1.1. EL *COMPLIANCE* HA LLEGADO PARA QUEDARSE

Una de las frases más escuchadas en los últimos tiempos en congresos del sector financiero, artículos de revistas especializadas y blogs de abogados, economistas y expertos varios es que "El *compliance* ha llegado para quedarse", como si de una nueva moda o una tía del pueblo se tratase.

Y no es que el *compliance* sea un concepto novedoso –en EEUU ya se lleva implementando desde los años 70– pero hasta hace unos pocos años parecía algo reservado a grandes compañías. Ahora se presenta como una de las cuestiones más novedosas a incorporar en las estrategias de las empresas del siglo XXI.

1.1.1. Historia del *compliance*

Los años 70 en EEUU son los del caso *Watergate* –recordemos que supuso la caída del presidente Nixon– y otros escándalos relacionados con prácticas fraudulentas empleadas por grandes corporaciones americanas especialmente en operaciones en países del tercer mundo. Las investigaciones llevadas a cabo en aquellos años y especialmente, las medidas de control implementadas para conseguir unos comportamientos empresariales más éticos, especialmente en el sector financiero, fueron sin duda el origen del *compliance* tal y como lo conocemos hoy en día.

- **FCPA**

  El Departamento de Justicia de los EEUU lideró este proceso con la publicación en 1977 de la FCPA (*Foreign Corrupt Practices Act*) cuyo objetivo principal era regular el comportamiento ético de las empresas americanas –especialmente las que operaban en otros países– y sobre todo, evitar la práctica de los sobornos a funcionarios.

La primera empresa en ser investigada bajo la FCPA fue la compañía aeronáutica Lockheed. Durante el proceso se comprobó cómo la entidad había pagado entre 1972 y 1974 más de veintidós millones de dólares en sobornos para asegurarse contratos con la justificación de que *"estos pagos eran coherentes teniendo en cuenta las prácticas existentes en compañías del extranjero incluidas algunas de la competencia"*. Finalmente la compañía se declaró culpable en 1979 de haber sobornado a funcionarios japoneses y fue multada con casi setecientos mil dólares.

A partir de ese momento, las compañías entendieron la importancia de contar con programas de cumplimiento. Sin embargo, la ausencia de un modelo de referencia claro reconocido por la ley hizo posible que empezasen a proliferar planes de prevención de delitos y programas de *compliance* de todo tipo y *pelaje*, en algunos casos, meros copia-pega de planes ya existentes –como si el plan de prevención de delitos de un banco fuese replicable a una empresa de construcción– y modelos genéricos válidos para cualquier empresa independientemente del sector, actividad o país de origen. Incluso llegó a acuñarse el término *make-up compliance* o *fake compliance* para denominar a determinados programas que únicamente tenían por misión "cubrir el expediente" y simular una apariencia de cumplimiento pero sin formar parte del resto de planes, políticas y documentos de la compañía.

La FCPA ha servido de referencia para otros muchos modelos de *compliance* y antisoborno desarrollados posteriormente.

- **COSO**

Como respuesta a los requerimientos de la FCPA, se fundó en 1985 el grupo COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), un foro de profesionales del sector del control interno y representantes de la industria y la bolsa de valores de Nueva York, que desarrolló su propio modelo de buenas prácticas en materia de

compliance que sigue actualmente vigente tras varias revisiones y ampliaciones.

- **El caso Odebrecht**

Ya en las últimas décadas del siglo XX, la liberación de los mercados en la Unión Europea, el fin de la guerra fría, el auge del Yihadismo, el surgimiento de las organizaciones criminales proveniente de los países del Este y el aumento de los delitos informáticos, entre otros, ha planteado grandes retos en materia de seguridad, cumplimiento y ética corporativa.

