dentro de la empresa. Al ser la función a cargo de la supervisión y vigilancia, es una percepción perfectamente comprensible, no obstante, las responsabilidades del oficial de cumplimiento deben ir mucho más allá de una mera detección de incumplimientos, debiendo entre otras cosas, identificar las obligaciones a que están sujetas las empresas, Hard Law y Soft Law; comprender los procesos y procedimientos de la empresa; coordinar las formaciones en materia de cumplimiento normativo; responderá por la adecuada comunicación del programa de Compliance, contribuir en la descripción de las obligaciones de Compliance que sean inherentes a cada área o cargo dentro de la empresa, como parámetro objetivo en la evaluación de desempeño del personal.

Además, implementar las medidas y controles que le permitan conocer oportunamente los riesgos e incidencias, por lo cual la visión del Compliance Officer como “policía” de la empresa, si bien puede ser una analogía válida, debe

ir complementada de una serie de elementos que dotan su función de una verdadera autoridad como garante del cumplimiento normativo corporativo.

El perfil, las aptitudes y las competencias de los miembros del departamento de Compliance deberán abarcar distintos aspectos: Perfil jurídico con conocimiento de las normas y con capacidad para interpretarlas, perfil de gestión de riesgos para evaluar los riesgos de Compliance, perfil auditor para realizar las tareas de monitorización, conocedor y gestor de procesos, perfil docente para formar a los empleados, etc. En definitiva, los miembros del equipo de Compliance deberán tener los suficientes conocimientos y experiencia para poder abarcar las diferentes tareas multidisciplinares que abarca la función.

Compliance Officer o Comité de Compliance

Nos hemos referido indistintamente al *Compliance Officer* o al Comité, en el entendido de que las funciones deberán ser ejecutadas por uno u otro de la misma manera. Sin embargo una de las primeras dudas que se plantea la empresa es cómo definir su estructura de Compliance.

La decisión de designar a una persona que ya ejecute otra función en la empresa, crear un nuevo cargo, instaurar un comité o contratar a un externo que se encargue del tema dependerá de la complejidad organizativa y tamaño de la empresa, teniendo en consideración sus singularidades y resultaría difícil recomendar a priori alguna estructura específica.

A veces las empresas pequeñas designen a una sola persona para ejercer estas funciones, como también lo es que decidan asignar estas responsabilidades a otra persona que ejerce labores de supervisión dentro de la empresa. Sin embargo, esta última alternativa, aunque aceptable en unos casos, tiene sus riesgos en tanto pueda generarse un conflicto de intereses o no se dote de una verdadera autonomía al *Compliance Officer*, poniendo en duda uno de los principios que debe regir la función.

Las personas jurídicas de pequeñas dimensiones, que por estar autorizadas para dejar la supervisión y vigilancia en manos del órgano de Administración, pueden incurrir no sólo en un conflicto de intereses (al estar sujetos a revisar sus propias actuaciones), sino en una falta de autonomía que podría hacer ineficaz el modelo. Es por ello que, en este supuesto, lo recomendable es que quien ejerza la función sea un director o administrador que no esté directamente vinculado con el área operativa, de manera que su labor no esté sujeta a la manera como se ejecutan los procesos.

En resumen, algunas consideraciones a tener en cuenta por la empresa al momento de definir su función de supervisión, vigilancia y control son:

a) La definición de la función del *Compliance Officer* será fundamental en la demostración de la eficacia del modelo, por tanto debe plantearse como una necesidad y darle la relevancia que tiene al cargo.
b) La figura debe estar dotada de autonomía funcional y presupuestaria.

c) Debe tener acceso a la Junta General y derecho a voz en los órganos de Administración.
d) Debe ser reconocido como una autoridad en el cumplimiento, tanto por el personal como por la propia administración de la empresa.
e) Su designación debe ser, en la medida de lo posible, realizada por la Junta General y no sujeta a revocación por parte de los Administradores.
f) Quien ejerza las funciones debe tener suficiente tiempo para atender los asuntos relacionados al cumplimiento normativo.
g) Debe tener acceso directo a expertos en materia de Compliance, Buen Gobierno, Fiscalidad, Penal, así como de cualquier otro tema en donde pudiera surgir un riesgo para la empresa.
h) El *Compliance Officer* debe ser partícipe de las decisiones estratégicas, de manera que pueda analizar los riesgos antes de que se ejecuten las acciones que puedan poner en peligro a la empresa.

La ubicación de Compliance

La Comisión Nacional del Mercado de Valores, CNMV, presentó el nuevo *Código de buen gobierno de las sociedades cotizadas*, que complementa la regulación sobre ciertas cuestiones relacionadas con el Compliance. Es importante conjugar el régimen de la *Ley de sociedades de capital* con las recomendaciones de dicho texto para ubicar correctamente la función de Compliance en el seno de estructuras empresariales complejas, como puedan ser las de sociedades cotizadas.

