EXPERIENCIAS DE *COMPLIANCE* EN LA GESTIÓN DE RIESGOS EN LAS ORGANIZACIONES: BUENAS PRÁCTICAS Y FACTORES DE ÉXITO

OLGA FRAGA GÓMEZ

> *"If you think compliance is expensive – try non-compliance"*
>
> Paul McNulty, ex Subsecretario de Justicia de Estados Unidos

La gestión de riesgos se configura como una pieza clave para el correcto funcionamiento de las empresas de nuestro país en la actualidad. Las empresas se enfrentan cada día a multitud de riesgos que clasifican, analizan y evalúan de forma distinta, aunque con el objetivo común de gestionarlos y mitigarlos. Una clasificación habitual distingue entre los riesgos estratégicos, financieros, operativos y de cumplimiento.

En general, los riesgos empresariales están interconectados. Pensemos por ejemplo en un delito de estafa cometido por un empleado de una empresa en su nombre y beneficio. Esta conducta supondría un riesgo de cumplimiento (de carácter penal) para la empresa y que, lógicamente puede conllevar un riesgo financiero (posible sanción económica), un riesgo operativo (posible sanción interdictiva -por ejemplo, el cierre de una planta de producción-), un riesgo estratégico (disminución de la producción que no permite lograr el crecimiento fijado en el plan de negocio, o la imposibilidad de cerrar ciertas alianzas previstas con la administración pública o con otros *stakeholders*) y, por último, el temido riesgo reputacional.

Es por tal interconexión que la gestión de riesgos de cumplimiento, como elemento crítico de todo modelo de *compliance*[1], requiere una visión holística por parte de la organización, analizando el potencial impacto que puede conllevar para la misma la infracción de la normativa que le sea aplicable[2]. Este análisis se configura como el primer paso a partir del cual se construye

1 A lo largo del presente artículo se utilizará la expresión modelo de *compliance* para referirse, de manera indistinta, a los programas o sistemas de prevención de riesgos de cumplimiento, de ética o integridad.

2 En este sentido, en España, la Circular 1/2016, de 22 de febrero, de la Fiscalía General del Estado sobre la responsabilidad penal de las personas dispone que: "*En puridad, los modelos de organización y gestión o corporate Compliance programs no tienen por objeto evitar la sanción penal de la empresa sino promover una verdadera cultura ética empresarial. La empresa debe contar con*

el sistema de cumplimiento a través de distintos mecanismos de control de carácter orgánico, normativo u operativo.

Vinculado con lo anterior, ya en el año 2004 la reforma de las directrices para la determinación individual de la pena de las personas jurídicas en los Estados Unidos ("*Sentencing Guidelines for Organizations*"), establecieron que las empresas deben "*promover una cultura organizativa que fomente la conducta ética y el compromiso con el cumplimiento del Derecho*", además de ejercer la debida diligencia para prevenir y detectar conductas criminales. Estados Unidos, que se erige como la cuna del *compliance*, ciertamente es testigo de la evolución de sus corporaciones en materia de integridad, impulsada lógicamente por la presión normativa y por los grandes escándalos financieros, si bien en la actualidad también por las exigencias de los consumidores y clientes, cada vez más concienciados con las políticas de sostenibilidad y ética empresarial.

Aunque por lo general en España las compañías han partido de los modelos de prevención penal, en los últimos años muchas empresas han evolucionado a modelos de ética e integridad[3] en un sentido amplio: cumplir con la regulación, pero también con los compromisos adquiridos contractualmente o las obligaciones autoimpuestas por las propias empresas conforme a sus principios y valores. En estos casos el eje de actuación es claro: la ética corporativa, porque las personas y las compañías a nivel mundial están cada vez más preocupadas por mantener una buena reputación corporativa y convertirse en buenos "ciudadanos" en consonancia con las exigencias sociales; los consumidores demandan empresas éticamente responsables.

En definitiva, en la sociedad actual en la que los principios de sostenibilidad, integridad y buen gobierno marcan el paso, las empresas que cuenten con sistemas de ética y cumplimiento sólidos y holísticos están mejor posicionadas en el presente, pero también en el futuro.

En este contexto, las empresas de nuestro país se enfrentan una serie de desafíos específicos al diseñar e implementar programas de cumplimiento. Dos de los principales retos son la volatilidad normativa y la integración cultural dentro de la organización. Además, alinear estas regulaciones con los objetivos estratégicos de la empresa sin comprometer la eficiencia operativa supone un desafío recurrente por la falta de recursos dedicados exclusivamente a la función de *compliance*, especialmente en medianas y pequeñas empresas. Esto puede llevar a una percepción de que el modelo de *compliance* es un gasto más que una inversión.