Uno de los mayores escándalos de corrupción que ha tenido lugar apenas iniciado el siglo XXI ha sido sin duda la investigación de la constructora brasileña Odebrecht por el Departamento de Justicia de EEUU (junto con otros 10 países de América Latina). Esta investigación sobre el soborno sistemático –más de setecientos millones de dólares y más de cien funcionarios involucrados– a presidentes, expresidentes, políticos, funcionarios, abogados y testaferros de gobierno de más de doce países para obtener beneficios en contrataciones públicas, aún a día de hoy, sigue llenando titulares en todo el mundo.

Titulares en prensa caso Odebrecht

Estos escándalos, ampliamente difundidos por los medios de comunicación y con un elevado coste reputacional a las empresas involucradas han tenido como consecuencia, que la cultura del cumplimiento haya empezado a arraigar en muchos sectores –no solo el financiero– y la aparición de diversos modelos y estándares tanto nacionales como internacionales que sirven como punto de partida para los planes de cumplimiento y programas de prevención de delitos.

1.1.2. *Compliance* penal en España

En España, el *compliance* aterrizó a nivel global en 2010 de la mano de la reforma del Código Penal Español que estableció que las **personas jurídicas podrían incurrir en responsabilidad penal** por delitos cometidos por sus representantes legales o por cualquiera de sus trabajadores actuando en su nombre y en su beneficio, especialmente si los hechos ocurriesen por falta de supervisión, vigilancia o control de dichas conductas. La posterior Reforma de 2015 y la publicación de la circular 1/2016 aclaró el panorama sobre la responsabilidad penal de las personas jurídicas, y en concreto, sobre la **exención de responsabilidad** en caso de que la organización contase con algún programa de gestión que incluyera medidas de vigilancia y control.

En este contexto, se produjo la publicación de la norma UNE 19601 en mayo de 2017 por parte de la organización normativa española. Esta norma, que se crea como un modelo de *compliance* penal alineado con el Código Penal viene a dar respuesta a la exigencia de las compañías españolas de contar con un modelo único validado y aceptado por la ley. Sin embargo, aún existe mucha controversia sobre si realmente UNE 19601 va a proporcionar la tan ansiada seguridad jurídica reclamada por las empresas.

En cualquier caso, en los últimos años hemos visto como aquello que en su momento muchos expertos vaticinaron que nunca ocurriría –la

imputación de una persona jurídica por un delito cometido por uno de sus trabajadores–, se ha visto finalmente respaldado por unos cuantos casos, algunos de los cuáles involucran empresas de gran calado en el territorio nacional e internacional.

1.1.3. *Compliance* en Latinoamérica

Latinoamérica es sin duda, junto con África, uno de los mercados más afectado por el delito de soborno y corrupción, y algunos de los países suramericanos han ido apareciendo de forma sistemática en las listas de países de alto riesgo de corrupción. Los países mejor puntuados en el *Global Corruption Index* publicado por Transparencia Internacional suelen ser Uruguay y Chile mientras que Venezuela suele liderar el ranking de país con mayor riesgo.

Mapa de riesgo de corrupción. Fuente: www.transparency.org

Por otro lado, Latinoamérica siempre se ha visto influenciada por las medidas adoptadas por Estados Unidos como uno de sus principales mercados cliente. Empujados por EEUU a emprender medidas similares a la FCPA, La Convención Interamericana Contra la Corrupción estableció, a finales del siglo XX, la necesidad de adoptar leyes y normas respecto de los sobornos de entidades extranjeras. Sin embargo, numerosos escándalos de corrupción –Ralp Lauren en Argentina, PetroTiger en Colombia o Walmart en México y Argentina– pusieron de manifiesto que los acuerdos alcanzados eran insuficientes.

En la mayoría de los países latinoamericanos, existe legislación tendente a prevenir la corrupción, el lavado de activos o la financiación del terrorismo. Es la ausencia de un modelo o referente único de *compliance* lo que hace que toda esa legislación local se acabe diluyendo en un conjunto de normativa difícil de vigilar por parte de las autoridades y de implementar por parte de las organizaciones, pues en contados casos la normativa local exige o incentiva la implementación de un programa de *compliance* a las empresas.