Los estándares internacionales más modernos de Compliance coinciden en recomendar que tal función disfrute de un fácil acceso a los máximos órganos de gobierno social, circunstancia que se traduce en una posición jerárquica elevada, cercana a los mismos. Se trata de un requisito sustancial para dotar de eficacia a la función, en la medida que no sólo refuerza su independencia sino que facilita una comunicación fluida y la rápida adopción de decisiones de alto nivel, llegado el caso.

A causa de las limitaciones inherentes a su tamaño, las pequeñas empresas desarrollan esquemas de Compliance simplificados, donde es el propio órgano de administración el que asume los roles de dicha función, aplicando principios de cumplimiento generalmente aceptados de manera proporcional a sus circunstancias internas (tamaño, recursos, etc.) y externas (sector de actividad, mercados en los que opera, etc). La normativa reconoce tal posibilidad en los modelos de prevención penal de las llamadas “personas jurídicas de pequeñas dimensiones”, las que presentan cuenta de pérdidas y ganancias abreviada.

En sociedades de mayores dimensiones, la función de Compliance suele encomendarse a un órgano con dependencia funcional del órgano de gobierno social, disposición que obviamente avala la proximidad a las máximas estructuras decisorias sugerida por los estándares de Compliance modernos.

No obstante, las organizaciones de un cierto tamaño, aun no siendo cotizadas, ya han venido dotándose de órganos y funciones relacionadas con la

gestión de riesgos, control interno y auditoría interna, que no pueden obviarse a la hora de impulsar un modelo de Compliance. De hecho, en no pocas ocasiones la función de Compliance es el resultado de un derivado o fracción de las mismas, nutriéndose de sus recursos y soportándose en ellas cuando resulta posible.

Lo importante radica no sólo en su estructura sino, sobre todo, en su adecuada integración con otros órganos necesarios para desarrollar su cometido.

De acuerdo con la Ley de sociedades de capital constituyen facultades indelegables del consejo de administración la determinación de la política de control y gestión de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control. Puesto que los riesgos de incumplimiento son tan sólo una porción de los que afectan a la organización en su conjunto, gestionados mediante sistemas específicos, es patente la posición de garante de los administradores respecto del cumplimiento de las normas.

Pueden crearse comisiones especializadas que, en función del perfil de sus componentes (independencia, formación y experiencia) acometan dicha labor de forma profesional. Dichas comisiones pueden auxiliarse, a su vez, de funciones o departamentos donde trasladen su cometido a la operativa diaria de la organización. Esta profesionalización alcanza su grado álgido en las sociedades cotizadas, obligadas a disponer, como mínimo, de una comisión de auditoría, y otra de nombramientos y retribuciones.

La Ley de sociedades de capital incluye dentro de las funciones mínimas de la Comisión de auditoría supervisar la eficacia del control interno de la sociedad y los sistemas de gestión de riesgos, incluidos los fiscales. Sobre la base de este entendimiento, ya generalizado antes de la modificación legal que lo consolidó, no pocas entidades cotizadas crearon estructuras de Compliance bajo la supervisión directa de su Comisión de auditoría.

Este ha sido un esquema clásico de emplazamiento de dicha función.

Al amparo de la posibilidad de crear comisiones especializadas reconocida por la vigente Ley de sociedades de capital, el nuevo Código de buen gobierno de las sociedades cotizadas otorga un notable protagonismo a la Comisión de responsabilidad social corporativa (RSC), que puede asumir roles relevantes en materia de Compliance. Se reconoce la capacidad de esta comisión para supervisar el cumplimiento de los códigos internos de conducta, así como evaluar todo lo relativo a los riesgos no financieros de la empresa, que incluyen expresamente, entre otros, los legales y los reputacionales, aunque éstos últimos no son verdaderamente una categoría de riesgos sino la mera consecuencia de los que sí lo son.

En cualquier caso, riesgos legales y daños reputacionales son materias típicamente tratadas en los marcos de referencia sobre Compliance.

El régimen que sugiere el Código de buen gobierno de las sociedades cotizadas se aparta de la ortodoxia propia de los modernos esquemas de gestión GRC (Governance, Risk management y Compliance), lo que desencadena una serie de consecuencias que dificultan sobremanera la rápida ubicación de una función tan crítica como la de Compliance.

