BOSCH

Mapa de riesgos penales y prevención del delito en la empresa

Coordinadores

Pere Simón Castellano
Alfredo Abadías Selma

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www.wolterskluwer.es

Primera edición: Septiembre, 2020

Depósito Legal: M-23690-2020
ISBN versión impresa: 978-84-7052-827-9
ISBN versión electrónica: 978-84-7052-828-6

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

Pere Simón Castellano
Alfredo Abadías Selma
Coordinadores

Ha pasado ya la época en que los empresarios podían crear empresas, contratar trabajadores y crear riqueza… sin control alguno.

Cierto es que, en el Código Penal anterior al vigente, el CP de 1970 —y su importante reforma del año 1983—, no contenía delitos específicos susceptibles de ser cometidos por Empresas y empresarios. Obvio es que sí se podían cometer estafas, apropiaciones indebidas, etc., pero no había delitos específicos. Expresado en otros términos, al final del régimen anterior no había una tipificación de los llamados «*delitos de cuello blanco*».

La ley penal predemocrática podría definirse, con cierta simplicidad, como una ley para los «*robagallinas*» y para los considerados delincuentes políticos. La estrecha relación entre los poderes económicos de la época y el régimen político hacía que no se plantease la necesidad de llevar al código punitivo estas conductas.

En la actualidad, el Derecho Penal debe enfrentarse a nuevos y complejos problemas. Uno de ellos es de la comisión de delitos a través o en el seno de estructuras empresariales, organizadas y complejas, basadas en principios de división funcional del trabajo y jerarquía.

En un mundo interconectado, como el presente, existen muchas posibilidades de cometer delitos, de diluir la responsabilidad de la comisión de delitos dentro de una empresa, no digamos ya en multinacionales. Y el legislador, siendo consciente de estos problemas, ya en el Código Penal vigente, el de 1995, ha ido introduciendo, en sucesivas reformas, numerosos bienes jurídicos susceptibles de protección y cuya vulneración da lugar a la comisión de delitos, con la consiguiente condena a multas cuantiosas y la posibilidad real de ingreso efectivo en prisión.

El legislador lleva años intentado introducir una cultura de cumplimiento normativo en las empresas en prevención de riesgos, sea respecto de sus trabajadores (delitos contra los derechos de los trabajadores, contratación de mano de obra ilegal, etc.), sea respecto de clientes y proveedores y de sus propios trabajadores (protección de datos de carácter personal), sea de prevención del blanqueo de capitales, en las transacciones internacionales, en las contrataciones del sector público, sea, en suma, de prevención de la comi-

sión de delitos en el seno de las empresas y entes públicos, bien por parte de trabajadores, bien por cuenta de directivos que actúen siempre en provecho y beneficio de la empresa (esto es, la responsabilidad penal de las personas jurídicas introducida, recientemente en nuestro Derecho Penal por la LO 5/2010, de 22 de junio y posterior reforma por LO 1 /2015, de 30 de marzo).

Y centrándonos en esta última, la responsabilidad penal de personas jurídicas, el clásico el aforismo según el cual «*societas delinquere non potest*» (las sociedades no pueden delinquir), principio que estuvo vigente a lo largo de muchos siglos en nuestro Derecho, dejó de estarlo por la LO 1/2010, de 22 de junio, de reforma del Código Penal, por el que se introdujo la responsabilidad penal de las personas jurídicas, aprovechándose la transposición de varias Directivas de la Unión europea. Actualmente, «*societas delinquere potest*» (las sociedades sí pueden delinquir).

Opción del legislador muy criticada por la doctrina —entre otros yo mismo en mi tesis doctoral y en mi conferencia de ingreso en la Academia de Jurisprudencia y Legislación como Académico Correspondiente— por cuanto las Directivas de la Unión Europea que el legislador español transpone en esta reforma del Código Penal no imponía que se estableciese una responsabilidad penal de las personas jurídicas, sino, simplemente, «*unas sanciones efectivas, proporcionadas y disuasorias*» y que, perfectamente, se podía haber resuelto por la sanción de estos incumplimientos o contravenciones por parte de las Empresas por la vía del Derecho Administrativo Sancionador al ser más práctico, efectivo y eficaz, al no tener la amplitud de garantías del Derecho Penal y poder imponerse unas sanciones (la multa es la pena tipo en la responsabilidad penal de las personas jurídicas) mucho más elevadas.

Y así lo han hecho otras legislaciones más respetuosas con la propia definición de delito (recogida en el art. 10 de nuestro Código Penal), de los principios de responsabilidad subjetiva, de culpabilidad y de personalidad de la pena, en suma, con la teoría general del delito, tales como el italiano y el alemán. Pero esta ha sido la opción que ha elegido el legislador español y que, como ha dicho algún autor, «*la responsabilidad penal de las personas jurídicas ha venido para quedarse*».

Y por la LO 1/2015, de 30 de marzo, se introdujo una nueva reforma en el Código Penal. Con esta nueva reforma en nuestro texto punitivo no se introdujeron modificaciones en la parte general del Código Penal en atención a los principios básicos citados, ni se suprimió el *numerus clausus* de delitos que pueden cometer personas jurídicas (la mayoría de los delitos pueden ser cometidos por personas jurídicas, al menos de forma imprudente, o, al menos, introducir nuevos tipos delictivos (recuérdese que la LO que introdujo este tipo de responsabilidad estableció un *numerus clausus* de delitos —pocos más de veinte— que podía cometer una persona jurídica), lo que sería loable por cuanto no se entiende la omisión por el legislador de ciertos delitos que se pueden cometer y de hecho se cometen en el seno de las empresa, tales son el homicidio y lesiones —al menos de forma imprudente—, el aborto y la omisión del deber de socorro, la eutanasia, delitos de manipulación genética, delitos contra la salud pública —en concreto, la ela-

boración de sustancias que causan grave daño a la salud—, el *mobbing* y acoso inmobiliario, las imprudencias profesionales, pero, esencialmente, los delitos societarios, delitos contra los derechos de los trabajadores y delitos contra la seguridad y salud de los trabajadores, cuya misión es inexplicable, así como la falta de regulación del delito de quebrantamiento de condena cometido por una persona jurídica, con las graves consecuencias que ello conlleva en el caso de incumplimiento de las penas impuestas a una empresa por sentencia firme por aplicación del principio de legalidad, básico en el Derecho Penal), sino respecto a la introducción de los planes de cumplimiento, de autocontrol, los *compliance programs*, que puede llegar a exonerar de responsabilidad penal a la persona jurídica de comprobarse su existencia, su debido cumplimiento y su efectividad.

¿Qué es lo que pretendía el legislador del año 2015 con la regulación como causa de extinción la responsabilidad criminal —o, en su caso, de minoración como circunstancia modificativa de la responsabilidad criminal— de los programas de *compliance*? Pues, simplemente, introducir una cultura de prevención de la comisión de delitos en una Empresa a través de una serie de programas de autocontrol.

Quiso, así, el legislador del 2015 establecer una cultura de cumplimiento que pretende seguir la cultura introducida de prevención de riesgos laborales y la protección de datos de carácter personal, sea de trabajadores, sea de clientes, sea de proveedores.

Se trata, en definitiva, de que las empresas establezcan en su seno una serie de medidas, de programas de autocontrol (*compliance programs*) para evitar incurrir en responsabilidad penal e instaurar, de tal forma, una cultura de cumplimiento de prevención de delitos. Cuestión distinta es si estos citados programas de cumplimiento, de autocontrol, son efectivos o no, lo que será en su caso objeto de prueba en el proceso penal.

Pero es que en la Empresa se pueden cometer otros delitos y sufrir otros delitos. Dentro de los primeros, coacciones, amenazas, hurtos, estafas, acoso *(mobbing*) o abusos sexuales y corresponde a los directivos de estas empresas evitarlos y, para ello, tiene que saber cuáles son los que se pueden cometer, la forma de prevenirlos y, en su caso, la manera de proceder en el caso de que llegue a su conocimiento su comisión.

Dentro de los segundos, especialmente destaca la ciberseguridad. Resulta difícil hoy en día no ser consciente de la importancia que han tomado los riesgos vinculados a la tecnología en nuestra sociedad. Empresas, Gobiernos, Administraciones públicas y ciudadanos en general, se afanan por no ser los siguientes de una larga lista de perjudicados por ataques informáticos que no sólo crecen de forma exponencial, sino que además nos sigue sorprendiendo con nuevos ataques cada vez más dañinos. Y sin embargo el futuro se dibuja todavía más sombrío, ya que más allá del negocio creciente de organizaciones criminales o contiendas *hacktivistas*, nuevos actores como Gobiernos y grupos terroristas han irrumpido en el escenario internacional con recursos casi ilimitados y causando daños cibernéticos verdaderamente importantes cuando no catastróficos.

En este complejo escenario geo—político en el que operan las organizaciones, y donde las empresas cada vez dependen en mayor medida de la tecnología para sobrevivir

en plena transformación digital, resulta indispensable establecer rigurosas medidas de protección para enfrentarse a amenazas cada vez más sofisticadas.

Todas las empresas, cualquiera sea el sector de su actividad, y administraciones públicas deben incidir en el desarrollo del conocimiento y las capacidades necesarias y básicas para el desempeño profesional de la gestión de la ciberseguridad en relación con la seguridad de la información y la protección de datos personales. En suma, prevenir, de forma práctica y operativa, las consecuencias de las amenazas a las que se expone cada día cualquier organización empresarial y/o pública.

Y en similares términos podríamos pronunciarnos en el ámbito de la contratación del sector público, en las transacciones internacionales, en los sectores financiero y sanitario, etc.

Todos estos temas son abarcados el interesante libro que tengo el honor de prologar. Bajo el título «*Responsabilidad penal y mapa de riesgos en la empresa. Análisis práctico de los distintos sectores de actividad*», coordinado por los profesores de la UNIR, Pere Simón Castellano y Alfredo Abadías Selma, y realizado por numerosos autores, todos ellos grandes expertos en sus respectivas materias —con la más alta cualificación profesional, siendo Profesores y Letrados, Magistrados, Fiscales, Secretarios de Administración Local, CEO y *Chiefs Compliance Officer— que* analizan desde un punto de vista teórico, pero también práctico, los distintos problemas en que puede verse incursas las Empresas y las Administraciones públicas, especialmente las delictivas.

Por ello no me queda sino felicitar, por supuesto a los coordinadores, por su magnífica labor de búsqueda de los mejores autores en cada materia y su labor de coordinación, tarea nada fácil. Y doy fe de ello. Pero también a todos y cada uno de los autores, quienes —de forma amena, sin perder categoría científica, pero también de forma muy práctica— exponen a los lectores los problemas sectoriales que, dentro del campo del cumplimiento normativo, cualquier Empresa, cualquier empresario, y aún los Entes Públicos, se pueden enfrentar, dando soluciones prácticas y operativas.

Es este un libro esencial para cualquier Empresa —grande, mediana o pequeña— que va a facilitar el conocimiento de la responsabilidad penal en que puede incurrir y los programas de prevención para evitarla, magníficamente expuestos por los autores en los sucesivos capítulos de esta magna obra en materia de conocimiento normativo de prevención de riesgos.

En suma, magnífica y magna obra que pensamos contribuirá a extender en la cultura empresarial de nuestro país el conocimiento normativo de prevención de riesgos y evitar que en el seno de las Empresas se cometan delitos o que los sufran. Sin duda este libro será un manual de referencia y consulta para Empresarios y *Compliance Officers,* cualquiera sea el sector de su actividad, y Administraciones públicas (locales, autonómicas o centrales).

No me queda sino felicitar a los coordinadores y a los autores por su magnífico trabajo y dar las gracias a la editorial *Wolters Kluwer* por su publicación.

Ricardo RODRÍGUEZ FERNÁNDEZ
Doctor en Derecho
Académico Correspondiente de la Academia de Jurisprudencia y Legislación
Magistrado
Consultor Internacional y Columnista
Ex letrado del Gabinete Técnico del Tribunal Supremo

Parte II

ESTUDIO POR SECTORES DE ACTIVIDAD

Las reformas introducidas por el legislador nacional en la última década abrazan una forma de entender el cumplimiento normativo desconocida hasta hace bien poco por nuestro ordenamiento jurídico y entrañan *de facto* cambios estructurales cuya profundidad y relevancia es tal que incluso podemos hablar sin problemas de una nueva cultura de cumplimiento normativo.

Nos referimos a un moderno sistema basado en la responsabilidad proactiva —heteroresponsabilidad o autorresponsabilidad, según se prefiera— de empresas y organizaciones, también por parte de los organismos del sector público, que se impone de forma decidida en nuestro ordenamiento fruto de experiencias y tendencias positivas que muestran los sistemas anglosajones del *common law*.

Los efectos de esta cultura de cumplimiento se despliegan y proyectan sobre ámbitos legales muy diversos y específicos: el diseño de los sistemas de prevención de riesgos laborales, de protección de datos personales, de gestión de riesgos medioambientales, de seguridad de los sistemas de información, etc. El enfoque en todos ellos es muy parecido y parte de metodologías y conceptos propios de sistemas de cumplimiento o *compliance* penal que exigen a empresas y organismos el compromiso por parte de toda la organización, el liderazgo vertical, la creación de estructuras por defecto y en el diseño orientadas al cumplimiento —códigos éticos, comité de buenas prácticas, desempeño de funciones por parte del *compliance officer* con autonomía, presupuesto y medios materiales, canales de denuncia, etc.—, garantizando la comunicación y consulta y llevando a la práctica el principio de mejora continua de los sistemas.

En este sentido debemos partir necesariamente de las normas y estándares internacionales de referencia, más concretamente, de las ISO 19600 —sistemas de gestión del cumplimiento—, ISO 31000 y 31010 —gestión de riesgos como elemento nuclear de cualquier programa de cumplimiento—, ISO 37001 y la recientemente publicada —mayo 2020— ISO 31022 para la gestión de riesgos legales, entre otras. Nos encontramos, además, en la antesala de la nueva ISO 37301, que vendrá a reemplazar a la ISO 19600, con importantes e interesantes novedades y que se convertirá sin lugar a duda en la norma de referencia en el mundo del compliance.

Resulta así de rabiosa actualidad e interés el objeto de la presente obra colectiva, que se divide en cuatro partes claramente diferenciadas. La primera parte reúne conocimientos teóricos y prácticos sobre el papel que el mapa de riesgos juega como elemento central en pos del cumplimiento normativo. De hecho, podemos afirmar sin temor a caer en error que no existe cumplimiento sin mapa de riesgos, sin una estrategia diseñada *ad hoc* para prevenir las amenazas y reducir los escenarios para el delito. Los capítulos uno a tres, cuya autoría corresponde respectivamente al Dr. Pere Simón Castellano —profesor contratado doctor en UNIR y abogado *of counsel* en FONT ADVOCATS—, al Sr. Albert Salvador Lafuente —secretario general de la WCA— y al Sr. Iván Martínez López —CEO Intedya y Vicepresidente Internacional de la WCA— exploran precisamente la noción del mapa de riesgos desde una óptica muy práctica, otorgando al lector las herramientas y conocimientos necesarios para poder activarlo en la práctica, en base a distintas metodologías.