Sin embargo, desde hace unos años se empiezan a ver claros esfuerzos legislativos en países latinoamericanos en materia de lucha contra la corrupción como Chile, Brasil o Perú.

1.2. EL *COMPLIANCE* MÁS ALLÁ DE LA RESPONSABILIDAD PENAL

1.2.1. Daño reputacional y económico

Pero no hay que ver el *compliance* únicamente como un eximente de responsabilidad penal en caso de que la empresa se vea involucrada en algún delito. Más allá de eso, el daño reputacional y las pérdidas económicas que suponen el no *compliance* a las empresas pueden acabar causando la quiebra económica y la desaparición de la misma.

Las conclusiones de un estudio realizado sobre el riesgo reputacional a más de 300 ejecutivos de grandes empresas, indican que el daño reputacional supone casi el 50% de la pérdida de clientes.

Fuente: Informe Deloitte 2014

En 2008, la compañía Siemens fue sancionada con una multa de 450 millones de dólares por pago de sobornos en los diferentes países en los que opera.

En el caso de la constructora Odebrecht, el daño reputacional –sufrido tanto por la compañía como por la clase política latinoamericana– se vio acompañado por la mayor multa impuesta a una empresa por corrupción: 3.500 millones de dólares, entre las autoridades de Brasil, EEUU y Suiza hasta que en 2014, el *Bank of America* tuvo que hacer frente a una multa de 16.560 millones (equivalente a los beneficios de la empresa en los tres últimos años) impuesta por el Departamento de Justicia de EEUU por el fraude de las hipotecas basura, la mayor sanción realizada a una empresa hasta el momento.

En España, desde la Reforma del Código Penal de 2015, las multas impuestas a las empresas por incumplimientos en los planes de *compliance* superan los dos mil millones de euros. Según ha confirmado recientemente el magistrado de la Audiencia Nacional Eloy Velasco, la mayor parte han estado relacionadas con el delito fiscal, seguidas por los casos de estafa y la insolvencia punible y más del 95% han sido los directivos –y no los trabajadores– los responsables de los mismos.

1.2.2. Contrataciones en el sector público

Actualmente muchos de los dosieres de contratación pública para la administración **otorgan más puntos a empresas que cuentan con**

programas de cumplimiento o directamente los exigen –por ejemplo, en Perú se exige que las empresas licitantes cuenten con un certificado acreditado en antisoborno según ISO 37001–.

1.3. ¿QUÉ ES EL *COMPLIANCE*?

Compliance significa **Cumplimiento Normativo**, entendiendo como tal no solo la regulación aplicable a la compañía o su sector en los países en los que opera, sino también a la normativa interna de la propia organización y compromisos adquiridos con los clientes y proveedores. Es decir, *compliance* significa cumplimiento en un sentido muy amplio, en el que también tienen cabida otros conceptos como la **ética corporativa** y la **responsabilidad social**.

CULTURA DE *COMPLIANCE*

- Valores, ética y creencias que existen en una organización y que interactuan con las estructuras y sistemas de control de la organización para producir normas de comportamiento que conducen a resultados de *compliance*.

Definición de Cultura de *Compliance*. Fuente: ISO 19600

Esta responsabilidad del cumplimiento, que tradicionalmente se ha asignado al área legal o jurídica de la empresa, se convierte ahora, por medio de los sistemas de gestión de *compliance*, en una responsabilidad global de toda la organización, en la que todos participan y todos importan.

1.4. MODELOS DE GESTIÓN DEL *COMPLIANCE*

El *compliance* no se consigue por sí mismo. Como cualquier otra "virtud" de una organización –léase calidad, respeto por el medio ambiente, vigilancia de la seguridad de las personas, etc.– requiere de un

esfuerzo sistemático, organizado y constante por parte de la misma que asegure que existe una cultura del cumplimiento en toda la organización, que se implementan procedimientos y políticas adecuadas y suficientes para cumplir con el marco normativo aplicable, que se analizan los riesgos que existen de incumplimiento, que se identifican oportunidades de mejora y desviaciones a dichas políticas y que se emprenden las acciones correctivas más adecuadas para resolverlas. En definitiva, que se implementa un sistema de gestión específico para la gestión del *compliance*.