Sugiriendo que la Comisión de RSC se ocupe de cuestiones estrechamente vinculadas con el buen gobierno, y que la Comisión de auditoría haga la propio respecto de la gestión del riesgo, es clara su correlación con los cometidos de Governance y de Risk management propios de un modelo GRC. Sin embargo, los cometidos de Compliance, cuya sustantividad brilla por su ausencia en el código, no quedan unívocamente asignados, sino que se distribuyen entre ambas comisiones según tengan naturaleza “no financiera” o “financiera”.

Esto conduce a algunas inconsistencias conceptuales y problemas prácticos.

Es cuestionable que los riesgos relacionados con el cumplimiento de la legalidad se califiquen de “no financieros”, a juzgar por el impacto en los estados financieros que se deriva de su régimen sancionador, según comprobamos en la prensa económica diaria. También es cuestionable que los riesgos fiscales, inevitablemente anclados a la comisión de auditoría por exigencia de la Ley de sociedades de capital, no compartan la condición de riesgo legal, considerando que su régimen regulador y sancionador deriva de la Ley General Tributaria y demás normativa fiscal.

Esta división artificial dificulta ubicar bajo una misma supervisión el conjunto de obligaciones de cumplimiento, que es precisamente el ánimo de las superestructuras de Compliance que pretenden las mejores prácticas.

En este planeamiento, la Comisión de auditoría, mantiene aquellos riesgos que puedan entenderse “financieros”, como los fiscales, y está habilitada para asumir también los que no lo son, pero que son igualmente riesgos a supervisar. Esto conlleva una notable concentración de responsabilidades en esta comisión y sus miembros.

En caso de que la Comisión de RSC u otra creada al efecto asuma los riesgos legales, tampoco podrá desvincularse completamente el sistema de gestión de cumplimiento (Compliance Management System, CMS) de la Comisión de auditoría, por cuanto no deja de ser interpretable en clave de sistema específico de gestión de riesgos, cuya supervisión constituye una de sus obligaciones ex lege. Por eso, la partición de las obligaciones de cumplimiento entre las dos comisiones (auditoría y RSC) precisará que la función de Compliance establezca vías de comunicación con ambas y añadirá complejidad al modelo.

COMPLIANCE Y PREVENCIÓN DEL BLANQUEO DE CAPITALES

La Prevención del delito de Blanqueo de Capitales, tiene como finalidad prevenir e impedir la utilización del sistema financiero para blanquear los capitales procedentes de cualquier tipo de participación delictiva, en la comisión de un delito castigado con pena de prisión superior a tres años.

En España, la vigilancia y el control de los riesgos relacionados con el delito de blanqueo de capitales corresponde al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, SEPBLAC, y desde un punto de vista normativo está regulado en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en el Real Decreto 925/1995, de 9 de junio, por el que se aprueba el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas Medidas de Prevención del Blanqueo de Capitales.

El lavado de dinero negro o blanqueo de capitales supone un "último eslabón" en la cadena criminal como proceso por el cual un dinero logrado de modo ilícito (negro) pasa a formar parte del flujo económico legal.

El art. 301 CP describe una variedad de conductas integradoras del tipo objetivo del delito:

1. Adquirir, convertir o transmitir bienes sabiendo que provienen de la realización de un delito grave.
2. Realizar actos que procuren ocultar o encubrir ese origen.
3. Ayudar a quien ha realizado la infracción o delito base, que ha de ser grave, a eludir las consecuencias de sus actos.
4. Ocultar o encubrir la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos a sabiendas de su procedencia ilícita.

Sujetos obligados a auditoria de prevención de blanqueo de capitales

La Ley 10/2010, de 28 de abril**,** de prevención del blanqueo de capitales y de la financiación del terrorismo será de aplicación a los siguientes sujetos obligados**:**

1. Las entidades de crédito. Finanzas. Cuentas bancarias.
2. Las entidades aseguradoras autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones, con las excepciones que se establezcan reglamentariamente.
3. Las empresas de servicios de inversión. Finanzas o Cuentas bancarias. Derechos reservados.
4. Las sociedades gestoras de instituciones de inversión colectiva y las sociedades de inversión cuya gestión no esté encomendada a una sociedad gestora.
5. Las entidades gestoras de fondos de pensiones.