La segunda parte de la obra colectiva ofrece un estudio por sectores de actividad que resulta de sumo interés, ya que permite observar aquellas peculiaridades o cuestiones que se concentran en determinados sectores por la propia naturaleza, y los riesgos intrínsecos, de determinados procesos de negocio. El capítulo cuarto, cuya autoría corresponde la Sra. Laura Gonzalvo Diloy —*Chief Compliance* en Ayuda en Acción—, estudia la prevención de riesgos en el tercer sector. El quinto lo rubrica la Sra. Sandra Soler Vidal —CEO de SOLER Compliance y FORMA Compliance— en relación con el mapa de riesgos en la pequeña y mediana empresa —SME's o PYMES—, que además incluye muchos subsectores de actividad de empresas de ese tamaño. Por su parte, la Sra. Laura Nieto Silvente —*Senior Associate* en la prestigiosa firma internacional Cases & Lacambra— proyecta en el capítulo sexto su vasta experiencia en el sector financiero, fruto también del desempeño durante años de tareas como *compliance officer* interna en *Crèdit Andorrà*. Finalmente, el capítulo séptimo corre a cargo de la Dra. Concepción Campos Acuña, probablemente la autora de referencia a nivel nacional en términos cuantitativos y cualitativos en temas de cumplimiento normativo en el sector público, que traslada y ofrece las herramientas para la creación y gestión del mapa de riesgos en el citado sector, haciendo hincapié en los procesos de contratación pública.

La tercera parte de la obra —capítulos ocho a diez— está dedicada al mapa de los (ciber)riesgos en relación con la seguridad de la información y la protección de datos personales. Para ello, contamos con profesionales contrastados como el Sr. Eloi Font Manté —Socio Director de FONT ADVOCATS—, el Dr. Juan Francisco Rodríguez Ayuso —Coordinador del Máster en Protección de Datos en UNIR— y el Sr. Oscar López Rodríguez —Socio Director de UBT Compliance—.

Finalmente, en la cuarta parte el lector encontrará estudios relacionados con la responsabilidad penal de las personas jurídicas que abordan los principales retos a los que los operadores jurídicos se enfrentan a diario. De un lado, encontramos estudios que analizan la prevención de riesgos y la comisión de tipos penales concretos en el seno de la empresa. Así, la Dra. Aurelia Carillo López, fiscal en el Tribunal Superior de Justicia

de Murcia, analiza el acoso laboral desde la óptica de la compliance; el Dr. Alfredo Abadías Selma —coordinador académico del Máster en Derecho Penal Económico en UNIR— estudia la corrupción en el deporte; la Dra. Demelsa Benito —profesora contratada doctora en la Universidad de Deusto— examina la corrupción transnacional; el Dr. Miguel Bustos —profesor contratado doctor en UNIR— hace lo propio en relación con el mobbing y el acoso sexual en la empresa, desde una visión teórico—práctica, planteando controles específicos como los protocolos antiacoso; el Dr. Rubén Herrero Giménez —profesor asociado en la Universidad Complutense de Madrid y abogado— rubrica un capítulo sobre la corrupción en los negocios y la imputación objetiva; el Dr. Manuel María Jaén Vallejo —magistrado— se centra en la corrupción en los negocios; el Dr. David Pavón Herradón —profesor asociado en la Universidad Complutense de Madrid y abogado *of counsel* en Ayuela Jiménez Abogados— analiza las falsedades contables; el Sr. Rubén Pérez Cordón —magistrado suplente de la Audiencia Provincial de Zamora con un dilatada trayectoria como director de desinversión de activos en una importante entidad bancaria— examina precisamente la renegociación de la deuda bancaria y los supuestos a medio camino entre el ilícito civil y el penal; el Sr. Miguel Ángel Martínez—Salinero Sanmartín —Socio Director de la firma Crown Acquisitions Law Firm— estudia la estafa piramidal como riesgo; el Dr. Carlos Bardavío —profesor en UNIR y abogado— analiza los principales problemas de la imputación objetiva de las personas jurídicas.

Del otro, en la cuarta parte también encontramos estudios específicos que afrontan y exploran los principales retos conexos a la responsabilidad penal de las personas jurídicas: la eventual responsabilidad el compliance officer, el dolo de las personas jurídicas, el compliance para los entes sin personalidad jurídica, los problemas específicos de los grupos de empresa o aspectos procesales, como la defensa de la persona jurídica a la búsqueda del siempre deseado eximente. Para ello, contamos con las destacadas aportaciones del Dr. Iñigo Segrelles de Arenaza —profesor titular de la Universidad Complutense de Madrid y socio en Del Rosal, Adame & Segrelles— que precisamente dedica su capítulo a la defensa de la persona jurídica en el proceso penal; el análisis del Dr. Alfredo Liñán Lafuente —profesor de la Universidad Complutense de Madrid y abogado— sobre los supuestos de responsabilidad penal del oficial de cumplimiento normativo; el interesante capítulo del Sr. Enrique Aznar —profesor en IE Law School, cofundador de diferentes *startups* y socio director de Aznar Legal & Compliance— sobre la importancia de la cultura ética corporativa para la prevención de riesgos, en la que despliega los conocimientos y prácticas adquiridas como *Chief Ethics & Compliance Officer* de empresas como *Nokia Siemens Networks* o como *Head of Corporate Governance & Compliance* en *Millicom International Cellular*, entre otros; el trabajo del Dr. Víctor Martínez Patón —profesor en UNIR y socio director de la firma Patón & Asociados— sobre la aplicación de los programas de compliance a los entes sin personalidad jurídica; el del Dr. Javier Gilsanz Usunaga —profesor en IE Law School y Director del Departamento Procesal de la prestigiosa firma Price Waterhouse Coopers (PwC)— que analiza

cuestiones prácticas del diseño e implementación de modelos de prevención y detección de delitos en grupos de empresa.

El libro presenta así, en definitiva, un estudio teórico—práctico que explora las metodologías para implementar y monitorizar un mapa de riesgos funcional, con detalle de las particularidades de distintos sectores de actividad e incluye además estudios que analizan los riesgos en función de tipos penales específicos o cuestiones tan relevantes como la creación y mantenimiento de una auténtica cultura ética empresarial, el cumplimiento en grupos de empresas, la responsabilidad del oficial de cumplimiento o cuestiones procesales como la defensa de la persona jurídica en el seno del proceso penal.

La Editorial Wolters Kluwer ha querido contar para este fin con los mejores *Compliance Officers* y expertos en Derecho Penal Económico en nuestro país. Esa era nuestra ambición, aunque lógicamente la dimensión y extensión del trabajo es limitada y, además, la obra ve la luz en el complejo e inquietante escenario en el que nos deja la pandemia del coronavirus. No están todos los que son, sí todos los que han podido participar.

La relación de autores que recorre el índice de la obra, incluido el autor del prólogo, el magistrado Dr. Ricardo Rodríguez Fernández —Académico Correspondiente de la Academia de Jurisprudencia y Legislación, ex Letrado del Gabinete Técnico del Tribunal Supremo y Cooperador Internacional—, evidencia que el lector está ante un libro de referencia que resuelve las cuestiones teórico—prácticas acerca del mapa de riesgos penales y sus peculiaridades en sectores de actividad clave. El origen y dedicación profesional de los autores así lo acredita.

Esperemos que el esfuerzo realizado por los coordinadores, los autores y la editorial para trasladar al lector un conocimiento teórico—práctico del mapa de riesgos penales, con el detalle y las peculiaridades de la visión sectorial, alcance el fin que la justifica: ser útil a la inmediata y creciente necesidad de profesionales preparados para liderar las demandas del mercado y el nuevo paradigma de la llamada *compliance,* que pasa necesariamente por un compromiso responsable con los principios de autorresponsabilidad de la empresa, prevención de riesgos en el diseño y por defecto y de monitorización y mejora continua de sistemas y programas de cumplimiento.

Pere SIMÓN CASTELLANO
Alfredo ABADÍAS SELMA
Coordinadores

PARTE I

PREVENCIÓN DEL DELITO Y MAPA DE RIESGOS EN LA EMPRESA

CAPÍTULO 1

Responsabilidad penal de las personas jurídicas, mapa de riesgos y cumplimiento en la empresa

Pere SIMÓN CASTELLANO
Profesor Contratado Doctor
Universidad Internacional de la Rioja UNIR
Grupo de investigación Penalcrim
Abogado of counsel FONT ADVOCATS

1. UN NUEVO PARADIGMA PARA EL CUMPLIMIENTO NORMATIVO

Nuestro ordenamiento jurídico recoge, desde hace bien poco, la noción de la responsabilidad penal de las personas jurídicas y la figura del oficial de cumplimiento normativo o *compliance officer*. Como es habitual, ciertas posiciones y roles aparecen como una auténtica necesidad fruto de nuevas realidades sociales, que exigen al legislador actuar en determinados ámbitos hasta ahora inexplorados.

Las razones para ese cambio, radical, de concepción, cuyos efectos se proyectan en el propio ADN de la cultura de cumplimiento normativo, se encuentran en la necesidad de hacer frente a las posibilidades de cometer ilícitos a través de distintas fórmulas jurídicas, así como a los complejos entramados que permiten en muchas ocasiones ocultar y distraer la persecución de los injustos, especialmente aquellos de naturaleza socioeconómica.

En la propia exposición de motivos de la Ley Orgánica 5/2010, de 22 de junio, por la que se modificó el Código Penal, el legislador hacía hincapié, precisamente, en lo complejo de perseguir determinadas figuras delictivas, como la corrupción en las transacciones comerciales internacionales, la corrupción en el sector privado, el blanqueo de capitales, la inmigración ilegal, la pornografía y prostitución infantil, entre otros.

La única forma razonable y funcional de perseguir buena parte de esos delitos y dar una respuesta penal eficaz es mediante la institución de la responsabilidad penal de las

personas jurídicas; es decir, aceptando y dando entrada en nuestro ordenamiento a técnicas y métodos que ya incluían determinados instrumentos jurídicos internacionales[1].

El legislador abraza ahora posiciones pragmáticas, más propias del derecho común anglosajón, sin que ello implique abandonar posturas tuitivas, lo que permite *de facto* un modelo más operacional o funcional en pos del cumplimiento normativo. La regulación vigente se basa, por el contrario, en el principio de responsabilidad proactiva[2]. La doctrina no ha tenido aún tiempo de reflexionar suficientemente sobre lo que esto, en realidad, implica.

El cambio de paradigma pivota sobre la afirmación que las empresas y organizaciones deben comprender los escenarios de riesgo inherentes que crean para las personas cuando establecen procesos o actividades de negocio o cuando adoptan decisiones en el Consejo de Administración u órgano de gobierno corporativo, lo que les exige hacer un esfuerzo conceptual de planificación e implementación para mitigar las amenazas. Por el camino, las organizaciones deben poder demostrar que manejan y monitorizan esos riesgos de manera adecuada y efectiva.

Como veremos al detalle a lo largo de este capítulo, ser proactivo implica planificar, hacer, verificar y actuar —ciclo PDCA— de forma recurrente a lo largo del tiempo, una técnica que no debería ser desconocida por nadie puesto que ya hace tiempo que estas metodologías han sido incorporadas por los estándares internacionales ISO y las normas españolas UNE—ISO, tanto para los sistemas de *compliance*, en general, como para la prevención de riesgos penales, en particular. Las ISO 19600 y 31000 constituyen el punto de partida o la mejor referencia sobre cómo planificar, accionar y monitorizar el cumplimiento normativo, como veremos más adelante en la parte que dedicamos a las metodologías de trabajo para el análisis y gestión del mapa de riesgos.

La obligación de aplicar una serie de controles o medidas técnicas y organizativas apropiadas, acordes con la naturaleza, ámbito y fines de las líneas o procesos de negocio, a fin de garantizar y poder demostrar que el mismo es conforme a la normativa, es más que una obligación; en realidad, se trata de un auténtico principio que, además, exige trabajar al detalle para cada caso concreto no perdiendo nunca de vista los principios del derecho penal y su conexión con las reglas éticas más elementales.

---

1. Véanse, por todas, las Decisiones Marco de la Unión Europa número 2002/629/JAI, sobre lucha contra la trata de seres humanos (más concretamente, véase el artículo 5); número 2003/568/JAI, sobre la corrupción en el sector privado (véase el artículo 6.1); número 2004/68/JAI, sobre lucha contra la explotación sexual de los niños y la pornografía infantil (más concretamente, véase el artículo 7.1); y, finalmente, la número 2004/757/JAI, sobre establecimiento de disposiciones mínimas de los elementos constitutivos de delitos y las penas aplicables en el ámbito del tráfico ilícito de drogas (artículo 7.1). Los citados artículos contienen la fórmula «Los Estados miembros tomarán o adoptarán las medidas necesarias para garantizar o asegurar que…», es decir, una fórmula que en ningún caso exige categóricamente el establecimiento de sanciones penales, dejando abierta una eventual respuesta vía sanción administrativa.

2. Se trata de un concepto cuya dicción literal procede de la más reciente normativa en protección de datos personales, pero que nada impide trasladarlo al ámbito del cumplimiento normativo general. Véase sobre este particular mi trabajo SIMÓN CASTELLANO, P. «El ejercicio de las funciones del delegado de protección de datos en la supervisión y gestión de procesos críticos», en SIMÓN CASTELLANO, P. y BACARIA MARTRUS, J. (Coords.) (2020*). Las funciones del delegado de protección de datos en los distintos sectores de actividad*. Madrid, Wolters Kluwer, págs. 27-74.

Este es el escenario, además, en el que aparece la figura del oficial de cumplimiento o *compliance officer*, cuyo nombramiento y designación como figura «independiente» o autónoma actúa, precisamente, como un control o medida dirigida a garantizar y supervisar el cumplimiento, a la vez que es un primer paso que ya demuestra una voluntad de liderazgo y compromiso con el cumplimiento.

El principio de responsabilidad proactiva, así entendida, encaja a la perfección con el concepto o la noción de autorresponsabilidad de las personas jurídicas, y entronca con el núcleo de la responsabilidad de la persona jurídica, que no es otro que la ausencia de las medidas de control adecuadas para la evitación de la comisión de delitos en el seno de la empresa.

No es menos cierto que durante los años siguientes a la reforma de 2010 se discutió vivamente, tanto a nivel doctrinal como jurisprudencial, sobre si el nuevo régimen de responsabilidad establecía un sistema vicarial de responsabilidad o un sistema de autorresponsabilidad, lo que propició una nueva reforma legal, introducida por la Ley Orgánica 1/1015, de 30 de marzo.

Empero las dudas sobre la naturaleza de la responsabilidad penal de las personas jurídicas han quedado resueltas por la doctrina de la Sala Segunda del Tribunal Supremo, de la que es exponente la STS 221/2016, de 16 de marzo, entre otras, en la que se establece que la sanción penal de la persona jurídica tiene su fundamento en la responsabilidad de la propia empresa por un defecto estructural en los mecanismos de prevención frente a sus administradores y empleados en los delitos susceptibles de ser cometidos en el ámbito de actuación de la propia persona jurídica.

A partir de la Ley Orgánica 1/2015, la responsabilidad penal de la persona jurídica se justifica entonces en el principio de autorresponsabilidad y debe ser respetuosa con el principio de presunción de inocencia, lo que tiene innegables consecuencias en el régimen de prueba, así como en las garantías procesales que deben ser observadas para llegar a un pronunciamiento de condena[3].

Así las cosas, uno de los principales riesgos de esta nueva cultura de cumplimiento sería que las empresas y organizaciones confundan los programas y sistemas de cumplimiento con una «tasa a pagar», algo que ha sucedido con frecuencia en otros ámbitos, como la protección de datos personales y la prevención de riesgos laborales. Año tras año el consultor adapta mi organización a la normativa y, cuando resulta necesario, se realiza la correspondiente auditoría. No se ha instalado, hasta el momento, en nuestro país, una cultura de cumplimiento que entienda las verdaderas ventajas competitivas de un modelo respetuoso con la normativa. No es exportable, bajo ningún concepto, al campo de prevención de riesgos penales, ese tipo de fórmulas que lamentablemente sí han gozado de cierta virtualidad en el contexto de la protección de datos y la prevención de riesgos laborales.