Sin embargo, en la era empresarial actual, y fruto de diversos factores geopolíticos, sociales, tecnológicos y regulatorios, estamos evolucionado hacia un modelo colaborativo en el que todas las organizaciones, bajo el principio de proporcionalidad, deben desplegar el sistema de cumplimiento interna y externamente. Por lo tanto, las empresas deben promover una conducta ética por parte del personal interno y, además, por parte de los terceros con los que se relacionan y que configuran su cadena de valor. Dicho de otro modo, lo que se pretende es una conducta corporativa éticamente responsable y en este contexto el modelo de

un modelo para cumplir con la legalidad en general y, por supuesto, con la legalidad penal". El Tribunal Supremo, por su parte, en su Sentencia 154/2016, de 29 de febrero, alude a la ausencia de *cultura de respeto al Derecho*, no limitándose, por tanto, únicamente al reproche penal, sino que se refiere al cumplimiento de la normativa en su conjunto. En el mismo sentido se pronuncia en su Sentencia 316/2018, de 28 de junio, estableciendo que no basta con gestionar los riesgos penales en los que puede incurrir una empresa perjudicando a un tercero, sino que es necesario identificar, analizar y gestionar los riesgos de cumplimiento que, aun no conllevando responsabilidad penal para la empresa, puedan ser constitutivos de un delito.

3 Es el ejemplo de Seat, perteneciente al grupo alemán Volkswagen. Tras el caso "*dieselgate*" nace «Together4Integrity», con el objetivo de convertirse en líderes en integridad a nivel empresarial. Más información en: https://mundoseat.seat.com Sobre el caso "*dieselgate*", en septiembre de 2015 salió a la luz que Volkswagen había instalado ilegalmente un software para alterar los resultados de los controles técnicos de emisiones contaminantes en 11 millones de automóviles con motor diésel, vendidos entre 2009 y 2015. La empresa alemana ha tenido que hacer frente a multas y compensaciones millonarias, entre las que se encuentran los 14.700 millones de dólares a los afectados en Estados Unidos. Además, debió asumir una multa de 4.300 millones de dólares impuesta por el Departamento de Justicia americano. En enero de 2017, el FBI detuvo al responsable de gestión de emisiones de Volkswagen en Estados Unidos por conspiración para defraudar, cargo del que pocos días después la propia marca se declaró culpable, acordando pagar 2.800 millones de dólares como multa penal y 1.500 millones de dólares como multa civil, siendo imputados seis ejecutivos. https://www.motor.es/que-es/dieselgate

compliance se convierte en un guardián de los valores corporativos.

Por otro lado, la evolución del *Compliance* en España no puede entenderse únicamente a través del marco normativo o de la teoría jurídica. Las experiencias reales de empresas que han implementado, desarrollado o, en algunos casos, ignorado programas de cumplimiento normativo ofrecen una perspectiva imprescindible. En este capítulo analizaremos en detalle cinco casos representativos (de éxito y fracaso) en el contexto español, cada uno procedente de un sector distinto: financiero, energía, construcción, distribución alimentaria y tecnología. Además, se expondrán dos casos a nivel internacional. En la exposición de los casos se indican algunas lecciones aprendidas, todo ello construido sobre la base de la información pública disponible, si bien, anonimizando las empresas en cuestión.

El último apartado de este capítulo abordará buenas prácticas con el objetivo de que sirvan a las compañías de nuestro país a la hora de fomentar su cultura de integridad y fortalecer sus sistemas de compliance holísticos y sobre la base de la ética corporativa.

ANÁLISIS DE CASOS PRÁCTICOS EN ESPAÑA: ÉXITOS, FRACASOS Y LECCIONES APRENDIDAS

Caso de éxito: sector financiero – modelo de *compliance* integral

El sector financiero ha sido históricamente uno de los primeros en desarrollar estructuras formales de cumplimiento, debido a la elevada regulación a la que está sometido. En particular, se hace referencia a un caso de éxito vinculado con una de las principales entidades financieras españolas, porque ha sido pionera en la implementación de un sistema integral de Compliance.

Tras la crisis financiera de 2008 y las sucesivas reformas regulatorias europeas (MiFID II, Basilea III, directrices de la EBA y otras normas y disposiciones como las del Comité de Basilea[4]), esta entidad implementó una estructura de *compliance* multinivel, con equipos especializados por área (blanqueo de capitales, prevención del fraude, protección de datos, entre otros) y con una clara independencia respecto a las unidades de negocio.

Durante el año 2010, tras la reforma del Código Penal, esta entidad definió y desarrollo un sistema de *compliance* penal alineado con los requisitos normativos a nivel organizativo y operativo. Años más tarde, evolucionó hacia un modelo de cumplimiento más transversal apalancándose en la estructura existente en otros ámbitos, como por ejemplo la prevención de blanqueo de capitales, la protección del consumidor financiero, la prevención de riesgos fiscales, la protección de los datos personales y estándares internacionales.