6. Las sociedades gestoras de entidades de capital-riesgo y las sociedades de capital-riesgo cuya gestión no esté encomendada a una sociedad gestora.
7. Las sociedades de garantía recíproca.
8. Las entidades de pago.
9. Las entidades de pago y las entidades de dinero electrónico.
10. Las personas que ejerzan profesionalmente actividades de cambio de moneda.
11. Los servicios postales respecto de las actividades de giro o transferencia.
12. Las personas dedicadas profesionalmente a la intermediación en la concesión de préstamos o créditos, así como las personas que, sin haber obtenido autorización como establecimientos financieros de crédito, desarrollen profesionalmente alguna de las actividades a que se refiere la Disposición adicional primera de la Ley 3/1994, de 14 de abril, por la que se adapta la legislación española en materia de Entidades de Crédito a la Segunda Directiva de Coordinación Bancaria y se introducen otras modificaciones relativas al Sistema Financiero.
13. Los promotores inmobiliarios y quienes ejerzan profesionalmente actividades de agencia, comisión o intermediación en la compraventa de bienes inmuebles.
14. Los auditores de cuentas, contables externos o asesores fiscales.
15. Los notarios y los registradores de la propiedad, mercantiles y de bienes muebles.
16. Los abogados, procuradores u otros profesionales independientes cuando participen en la concepción, realización o asesoramiento de operaciones por cuenta de clientes relativas a la compraventa de bienes inmuebles o entidades comerciales, la gestión de fondos, valores u otros activos, la apertura o gestión de cuentas corrientes, cuentas de ahorros o cuentas de valores, la organización de las aportaciones necesarias para la creación, el funcionamiento o la gestión de empresas o la creación, el funcionamiento o la gestión de fideicomisos («trusts»), sociedades o estructuras análogas, o cuando actúen por cuenta de clientes en cualquier operación financiera o inmobiliaria.
17. Las personas que con carácter profesional y con arreglo a la normativa específica que en cada caso sea aplicable presten los siguientes servicios a terceros: constituir sociedades u otras personas jurídicas; ejercer funciones de dirección o secretaría de una sociedad, socio de una asociación o funciones similares en relación con otras personas jurídicas o disponer que otra persona ejerza dichas funciones; facilitar un domicilio social o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una asociación o cualquier otro instrumento o persona jurídicos; ejercer funciones de fideicomisario en un fideicomiso («trust») expreso o instrumento jurídico similar o disponer que otra persona ejerza dichas funciones; o ejercer funciones de accionista por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado y estén sujetas a requisitos de información conformes con el derecho comunitario o a normas internacionales equivalentes, o disponer que otra persona ejerza dichas funciones.
18. Los casinos de juego.
19. Las personas que comercien profesionalmente con joyas, piedras o metales preciosos.

20. Las personas que comercien profesionalmente con objetos de arte o antigüedades.
21. Las personas que ejerzan profesionalmente las actividades a que se refiere el art. 1 de la Ley 43/2007, de 13 de diciembre, de protección de los consumidores en la contratación de bienes con oferta de restitución del precio.
22. Las personas que ejerzan actividades de depósito, custodia o transporte profesional de fondos o medios de pago.
23. Las personas responsables de la gestión, explotación y comercialización de loterías u otros juegos de azar respecto de las operaciones de pago de premios.
24. Las personas físicas que realicen movimientos de medios de pago, en los términos establecidos en el art. 34.
25. Las personas que comercien profesionalmente con bienes, en los términos establecidos en el art. 38.
26. Las fundaciones y asociaciones, en los términos establecidos en el art. 39.
27. Los gestores de sistemas de pago y de compensación y liquidación de valores y productos financieros derivados, así como los gestores de tarjetas de crédito o débito emitidas por otras entidades, en los términos establecidos en el art. 40.

El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes.

La *Financial Action Task Force on Money Laundering* (FATF), más conocida en España por sus siglas en francés GAFI, *Groupe d'Action Financière sur le Blanchiment de Capitaux*, desarrolla evaluaciones continuas a sus países miembro a fin de valorar el nivel de aplicación de sus recomendaciones para combatir el blanqueo de capitales y la financiación del terrorismo.

Dicho organismo emitió un informe donde se refiere a la situación general y de riesgo en España y relaciona los diversos peligros de blanqueo de capitales, llegando a plantear que operan en España grupos criminales organizados tanto nacionales como extranjeros, y es un lugar de entrada a Europa de drogas procedentes del norte de África y Sudamérica. Las principales ganancias criminales, se obtienen de los delitos relacionados con las drogas, el crimen organizado, el delito fiscal y el tráfico de seres humanos.

Estas *actividades ilícitas* terminan engarzando con *actividades y operadores legales*, siendo en ese contexto donde la imprudencia puede derivar en un delito de blanqueo de capitales, aunque no sea sujeto obligado a las medidas establecidas en la normativa para la prevención del blanqueo de capitales y financiación del terrorismo. De hecho, muchas de las noticias que aparecen en los medios sobre imputaciones por delito de blanqueo de capitales,

se refieren a personas u organizaciones que no estaban obligadas a establecer las medidas de prevención exigidas en estas normas.