Paralelamente a lo anterior, debe extenderse la idea de que nunca más se va a poder afirmar que la empresa «ya cumple» o que ya «ha cumplido». La nueva realidad debe expresarse necesariamente con la perífrasis verbal del verbo estar más gerundio, es decir,

3. Sobre este particular véase la STS 234/2019, de 8 mayo.

«estoy cumplimiento» y, además, puedo acreditarlo. El cumplimiento no cesa ni acaba, la responsabilidad proactiva implica entrar dentro del círculo virtuoso de planificar, hacer, verificar y actuar —ciclo PDCA—, entre muchas otras metodologías, que garantizan la mejora continua.

Finalmente, otro de los peligros que también nos demuestra los años de trayectoria y experiencia en la protección de datos y en la prevención de riesgos laborales es el elevado nivel de intrusismo en el sector, la falta de profesionalidad de determinados «expertos» y el ofrecimiento de «adaptaciones» o incluso acciones de «consultoría» a coste cero, a cambio de formaciones bonificadas. Este fraude que ha sido denunciado por asociaciones profesionales, como APEP, y rechazado frontalmente por la propia AEPD, es una realidad que lamentablemente nos ha acompañado las últimas dos décadas en el ámbito de la protección de datos.

Debemos alertar de este riesgo y rechazar de lleno tal posibilidad para el ámbito del cumplimiento penal, recordando que los no juristas de entrada no tienen cabida en este modelo salvo excepciones muy singulares en las que se pueda acreditar un *track* y conocimiento exhaustivo del sector, así como un bagaje o experiencia acreditable en entornos legales. Además, la implicación del sector público será fundamental para aprobar esquemas de certificación y dar seguridad jurídica tanto para el desarrollo de tareas propias del oficial de cumplimiento o *compliance officer*[4], como para los auditores[5] de sistemas y programas de cumplimiento o incluso para establecer la lista de peritos judiciales de sistemas de cumplimiento normativo.

1.1. Concepto, origen y evolución del cumplimiento

La idea del cumplimiento normativo proactivo es originaria del mundo jurídico anglosajón. Más concretamente, el término *compliance* significa en esencia «cumplimiento». Un concepto exageradamente amplio, que en base a la casuística y al pragmatismo del espacio jurídico que le ha visto nacer se ha ido perfilando como cumplimiento normativo, y aún más precisamente como cumplimiento de las normas jurídicas y éticas por parte de las empresas.

El término cumplimiento normativo o *compliance* es un concepto jurídico indeterminado, de los más vagos e inexpresivos que se incorporan en nuestro Código Penal. Por sí sólo no dice apenas nada, salvo lo evidente, esto es, cumplir y actuar conforme a las leyes —civil, penal, administrativa, laboral, del mercando de valores, etc.— en un sentido amplio, es decir, incluyendo también las directrices internas de la empresa y en especial su código ético.

Con todo, el cumplimiento normativo en el seno de la empresa se ha definido como la implementación de medidas mediante las cuales las empresas pretenden asegurarse de

---

4. Véase el Esquema de certificación para Compliance Officer aprobado por la World Compliance Association, disponible en: https://cutt.ly/pyNExro (fecha de última consulta: 7 de junio de 2020).

5. Véase el Esquema de certificación para Auditores de Sistemas o Programas de Cumplimiento normativo aprobado por la World Compliance Association, disponible en: https://cutt.ly/jyNE1Uz (fecha de última consulta: 7 de junio de 2020).

que sean cumplidas las reglas vigentes para ellas y su personal, que las infracciones se descubran y que eventualmente se sancionen.

Seguimos aquí la definición propuesta por LOTHAR KUHLEN[6], una definición suficientemente amplia que permite agrupar todos los sistemas y subsistemas de cumplimiento: desde los riesgos financieros hasta los reputacionales, pasando por los sistemas de seguridad de la información, la gestión de calidad, los riesgos medioambientales y por supuesto, los riesgos penales.

El cumplimiento normativo entonces requiere de herramientas que permitan a la empresa descubrir infracciones, sancionarlas y, muy especialmente, detectar y prevenir escenarios de riesgos penales. Los sistemas o programas de cumplimiento son precisamente esas herramientas que promueven la cultura de cumplimiento y que fijan una serie de reglas estables para la gestión empresarial del riesgo.

Por su parte, el análisis de riesgos es una parte fundamental de cualquier sistema o programa de cumplimiento normativo que pretenda ser eficaz, puesto que es la herramienta clave para detectar, corregir y prevenir conductas delictivas. Evidentemente, la metodología utilizada y la recurrencia, así como el establecimiento de controles periódicos y la revisión y mejora continua del sistema depende, fundamentalmente, del tamaño de la empresa y de su estructura, así como de la naturaleza y fines de las operaciones de negocio. Así, por ejemplo, nunca serán los mismos riesgos inherentes, independientemente de su tamaño y estructura, si comparamos un fondo de inversiones con una pastelería, o una empresa de seguridad privada con un pequeño comercio local.

La naturaleza de determinadas organizaciones —sociedades cotizadas, grupos de empresa con actividades diversificadas, empresas transnacionales, etc.— les exige un grado de proactividad superior, por las propias exigencias de la legislación sectorial, y el programa de cumplimiento deberá adaptarse precisamente a la situación de interlegalidad en la que actúan, por ello resulta de especial interés el estudio por sectores de actividad que encontraran en la Parte II de la presente obra colectiva.

Los orígenes de la función de Compliance se sitúan en Estados Unidos, a comienzos del siglo XX y como respuesta a la necesidad de luchar contra la corrupción, la mafia y el blanqueo de capitales obtenido de actividades delictivas. Surgen así normas orientadas a atajar fenómenos delictivos concretos en el ámbito de los negocios y que poco a poco van constituyendo un entorno legal de funcionamiento que obliga a las empresas a preocuparse del cumplimiento de dichas normas en el seno de sus actividades.

Más concretamente, en los Estados Unidos de América se desarrollan tres estrategias jurídico penales diferentes: las sanciones antitrust, el *insider trading*[7] y la determinación de la responsabilidad penal de las personas jurídicas, cuya finalidad es motivar a sus gestores para que adopten medidas de organización interna que garanticen el respeto a la legalidad.

---

6. KUHLEN, L. «Cuestiones fundamentales de compliance y Derecho Penal», en KUHLEN, L.; MONTIEL, J. Pág. y ORTIZ DE URBINA GIMENO, I. (Eds.) (2013). *Compliance y teoría del derecho penal*. Madrid, Marcial Pons, pág. 51.

7. Véase la *Insider Trading and Securities Enforcement Act* de 1988.

Con los escándalos financieros de cambio de siglo —WorldCom, Enron, HSBC, Odebrecht, Olympus, etc.—, el cumplimiento normativo adquiere una orientación más punitiva, a través de la *Sarbanes Oxley Act* de 2002, en lo que concierne a las empresas cotizadas. La citada Ley norteamericana supuso un cambio definitivo en la orientación general del cumplimento, ahora más centrado en obligaciones formales como disponer de un código ético, mantener canales de denuncia confidenciales u otras medidas organizativas internas de carácter preceptivo —la también llamada *mandatory compliance*—.

El cumplimiento normativo forma parte así del fenómeno de americanización que están experimentando los ordenamientos jurídicos europeos, una traducción en nuestro modelo de sistemas de cumplimiento más pragmáticos o utilitaristas, que otorgan la confianza en las empresas y organizaciones y las hacen responsables, desde la madurez que se les presupone para actuar en el mercado. Si no evitan el delito en su seno deberán acreditar que hicieron lo posible, que actuaron de forma diligente mediante programas y sistemas operacionales y funcionales, y solo así serán capaces de eximir su responsabilidad penal.

Con todo, y recapitulando, es difícil encontrar hoy en día un país económicamente relevante, desarrollado, en el que se pueda afirmar tajantemente que no hay prevista una responsabilidad especial de la persona jurídica en caso de producirse ciertos hechos, sobre todo teniendo en cuenta que una mayor y mejor industrialización lleva necesariamente a una colectivización de la vida económica y social. El modelo de cumplimiento normativo o compliance anglosajón se ha acabo imponiendo y exportando prácticamente a todos los países de la OCDE[8].

1.2. El nacimiento de la responsabilidad penal de las personas jurídicas en España

La Ley Orgánica 5/2010, de 22 de junio introdujo en nuestro ordenamiento la responsabilidad penal de las personas jurídicas con la incorporación al Código Penal del artículo 31 bis CP. Este artículo sufrió una primera modificación en el año 2012, que afectó a su apartado quinto, para incluir a los partidos políticos y sindicatos entre las entidades que podían ser penalmente responsables, y una segunda, más profunda, por la Ley Orgánica 1/2015, de 30 de marzo. Esta reforma no solo modificó el artículo 31 bis, sino que introdujo en el Código Penal nuevos artículos destinados a completarlo. De esa forma se desarrolla con más detalle el modelo de responsabilidad penal de las personas jurídicas, entre otros aspectos, en aquel relacionado con los denominados modelos de organización y gestión —programas o sistemas de cumplimiento—, cuya implementa-

8. En 1999 la OCDE emitió los denominados *Principios de Gobierno Corporativo*. Concebidos inicialmente como recomendaciones generales sobre gobernanza, constituyen el entorno genérico mayoritariamente aceptado para la gestión del cumplimiento al abordar cuestiones tales como los procesos decisorios en materias medioambientales, cuestiones de índole ética y aspectos relativos a la lucha contra la corrupción. Si bien no reconocen la existencia de un único modelo de gobierno corporativo, establecen principios de gran valor para la adopción de prácticas de buen gobierno que han constituido históricamente la base de referencia para la legislación muchos Estados.

ción por las personas jurídicas, cuando cumplan ciertos requisitos, puede conducir a la exención de su responsabilidad penal.

Los programas de prevención constituyen, desde entonces, una exigencia ineludible para cualquier empresa u organización que pretenda estar bien gestionada, y por el camino mitigar o reducir riesgos penales o de cualquier otra índole —reputacionales, privacidad y seguridad de la información, operacionales, financieros, medioambientales, laborales, calidad, etc.—. La doctrina, desde 2010 hasta la fecha, ha estudiado con profundidad los efectos y transformaciones que implica este cambio de paradigma en la cultura de cumplimiento normativo[9].

La implantación y ejecución de programas y sistemas de cumplimiento ha planteado, empero, numerosos retos para las empresas, que han tenido que diseñarlos sin apenas ayuda y orientación del legislador. Tampoco existía lógicamente en España un cuerpo o grupo de profesionales del cumplimiento normativo o *compliance officers*.

De ahí la importancia de la creación *ex novo* de asociaciones y entidades, como la World Compliance Association, entre otras, que han agrupado y liderado el nacimiento de una profesión, la del profesional del cumplimiento, y han realizado un esfuerzo considerable al crear unos primeros esquemas de certificación, sin el apoyo por el momento del sector público, que pretenden aportar seguridad jurídica, garantizar la calidad de la prestación de servicios y establecer un estándar elevado de conocimientos y competencias que el profesional del cumplimiento debe dominar.

Con todo, los primeros oficiales de cumplimiento tuvimos que empezar nuestra andadura sin disponer en muchos casos no ya de una formación especializada, sino ni siquiera del material formativo necesario para el autoaprendizaje. Tampoco fue fácil delimitar una línea clara que diferenciase el nuevo rol, como oficial del cumplimiento,

---

9. ARTAZA VARELA, O. (2013). *La empresa como sujeto de imputación penal*. Barcelona, Marcial Pons; AYALA DE LA TORRE, J. M. (2018). *Compliance. Claves Prácticas*. Madrid, Editorial Francis Lefebvre; BAJO ALBARRACÍN, J.C. (2017). *Sistemas de gestión compliance. Guía práctica para el compliance officers*. Madrid, Editorial CEF; BAJO FERNÁNDEZ, M.; FEIJOO SÁNCHEZ, B. J. y GÓMEZ JARA, C. (2016). *Tratado de responsabilidad de las personas jurídicas*. Cizur Menor, Civitas; BONATTI, F. (2017). *Implementación y certificación de Sistemas de compliance penal conforme a la norma UNE 19601: 2017*. Madrid, Lefebvre El Derecho; BRODOWSKI, D.; ESPINOSA DE LOS MONTEROS, M.; TIEDEMANN, K. y VOGEL, J. (2014). *Regulating Corporate Criminal Liability*. Múnich, Springer; DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J. (Dirs.) (2013). *Responsabilidad penal de las personas jurídicas*. Cizur Menor, Aranzadi; DE VICENTE REMESAL, J. (2014). «Control de riesgos en la empresa y responsabilidad penal», *Revista Penal,* 34; ESTUPIÑÁN, R. (2016). *Administración de riesgos ERM y la auditoría interna*. Bogotá, ECOE Ediciones; GÓMEZ TOMILLO, M. (2010). *Introducción a la responsabilidad penal de las personas jurídicas en el sistema español*. Valladolid, Lex Nova; NIETO MARTÍN, A. (Coord.) (2013). *El derecho penal económico en la era compliance*. Valencia, Tirant lo Blanch; NIETO MARTÍN, A. (Dir.) (2015). *Manual de cumplimiento penal en la empresa*. Valencia, Tirant lo Blanch; PASCUAL, A. (2016). *El plan de prevención de riesgos penales y responsabilidad corporativa*. Barcelona, Editorial Bosch; RIBAS, X. (2018). *Practicum Compliance*. Pamplona, Aranzadi; SAIZ PEÑA, C. A. (coord.). (2015). *Compliance. Cómo gestionar los riesgos normativos en la empresa (Gran Tratado)*. Pamplona, Aranzadi; Thomson Reuters. (2017). *Compliance. Guía Práctica de identificación, análisis y evaluación de riesgos*. Pamplona, Aranzadi. Véase por todos SIMÓN CASTELLANO, P. «La responsabilidad penal de las personas jurídicas y el nacimiento de los sistemas de compliance», en ABADÍAS SELMA, A. y BUSTOS, M. (coords.) (2020). *Una década de reformas penales*. Colección Penalcrim. Barcelona, J. M. Bosch.

en relación con las funciones que a vueltas ejercen los miembros de otros departamentos o secciones, como las asesorías jurídicas, internas o externas, de empresa, o los responsables de la auditoría interna.

Sea como fuere, con la introducción de la responsabilidad penal de las personas jurídicas el legislador abraza posturas más utilitarias o pragmáticas, propias de sistemas del common law. De conformidad con la jurisprudencia de la Sala de lo Penal del Tribunal Supremo, la imputación de un delito a una persona jurídica exige indagar sobre aquellos elementos organizativo—estructurales de la entidad que han posibilitado un déficit de los mecanismos de control y gestión, con influencia decisiva en la relajación de los sistemas preventivos llamados a evitar la criminalidad en la empresa. Esto es, la constatación de que por parte de la organización no se han adoptado las medidas de control eficaces para la evitación de la *conducta delicti*va de que se trate. Como veremos en este capítulo tales objetivos se pueden acreditar con sistemas que garanticen la trazabilidad de los controles y acciones, el histórico de los indicadores de cumplimiento y un mapa de riesgos funcional, con roles y responsabilidades, orientado a la mejora continua.

1.3. Fenómenos conexos al cumplimiento normativo

1.3.1. Autorregulación y estandarización

La autorregulación puede definirse como la imposición voluntaria de estándares de conducta y normas internas por parte de empresas y organizaciones en pos del cumplimiento normativo. Podemos clasificar el fenómeno en función del nivel o grado de voluntariedad: de un lado, las íntegramente voluntarias; del otro, la autorregulación regulada dentro del marco legal que fija el Estado y la autorregulación estimulada o coaccionada, por la existencia de sanciones positivas o negativas que incentivan a las empresas a autorregularse.