Existen actualmente varios modelos de gestión de *compliance*. Algunos basados en estándares internacionales y otros, en modelos nacionales o sectoriales. En cualquier caso, todos representan un grupo de buenas prácticas y son interesantes de analizar como se muestra a continuación.

Ahora bien, los modelos de gestión de *compliance* no hacen *milagros* ni garantizan el cumplimiento o mejor dicho, la ausencia de incumplimiento. Estos modelos proporcionan herramientas para evaluar el riesgo de *no compliance*, identificar los incumplimientos, hacerles frente e investigarlos –si finalmente tienen lugar– y establecer medidas adecuadas y razonables para controlarlos… pero es la organización y especialmente las personas que la componen quienes finalmente son responsables de que la cultura del cumplimiento realmente cale en la organización y en sus actividades.

1.4.1. Modelos internacionales

COSO

El informe o modelo COSO establece una serie de directrices fundamentales para la implementación y control de un sistema de *compliance* que persigue los siguientes objetivos:

- Operaciones eficaces y eficientes.
- Información financiera fiable y confiable.
- Cumplimiento de la ley aplicable a la entidad.

Publicado en 1992 por el grupo del mismo nombre, este modelo –que inicialmente fue aplicado por parte de entidades financieras– sigue siendo utilizado hoy en día por numerosas empresas de todos los sectores como modelo de gestión.

Actualmente existen dos versiones del modelo (COSO I y COSO II):

COSO I (denominado originalmente *Internal Control Integrated Framework*) fue el primer informe emitido por COSO y que estableció las bases de la estructura del modelo consistentes en:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión.

COSO II (*Enterprise Risk Management-Integrated Framework*) fue publicado en 2004 ampliando el concepto del control interno a la gestión de los riesgos. Este nuevo modelo, amplía la estructura del original con tres componentes más:

- Establecimiento de objetivos.
- Identificación de eventos.
- Respuesta a los riesgos.

COSO I	COSO II
• Ambiente de control • Evaluación de riesgos • Actividades de control • Información y comunicación • Supervisión	• Ambiente de control • **Establecimiento de objetivos** • **Identificación de eventos** • Evaluación de riesgos • **Respuesta a los riesgos** • Actividades de control • Información y comunicación • Supervisión

Estructura de COSO I y COSO II. Fuente: propia

En 2013 se publicó una revisión del Informe I*nternal Control-Integrated Framework* (COSO I) en el que se incluían mejoras relacionadas con la capacidad de adaptación del sistema al entorno, la gestión de los riesgos y la claridad en la información y comunicación.

EN 2017 se publicó una revisión del Informe *Enterprise Risk Management –Integrated Framework* (COSO II) también haciendo más hincapié en la gestión de los riesgos y su alineamiento con la política y estrategia de la compañía.

Finalmente en 2020, COSO publicó una Guía para la implementación de ERM *"Creating and Protecting Value: Understanding and Implementing Enterprise Risk Management"*.