Bajo esta perspectiva, no es extraño que en algunos países se consideren las medidas de prevención del blanqueo de capitales como un *módulo indispensable de todo modelo de Compliance*. Esto es algo que sucede, por ejemplo, en filiales de organizaciones alemanas, país donde se percibe la lucha contra el blanqueo de capitales como un objetivo de cumplimiento general, con independencia de que se ostente la condición de sujeto obligado según la normativa local.

Realmente, la filosofía de los controles "*know your customer*" (KYC) que establece la normativa para la prevención del blanqueo pueden interpretarse en clave de diligencia debida en cualquier actividad de negocios, salvo para quienes quieran propiciar un entorno de *ignorancia deliberada* "*willful blindness*".

Los estándares modernos en materia de *Compliance* se amparan en el *principio de proporcionalidad* a la hora de definir los modelos aplicables a cada organización y sus respectivos controles. Por ello, la extensión de los controles KYC para sujetos no obligados se supedita también a ese principio, aunque no parecería razonable omitirlos por completo al desarrollar una aproximación basada en el riesgo ("*Risk Based Approach*", RBA), y conocer positivamente que España constituye entorno de riesgo en materia de blanqueo de capitales, según atestiguan los expertos del GAFI en el citado *Mutual Evaluation Report*.

La Norma ISO 37001, sistemas de gestión de la lucha contra el soborno, parte de la tesis de que los riesgos de toda organización pueden acechar tanto desde su interior como en su *perímetro exterior* y, por eso, las políticas, procedimientos y controles de cumplimiento no sólo deben proyectarse hacia sus empleados, sino también en dirección a *cualquier foco de riesgo externo*, como puedan ser proveedores (contratistas y subcontratistas en la cadena de suministro, etc.), socios comerciales (*joint-ventures*, agentes, comisionistas, etc.) o incluso clientes. Obviamente, esta doctrina tiene aplicación más allá de la prevención del soborno, y otorga pleno sentido a los controles KYC como medio para prevenir que la empresa se vea afectada por otras actividades igualmente penales (el blanqueo como delito autónomo).

La *esencia* de los controles para la prevención del blanqueo de capitales y financiación del terrorismo debería figurar en la agenda del *Compliance Officer*, como ya sucede en otros países de nuestro entorno, incluso para entidades que no ostentan la condición de sujetos obligados. Es un aspecto a considerar cuando se reflexiona acerca de cuál debe ser el *"núcleo duro" de Compliance* de una organización, ésto es, aquellas obligaciones y controles de cumplimiento a priorizar para definir un Sistema de Gestión de Cumplimiento ("*Compliance Management System*", CMS) razonable.

COMPLIANCE EN EL ÁMBITO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Son muchos los incidentes que pueden ocurrir en este ámbito y que dan lugar a la responsabilidad penal de la empresa tecnológica, por lo que estructurar una política de Compliance es necesario e imprescindible. Por ejemplo: Un empleado obstaculiza el funcionamiento de la plataforma web de la competencia, o una en la que en la página web corporativa se utilicen contenidos propiedad intelectual de otra empresa sin la debida autorización.

Muchas razones justifican la necesidad de establecer mecanismos de control y formación en los departamentos de marketing y ventas.

Algunos delitos conectados con la actividad tecnológica de las empresas:

a) E-commerce y marketplace

La venta de productos a través de internet ha teniendo un crecimiento exponencial, aquí puede darse la estafa y el fraude: Empleado que publica falsas ofertas en la web de la empresa. Serían actividades constitutivas de estos delitos las siguientes:

- Utilizar, con ánimo de obtener un beneficio económico, del engaño para producir error en una persona, induciéndola a realizar actos de compra, venta o disposición en perjuicio propio o ajeno.

- Manipulaciones informáticas para conseguir transferencias no consentidas de cualquier activo patrimonial, como dinero.

- Fabricación, introducción, posesión o facilitación de programas informáticos destinados a la comisión de estafas.

- Utilizar de tarjetas de crédito o débito, o cheques de viaje, o datos obrantes en cualquiera de ellas para realizar operaciones en perjuicio de su propietario o de un tercero.