La autorregulación empresarial, además de desplegar una función propia dentro del sistema de normas penales, ha generado un sistema de ejecución y aplicación autónomo que ha contribuido a la expansión de los programas de cumplimiento. Sirva como ejemplo la creciente práctica de auditorías anuales y las *due diligence*, muy empleadas cuando de lo que se trata es de medir el nivel de cumplimiento en procesos de *merge and acquisition,* de *joint venture* o previa ampliación de capital en el marco de una ronda de inversión.

Una autorregulación que crece especialmente por los requisitos que introducen para la firma de contratos internacionales o transnacionales muchas empresas cuya acción es global. En un mundo interconectado, las exigencias y condiciones despliegan efectos hacía dentro y hacía fuera de las empresas, con lo que cada vez es más habitual que proveedores y prestadores de servicios exijan ciertos estándares de calidad y cumplimiento normativo, y viceversa. Antes de contratar con un determinado prestador o proveedor, quiero que este me acredite, bajo su exclusiva responsabilidad, que su organización cumple con la normativa de prevención de riesgos laborales, de protección de

datos, de seguridad de la información, de prevención del blanqueo de capitales, de antifraude, del mercado de valores, etc.

1.3.2. El gobierno corporativo

La profunda crisis económica y financiera mundial acaecida en 2008 ha acelerado de forma decisiva las iniciativas y la toma de decisiones sobre la ampliación, concreción y consolidación de las llamadas «buenas prácticas», especialmente por lo que se refiere a las entidades cotizadas, que se han lanzado a construir estructuras de buen gobierno corporativo.

El informe COSO II define el gobierno corporativo como «la combinación de procesos y estructuras implantados por el Consejo de Administración para informar, dirigir, gestionar y vigilar las actividades de la organización con el fin de lograr sus objetivos»[10].

Son muchos los elementos, aspectos y principios que el cumplimiento normativo comparte con el gobierno corporativo. Este último nace para que en la gestión de las empresas cotizadas se atienda tanto a los derechos de los socios como a los de los grupos o personas que pueden verse afectadas por los procesos de negocio y actividades económicas de la sociedad. De esta forma, el gobierno corporativo exige liderazgo y compromiso vertical, lo que debe empezar por la propia dirección o gerencia, de igual modo que se exige en el ámbito de la compliance penal, en la que frecuentemente se recurre a la expresión *tone from the top* para recordar que el cumplimiento empieza y se alcanza desde la cúpula.

La gestión de riesgos, desde la apreciación hasta el tratamiento, las acciones preventivas y el establecimiento de controles, es otro punto de confluencia entre el gobierno corporativo y el cumplimiento normativo. Ninguno de los dos podría existir sin la gestión y mapa de riesgos, conceptos y métodos que estudiaremos a lo largo de los epígrafes 2 y 3 de este capítulo.

Por su parte, una parte esencial de los códigos de buen gobierno o de buenas prácticas son las relativas a las retribuciones de los consejeros o a la evitación de conflictos de intereses, lo que directamente ayuda a la prevención de delitos específicos y que, en la práctica, serán tratados como controles cuya eficacia se evaluará periódicamente. De este modo contar con un sistema de gobierno corporativo eficiente contribuye a minimizar riesgos penales y, por ende, contribuye al principal objetivo del cumplimiento normativo, que no es otro que evitar la comisión de injustos en el seno de la empresa[11].

---

10. Véase el informe del *Committee of Sponsoring Organizations* (COSO), 2004, pág. 22.

11. Véase sobre esta cuestión ARJONA, A.; YUBERO, M. P.; MANZANEQUE, M. y BANEGAS, R. (2017). *Gobierno corporativo, control de riesgos y auditoría interna. El cambio y valor de las empresas del siglo XXI*. Valencia, Tirant lo Blanch, págs. 32-38.

1.3.3. La Responsabilidad Social Corporativa

La Responsabilidad Social Corporativa (en adelante, RSC) se asemeja a la autorregulación en la medida que se concreta en un acuerdo asumido voluntariamente por una empresa con respecto a ciertas reglas que van más allá de sus obligaciones legales, comprometiéndose con una buena causa y mejorando al mismo tiempo su imagen pública.

La RSC conlleva una moderna visión de la empresa que la hace responsable con la sociedad, lo que la aleja de posturas tradicionales que la conciben como un mero actor económico, y la aproxima a un social y político, con obligaciones hacia la comunidad, que se extiende en la actualidad a nivel global. Como decía anteriormente, esto a su vez contribuye a mejorar o reforzar la imagen pública de la empresa u organización, su marketing y su credibilidad.

Dentro del paradigma de la RSC se incluyen hasta tres áreas, la de responsabilidad interna, la central y la externa. La primera comprende todas las estrategias y procesos internos que no llegan al público, pero que determinan esencialmente la orientación ética de la empresa. La central incluye todos aquellos campos que son públicamente eficaces y tienen un efecto directo sobre el medio ambiente, las personas y la sociedad y que siguen formando parte del proceso normal de trabajo. Finalmente, la responsabilidad externa cubre los campos de acción más caritativos, en términos económicos, dentro del que se incluyen los patrocinios, las contribuciones o donaciones corporativas y las actividades sociales, incluido el voluntariado corporativo. Las áreas interna y central se aproximan conceptualmente a ciertos mecanismos de autorregulación y, también, a disponer voluntariamente de programas y sistemas de cumplimiento.

1.3.4. La ética empresarial

La ética empresarial es otro fenómeno paralelo al cumplimiento normativo, con conexiones también evidentes con la RSC que acabamos de definir. La ética empresarial es una de las ramas en las que se divide la ética aplicada. Se encarga de estudiar cuestiones de naturaleza moral que tienen lugar dentro del mundo de los negocios, como por ejemplo las referentes a la gestión de la empresa, las conductas a seguir en el mercado, la forma de organización y división del trabajo, etc.

Decir que una empresa es un buen ciudadano, que debe respetar determinados principios o valores éticos, implica que debe prestar atención a los valores que comparten empleados, proveedores, socios o miembros del órgano de gobierno de la sociedad. Los códigos éticos o de conducta son muy habituales en los sistemas de cumplimiento normativo, y normalmente incluyen también planes formativos que obligan a prestar especial atención a los principios y valores que se describen en el código ético o de buenas prácticas.

Las empresas que cuentan con códigos éticos eficaces y con planes de formación relacionados con el primero se aseguran de que todos sus componentes entienden que la consecución de unos objetivos no puede situarse por encima del respeto a la ética, lo que lleva a generar una sensación de unidad y de identificación personal con los valores de la empresa. Los efectos se proyectan también en los empleados de forma significativa,

les aleja de caer en el desánimo o de tener conflictos internos, puesto que no se les obliga a olvidar sus convicciones morales para poder conseguir los objetivos marcados.

1.3.5. Auditoría interna, controlling financiero y asesoría jurídica

Muchos consejeros delegados o gerentes de empresa se preguntan si resulta verdaderamente necesario dotarse de una unidad de cumplimiento normativo si ya se dispone de un departamento bien consolidado de asesoría jurídica. Sin embargo, las funciones de ambas son bien distintas y sus objetivos están muy alejados. Mientras que el asesor jurídico o legal tiene como misión la defensa de la propia organización, la función del oficial de cumplimiento es velar por el cumplimiento *stricto sensu*, y esto muchas veces implica proteger los intereses de terceras partes dentro o fuera de la empresa —clientes, accionistas, proveedores, sociedad en general— por encima de los intereses de la propia empresa.

Por su parte, un afluente importante de los programas de cumplimiento es la auditoría interna que en las últimas tres décadas ha ido ampliando progresivamente sus funciones. La auditoría interna cumple la función de verificar los registros contables con el fin de comprobar si las transacciones que en estos se detallan realmente habían tenido lugar. En el marco de esta actividad de controlling financiero la auditoría interna ha desarrollado técnicas que han contribuido significativamente a descubrir posibles ilícitos en el seno de las organizaciones.

La auditoría y los controles financieros se han convertido en un instrumento de gobierno corporativo imprescindible, destinados a generar información vital para que los administradores supervisen y gestionen correctamente la empresa, pero también para que otros actores —inversores, accionistas, consejeros, etc.— puedan confiar en la buena gestión de la entidad y en la fiabilidad de la información que esta lanza al mercado.

La auditoría interna forma parte de una de las tres líneas de defensa del cumplimiento normativo. No obstante, existen diferencias importantes entre la monitorización que realiza el oficial de cumplimiento y las revisiones de la auditoría interna. El oficial de cumplimiento habitualmente monitoriza sólo los controles de su ámbito, estableciendo roles y responsabilidades para cada uno de los controles, mientras que auditoría interna supervisa todos los controles, incluida la propia asignación o partida presupuestaria del oficial de cumplimiento. El oficial de cumplimiento, además, monitoriza de forma más continua, ágil e inmediata, con una recurrencia o frecuencia más elevada, mientras que las revisiones de auditoría suelen ser casi siempre *a posteriori* de que hayan saltado las alertas o banderas rojas.

2. La apreciación y el análisis de riesgos penales

El artículo 31 bis del Código Penal español incorpora, como requisito fundamental de los modelos de cumplimiento, que incorpore mecanismos o métodos para identificar las posibles actividades en las que podría materializarse la comisión de un delito. Lo anterior exige u obliga a la realización de una evaluación de riesgos penales, que puede tener su punto de partida en un cuestionario o análisis preliminar de riesgos, como

veremos *infra*, o en evaluaciones y análisis más pormenorizados por procesos de negocios o departamentos.

En una dirección muy parecida la Fiscalía General del Estado ha señalado, en su circular 1/2016, que los programas y sistemas de cumplimiento normativo deben ser aptos para identificar, gestionar, controlar y comunicar los riesgos reales y potenciales derivados de las actividades de la empresa.

No existe cumplimiento normativo sin inventarios y registros de activos, sedes, departamentos, etc., que sean operativos y funcionales, que estén interconectados —que se hablen y lean—, y todo coordinado bajo los principios de liderazgo vertical —*tone from the top*—, de comunicación y consulta, de mejora continua —revisión periódica— y empleando uno o varios métodos de evaluación y medición de riesgos penales.

Veamos, antes de estudiar los métodos en el epígrafe tercero, las fases comunes para el ciclo de evaluación y análisis de riesgos, cuyo punto de partida se encuentra en la identificación o apreciación de las amenazas, se desarrolla en el análisis y valoración del riesgo *obiter dicta*, y finaliza en el tratamiento y gestión del riesgo.

A efectos conceptuales y terminológicos, procede señalar que el riesgo se deriva de la exposición a amenazas, por tanto, desde la perspectiva del derecho penal, es fundamental entender qué es una amenaza y cómo se pueden identificar escenarios de riesgo para los bienes jurídicos que protegen los tipos penales. Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los bienes jurídicos que tutelan los tipos penales que aceptan la responsabilidad penal de las personas jurídicas.

El riesgo, en cambio, se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide normalmente según su probabilidad de materializarse y el impacto o gravedad que tiene en caso de hacerlo. Aunque como veremos más adelante, en realidad hay muchos métodos que incorporan más parámetros, como es el caso del método Mosler, que mide y tiene en consideración la función, la sustitución, la profundidad, el grado de externalización, el nivel de agresión y la vulnerabilidad. Con todo, las amenazas y los riesgos asociados están directamente relacionados, y en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar.

2.1. La fase de identificación

La finalidad de la identificación del riesgo consiste en proporcionar evidencias basadas en distintos métodos para el descubrimiento de las amenazas y los escenarios de riesgo dentro de la organización, y en función de esto tomar decisiones informadas que a la postre deberían contribuir a minimizar o mitigar el nivel del riesgo. En este ámbito precisa recordar que los riesgos nunca desaparecen mientras no desaparezca el proceso de negocio o el departamento en el que este despliega sus efectos. Los riesgos se pueden mitigar hasta un nivel aceptable, dentro del umbral que establezca la organización, pero siempre podrán concretarse por bajo que sea su impacto, probabilidad y nivel.

La apreciación del riesgo permite comprender el riesgo y su impacto potencial, proporciona información relevante para el órgano de administración de la empresa,

ayuda en la selección de las opciones de tratamiento y simplifica el establecimiento de prioridades, identifica los factores principales y los puntos débiles en los sistemas y organizaciones, contribuye a la prevención de incidentes y proporciona información decisiva a la hora de evaluar si se debería aceptar el riesgo cuando se compara con criterios predefinidos.

La apreciación del riesgo comprende los elementos centrales del proceso de gestión del riesgo que se definen en las normas o estándares internacionales ISO 19600 y 31000. Entre los elementos se encuentra la comunicación y consulta y el establecimiento del contexto de organización, claves para la identificación del riesgo. Es fundamental en relación con esto último tener en cuenta la naturaleza de las operaciones y procesos de negocio de la empresa en cuestión. La identificación del riesgo no es una actividad aislada, y debería estar totalmente integrada con los otros componentes del proceso de gestión del riesgo, esto es, la evaluación y el tratamiento, y los procesos de gestión y revisión continua.

Entre las herramientas más utilizadas para la identificación *stricto sensu* destacan la lluvia o tormenta de ideas, las entrevistas estructuradas, las listas de verificación, el análisis previo de riesgos, los estudios de peligros y de operatividad, el análisis de escenario, el análisis de los modos de fallo y de los efectos, el análisis del árbol de fallos, en análisis del árbol de sucesos, el diagrama de sucesiones, los análisis de costes y beneficios, el análisis de fiabilidad humana y el análisis de pajarita.

Probablemente se trata de las técnicas más utilizadas, todas ellas explicadas *in extenso* en la norma internacional ISO 31010:2010, muchas de ellas ejemplificadas con figuras o diagramas. Lógicamente aquí sólo hemos citado algunas de las técnicas que incorpora la citada norma internacional, cuyas listas y tablas deben estar también al alcance del oficial de cumplimiento como máximo responsable de liderar la cultura de cumplimiento normativo y gestionar —identificar, evaluar y monitorizar— los riesgos y amenazas para los bienes jurídicos que tutelan los tipos penales que admiten la responsabilidad penal de las personas jurídicas. Buena parte de las técnicas y herramientas descritas se encuentran en la Figura 1, con detalle de su grado de aplicación y eficacia (1 - Muy aplicable; 2 - No aplicable; 3 - Aplicable) en las distintas fases de la gestión del riesgo.

Herramientas y técnicas	Proceso de apreciación del riesgo				
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo
		Consecuencia	Probabilidad	Nivel de riesgo	
Tormenta de ideas	MA[1)]	NA[2)]	NA	NA	NA
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA
Delphi	MA	NA	NA	NA	NA
Listas de verificación	MA	NA	NA	NA	NA
Análisis preliminar de peligros	MA	NA	NA	NA	NA
Estudios de peligros y de operatividad (HAZOP)	MA	MA	A[3)]	A	A
Análisis de peligros y puntos de control críticos (HACCP)	MA	MA	NA	NA	MA
Apreciación de riesgos ambientales	MA	MA	MA	MA	MA
Estructura «y si….» (SWIFT)	MA	MA	MA	MA	MA
Análisis de escenario	MA	MA	A	A	A
Análisis del impacto económico	A	MA	A	A	A
Análisis de la cauMA primordial	NA	MA	MA	MA	MA
Análisis de los modos de fallo y de los efectos	MA	MA	MA	MA	MA
Análisis del árbol de fallos	A	NA	MA	A	A
Análisis del árbol de sucesos	A	MA	A	A	NA
Análisis de cauMA-consecuencia	A	MA	MA	A	A
Análisis de cauMA-y-efecto	MA	MA	NA	NA	NA
Análisis de capas de protección (LOPA)	A	MA	A	A	NA
Diagrama de decisiones	NA	MA	MA	A	A
Análisis de fiabilidad humana	MA	MA	MA	MA	A
Análisis de pajarita	NA	A	MA	MA	A
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA
Análisis del circuito de fuga	A	NA	NA	NA	NA
Análisis Markov	A	MA	NA	NA	NA
Simulación Monte-Carlo	NA	NA	NA	NA	MA
Estadísticas Bayesian y redes Bayes	NA	MA	NA	NA	MA
Curvas FN	A	MA	MA	A	MA
Índices de riesgo	A	MA	MA	A	MA
Matriz de consecuencia/probabilidad	MA	MA	MA	MA	A
Análisis de costes/beneficios	A	MA	A	A	A
Análisis de decisión multi-criterios (MCDA)	A	MA	A	MA	A

1) Muy aplicable.
2) No aplicable.
3) Aplicable.