Así, desde un prisma de sistema de *compliance* integral, algunas medidas clave para el éxito de esta compañía han sido:

- Fuerte compromiso del Consejo de Administración: este compromiso se pone de manifiesto a través de distintas acciones, entre ellas, el respaldo absoluto a las decisiones adoptadas por los responsables de cumplimiento, por la asignación de recursos suficientes cuantificados de manera proporcional al tamaño de la compañía y atendiendo a las peticiones del equipo de cumplimiento, sanción disciplinaria de los incumplimientos sin excepción -por tanto sin interferir el cargo, posición o el aporte comercial/económico a la cuenta de resultados por parte de la persona que incumple la norma-, supervisión directa del desempeño del sistema de compliance a través de un sólido sistema de Reporting compuesto por diversos indicadores cuantitativos y cualitativos.
- Modelo de gobierno en el ámbito de cumplimiento: con separación clara de funciones entre las líneas de defensa, contando con un modelo de tres líneas de defensa robusto.

4 En 2005, el Comité de Basilea publicó el documento Compliance y la función de Compliance en los bancos, que determina, en forma de principios, las recomendaciones sobre la función de cumplimiento.

- Formación continua a todos los empleados, con programas específicos por nivel de riesgo.
- Cultura de integridad reforzada con campañas internas.
- Canales éticos de denuncia accesibles, confiables y anónimos.
- Decisiones estratégicas alineadas con *compliance*: mediante la integración del criterio de los equipos de Compliance en el proceso de toma de decisiones estratégicas a nivel de toda la compañía.
- Tecnología: implementación de herramientas de monitorización y alertas tempranas específicas en materia de *compliance* y uso de datos gestionados en otro tipo de aplicaciones existentes en la compañía para una mejor gestión del sistema transversal de *compliance*.

Gracias a estas iniciativas, la entidad ha logrado disminuir la ratio de incumplimientos por parte de su personal, mejorar su calificación de riesgo ante supervisores como el Banco Central Europeo y obtener reconocimiento internacional por sus políticas de integridad.

Estos resultados son ejemplo de cómo un enfoque integral de *Compliance* puede convertirse en una ventaja competitiva, de las que las lecciones aprendidas son:

- El liderazgo desde la alta dirección es clave.
- La formación continua es esencial para la eficacia del programa.
- Un enfoque multirriesgo considerando múltiples normas mejora la robustez del sistema.

Caso de éxito: sector energía – integridad y sostenibilidad

En el sector energético, existen múltiples empresas con sistemas de *compliance* también muy avanzados dado que se trata de un sector, igualmente, altamente regulado, lo que facilita la transformación cultural de las organizaciones. En este caso, la compañía fue una de las primeras en implementar un modelo de prevención de delitos, adaptado a los requisitos del artículo 31 bis del Código Penal español. Sin embargo, el salto cualitativo se produce cuando esta empresa desarrolla un modelo más global de *compliance* y ética en el marco de su estrategia de sostenibilidad y gobierno corporativo.

El compromiso con la ética y la sostenibilidad forma parte del posicionamiento estratégico de la empresa, lo que se refleja en sus políticas de Compliance.

- Un Código Ético alineado con los ODS de Naciones Unidas.
- Programas específicos de prevención de delitos medioambientales.
- Evaluación de riesgos regulatorios por país y unidad de negocio.
- Canal ético robusto con garantía de anonimato.

Hace algunos años, como fruto del proceso de mejora continua, la entidad realizó una revisión exhaustiva de sus relaciones con intermediarios en mercados internacionales de alto riesgo, detectando potenciales irregularidades que implicó la activación de medidas correctivas permitiendo a la compañía mejorar su cultura de cumplimiento y por supuesto evitar sanciones y otros daños reputacionales u operativos.

Las lecciones aprendidas de este caso son:

- El análisis de riesgos debe adaptarse a cada negocio.
- La detección temprana de riesgos es vital.
- La transparencia en la relación con terceros es un pilar preventivo.

Caso de fracaso: sector construcción – deficiencias en el control sobre terceros

En el sector de la construcción, históricamente han sido habituales los casos de corrupción y lavado de activos, entre otros. En

este caso, la empresa se enfrentó a un grave problema de cumplimiento tras la investigación judicial por supuestos pagos ilícitos a autoridades públicas para la adjudicación de contratos. Bajo nuestra perspectiva, la ausencia de una sólida cultura ética corporativa (generalizada en muchas empresas en esa época), junto con las siguientes carencias, ayudó a que determinadas personas pudieran actuar de manera ilícita:

- Deficiencias en los controles sobre la relación con proveedores y socios comerciales.
- Ausencia de registros claros sobre determinadas transferencias económicas.
- Inexistencia de un programa formativo y de sensibilización.