Además:

a) Delitos contra la propiedad intelectual e industrial como puede ser la venta online de productos falsos o plagiados o de productos pirateados.

b) Delitos de publicidad engañosa

c) Cualquier manifestación incierta, alegación falsa o incluso indicación de características inciertas de los productos a la venta puede dar lugar a la responsabilidad penal de la empresa.

d) Delitos contra los consumidores.

e) Delitos de competencia desleal.

b) Desarrolladores de software, apps, webs o videojuegos por en el alto riesgo de comisión de delitos relativos a la propiedad intelectual. Como puede ser el uso de imágenes sobre las que no tiene cedidos los derechos de propiedad intelectual.

c) Economía colaborativa
El marco legal de estas empresas aún no es claro por lo que su situación y riesgo de cometer delitos aumenta, como es el derecho de los trabajadores o posibles delitos vinculados a la utilización de imágenes sobre las que no se tienen derechos en la plataforma de economía colaborativa de una empresa, o la utilización de fragmentos de código informático sobre los que no se tienen derechos.

d) Publicidad y marketing por el riesgo de cometer delitos de estafas y fraudes como puede ser la utilización de engaño para producir error en una persona, induciéndola a realizar actos de compra o venta o como puede ser una campaña que para lograr un mayor número de ventas, engañe sobre las características de un producto o servicio, propiedad intelectual, competencia desleal y los delitos contra los consumidores.

e) Empresas dedicadas a la investigación donde uno de los mayores riesgos está vinculado a la recepción de subvenciones públicas, pudiendo cometerse delitos contra la hacienda pública. El fraude en la obtención de subvenciones o desgravaciones o la ayuda de las Administraciones Públicas falseando las condiciones para obtenerlas u ocultándose las que la hubiesen impedido constituye un delito sobre el cual son responsables penalmente las empresas. También los delitos contra la propiedad intelectual, los daños informáticos y otros delitos informáticos, las estafas y fraudes, el blanqueo de capitales, los delitos contra el medio ambiente, los provocados por explosivos y el tráfico de influencias.

NORMA ISO 37001 CONTRA EL SOBORNO

La Organización Internacional de Estandarización (ISO) publicó esta norma contra el soborno, donde se establecen los requisitos y proporciona una guía para un sistema de gestión diseñado para ayudar a una organización a prevenir, detectar, responder y cumplir con las leyes contra el soborno, los compromisos voluntarios aplicables a sus actividades y velar por el cumplimiento

del modelo de Compliance establecido; formación del personal, evaluación del riesgo de soborno y realización de procesos de Due Diligence.

La norma tiene por objeto uno de los delitos tipificados en el Código Penal español como susceptible de responsabilidad penal de la persona jurídica.

Todo depende del "apetito de riesgo" de cada empresa y de la voluntad de cada empresario de progresar de modo sostenible en el tiempo**.** Todos conocemos los límites y sabemos que podemos imponer normas a nuestros colaboradores y grupos de interés, a pesar de las dificultades iniciales. La única condición es que esas normas estén orientadas a un comportamiento sostenible, que sean conocidas por todos en las organizaciones y que podamos denunciar las actitudes contrarias a ellas. En definitiva, que seamos capaces de evitar la tentación del atajo.

Esta nueva norma ISO 37.001**,** establece un modo de gestión de la empresa dirigido a evitar el soborno en todas sus modalidades. En una línea estructural similar a la de las ISO 19.600 y 27.000**,** ayuda a la organización a establecer, implementar y mejorar un sistema de gestión del cumplimiento dirigido a evitar el soborno. Contiene, por tanto, una serie de medidas y controles reconocidos internacionalmente como buenas prácticas en este sentido, constituyendo una buena ayuda a la hora de establecer la arquitectura del sistema. A diferencia de las otras normas sobre cumplimiento, es bastante específica, definiendo pautas concretas de actuación. Además, es certificable.

Es aplicable a toda organización de un tamaño mínimo, incluidas asociaciones y organizaciones no gubernamentales, con y sin ánimo de lucro. En particular, es de aplicación evidente a toda empresa naviera, especialmente si se dedica al tráfico internacional.

Como la norma ISO 19.600, es un sistema de "alto nivel", que debe implantarse en conexión con los otros sistemas ISO preexistentes**,** normalmente las normas ISO 9001, ISO 14001, ISO 27001, ISO 26001, ISM, etc. En las navieras, al menos, dispondremos de un sistema de Gestión Segura de Buques, ISM, o de una norma ISO de calidad o medioambiente, por lo que siempre existirá una base de implantación y una experiencia en la organización que hará más fácil el despliegue.

Como el soborno y la corrupción pueden tener distintas definiciones legales según los países; la norma no proporciona ninguna definición concreta de soborno. No obstante, proporciona guías de lo que se entiende internacionalmente por soborno para que se entienda su intención y alcance:

El término "*soborno*" se utiliza para referirse a la oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, y sea cual sea la ubicación del hecho, en violación de la ley aplicable, tanto como incentivo como recompensa para una persona que actúe, o deje de actuar, en relación con el ejercicio de las funciones que le han sido asignadas.