Figura 1. Detalle del grado de aplicabilidad de las herramientas utilizadas para la apreciación del riesgo. Fuente UNE ISO 31010:2011.

2.2. Análisis o evaluación del riesgo

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice. El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre los bienes jurídicos protegidos o, por el contrario, un impacto sería significativo si el daño ocasionado sobre estos fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente.

La valoración del riesgo está inextricablemente vinculada a la matriz de riesgos que se construye en función del método que se emplea. Por lo que se refiere a los métodos para cuantificar, los ejemplos y modelos de matrices y de mapas de riesgo, me remito al capítulo 2 de esta obra colectiva, que rubrica el secretario general de la World Compliance Association, Albert Salvador, que se dedica a analizar con profundidad todos los elementos y conceptos que se están señalando a modo introductorio en este epígrafe.

Las matrices de riesgos más utilizadas son las de 3x3 y 5x5 y normalmente cuentan con los factores de probabilidad e impacto o gravedad, si bien se pueden utilizar distintas matrices y fórmulas que también apliquen otros elementos o criterios como la función, la sustitución, la profundidad, el grado de externalización, el nivel de agresión y la vulnerabilidad

2.3. La gestión y tratamiento del riesgo

La última fase del proceso de gestión de riesgos es el tratamiento para minimizar o mitigar sus efectos. El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable. El riesgo residual será el resultado de reducir el nivel de riesgo inherente en función de la eficacia de los controles activos que se calcula, entre otros, teniendo en cuenta el porcentaje de vulnerabilidad de estos. La vulnerabilidad se puede calcular de distintas formas, para lo que nos remitimos una vez más al capítulo 2 de esta obra colectiva.

Sea como fuere, para lo que aquí interesa y a modo introductorio, resulta fundamental comprender qué consecuencias prácticas tiene el principio de mejora continua, que exige la revisión constante o periódica de los sistemas y programas de cumplimiento.

La mejora continua se alcanza básicamente con la participación e impulso de forma periódica del órgano de cumplimiento normativo, unipersonal o colegiado, en dos ámbitos que han sido destacados anteriormente —la gestión de los registros e inventarios de la empresa y la comunicación, consulta, seguimiento y revisión de las evaluaciones de riesgo—.

Los registros e inventarios permiten relacionar y conectar el contexto de la organización con los riesgos y también con los controles que derivan de las evaluaciones de

riesgo, lo que permite tener una visión actualizada a las necesidades de la organización. Se trata de un instrumento funcional, operativo y accionable, que debe ser consultado y revisado por el oficial de cumplimiento de forma recurrente. De hecho, debe informarse al órgano de cumplimiento o al *compliance officer* de cualquier cambio o modificación en los citados inventarios.

La mejora también se alcanza con el encargo de auditorías internas o externas, y con la gestión y resolución de incidencias concretas o mediante la depuración de responsabilidades a través de canales específicos, como los de denuncia, que necesariamente deben contar con medidas para proteger al alertador o denunciante. El proceso de mejora continua exige así definir un plan de auditorías y de revisiones periódicas en base a las actividades y procesos de negocio de la organización, así como en función de los resultados de las evaluaciones de riesgos.

Lo anterior sólo será posible si el órgano de cumplimiento, unipersonal o colegiado, cuenta con medios materiales, personales y un presupuesto suficiente que le permita actuar proactivamente y prevenir el delito. El establecimiento de cuadros de mando, indicadores y paneles de control de obligaciones y gestión de evidencias de cumplimento se configuran en la práctica como herramientas muy útiles para el órgano de cumplimiento. También es cada vez más frecuente el empleo de softwares específicos de cumplimiento normativo y prevención de riesgos penales, que permiten dar trazabilidad a todas las comunicaciones internas y externas, posibilitan asignar roles y responsabilidades y vincularlos a riesgos específicos, departamentos o procesos de negocio, y simplifican la tarea de acreditar las medidas y controles adoptados en pos del cumplimiento.

3. Metodologías para el análisis y mapa de riesgos

Veamos a continuación las principales metodologías de trabajo para el análisis de riesgos penales, que el órgano de cumplimiento normativo, unipersonal o colegiado debe conocer y aplicar en la práctica[12]. Todas las metodologías son válidas, de hecho, para una misma actividad o escenario de riesgo podemos aplicar métodos diversos tanto para la apreciación como para la valoración, evaluación y tratamiento de la amenaza. De ese modo podemos seguir distintas metodologías de forma paralela para luego contrastar resultados.

No se trata, en cualquier caso, de un estudio exhaustivo de todas las metodologías al uso, aunque sí estudiaremos a continuación las más habituales y comunes, algunas más propias de sistemas de seguridad de la información que pueden entroncarse más allá de los delitos informáticos y de los delitos contra la intimidad, la propia imagen y la inviolabilidad del domicilio, con prácticamente todos los tipos penales que soportan la responsabilidad penal de las personas jurídicas.

---

12. Buena parte de las metodologías que aquí se analizarán han sido ya objeto de estudio por parte de este autor, más concretamente, del epígrafe 3.1 al epígrafe 3.12, en SIMÓN CASTELLANO, P. «El ejercicio de las funciones del delegado de protección de datos en la supervisión… *op. cit*, págs. 46-64. En ese trabajo se estudian las citadas metodologías, aunque desde la óptica de la participación del Delegado de Protección de Datos y de los riesgos de la seguridad de la información.

El órgano de cumplimiento es quién debe advertir en el seno de la empresa de la necesidad de hacer un análisis de riesgos siguiendo una u otra metodología, y valorar los resultados de esta, para asesorar certeramente a la dirección o gerencia de la organización. A veces puede ser el propio *Compliance Officer* quién la lleva a cabo o, en muchas ocasiones, este simplemente contrasta los resultados y los presenta, asesorando al Consejo de Administración o al órgano de gobierno de la sociedad en la toma de decisiones.

Consideramos que el rol del oficial de cumplimiento o *compliance officer* es tan relevante en este ámbito que no puede ser que desconozca o no esté habituado a trabajar con todas las distintas metodologías de identificación, evaluación y monitorización de riesgos. Al órgano de cumplimiento le corresponde asesorar sobre cualquier tipo de evaluación de riesgos, siendo proactivo en la petición y monitorización de distintos análisis, siguiendo metodologías diversas, sobre un mismo departamento o proceso de negocio.

3.1. Análisis preliminar de riesgos (APR)

Esta fase del análisis de riesgos también forma parte del análisis inicial. Se utiliza para identificar posibles riesgos cuando el proyecto de cumplimiento normativo apenas está comenzando. A veces incluso se utiliza un análisis preliminar de riesgo general de toda la organización, es decir, no un análisis específico para cada actividad o proceso de negocio, especialmente cuando hablamos de pequeñas y medianas empresas o PYMES. No se trata lógicamente de un método exhaustivo, pero lo que pretende es, rápidamente, situar el foco y detectar los principales problemas de cumplimiento.

Digamos que con un sencillo cuestionario de no más de 100 preguntas cuya respuesta, normalmente, es un sí o un no y que, además, es un cuestionario «inteligente», por llamarlo de alguna manera, puesto que en función de las respuestas se despliegan unas preguntas u otras, y gracias a ello ya somos capaces de detectar dónde y cuáles son los principales problemas que debemos resolver con urgencia.

El análisis preliminar se puede realizar antes de empezar a trabajar en el cumplimiento y luego ir reelaborándolo de forma recurrente para observar como la organización ha evolucionado en su nivel de cumplimiento. Como decía, esta fórmula es muy útil para PYMES y conlleva algunas ventajas, con indiferencia del tamaño de la organización.

Veamos más concretamente cuáles son esas ventajas. Pensemos que el primer paso en el análisis preliminar de riesgos es identificar todos los hitos, tareas u operaciones que forman parte de un proyecto o de un proceso, intentando reconocer los posibles problemas o escenarios de riesgo para cada fase. La ventaja de este análisis preliminar ya sea específica por actividad o general por organización, es que aparecen las alertas más graves y es muy fácil priorizar. Ya habrá tiempo de estudiar posteriormente, a nivel de detalle, y pulir el cumplimiento cuando nuestro nivel se acerque al excelente. Primero lo más grave, y precisamente este estudio por sectores o grandes bloques, permite arrojar unas primeras banderas rojas que nos ayudan a centrar nuestros esfuerzos.

El objetivo que se persigue con los datos del resultado de ese primer cuestionario o análisis preliminar es elaborar una tabla de registro, que contiene la descripción de los riesgos identificados, las posibles causas, las consecuencias y, finalmente, las categorías

de riesgos, combinando la frecuencia o probabilidad y la gravedad o impacto del riesgo para crear una clasificación de prioridades.

Cuanto más probable sea un riesgo y más graves sean sus consecuencias, mayor atención debe dársele. Existen también diferentes metodologías para trabajar en tres, cuatro o cinco niveles de probabilidad, impacto y nivel, pero eso ya depende también del nivel de detalle. Para llevar a cabo la priorización del riesgo, es conveniente contar con una matriz de riesgo, que se decante por una u otra metodología (véase sobre este particular el segundo epígrafe de este capítulo y el capítulo 2 de la presente obra colectiva).

3.2. Metodología FRAP

Cuando hablamos de la *Facilitated Risk Analysis Process* (en adelante, FRAP) nos referimos a un proceso eficiente y sistemático que pretende asegurar que todos los riesgos relacionados con la seguridad de la información para las operaciones comerciales se identifican y documentan correctamente.

El proceso implica analizar un sistema, aplicación o segmento de operación comercial, mediante la convocatoria de un equipo o grupo de personas que incluya a los gerentes comerciales, a los responsables de ventas y marketing que estén familiarizados con las necesidades de información comercial, así como al personal técnico que tenga un conocimiento detallado de las vulnerabilidades potenciales del sistema y los controles relacionados que ya se hayan aplicado o estén operativos.

Las sesiones, que siguen una agenda estándar, son facilitadas por un miembro de la oficina del proyecto, que puede ser el propio oficial de cumplimiento o la persona que este establezca como responsable, que es quien garantizará que los miembros del equipo se comuniquen de manera efectiva y se adhieran a la agenda.

La función principal del citado equipo es realizar una lluvia de ideas sobre las amenazas potenciales, las vulnerabilidades y los impactos negativos resultantes sobre la integridad, confidencialidad y disponibilidad de los datos, activos y recursos de la empresa. Así se produce la identificación de los riesgos, para posteriormente analizar el impacto que estos tienen sobre las operaciones y el negocio de la empresa, priorizando amenazas y riesgos e identificando los controles que los mitigan o los pueden reducir a futuro.

El trabajo o análisis siguiendo el método FRAP se divide en tres fases claramente diferenciadas:

- Reunión pre-FRAP (aprox. 1 hora)
  a) Establecer el alcance
  b) Diagrama visual (proceso de negocio comercial a analizar)
  c) Miemb-ros del equipo
  d) Mecánica de las reuniones
- Sesión FRAP (aproximadamente media jornada)
  a) Lluvia de ideas e identificación de riesgos
  b) Priorización de riesgos y amenazas
  c) Controles sugeridos y medidas para mitigar los riesgos

- Proceso post FRAP (hasta dos semanas)
  a) Llenar hoja de referencias cruzadas
  b) Identificación de controles existentes
  c) Selección de controles para riesgos abiertos y definición del umbral de riesgo

3.3. Metodología MAGERIT

La metodología MAGERIT es un método formal para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que deberían adoptarse para controlar esos riesgos. Las siglas MAGERIT responden más concretamente a la «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información» que ha sido elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información.

MAGERIT es una metodología de carácter público, perteneciente al Ministerio de la Presidencia de España; su utilización no requiere autorización previa del mismo. La herramienta PILAR está basada en el método MAGERIT, y todos los organismos de la administración pública pueden solicitar una licencia libre de cargos al Centro Criptológico Nacional; siendo muy recomendable tal extremo, al tratarse de una aplicación creada *ad hoc*.

La metodología MAGERIT ha sido diseñada como un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad (en adelante, ENS) proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información. El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, que afecta a todas las administraciones públicas y a todas las empresas y organizaciones que colaboran o contratan con estas.

Sin embargo, el método MAGERIT interesa y puede ser utilizado por todas aquellas organizaciones que trabajan con información digital y sistemas informáticos, sin necesidad de que sean entidades obligadas por el ENS. La utilidad de trabajar con este sistema metodológico es que nos permitirá saber cuánto valor está en juego y esto nos ayudará a tomar decisiones formadas, encaminadas a proteger esos activos tan valiosos. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

El sistema o método de trabajo también es cíclico, en una suerte de círculo virtuoso de mejora continua muy parecido al que veremos con la metodología PDCA que ya ha sido apuntada anteriormente, y que se observa en la Figura 1.

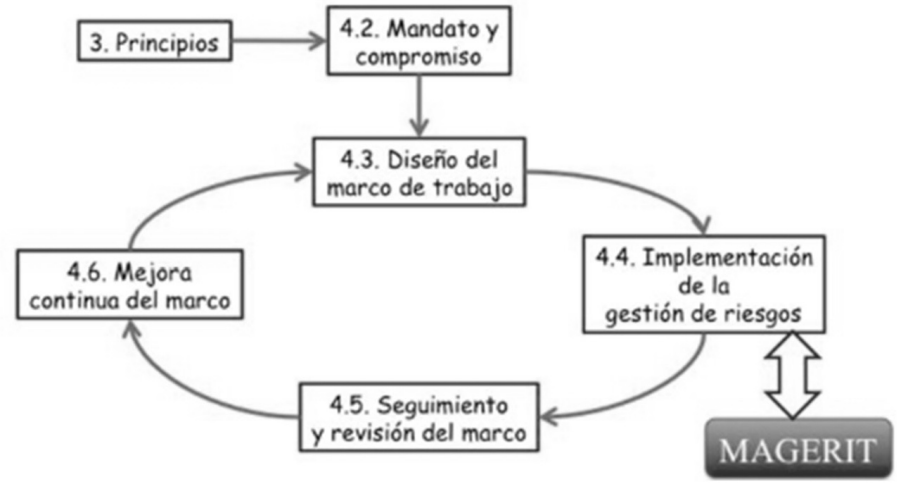

Figura 2. Método MAGERIT y sistema de mejora continua. Fuente: administracion.gob.es

Con ello se pretende concienciar a los responsables de las organizaciones de la existencia de riesgos y de la necesidad de gestionarlos, ofreciendo un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y de la comunicación, que ayuda a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. Además, indirectamente, se prepara a la organización para los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT facilita la labor de las personas que acometen el proyecto, en el sentido que les ofrece elementos estándar, fáciles o simples de comprender, a los que pueden adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis. Además, también contribuye a homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permiten comparar e incluso integrar análisis realizados por diferentes equipos.

Los resultados del análisis de riesgos permitirán al oficial de cumplimiento recomendar y asesorar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. En este sentido resulta muy útil la Figura 2 que se aporta con el fin de comprender mejor la conexión entre las fases de seguimiento y revisión, de tratamiento de los riesgos y de comunicación y consulta.