Todo ello provocó un daño reputacional significativo, la investigación penal a directivos de la empresa y la revisión forzosa de su modelo de *compliance*. Con posterioridad, esta empresa emprendió un profundo proceso de transformación en su modelo de cumplimiento a través de:

- Creación de un Comité de Ética independiente.
- Revisión integral de su mapa de riesgos penales.
- Implementación de controles reforzados en la contratación de terceros.

Las lecciones aprendidas de este caso de éxito son:

- No basta con tener un programa teórico de *compliance*: debe estar implementado y ser efectivo.
- La supervisión de terceros es un foco crítico en sectores con alta exposición a los riesgos de corrupción.

Caso de éxito: sector alimentación – *compliance* en el ámbito de la distribución

Una empresa del sector alimentación en nuestro país fue investigada en el marco de un proceso judicial por supuestas prácticas anticompetitivas hace algunos años. La Fiscalía consideró inicialmente imputar a la empresa, pero el modelo de *compliance* implantado años atrás fue determinante en el desenlace del caso:

- La empresa acreditó la existencia de un modelo de prevención de delitos adaptado y operativo.
- Presentaron evidencia documental de formación periódica en materia de derecho de la competencia.
- Se aportaron registros de control interno y acciones de revisión continua del programa y controles específicos.

La empresa quedó exenta de responsabilidad penal tras el examen judicial de su sistema de prevención calificándolo como adecuado no pudiendo imputar la conducta penal a un defecto organizativo.

Las lecciones aprendidas de este caso de éxito son:

- Un modelo de *Compliance* sólido puede ser una línea de defensa clave.
- La trazabilidad documental resulta esencial en un proceso judicial.
- La formación especializada de los equipos directivos es imprescindible.

Caso de éxito: sector tecnológico – *compliance* tecnológico y protección de datos

El sector tecnológico afronta nuevos riesgos vinculados a la protección de datos y ciberseguridad. Esta empresa ha sido líder en anticiparse a estos retos a través de un modelo de *compliance* en materia de protección de datos mediante el uso de nuevas tecnologías, por ejemplo, a través de las siguientes iniciativas destacadas:

- Desarrollo de un sistema de gestión de riesgos basado en Big Data.
- Integración del cumplimiento normativo en la gestión de ciberincidentes.

- Creación de un equipo específico de Privacy Compliance.

En el año 2020, esta empresa sufrió un intento de ataque de *ransomware* que podría haber sido devastador, sin embargo, gracias a sus protocolos de detección y respuesta, la compañía evitó la materialización de daños significativos y notificó a la Agencia Española de Protección de Datos (AEPD) en plazo, conforme a las exigencias de la normativa de protección de datos.

Las lecciones aprendidas de este caso de éxito son:

- La digitalización del *Compliance* mejora la capacidad de anticipación.
- La gestión de crisis debe estar integrada dentro del plan de cumplimiento.
- La coordinación entre los equipos de IT y Compliance es un factor de éxito.

ANÁLISIS DE CASOS PRÁCTICOS A NIVEL INTERNACIONAL: ÉXITOS, FRACASOS Y LECCIONES APRENDIDAS

Las empresas internacionales operan en un entorno complejo y diverso, enfrentándose a múltiples regulaciones que varían significativamente según cada jurisdicción. Este contexto globalizado requiere una planificación meticulosa y una ejecución precisa para el diseño e implementación de modelos de *compliance* eficaces. Entre los principales desafíos se encuentran:

1. Diversidad Normativa: La necesidad de cumplir con leyes y regulaciones que pueden diferir ampliamente no solo entre países, sino también entre regiones de un mismo país. Las empresas deben navegar por un entramado legal que afecta áreas desde la protección de datos hasta normas ambientales y laborales.
2. Diferencias Culturales: Las prácticas y expectativas culturales pueden influir en la manera en que se implementan y perciben las políticas de *compliance*. La diversidad cultural requiere que las empresas adapten sus estrategias de comunicación y capacitación para ser efectivas.
3. Coordinación y Consistencia: Gestionar operaciones dispersas geográficamente sin perder coherencia en sus políticas centralizadas, lo cual exige un equilibrio afinado entre la autonomía local y la supervisión central.
4. Riesgos Geopolíticos: La volatilidad política y económica en distintas regiones puede afectar la estabilidad regulatoria, creando incertidumbres adicionales en el cumplimiento normativo.

En este apartado, analizamos dos casos de éxito a nivel internacional, extrayendo igualmente lecciones aprendidas.