En particular, se contemplan los siguientes modos de soborno:

1. En el sector público, privado y sectores sin ánimo de lucro.
2. De terceros por parte de la organización.
3. De terceros por parte del personal de la organización que actúe en nombre de la organización o en su beneficio.
4. De terceros por parte de socios o colaboradores de la organización que actúan en nombre de la misma o en su beneficio.
5. De la propia organización por parte de terceros.
6. Del personal de la organización en relación con las actividades de la misma por parte de terceros.
7. De socios o colaboradores de negocios de la organización por parte de terceros en relación con las actividades de la misma.
8. Directo e indirecto (por ejemplo, un soborno ofrecido o aceptado a través o por un tercero).

Esta Norma no trata específicamente de fraude, carteles ni de otros antimonopolios o delitos de competencia, el blanqueo de dinero u otras actividades relacionadas con las prácticas corruptas, aunque una organización puede optar por ampliar el alcance del sistema de gestión para incluir este tipo de actividades, en cuyo caso quizás fuese más recomendable recurrir a la norma ISO 19.600, dejando la 37.001 como subordinada al sistema general de cumplimiento.

La norma requiere una serie de medidas y controles que traten de prevenir, detectar y evitar el soborno, entre otros:

a) Un conjunto de políticas, procedimientos y controles contra el soborno en la organización (tanto en caso de sobornos a terceros como en el caso de sobornos desde terceros).
b) El liderazgo, compromiso, responsabilidad y ejemplo de la alta dirección.
c) El control desde la alta dirección, mediante sistemas adecuados de reporte e investigación y canalizando dicho reporte a través de una persona o función encargada, que es conveniente que coincida con la función de cumplimiento de la norma ISO 19.600.
d) Un Plan de Formación adecuado.
e) Un análisis de riesgos.
f) Procesos de diligencia debida sobre proyectos y sobre colaboradores de negocio externos.
g) Mecanismos de reporte, monitorización de la efectividad del sistema, investigación de incidentes y de revisión de las políticas.
h) Procedimientos de tratamiento de incidencias o no conformidades, acciones correctoras y mejora continua.

Los apartados de la norma son conceptualmente similares a los de la 19.600. Parte del contexto empresarial (grupos de interés, sector, nivel de internacionalización…), define el alcance del sistema, analiza riesgos de cometer soborno y establece políticas que los mitiguen. Para la implantación, establece sistemas de comunicación y formación. Las políticas derivan en procedimientos medibles, mediante indicadores de cumplimiento y auditables, que sean

susceptibles de mejora continua. Se recomienda disponer de una posición similar a la función de cumplimiento de la norma 19.600 y de sistemas de reporte e investigación protegidos.

Como novedad, se describe una política anti-soborno, radicando en esta descripción la mayor concreción que esta norma aporta respecto de las anteriores, mucho más generalistas.

Como siempre, se enfatiza la importancia de "predicar con el ejemplo" de la alta dirección y de revisar y mejorar el sistema de modo continuo; asimismo con su impulso, y se definen los procesos de "diligencia debida" sobre colaboradores, en el sentido que ellos deben seguir también las directrices establecidas para la organización principal.

PROPIEDAD INTELECTUAL Y COMPLIANCE

El Código Penal intenta incluir las conductas relacionadas con la publicación de contenidos en internet sin la autorización de su titular a través de canales que hasta ahora no estaban previstos en la norma. Intenta criminalizar no solo la comunicación pública de las obras sin el consentimiento de su titular, sino también de los enlaces a dichas obras o a los programas que permiten copiarlas o descargarlas. De acuerdo con este texto, el administrador de un sitio web podría ser condenado a prisión por haber permitido que un usuario publicase enlaces a obras de terceros, sin conocer su ilicitud ni su contenido.

El tipo agravado (artículo 271) y el tipo contra la propiedad industrial (artículo 274) incrementan hasta un 50% las penas asociadas con este delito en determinadas circunstancias.

CONCLUSIONES

A grandes rasgos un Compliance tiene entre sus fases la identificación de los riesgos penales que pueden afectar a la empresa y priorizarlos, a través de un Mapa de Riesgos; detectar los procesos donde pueden residir esos riesgos y analizar los mecanismos de control y defensa de los mismos; determinar la supervisión y Plan de Acción para implantar los controles que mitigarán los riesgos que deberán estar incorporados en el Manual de Compliance.

En todo caso, la responsabilidad penal de las personas jurídicas, además de la cuantiosa sanción para el sujeto impuestas por el Legislador, lo que esconde es un castigo a la imagen de la empresa**,** un daño reputacional que puede llegar a ser irreparable. La reputación corporativa todavía no está suficientemente valorada en España, a excepción de las grandes corporaciones, sociedades cotizadas y compañías de producto y marca.