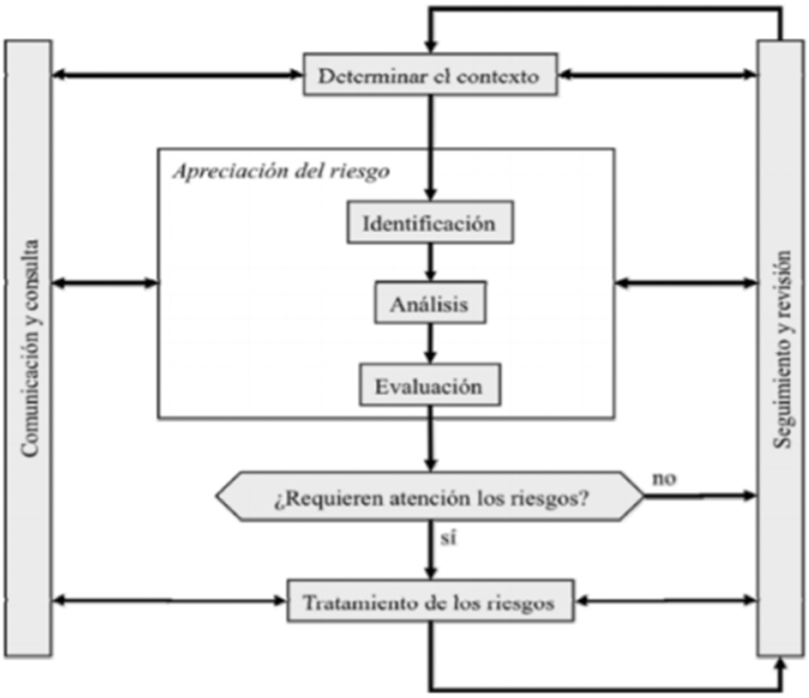

Figura 3. Gestión de riesgos método MAGERIT. Fuente: administracion.gob.es

La versión actual de MAGERIT es la tercera, actualizada en 2012. La metodología se plasma en 3 guías: la primera, dedicada al método; la segunda, donde se recoge el llamado «Catálogo de Elementos»; y la tercera, dedicada a la «Guía de Técnicas». Esta última se refiere tanto a las técnicas específicas para el análisis de riesgos —análisis mediante tablas, análisis algorítmico y árboles de ataque— como a técnicas generales —técnicas gráficas, sesiones de trabajo: entrevistas, reuniones y presentaciones, y sistema de valoración Delphi—.

Con independencia de que se siga o no esta metodología de análisis, evaluación y tratamiento de riesgos, lo cierto es que esas técnicas pueden ser luego extrapoladas a otras metodologías o análisis de riesgos específicos. El oficial de cumplimiento o incluso a través de su equipo, en el que puede integrarse un Delegado de Protección de Datos, debe tener un amplio conocimiento de estas para poder valorar los distintos estudios y asesorar a la dirección de la empresa.

En la Figura 3 se detallan todas las actividades y tareas dentro de cada proceso, diferenciando claramente entre la planificación del proyecto de análisis y gestión de riesgos, el análisis o valoración de riesgos propiamente dicho y el proceso de gestión, que requiere acciones de ejecución, implementación y monitorización. Además, las citadas guías MAGERIT acompañan al lector en la realización de las tareas del proyecto, recomendando el uso de ciertas técnicas específicas. Lógicamente, el nivel de detalle no es profundo y las guías se

limitan a proporcionar referencias para que los responsables de las organizaciones u organismos puedan introducirse al complejo universo de los sistemas de gestión de riesgos.

Figura 4. Procesos, actividades y tareas según el método MAGERIT. Fuente: administracion.gob.es

3.4. Metodología OCTAVE

Esta metodología permite que la organización comprenda cuáles son las necesidades de seguridad de la información mediante la planificación y consultoría estratégica en seguridad basada en el riesgo. No se focaliza en la tecnología, sino en el riesgo que esta entraña. La principal diferencia o aportación de este método es trabajar en la dimensión de los riesgos tecnológicos, lo que nos permite a la postre focalizar temas tácticos, como los riesgos organizacionales, así como cuestiones estratégicas.

Existen tres métodos OCTAVE, el método genérico, el OCTAVE—S y el OCTAVE Allegro. Todos ellos comparten elementos y criterios comunes, con un estándar de evaluación de la seguridad basada en la información de riesgo. Para realizar este tipo de análisis resulta necesario implicar a los responsables o coordinadores de los sectores operativos o de negocio de la organización, así como aquellos que se encargan de los departamentos de tecnología de la información. El trabajo colaborativo entre estos distintos departamentos o procesos de negocio es fundamental en el método OCTAVE, que aúna los riesgos operativos, las prácticas de

seguridad y la tecnología implicada para obtener conclusiones sobre las necesidades de seguridad de la organización.

El método OCTAVE especifica las fases diferenciando claramente entre la fase de análisis y la fase de gestión. Para la primera establece criterios específicos para la identificación de riesgos, para su análisis y para la evaluación. En relación con la segunda, con la gestión, en lugar de tres incorpora cuatro fases, con criterios para guiar el asesoramiento del riesgo, el tratamiento, su aceptación y la comunicación de este.

El método OCTAVE, es su versión principal o genérica, fue desarrollado teniendo en cuenta grandes organizaciones de trescientos o más empleados, pero el tamaño no fue la única consideración relevante, puesto que también se tuvo en cuenta el volumen y el contexto de la organización, así como el sector de negocio. El método se compone de una serie de talleres, facilitados o llevados a cabo por un equipo de análisis interdisciplinario de tres a cinco personas de la propia organización.

El sistema implica así a distintos empleados de la organización provenientes de diversos departamentos con el fin de aprovechar el conocimiento de múltiples niveles de la organización. Ese *know—how* multidisciplinar permitirá evaluar e identificar mejor los activos y las amenazas, las vulnerabilidades —tanto organizativas como tecnológicas—, y desarrollar una estrategia basada en la protección de prácticas y planes de mitigación de riesgos para apoyar la misión de la organización y sus prioridades.

Por su parte, el método OCTAVE—S fue desarrollado en respuesta a las necesidades de organizaciones más pequeñas, alrededor de cien personas o menos. Cumple con los mismos criterios que el método OCTAVE, pero está adaptado a los medios más escasos o limitados de los que disponen las pequeñas organizaciones. Básicamente es el mismo proceso, pero simplificado; se utilizan hojas de trabajo distintas y el *layout* o la presentación de resultados es prácticamente idéntica. El método OCTAVE—S también requiere formar un equipo de tres a cinco personas, que provienen de distintos departamentos e integran una visión completa o sistemática de la organización.

Por su parte, el método OCTAVE Allegro también es una variante simplificada del método de OCTAVE, aunque su principal diferencia o aportación en relación con el OCTAVE—S es que está focalizado en los activos de la información. Digamos que en el sistema OCTAVE Allegro se organizan los activos, se identifican y evalúan en función de los demás activos de información con los que se conectan.

Este subsistema, el OCTAVE Allegro, consta de ocho etapas distribuidas en cuatro fases. La primera, para la evaluación de los participantes, desarrollando criterios de medición del riesgo; la segunda, en la que cada uno de los participantes crea un perfil de los activos críticos del sistema de información; la tercera, en la que se identifican las amenazas a la información de cada activo en el contexto de sus contenedores; por último, la cuarta, cuando se identifican y analizan los riesgos para los activos de información y empiezan a desarrollar planes de mitigación.

3.5. Metodología GIRO

El Método GIRO es un sistema de gestión de riesgos que incorpora los siguientes elementos:

a) Se utiliza el concepto vulnerabilidad como elemento clave para la determinación del impacto de los eventos posibles. Se utilizan seis factores para determinar el nivel de vulnerabilidad: personas, valores, operaciones, contexto, imagen o reputación empresarial e información.
b) Se utilizan escalas de medición en función de la probabilidad del evento y de sus consecuencias.
c) Incorpora el umbral de riesgo, esto es, el concepto de «nivel aceptable de riesgo» para determinar la seguridad de referencia.
d) El escenario de riesgo actúa como una unidad objetiva de análisis, lo que permite puntualizar en forma diferencial la evaluación.
e) Existen estrategias predefinidas para intervenir el riesgo en cada escenario evaluado, esto es, en función del escenario de riesgo se precargan automáticamente los controles más habituales que mitigan el mismo.
f) Incorpora un contador de riesgos que permite conocer el estado y distribución de los riesgos en el sistema.
g) Mide la efectividad de los controles o medidas de intervención bajo el término «contabilidad de costos».
h) Incluye indicadores de gestión y calidad para determinar variables como el impacto de las medidas de intervención y controles, la eficacia y eficiencia de las medidas proyectadas, la rentabilidad de las medidas, los índices de vulnerabilidad del sistema, y la estabilidad del sistema ante los riesgos.

Esta metodología está basada en la teoría del análisis global de peligros, en los planteamientos de la *Society for Risk Analysis* y la *Global Association of Risk Professionals*, y por ello puede ser utilizada también para afrontar amenazas que no sean exclusivas de la seguridad de la información. Es un método útil para riesgos financieros, sociales, reputacionales, penales, etc., e incorpora conceptos de calidad total, planificación estratégica, árbol de eventos, etc.

3.6. Metodología CRAMM

La metodología CRAMM, que responde a las siglas de *CCTA Risk Analysis and Management Method,* es una metodología de análisis de riesgos creada por la CCTA o *Central Computer and Telecommunications Agency*, que comprende tres fases claramente diferenciadas: primero la determinación de los objetivos de seguridad; en segundo lugar, la evaluación de los riesgos del sistema y los requisitos de seguridad; finalmente, se identifican y seleccionan las medidas y controles a aplicar.

Si seguimos el sistema CRAMM calcularemos los riesgos para cada grupo de activos contra las amenazas a las que es vulnerable en una escala de 1 a 7, utilizando una matriz de riesgo con valores predefinidos comparando los valores de activos a

las amenazas y niveles de vulnerabilidad. En esta escala, el 1 indica una línea de base de bajo nivel de exigencia de seguridad y el 7 indica un requisito de seguridad muy alto.

Basándose en los resultados de ese análisis de riesgos, CRAMM produce una serie de propuestas de controles o contramedidas aplicables al sistema o red de información que se consideran necesarias para gestionar los riesgos identificados. El perfil de seguridad recomendado se compara con los controles existentes, e identificar así las áreas de debilidad o de mayor exposición.

El método CRAMM incluye un *software*, que contiene más de cuatro mil controles y. medidas predefinidas agrupadas por bloques que activos de *software*, hardware e incluso cuestiones medioambientales. Interesa señalar que una versión de prueba del *software* puede descargarse directamente de la web de la CCTA.

3.7. El estándar Norma ISO/IEC 19600:2015

Esta norma internacional proporciona orientación para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de compliance penal eficaz y que genera respuesta por parte de la organización. Las directrices sobre sistemas de gestión de compliance que incorpora son aplicables a todo tipo de organizaciones. El alcance de la aplicación de estas directrices depende del tamaño, estructura, naturaleza y complejidad de la organización. Este estándar se basa en los principios de buen gobierno, proporcionalidad, transparencia y sostenibilidad.

La figura 4 recoge perfectamente la metodología del sistema de gestión de riesgos propuesto por la norma. ISO/IEC 19600:2015.

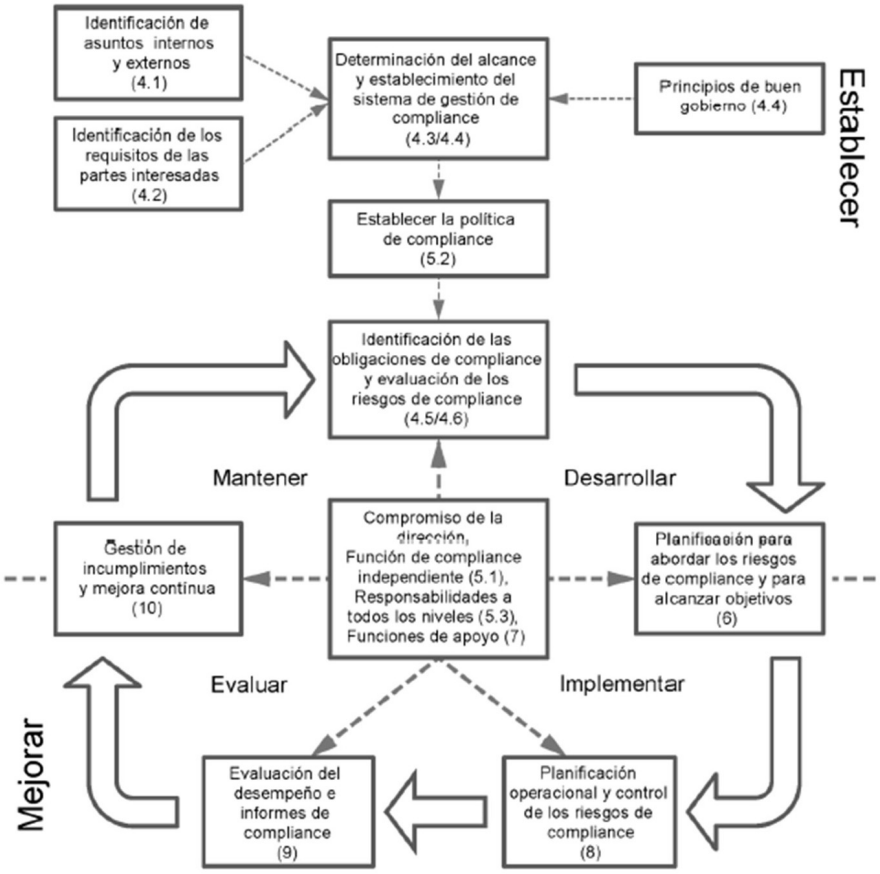

Figura 5. Organigrama de un sistema de gestión de compliance. Fuente: UNE—ISO 19600

3.8. El estándar Norma ISO/IEC 31000:2018 e ISO/IEC 31010:2009

Esta metodología establece una serie de principios para la implementación de un sistema de gestión de riesgos en las empresas dirigida a identificar, evaluar, tratar y monitorizar los riesgos asociados a una actividad, función o proceso. La citada norma internacional proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones, cuya aplicación puede adaptarse a cualquier organización y a su contexto. Ese mismo enfoque puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.

La figura 5 recoge perfectamente los componentes del sistema de gestión de riesgos propuesto por la norma.

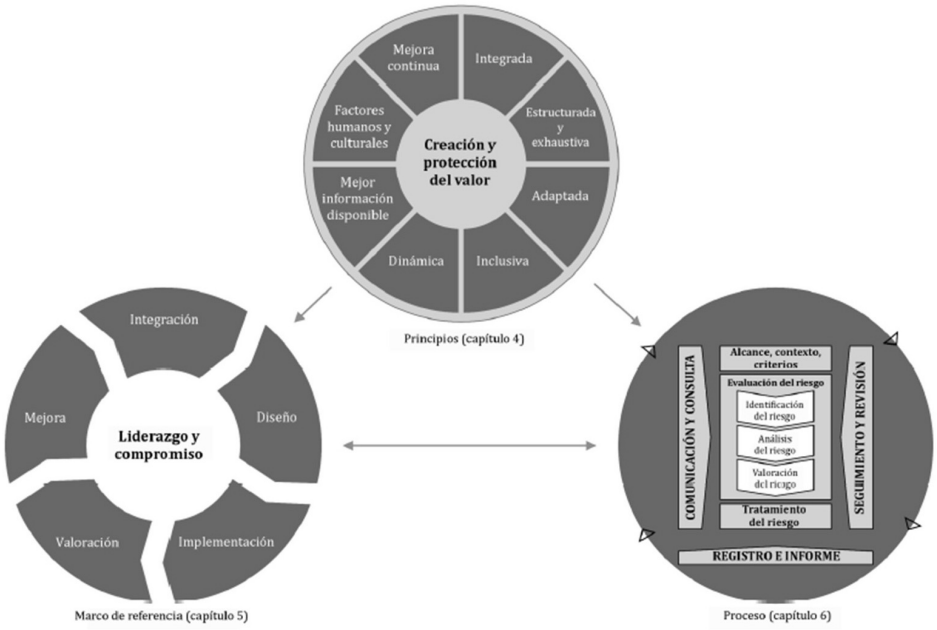

Figura 6. Principios, marco de referencia y proceso. Fuente: UNE—ISO 31000:2018

La norma ISO/IEC 31010:2009, por su parte, es una norma de apoyo de a la norma ISO 31000, por eso las estudiamos en el mismo epígrafe, y proporciona directrices para la selección y aplicación de técnicas sistemáticas para la apreciación del riesgo. La apreciación del riesgo realizada de acuerdo con esa norma contribuye a otras actividades de gestión del riesgo.