Caso de éxito: sector consumo – cadena de suministro

Una empresa dedicada a bienes de consumo masivo y *retail* se enfrentó a desafíos en la implementación de su modelo de *compliance* debido a la gran diversidad de mercados en los que opera, desde economías desarrolladas hasta emergentes. En este difícil contexto la empresa empleó las siguientes herramientas:

- Radar regulatorio: empleó un sistema de detección y evaluación normativa a nivel mundial que le permitió anticiparse al cumplimiento de la legislación mediante la identificación temprana y adaptación interna de sus procesos operativos.
- Compliance en la Cadena de Suministro: desarrolló un sistema de verificación escalonado que asegura que sus proveedores, subcontratistas y distribuidores cumplen con los estándares internacionales y la legislación local.
- Sistema de alerta temprana y *whistleblowing*: mucho antes de que existiera la normativa de protección del denunciante a nivel europeo o español, esta empresa comenzó a utilizar un software como mecanismo de notificación de incumplimientos a nivel mundial bajo los

principios de anonimato, gestión independiente y política de no represalias.

- Capacitación continua: la empresa implementó un programa de capacitación obligatoria semanal para todos sus empleados, donde se abordaban no solo las nuevas regulaciones, sino también los valores corporativos y la ética que debía imprimir cada actuación profesional. Este enfoque permitió a los empleados ver el *compliance* no solo como una obligación legal sino como una parte clave de sus valores empresariales.
- Compromiso de la Alta Dirección: los líderes de la empresa de las distintas unidades de negocio recibieron formación específica y fueron nombrados embajadores del programa de *compliance*. Esta iniciativa aseguró que las políticas y procedimientos fueran interiorizadas en la gestión diaria en cada una de las decisiones operativas.

Al adoptar este enfoque, la empresa no solo logró cumplir plenamente con las regulaciones nacionales, sino también incrementar su eficiencia operativa y mejorar su reputación ante socios comerciales y consumidores. La ética corporativa, al ser interiorizados los valores y principios de los profesionales como parte de su proyección laboral, también sufrió un aumento significativo, de acuerdo con las distintas mediciones internas y, todo ello, resultó en mejoras en la productividad.

Caso de fracaso y éxito absoluto: sector tecnológico, energía y transporte

En este caso, la empresa invirtió 1,6 mil millones de dólares en su programa de cumplimiento después de un escándalo de corrupción en 2008. La empresa asumió que había estado pagado sobornos a funcionarios públicos en diferentes países para obtener contratos en sectores como energía, transporte y comunicaciones. La empresa acordó pagar una multa de 450 millones de dólares en Estados Unidos tras declararse culpable por violaciones a la legislación que castiga la corrupción *Foreign Corrupt Practices Act* (FCPA).

Como parte de su actual programa destaca:

- Cultura ética empresarial: la empresa desarrolló un sistema de capacitación global que ha generado un mayor *engagement* por parte de los profesionales logrando disminuir los niveles de rotación.
- Inteligencia artificial: la empresa ha implementado herramientas de inteligencia artificial que evalúan el riesgo de *compliance* en tiempo real, lo que ha llevado a una caída del 75% en los incumplimientos normativos en menos de cinco años.

Actualmente, el programa de *compliance* de esta empresa es uno de los más paradigmáticos a nivel internacional.

CONCLUSIONES: PAUTAS PARA CONTAR CON UN SISTEMA DE ÉTICA Y *COMPLIANCE* EFICAZ

Existen múltiples variables a la hora de identificar los aspectos esenciales que debe reunir un Sistema de Ética y Compliance para que pueda ser considerado eficaz. Y ello varía, principalmente, por las circunstancias de la propia empresa. El sistema debe ser, por tanto, un traje a medida atendiendo a distintos factores, entre otros, el tamaño, sector, ubicación geográfica, madurez a nivel de procesos, tecnología utilizada y, en todo caso, considerando el principio de proporcionalidad y en función del nivel de riesgo que cada empresa pueda presentar[5]. No obstante, a lo largo de este apartado, se ofrece un listado de buenas prácticas que podrían ayudar a que el sistema sea eficaz.

5 El enfoque basado en riesgos, conocido como *risk based approach* (RBA), es uno de los principios más utilizados en materia de prevención del blanqueo de capitales y cumplimiento. Los reguladores que operan en el campo del lavado de activos, principalmente el GAFI, recomiendan un enfoque basado en el riesgo para que las instituciones y las organizaciones combatan eficazmente los delitos financieros. La definición más simple del RBA es que la organización realiza controles basados en la percepción de riesgo propia y el nivel de riesgo de los clientes. Para más información: http://www.fatf-gafi.org/documents/riskbasedapproach/

Así, lo primero que la empresa debe plantearse es qué persigue con el diseño e implementación de un sistema de ética y *compliance*. Hemos visto a lo largo de este capítulo empresas cuyo sistema le ha permitido exonerar responsabilidades legales. Sin embargo, es más que probable que si la empresa busca, únicamente, liberarse de una eventual responsabilidad en el marco de un procedimiento judicial finalmente, y llegado el caso, fracase porque no existirá cultura ética y el programa será más teórico que otra cosa, como también ha pasado en nuestro país. En ese supuesto, el propio modelo de *compliance* supondrá únicamente un coste. La tendencia actual pasa por entender los programas de cumplimiento como una inversión; una oportunidad de crecimiento, de eficiencia, de mayor impacto social para la comunidad, de sostenibilidad para el negocio e incluso de ahorro de costes porque incumplir genera muchos gastos (v.g. pago de sobornos, asunción de compromisos que no obedecen a una mejor productividad, rotación de personal, posibles sanciones, costes operativos, daños reputacionales y pérdida de valor...)[6].