Como ejemplo, algunas malas prácticas que se pueden presentar en la empresa:

1. La descarga ilegal de programas informáticos o copias piratas que se instalan provisionalmente a la espera de formalizar la compra legal del programa y que

por diversas circunstancias nunca se realiza con lo cual la copia pirata se mantiene de forma indefinida.

2. Con el objetivo de dar una mayor eficiencia a los presupuestos de inversiones o de compra de ciertos equipos se opta, de buena fe, por la compra de un supuesto equipo casi nuevo por un coste muy inferior al real y que posteriormente se descubre que procede de un robo.
3. Siendo que una venta es una venta, se aceptan la realización de operaciones con cobro en efectivo, superando los límites establecidos al respecto.
4. Con el objeto de reducir gastos industriales se opta por limitar o contratar sin las debidas garantías a profesionales más baratos para el mantenimiento de instalaciones sensibles, con el resultado de funcionamientos anómalos que pueden producir vertidos, emisiones tóxicas o contaminación acústica.
5. Errores, por falta o deficiente asesoramiento profesional, en las liquidaciones de impuestos, cuotas de la seguridad social y/o contratación de trabajadores.
6. Permitir o no tener conocimiento, al no existir los controles y canales de comunicación necesarios, de ciertas situaciones entre empleados de la empresa que puedan ser susceptibles de considerarse como acoso o discriminación por razones de raza, color o ideológicas.
7. El incumplimiento por falta de seguimiento o establecimiento de los niveles de acceso necesarios de la Normativa de Protección de Datos.

Independientemente de cuál sea el origen del modelo de gestión y de cómo haya decidido implementar la empresa su modelo de Compliance; sea porque viene dado por su cultura corporativa a través de decisiones voluntarias; o porque ha decidido llevar a cabo su implementación a través de un modelo de prevención de delitos, ambos deberán combinarse y desarrollar elementos propios y novedosos que formarán parte de eso que ahora llamamos «Compliance Penal», y que no es otra cosa que la adopción de medidas propias del *Corporate Compliance* adaptado a las exigencias legales del nuevo régimen de responsabilidad penal de la persona jurídica.

Por esta razón, cuando se habla de un buen modelo de prevención de delitos no puede quedarse en la mera exigencia de no cometer los delitos que pueden generar responsabilidad penal a la persona jurídica, sino que resulta esencial que contemplen y respeten principios y sistemas adoptados del *Corporate Compliance* y de los compromisos voluntarios de la compañía, como es el caso de la Responsabilidad Social Corporativa, entre otras.

Los dictados de la cultura de Compliance son absolutamente útiles y adaptables en el escenario de la responsabilidad penal de la persona jurídica, siempre que contemplen análisis de riesgos penales (*ad intra* y *ad extra*) como medida para paliar una responsabilidad, la penal, cuyas normas imponen prohibiciones y cuyas consecuencias desbordan las meras sanciones para convertirse en auténticas penas de mayor contundencia (cierre de establecimientos, suspensión de actividades) y daño reputacional, si se quiere. Ello sin perjuicio de que la empresa mitigue el resto de sus riesgos dentro de un sistema integral de Compliance.

Desde la perspectiva del abogado defensor, se habrá de pensar cómo se prueba el hecho negativo de que el sistema implementado por el cliente no era ineficaz (se imputa por «defecto de organización»), puesto que la comisión de un delito en el seno corporativo ya es considerado como indicio de ineficacia por la Fiscalía. Y, desde la órbita del asesor en Compliance, hay que poner el acento claramente en el sistema de evidencias físicas de los protocolos y controles de la empresa llamados a evitar la comisión de delitos y/o instaurar una cultura de cumplimiento normativo.

Los postulados de la Fiscalía a la hora de interpretar la responsabilidad penal de las personas jurídicas configuran una verdadera estrategia procesal que pretende la disociación entre los intereses del individuo (trabajador, directivo) y de la empresa, como elemento *desincentivador* (enfoque negativo) de la criminalidad.

Solamente sometiendo al mismo proceso -penal- a ambos y vinculando la responsabilidad penal de la empresa con la de quienes la integran, se disocian sus estrategias procesales promoviendo el afloramiento del delito, el “yo no soy responsable, sino el otro”. Por desgracia, se ha olvidado que objetivamente un modelo vicarial incentiva esconder el delito del otro para no ser responsable por «defectos de organización» por bueno que sea el sistema de prevención adoptado dada la inversión de la carga de la prueba que opera, mientras que un modelo de autoresponsabilidad, por el contrario, fomenta la colaboración: Si el delito me pertenece, más vale que ponga remedios cuanto antes o que colabore, en su caso, desde el principio.