La citada norma internacional presenta la aplicación de una serie de técnicas, con referencias específicas a otras normas internacionales, donde el concepto y la aplicación de técnicas se describen con mayor detalle, si bien no proporciona criterios específicos para identificar la necesidad de aplicar el análisis del riesgo, ni especifica el método de análisis del riesgo que se requiere para una aplicación particular.

La apreciación del riesgo puede requerir un enfoque multidisciplinar puesto que los riesgos pueden cubrir un amplio abanico de causas y consecuencias. La figura 6 recoge la contribución de la citada norma internacional a la apreciación del riesgo al proceso de gestión de riesgo. Como se puede observar, su parecido es más que razonable con el método MAGERIT de la Figura 2.

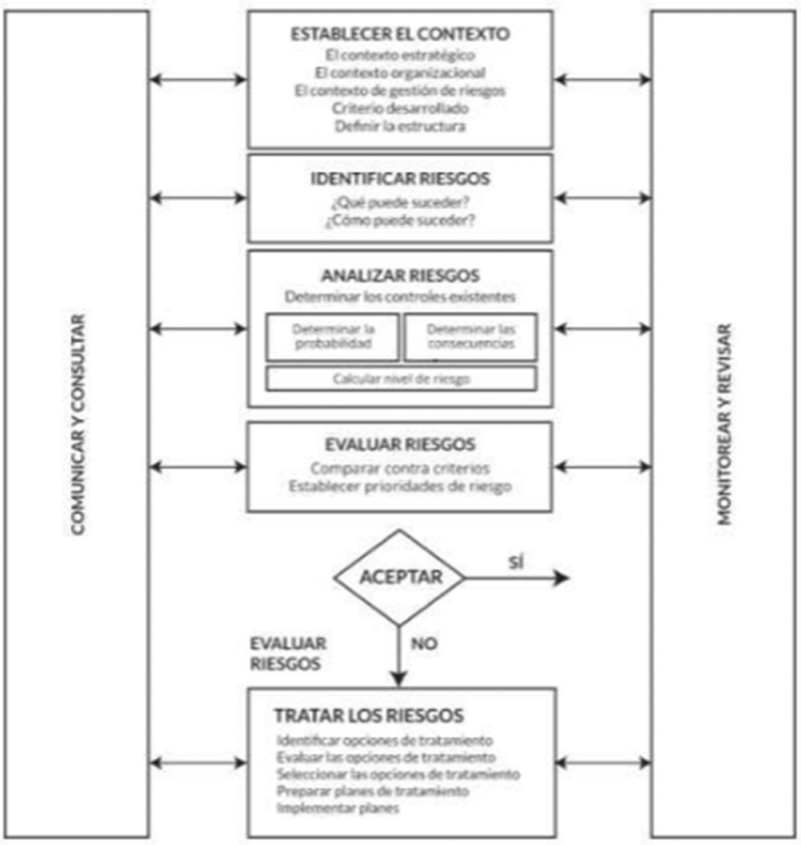

Figura 7. Componentes del Sistema de Gestión de Riesgos. Fuente: UNE—ISO 31000:2010

En la ISO 31010 se sigue el mismo esquema, aunque algo más simplificado. Por lo que aquí interesa, la norma ISO 31010 es especialmente útil en la descripción tanto de herramientas o técnicas para apreciar o identificar el riesgo, como en su clasificación por niveles basados en diversos factores —complejidad, grado de incertidumbre, recursos y capacidades, resultados cualitativos—. Ya hemos estudiado buena parte de esas herramientas en el epígrafe 2.1 del presente trabajo, al que nos remitimos.

3.9. La ISO/IEC 27005:2018 sobre tecnologías de la información, técnicas de seguridad y gestión de riesgos

La ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de la información. El enfoque descrito en esta norma internacional apoya los conceptos generales que se especifican en la Norma ISO/IEC 27001.

La citada norma internacional proporciona directrices sobre la aplicación de un enfoque de gestión de riesgos orientado a procesos para ayudar en la aplicación de manera satisfactoria y al cumplimiento de los requisitos de gestión de riesgos de seguridad de la Norma ISO/IEC 27001.

Veamos un gráfico con el detalle de las relaciones entre las normas ISO/IEC de la familia de los Sistemas de Gestión de la Seguridad de la Información (en adelante, SGSI).

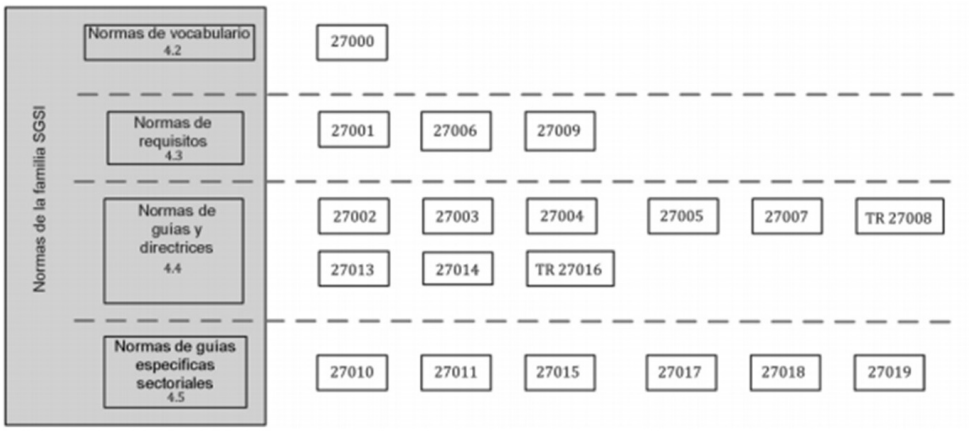

Figura 8. Normas de la familia SGSI. Fuente: UNE—EN ISO/IEC 27000:2019

La norma ISO/IEC 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en los SGSI. En ella se define el riesgo como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños y se relaciona el riesgo con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. El estándar internacional utiliza un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de tratamiento de riesgos. A través de este sistema de gestión se identifican los activos de información que se deben proteger, entre ellos protección de datos personales, y se valoran los riesgos desde una perspectiva de debilidades o vulnerabilidades y amenazas a las que están expuestos proponiéndose controles de para tratar el riesgo reduciéndolo, aceptándolo, transfiriéndolo o incluso eliminándolo.

La norma internacional es muy completa e incluye anexos específicos de matriz de riesgos, para definir el alcance y límites del sistema de seguridad, para identificar y valorar los activos en función de su impacto, para cuantificar la probabilidad y el impacto del riesgo, así como propone métodos para asesorar en relación con las vulnerabilidades, la amenazas tradicionales y definición de riesgo aceptable y criterios para su modificación.

En la figura 8, en inglés, se detalla el paso del riesgo inherente al riesgo residual, en el tratamiento de riesgos aceptables como consecuencia de un asesoramiento satisfactorio.

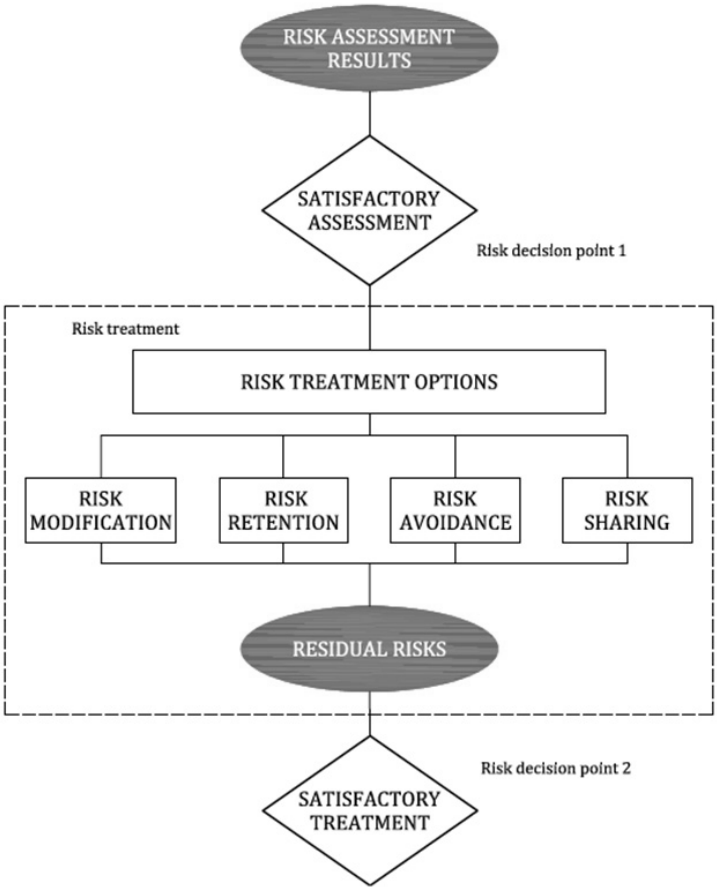

Figura 9. De la evaluación al tratamiento aceptable. Fuente: UNE—EN ISO/IEC 27005:2018

3.10. La norma NIST SP 800-39 sobre gestión de riesgos de la seguridad de la información

Esta metodología esta creada *ad hoc* de los sistemas de seguridad de la información y su enfoque gira entorno al riesgo, que se encuentra relacionado con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. La norma internacional citada recomienda utilizar un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de mitigación de estos.

Los factores e indicadores con los que se trabajan muestran si la empresa se encuentra sujeta o tiene una alta probabilidad de ser sometida a un riesgo que excede el riesgo permitido o riesgo aceptable. O, dicho con otras palabras, se trabaja con el indicador de los riesgos que están dentro y fuera del llamado «umbral» de riesgo. A través de este sistema de gestión se identifican los activos de información que se deben proteger, entre

ellos también los derechos de la protección de datos personales, y se valoran los riesgos desde una perspectiva de debilidades o vulnerabilidades y amenazas a las que se exponen, proponiéndose controles para tratar el riesgo reduciéndolo, aceptándolo, transfiriéndolo o incluso eliminándolo.

3.11. El método Mosler

El método Mosler es un método eficaz que permite identificar, analizar y evaluar los riesgos, muy utilizado especialmente en el ámbito de la compliance penal y específico para la prevención de riesgos penales. A nivel genérico, el método de Mosler se suele utilizar para evaluar los riesgos que se producen en determinadas actividades, así como aquellos que vienen dados por factores externos a las mismas, pero siempre en el ámbito de los riesgos físicos.

Su aplicación es trasladable al ámbito de riesgos físicos, lo que incluye también catástrofes o causas naturales, y tiene el punto de partida de su enfoque en la visión de la organización en su conjunto. El primer paso es determinar qué escenarios de riesgos o delitos, por ejemplo, el de revelación de secretos, podrían llegar a afectar en la práctica a la organización. El segundo es el análisis de riesgos y por último habrá que contemplar qué elementos debería tener la organización para prevenir cada escenario de riesgo.

De esta forma, el análisis del riesgo se determina en función de los siguientes parámetros:

- Función: afectación del delito al funcionamiento del día a día de la empresa.
- Sustitución: mide la facilidad de sustituir a las personas/cosas afectadas.
- Profundidad: mide el efecto psicológico sobre los trabajadores y sus consecuencias.
- Externalización: se calcula si los efectos negativos serían de carácter individual, local, regional, estatal o internacional.
- Agresión: valora la sanción que el Código Penal impone a cada delito.
- Vulnerabilidad: se valora la posibilidad real de que se llegue a materializar el riesgo.

Cada uno de estos parámetros se puntúa en una escala del uno al cinco y en el que la puntuación otorgada viene definida por una serie de criterios individualizados que el propio modelo define. A partir de ahí, se establecen tres campos para la valoración del riesgo:

- Importancia del riesgo = función x sustitución
- Daño ocasionado = profundidad x externalización
- Peligro = agresión x vulnerabilidad

El método de Mosler también define que el llamado carácter del riesgo es igual a importancia x daño, para finalmente sintetizar la descripción final del riesgo en torno a dos criterios definitivos: peligro y carácter. La multiplicación de estos dos valores es la que ofrece el dato que sirve para analizar el riesgo: de 2 a 250, riesgo muy bajo; de 251

a 500, riesgo bajo; de 501 a 700, riesgo medio; de 701 a 1000, riesgo alto; entre 1001 y 1250, riesgo muy alto.

3.12. El Esquema Nacional de Seguridad

El ENS no constituye ni incorpora una metodología en sentido escrito, sino que establece unos principios básicos y medidas de seguridad mínimas que son asignadas en base a tres niveles de seguridad. El nivel de seguridad bajo se aplicará cuando las consecuencias de un incidente de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados; el nivel de seguridad medio se aplicará cuando supongan un perjuicio grave y el nivel de seguridad alto se aplicará cuando las consecuencias supongan un perjuicio muy grave.

Una de las principales novedades de la LOPDGDD es que el ENS resulta de aplicación preceptiva tanto para el sector público como para aquellos terceros que presten un servicio en régimen de concesión, encomienda de gestión o contrato con este. La disposición adicional primera de la LOPDGDD establece que:

> «El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del (RGPD) Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad».

La implantación y aplicación del ENS puede realizarse siguiendo la metodología MAGERIT, que hemos analizado anteriormente, y que ha sido desarrollada *ad hoc* del ENS y de sus medidas de seguridad.

3.13. Metodología OCEG

El modelo *Open Compliance and Ethics Group* (en adelante, OCEG) constituye un estándar con reconocimiento internacional. Surge de un grupo de discusión diverso que integra economistas, filósofos, financieros, contables y también a la comunidad jurídica. OCEG se centra en el estudio e interrelación de tres elementos esenciales: gobernanza, gestión del riesgo y cumplimiento normativo, para definir la gestión integrada de todos ellos en un único modelo de *Governance, Risk and Compliance* —GRC, unas siglas muy utilizadas en los entornos de cumplimiento normativo—.

OCEG declara expresamente que su modelo permite a las organizaciones operar dentro de los condicionantes legales y contractuales, e incluye una serie de recomendaciones de elementos comunes de los que deberían disponer todos los entornos de cumplimiento: respaldo cultural; estructuras de cumplimiento; identificación de riesgos;

políticas y procesos; comunicación, corrección y consulta; monitoreo, monitorización y mejora continua.

3.14. COSO I

La metodología desarrollada por el *Committee of Sponsoring Organizations of the Treadway Commission* (en adelante, COSO) es comúnmente aceptada por los profesionales del cumplimiento normativo. El método pone el foco en el control interno en el ámbito de la información financiera. No obstante, si bien el modelo sólo es aplicable en aquellos ámbitos directamente relacionados con los reportes financieros, sus principios son aplicables de modo genérico en el ámbito del cumplimiento normativo, y de forma singular en la prevención de riesgos penales[13].