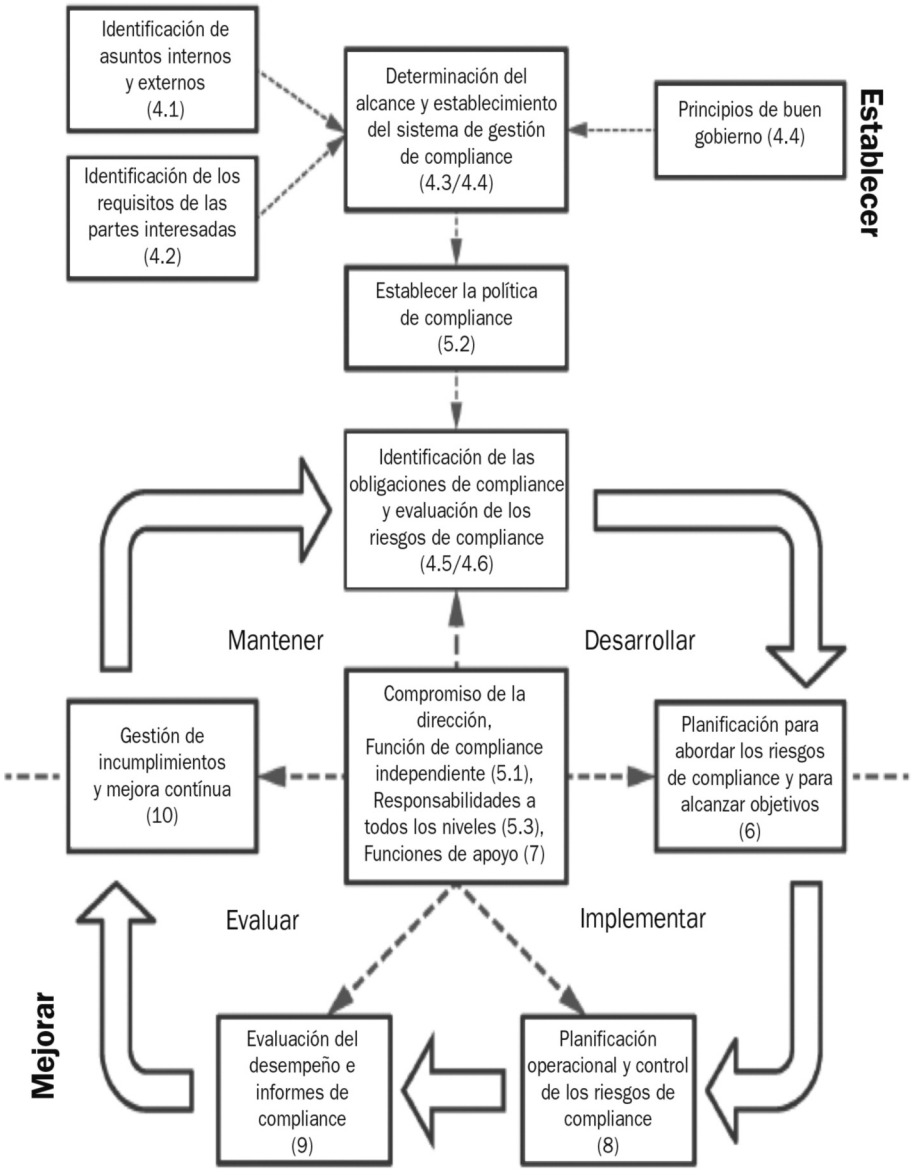
- **ISO 19600 Sistemas de gestión de *compliance***

  En 2014, la organización internacional de normalización ISO publicó la norma **ISO 19600 Sistemas de gestión de *compliance*. Directrices,** elaborada por el Comité Técnico AEN/CTN 307 Gestión de riesgos.

Esta norma establece que la única forma de que una organización cumpla con sus obligaciones es integrando la cultura de *compliance* en toda la organización y en el comportamiento y en la actitud de las personas que forman parte de ella. Estos valores fundamentales deberían emanar de la alta dirección y convierte a los directivos de la compañía, en todos sus niveles, en los responsables máximos del éxito del sistema de cumplimiento.

A contrario de otras normas ISO de sistemas de gestión (por ejemplo: ISO 9001 en materia de calidad, ISO 14001 en materia de medio ambiente o ISO 27001 en materia de seguridad de la información) esta norma no especifica requisitos sino que proporciona una serie de recomendaciones o buenas prácticas que las organizaciones pueden implementar adaptándolas a su tamaño, sector, naturaleza y complejidad de sus actividades.

ISO 19600 está basada en el proceso de mejora continua PDCA (Plan-Do-Check-Act) y tiene estructura de alto nivel (al igual que las últimas versiones de otras normas de gestión) lo que le permite una fácil integración con otros sistemas de gestión ya existentes (calidad, medio ambiente, seguridad de la información, seguridad alimentaria…).