Profundizando en la parte práctica, en la medida en la que la compañía opte por diseñar un sistema de prevención guiado por la ética y la integridad, presentará los siguientes síntomas o evidencias o aplicará alguna de las siguientes buenas prácticas:

- El órgano de gobierno/administración constituirá una función ética y de cumplimiento autónoma y con suficiente autoridad. La persona o personas encargadas de cumplir dicha función deberán tener la capacitación suficiente (que podría ser jurídica, de control interno o una formación mixta), la dedicación necesaria, la honorabilidad oportuna (no contar con antecedentes delictivos o con un histórico conflictivo) y las habilidades necesarias (confiabilidad, dotes comunicativas, etc.)[7]. La autonomía se pone de manifiesto a través de la discrecionalidad para acceder a información interna y/o adoptar decisiones alineadas con la regulación de la empresa, entre otros;

- El órgano de gobierno destinará recursos humanos y financieros suficientes y razonables para que la función ética y de cumplimiento sea realmente autónoma y pueda ejecutar sus propias decisiones (v.g. realización de una auditoría, una investigación, obtención de soporte externo o una formación);

- La empresa contará con un sistema de *governance* lo más descentralizado posible y cercano al modelo de las tres líneas de defensa, de manera que exista separación operacional y del negocio (que son la primera línea de defensa), de las áreas de aseguramiento (que son la segunda línea de defensa) y la función de auditoría (como tercera línea de defensa);

- La función ética y de cumplimiento estará ubicada en el organigrama al más alto nivel, reportando directamente a los órganos de gobierno/administración. Además, el órgano de gestión/dirección presentará formalmente a la persona o personas que desempeñen la función ética y de cumplimiento e informará de la importancia que dicha función tiene para toda la organización, como pilar estratégico de la compañía;

- El órgano de gobierno/administración participará activamente en la revisión y aprobación de la normativa esencial del sistema de *compliance* y de los informes o memorias que se produzcan y, entre otros, establecerá la obligación de cumplir con esta normativa por parte de todos los profesionales. En la normativa básica deberá incluirse una descrip-

6 "*El 50% de los fraudes en las empresas se produce por una falta de control*" según el testimonio de Daniel Alonso, exfiscal de Manhattan y del caso "Lobo de Wall Street", expuesto en el II Congreso Internacional de Compliance Officer, organizado por la World Compliance Association y celebrado en abril de 2023 en Barcelona.

7 En este sentido LASCURAÍN atinadamente asevera que: "*Si ya existe un delegado encargado de controlar un riesgo, la estrategia consiste en no sumar al responsable de cumplimiento a ese control, sino en asignarle otras funciones que no son directamente de seguridad sino de organización, de asesoramiento o policiales respecto a tales controladores*" en LASCURAIN SÁNCHEZ, "La responsabilidad penal individual en los delitos de empresa", *Derecho Penal Económico y de la Empresa*, NORBERTO J. DE LA MATA BARRANCO, JACOBO DOPICO GÓMEZ-ALLER, JUAN ANTONIO LASCURAÍN SÁNCHEZ, ADÁN NIETO MARTÍN DYKINSON, 2018 pp. 122 y ss.

ción detallada del sistema de *compliance*, a título ejemplificativo: (i) los roles y responsabilidades o modelo de gobernanza; (ii) las líneas de *reporting*; (iii) las obligaciones en materia de monitorización; (iv) la metodología de identificación y evaluación de riesgos; (v) el canal ético o de denuncias, incluyendo la previsión de potenciales conflictos de interés; (vi) planificación de revaluaciones, procesos de autoevaluación por parte de la primera línea o auditorías -incluyendo la metodología, la persona encargada de realizar la auditoría, el tamaño de la muestra, el método para definir el plan de pruebas y la periodicidad-; (vii) descripción de los recursos disponibles; (viii) los medios de difusión y formación, incluyendo canales o formatos específicos en función de los perfiles y los niveles de riesgo que presenten. También puede incluir la vinculación de la asistencia a las formaciones a la retribución variable; (viii) descripción del sistema disciplinario aplicable en caso de que alguna persona infrinja la normativa interna y/o externa;

- El órgano de gobierno/administración deberá seleccionar los valores y principios que desee rijan la actividad y documentarlos en un Código Ético o de Conducta y publicitarlo (*mailing* interno, web, anexo a los contratos con terceros, etc.);

- La función ética y de cumplimiento se configura como la segunda línea de defensa, debiendo coordinar actividades, impulsar el desarrollo de normas y/o la implementación de controles operativos, así como actividades de difusión y formación, gestión de las comunicaciones, planificación de revisiones periódicas y revaluaciones y ejecutar planes de monitoreo continuos pero será la primera línea de defensa quien deba ejecutar los controles y monitorizar los riesgos operativos que tienen asignados, fruto de sus actividades ordinarias de negocio o de soporte. Son la primera línea porque se configura como los propietarios de las actividades que realizan y que son generadoras de riesgos, así como propietarios de los controles vinculados. *De facto* tienen, en términos jurídicos, el dominio del hecho. La tercera línea está formada por la función independiente de auditoría (que puede ser desempeñada interna o externamente) y que se encarga de verificar o comprobar la eficacia operativa del entorno de control y el cumplimiento de la regulación;

- No se cuestionarán las decisiones de la función de ética y cumplimiento, sin perjuicio del apetito del riesgo de los órganos de gobierno/administración, que adoptarán decisiones informadas y teniendo en consideración las advertencias de la función de cumplimiento. Es lo que comúnmente se denomina *tone from the top*[8], la ética corporativa nace en la alta dirección;

- Se tendrán en cuenta los consejos de la función de ética y cumplimiento desde un punto de vista del negocio y, en la medida de lo posible, se involucrará a la función de cumplimiento desde el principio en cualquier posible operación, proyecto, *joint venture* o afiliación con un socio comercial y apertura de negocio en otros países (procesos de diligencia debida, incluyendo procesos KYC[9] y rechazo de terceros cuyo riesgo supere el umbral establecido). Además, se incluirán en los clausulados con terceras partes pautas éticas y de cumplimiento cuyo cumplimiento se supervisará proactivamente;

8 En España, la Circular 1/2016, de 22 de febrero, de la Fiscalía General del Estado sobre la responsabilidad penal de las personas dispone que: *Cualquier programa eficaz depende del inequívoco compromiso y apoyo de la alta dirección para trasladar una cultura de cumplimiento al resto de la compañía. Si son los principales responsables de la entidad quienes incumplen el modelo de organización y de prevención o recompensan o incentivan, directa*
o indirectamente a los empleados que lo incumplen, difícilmente puede admitirse que exista un programa eficaz

9 KYC (*Know Your Customer* or *Know Your Counterparty*) es un proceso fundamental para las relaciones de la empresa y terceros, ya sean socios o clientes. Este procedimiento KYC supone el punto de partida para las relaciones entre una organización y las terceras partes y se materializa a través de cuestionarios que incluyen preguntas sobre la titularidad real si es una empresa, procedencia de fondos con los que paga, datos de filiación a efectos de evaluar el riesgo país, o riesgo sector, etc. Actualmente existen multitud de mecanismos basados en inteligencia artificial para agilizar este tipo de procesos de diligencia debida.

- Se aplicarán procesos de diligencia debida en la selección y/o promoción de personal, valorando expresamente aspectos éticos y de cumplimiento;
- Existirán incentivos económicos para el personal que actúe de forma ética (participando en las formaciones de cumplimiento, comunicando comportamientos sospechosos o irregulares a la función de cumplimiento, etc.)[10];
- Existirán reportes ordinarios recurrentes desde la función ética y de cumplimiento a los órganos de gobierno/administración con información, a título ejemplificativo, sobre (i) la evolución del mapa de riesgos de cumplimiento, (ii) la volumetría de las incidencias detectadas, (iii) el grado de participación de la organización en las tareas de cumplimiento, (iv) el porcentaje de profesionales que hayan cumplimentado las formaciones, (v) estadísticas acerca de las acciones de difusión realizadas, (vi) el grado de avance de los planes de acción o mejora, (vii) la suficiencia o insuficiencia de recursos, (viii) resultado de las revaluaciones, verificaciones o auditorías/testeos realizadas interna o externamente, (ix) acciones previstas para los siguientes periodos, (x) resultados de inspecciones externas o relaciones con reguladores y/o supervisores, (xi) resultados de encuestas sobre clima ético, (xii) estadísticas de reclamaciones de clientes, (xiii) volumetría de las denuncias recibidas, gestionadas y sanciones derivadas;
- Los canales éticos o de denuncias serán gestionados, en la medida de lo posible por expertos externos, de manera que se le otorgue la máxima confiabilidad e independencia. En caso de que sea inviable la externalización por una razón de costes, será gestionado con las máximas garantías de confidencialidad por parte de la función ética y de cumplimiento (preferiblemente mediante tecnología que permita la trazabilidad de las comunicaciones) que no debe sufrir ningún tipo de coacción para desvelar la identidad de la persona denunciante, incluso aunque el denunciado sea un miembro del órgano de gobierno/administración u alto directivo. Se protegerá al denunciante de buena fe mediante políticas activas de no represalias, mediante la sanción de comportamientos inadecuados, mediante soporte personal al denunciante, incluso activando medidas físicas de cambio de ubicación o permiso retribuido temporal aplicable a la persona en cuestión;
- La identificación de riesgos de cumplimiento seguirá las pautas establecidas en las normas ISO, de manera que se identifiquen los procesos estratégicos, de negocio y operativos y, posteriormente, se analicen diversas fuentes de riesgo, sus causas y se valore el riesgo potencial en virtud del posible impacto y probabilidad que presenten. La metodología de identificación y valoración debe atender a criterios lo más objetivos posible siguiendo los estándares internacionales. Sin perjuicio de que le corresponde a la función de cumplimiento la documentación de la metodología y el proceso de identificación, deben participar en el mismo los responsables de los riesgos que deban ser identificados, la primera línea;
- La primera línea de defensa también participará en la identificación de controles preventivos, detectivos o reactivos vinculados con los riesgos y procesos antedichos. Los controles pueden tener diversa naturaleza (normativos, organizativos, operativos, financieros, formativos, de seguimiento...);
- La empresa contará con un plan de acción o de remediación que incluya las medidas de mejora detectadas fruto de la identificación de riesgos, eficacia de los controles y/o los indicadores (KRI, KPI) que se hubieran desarrollado. La función ética y de cumplimiento impul-