Sistema de gestión de *Compliance* según ISO 19600

Como todas las normas ISO que siguen la estructura de alto nivel, esta norma se estructura en 10 cláusulas.

Las directrices se encuentran entre la cláusula 4 y la 10:

Cláusula	Título
0	Introducción
1	Objeto y campo de aplicación
2	Normas para consulta
3	Términos y definiciones
4	**Contexto de la organización**
5	**Liderazgo**
6	**Planificación**
7	**Apoyo**
8	**Operación**
9	**Evaluación del desempeño**
10	**Mejora**

Estructura de alto nivel de ISO 19600:2014. Fuente: propia

ISO 19600 es, en el fondo, una **recopilación de buenas prácticas ya existentes** en materia de *compliance* y por tanto, incorpora recomendaciones y directrices de otros modelos (COSO, FCPA…) como son el enfoque al riesgo, los controles internos y el seguimiento/ medición de las medidas de control implementadas.

- **ISO 37001**

En 2016, apenas un par de años después de la publicación de ISO 19600, aparece **ISO 37001 Sistemas de gestión antisoborno. Requisitos con orientación para su uso,** un modelo de *compliance* específico para el delito de soborno.

SOBORNO

- Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

Definición de soborno. Fuente: ISO 37001:2016

A diferencia de ISO 19600, esta norma sí establece requisitos que pueden ser verificados y auditados, lo que la convierte en una norma certificable. Por otro lado, comparte la misma estructura de alto nivel de diez cláusulas de ISO 19600 lo que las hace perfectamente integrables.

Como en el caso anterior, ISO 37001 también es un compendio de buenas prácticas internacionales en materia de control del soborno, por lo que su implementación es posible en cualquier país y bajo cualquier jurisdicción.

La norma es lo suficientemente flexible para que distintas organizaciones con muy diferentes riesgos de soborno, puedan implementarla de forma eficaz sin más que crear los procedimientos, políticas y controles antisoborno de forma coherente, razonable y proporcional a los riesgos de soborno a los que se enfrente. Obviamente no deberían ser idénticos los controles establecidos por una pequeña empresa de servicios que opera a nivel regional que los establecidos por una gran corporación bancaria internacional con sucursales en países de alto riesgo.

Es importante destacar que ISO 37001 –al igual que cualquier otro modelo de *compliance*– en modo alguno garantiza que el soborno no

pueda llegar a producirse en el seno de la organización, puesto que **el riesgo nunca llega a eliminarse por completo**. La misión de ISO 37001 es ofrecer una forma de que la organización pueda implementar medidas razonables para prevenir el soborno, identificarlo y enfrentarse a él –si finalmente llegase a ocurrir– e implementar las mejores acciones para que no vuelva a ocurrir.

No es posible eliminar por completo el riesgo de soborno y ningún sistema de gestión antisoborno será capaz de prevenir y detectar todos los sobornos.

Fuente: ISO 37001:2016

Algunos de los aspectos de la gestión del soborno que permite abordar ISO 37001 son los siguientes:

- Soborno por parte del personal de la organización, actuando en nombre de la organización o de su propio beneficio.
- Soborno por parte de los socios de negocio de la organización, actuando en nombre de la organización o de su propio beneficio.
- Soborno a la organización por parte de terceros.

La norma se ha elaborado pensando en el delito concreto de soborno y no aborda explícitamente otros delitos y prácticas corruptas como el fraude, el lavado de activos, el monopolio, la colusión o la financiación del terrorismo. Sin embargo, en el apartado **1 Objeto y campo de aplicación** de la norma, se indica que *"una organización puede optar por ampliar el alcance del sistema de gestión para incluir este tipo de actividades".*

A falta de normas ISO específicas para el control de este tipo de delitos, muchas organizaciones optan por esta solución y amplían el alcance de su sistema de gestión ISO 37001 a otros delitos.