10 La «*Consultation on guidance about commercial organisations preventing bribery (section 9 of the Bribery Act 2010)*» publicada por el Ministerio de Justicia del Reino Unido, prevé entre las medidas para asegurar el cumplimiento de los programas anticorrupción, premiar a los empleados con complementos variables de su salario basados en la evaluación de su cumplimiento normativo ("*performance appraisals*"). Vid. también en ese sentido: KAPLAN, "The first world on "compliance" incentives", en *The FCPA* Blog, 19 de enero de 2011 http://www.fcpablog.com/blog/2011/1/19/the-first-word-on-"compliance"-incentives.html

será el desarrollo de hojas de ruta que incluyan medidas específicas por parte de la primera línea de defensa a fin de planificar adecuadamente el diseño e implementación de tales medidas y realizará una monitorización de su efectiva implementación. El incumplimiento de los planes por parte de la primera línea sin causa justificada será sancionado de forma proporcional y/o su grado de avance se vinculará a la retribución variable:

- La función ética y de cumplimiento contará con un plan de *compliance* anual en el que se incluirán las actividades específicas planificadas cuyo resultado elevará al órgano de gobierno/administración, al menos, anualmente;
- En la medida de lo posible, la función ética y de cumplimiento contará con herramientas informáticas (propias o subcontratadas) que permitan la gestión de los riesgos y monitorización de los controles, nos referimos a sistemas de GRC (*Governance Risk & Compliance*) y que pueden basarse en tecnologías como la inteligencia artificial para detectar patrones de conducta, realizar monitoreos o responder consultas frecuentes.

REFERENCIAS

GIMENO SENDRA, "Corrupción y propuestas de reforma".DIARIO LA LEY nº7990, 26 de diciembre 2012.

NORBERTO J. DE LA MATA BARRANCO, JACOBO DOPICO GÓMEZ-ALLER, JUAN ANTONIO LASCURAÍN SÁNCHEZ, ADÁN NIETO MARTÍN, Derecho Penal Económico y de la Empresa.DYKINSON, 2018.

RODRÍGUEZ MOURULLO, "La responsabilidad penal de las personas jurídicas". TIEDEMANN, K., «La responsabilidad penal de las personas jurídicas», en VV.AA., Anuario de Derecho Penal de la Universidad de Fribourg, 1996, págs. 97 y ss.

WARIN, F.J, & SCHWARTZ, J.C, "Deferred Prosecution: The need for Specialized Guidelines for Corporate Defendants", JOURNAL OF CORPORATION LAW, Iowa, Otoño de 1997, p.121-134.

WELLNER, "Effective "compliance" Programs and Corporate Criminal Prosecutions", CARDOZO LAW REVIEW nº27, Octubre 2005, p.497-528.

ZUGALDÍA ESPINAR, J. M., «Jurisprudencia aplicada a la práctica: modelos dogmáticos para exigir responsabilidad criminal a las personas jurídicas (A propósito de las SSTS de 2 de septiembre de 2015, 29 de febrero de 2016 y de 16 de marzo de 2016)», La Ley Penal, núm. 119, marzo-abril, 2016., pág. 4.

SOBRE LA AUTORA

Olga Fraga Gómez es Socia de Deloitte Legal. Profesora colaboradora en ESADE, IEB, ISDE, CEU y Universidad de Castilla- La Mancha. Miembro del Comité Técnico y de Estudio de *Compliance Officers* en la *World Compliance Association*. Miembro de la *Woman in a Legal World* y de la Asociación Internacional de Derecho Penal.