El entorno definido por COSO ha devenido con el tiempo en el estándar por excelencia en cuanto a control interno. La parte esencial compartida por el entorno de cumplimiento COSO define un marco integrado de control genérico que se basa en la existencia de información fiable y se estructura en torno a una matriz de tres dimensiones: (1) objetivos (estrategia, operaciones, información y cumplimiento); (2) componentes (elementos sobre los que hay que actuar, en relación a cada uno de los objetivos anteriores, y que determinarán el nivel de efectividad con el que una organización controla sus riesgos y oportunidades); y, finalmente (3) aplicación y evaluación (las dos dimensiones anteriores deben aplicarse tanto a nivel de entidad como de actividad).

Con el informe COSO I, de 1992, se modificaron los principales conceptos del control interno dándole a este una mayor amplitud. El control interno se define desde entonces como un proceso integrado a los procesos, valga la redundancia, y no como un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos.

El nivel de seguridad que se aspira obtener solo es el razonable, en tanto siempre existirá el limitante del costo en que se incurre por el control, que debe estar en concordancia con el beneficio que aporta; y, además, siempre se corre el riesgo de que las personas se asocien para cometer fraudes. Como hemos indicado *supra* un riesgo nunca desaparece mientras exista la línea o proceso de negocio y siempre tiene un costo.

Las categorías de los objetivos a los que está orientado el proceso de control interno también son parte del foco principal del informe COSO, que parte de una orientación meramente contable, y pretende garantizar la efectividad y eficiencia de las operaciones, la confianza en la información financiera, el cumplimiento de las leyes y normas que sean aplicables y la salvaguarda de los recursos.

Esas categorías genéricas de objetivos se tutelan mediante la implementación de cinco componentes:

---

13. En particular, sobre la metodología COSO y sus implicaciones, véase ESTUPIÑÁN GAITÁN, R. (2017). *Control interno y fraudes con base en los ciclos transaccionales. Análisis del informe COSO I, II y III*. Bogotá, ECOE ediciones.

- **Ambiente de control**. Marca el comportamiento en una organización. Tiene influencia directa en el nivel de concientización del personal respecto al control.
- **Evaluación de riesgos**. Mecanismos para identificar y evaluar riesgos para alcanzar los objetivos de trabajo, incluyendo los riesgos particulares asociados con el cambio.
- **Actividades de control**. Incluye acciones, normas y procedimientos que tienden a asegurar que se cumplan las directrices y políticas de la dirección para afrontar los riesgos identificados.
- **Información y comunicación**. Sistemas que permiten que el personal de la entidad capte e intercambie la información requerida para desarrollar, gestionar y controlar sus operaciones.
- **Supervisión**. Evalúa la calidad del control interno en el tiempo. Es importante para determinar si éste está operando en la forma esperada y si es necesario hacer modificaciones.

Figura 10. Los cinco componentes en la estructura COSO I.

El informe COSO plantea una estructura de control que se identifica con la Figura 10, que parte de la definición de los objetivos, cuya parte nuclear es la evaluación y el tratamiento o gestión de los riesgos, y que incluye finalmente la mejora continua, la supervisión y monitorización del cumplimiento.

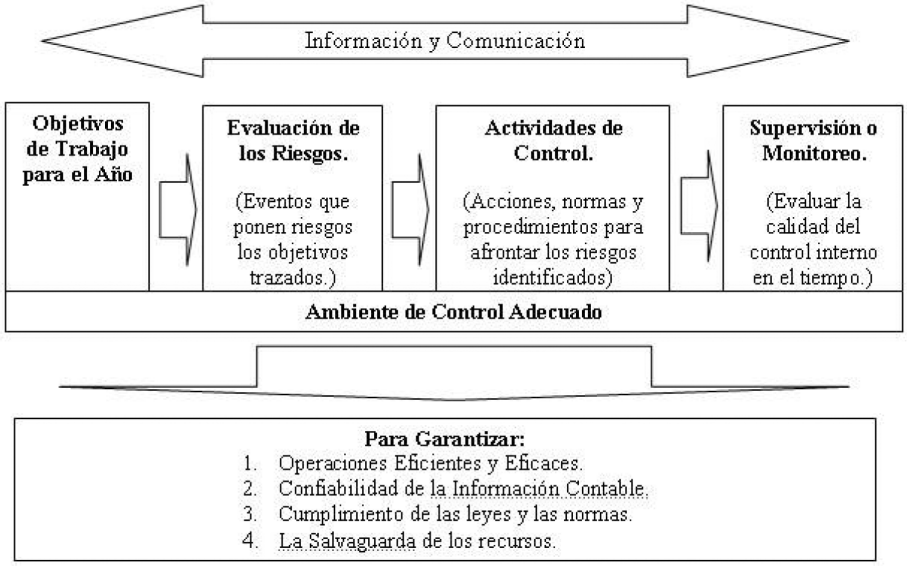

Figura 11. Esquema estructura de control COSO I.

3.15. COSO II

En septiembre de 2004, el Comité COSO emitió el Informe sobre el Marco de Gestión de Riesgos COSO II, que se ha impuesto como el marco metodológico considerado por muchos como la mejor práctica global en materia de gestión de riesgos. En el citado informe se define la gestión de riesgos como un proceso impulsado y creado por decisión del órgano de gobierno de las empresas o sociedades, que afecta a la definición estratégica y a todo el negocio, diseñado *ad hoc* de la identificación temprana de potenciales escenarios de riesgo que puedan afectar a la empresa, y gestionarlo según el nivel de riesgo aceptado o umbral de riesgo, con el objeto de proporcionar una seguridad razonable respecto al logro de los objetivos y así generar valor para los grupos de interés.

Figura 12. Las capas del cumplimiento normativo según la estructura COSO II.

En COSO II (2004), se indica que la gestión de riesgos empresariales debe incluir, además de lo señalado ya anteriormente en relación con el informe COSO I, un amplio abanico de capacidades muy concretas, que viajan desde la habilidad para alinear el riesgo aceptado por la dirección con la estrategia empresarial y desarrollar mecanismos para gestionar los riesgos asociados, pasando por el talento en la gestión de la diversidad de riesgos en el seno de la empresa, hasta la aptitud para identificar acontecimientos potenciales y mejorar las decisiones de respuesta a los riesgos y seleccionar a la postre las mejores alternativas al alcance de la organización que permitan evitar, reducir, compartir o aceptar riesgos.

Como se pueden observar en la Figura 12, el marco COSO II identifica cuatro categorías de objetivos: los estratégicos —alineados con la misión de la empresa—, los operacionales —vinculados al uso eficaz y eficiente de recursos—, los vinculados a la transparencia y reporting interno —fiabilidad de la información suministrada— y, finalmente, los vinculados al cumplimiento —cumplimiento de leyes y normas aplicables—.

Además, el marco COSO II identifica ocho componentes de la gestión de riesgos, añadiendo a los ya estudiados en COSO I, la fijación de objetivos, la identificación de eventos o acontecimientos y la respuesta al riesgo. Por lo que se refiere a la identificación de eventos nos remitimos a la Figura 13, extraída del informe COSO II en la que se detallan las categorías de eventos o acontecimientos.

Categorías de eventos	
Factores externos	**Factores internos**
Económicos • Disponibilidad del capital • Emisión de deuda, impago • Concentración • Liquidez • Mercados financieros • Desempleo • Competecia • Fusiones/Adquisiciones	**Infraestructura** • Disponibilidad de activos • Capacidad de los activos • Acceso al capital • Complejidad
Medioambientales • Emisiones y residuos • Energia • Catástrofes naturales • Desarrollo sostenible	**Personal** • Capacidad del personal • Actividad fraudulenta • Seguridad e higiene
Políticos • Cambios de gobierno • Legislación • Políticas públicas • Regulación	**Procesos** • Capacidad • Diseño • Ejecución • Proveedores/Subordinados
Sociales • Demografía • Comportamiento del consumidor • Responsabilidad social corporativa • Privacidad • Terrorismo	**Tecnología** • Integridad de datos • Disponibilidad de datos y sistemas • Selección de sistemas • Desarrollo • Despliegue • Mantenimiento
Tecnológicos • Interrupciones • Comercio electrónico • Datos externos • Tecnología emergente	

Figura 13: Categorías de eventos siguiendo el Informe Coso II (2004, pág. 61).

En COSO II se remarca que todas las personas que integran o forman parte de la empresa, desde la dirección o gerencia, pasando por empleados, hasta los proveedores y terceros prestadores de servicios, tienen alguna responsabilidad de manera directa o indirecta en la gestión de riesgos, siendo el responsable último el consejero delegado y el órgano de administración de la compañía.

Los directivos sólo son responsables de la gestión del riesgo en sus áreas de actuación, mientras que la dirección de riesgos y auditoría desarrollan funciones de apoyo claves para la gestión y supervisión de todo el sistema. La efectividad de este depende de los cuatro objetivos, cuando los ocho componentes (están presentes y funcionando correctamente.

3.16. COSO III

La tercera versión, COSO III, se publicó en el año 2013, con lo que es la última reforma del marco integrado de gestión de riesgos hasta la fecha, que incluye novedades respecto a lo comentado en los epígrafes anteriores, y que más concretamente se pueden agrupar en tres grandes bloques. En primer lugar, aumenta la confianza en cuanto a la eliminación de riesgos y consecución de objetivos. En segundo lugar, se aportan criterios para mejorar la agilidad de los sistemas de gestión de riesgos en su adaptación con los entornos de cumplimiento. Finalmente, se traslada con prístina claridad recursos que permiten trabajar tanto la comunicación como la información.

A modo de ejemplo, en este último y tercer bloque, se integran muchas novedades y mejoras, tales como la puntualización de la importancia de la calidad de la información dentro del sistema de control interno; el detalle en la necesidad de información y comunicación entre la entidad y terceras partes; se exalta el impacto de los requisitos legales sobre seguridad y protección de la información; se muestra el impacto de la tecnología y otros medios de comunicación en la rapidez y calidad del flujo de información interna o externa; se utiliza una terminología más clara en relación con la monitorización y supervisión de los sistemas, a través de la definición de dos categorías de actividades de seguimiento —las evaluaciones independientes y las evaluaciones continuas—; se profundiza en la relevancia del uso de proveedores de servicios externos y la tecnología.

4. La evaluación de la eficacia de los programas de cumplimiento

La existencia de modelos de organización y gestión del riesgo y de programas y sistemas de cumplimiento y prevención de riesgos penales que, siempre que se cumplan las exigencias concretamente enumeradas en el actual art. 31 bis 2 y 5, podrían dar lugar a la concurrencia de la eximente que en ese mismo precepto el legislador ha previsto expresamente.

Se eximiría así la responsabilidad penal de las personas jurídicas, un aspecto que la doctrina ha discutido por lo que se refiere a la naturaleza de tan singular eximente, que no debería vincularse tanto a la exclusión de la culpabilidad, sino más bien a un elemento objetivo que encuentra los cimientos de la exoneración en los hechos probados que nos remiten a la existencia de herramientas de control idóneas y eficaces. Lo que equivale a decir que la persona jurídica ha hecho lo posible para mitigar y minimizar el riesgo, e incluso así este finalmente se ha acabado materializando. La ausencia de las herramientas de control y sistemas de cumplimiento integran así el núcleo típico de la responsabilidad penal de la persona jurídica, complementario de la comisión del ilícito por parte de la persona física.

Según la Circular 1/2016 de la Fiscalía General del Estado, partiendo de un planteamiento diferente acerca de la tipicidad, la eximente habría de situarse más bien en las proximidades de una excusa absolutoria vinculada a la punibilidad.

Sea como fuere, y más allá del debate doctrinal, lo cierto es que sobre la «eficacia» de los programas y sistemas de cumplimiento, debemos tener en especial consideración la citada Circular 1/2016 de la Fiscalía General del Estado, la cual establece los «criterios» que los Fiscales del Estado deberán seguir para poder afirmar que una organización cuenta con un programa de cumplimiento eficaz que permita por tanto a la persona jurídica «eximirse» de la correspondiente responsabilidad penal en el caso de cometerse delitos en su seno.

4.1. Criterios

Sobre el contenido de la Circular 1/2016 debemos hacer referencia a ciertos criterios muy básicos como contar con un código ético, con políticas internas, con un órgano de cumplimiento, mejor interno a juicio de la Fiscalía General del Estado —unipersonal o colegiado— y con procedimientos previos para la identificación, evaluación y gestión de los riesgos penales.

El Instituto Español de Ética y Compliance se hizo eco de la citada Circular y publicó en febrero de 2016 la Alerta 1/2016 con el marco de referencia en la evaluación de los programas de compliance de las empresas españolas, la cual incluye como documento adjunto un *checklist* o cuestionario de verificación con una relación sumaria de los «criterios» que pueden tenerse en cuenta a la hora de valorar la eficacia del programa de cumplimiento normativo, cuyo conocimiento trasladamos al lector mediante la Figura 14.

CRITERIO		DEFINICIÓN/REQUISITOS
1	CLARIDAD	Los Programas de Cumplimiento han de ser claros y precisos.
2	ESCRITO	Los programas de Cumplimiento han de ser redactados por escrito.
3	ADECUACIÓN A LOS DELITOS	Los Programas de Cumplimiento han de ser eficaces. 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. Se realizará para valorar la eficacia un juicio de idoneidad entre el contenido del programa y la infracción.
4	ADAPTACIÓN A LA NATURALEZA Y TAMAÑO DE LA EMPRESA	Los Programas de Cumplimiento deben estar perfectamente adaptados a la empresa y a sus concretos riesgos. Copiar un programa elaborado por otra empresa, aunque sea del mismo sector, e implantarlo en la organización puede poner en tela de juicio la idoneidad del modelo y el verdadero compromiso de la empresa con la prevención de delitos.
5	PROMOCIÓN DE UNA CULTURA EMPRESARIAL	Los Programas de cumplimiento no pueden ser un salvoconducto para evitar la sanción penal, sino que tienen que promover una verdadera cultura empresarial «donde el delito constituya un acontecimiento accidental y la exención de la pena una consecuencia natural de dicha cultura».
6	IDENTIFICACIÓN Y GESTIÓN DE RIESGOS	Es necesario que la persona jurídica identifique y gestione adecuadamente los riesgos, estableciendo, aplicando y manteniendo las medidas y procedimientos eficaces para identificarlos, neutralizarlos, controlarlos y comunicarlos. Todo ello teniendo en cuenta tanto los riesgos reales como los potenciales, y de acuerdo con el nivel de riesgo global aprobado por la alta dirección.
7	PROCESOS INTERNOS Y APLICACIONES INFORMÁTICAS	Es necesario que se controlen los procesos internos de negocio de la empresa y, sobre todo si ésta tiene un cierto tamaño, es muy recomendable que esto se realice a través de aplicaciones informáticas exhaustivas.
8	CONTRATACIÓN Y PROMOCIÓN DE DIRECTIVOS Y MIEMBROS DEL ÓRGANO DE ADMINISTRACIÓN: ANTECEDENTES ÉTICOS	Los Programas de Cumplimiento deben establecer protocolos y procedimientos con altos estándares éticos en la contratación y promoción de directivos y en el nombramiento de los miembros de los órganos de administración, teniendo en cuenta la trayectoria profesional y los antecedentes.
9	REDUZCAN SIGNIFICATIVAMENTE LOS RIESGOS DE COMISIÓN DE DELITOS	Un Programa de Cumplimiento puede haber sido diseñado e implementado adecuadamente sin llegar a tener una eficacia absoluta. Sin embargo, no puede decirse automáticamente que un programa sea ineficaz por el hecho de haberse producido un delito en el seno de la empresa. Se considera eficaz un programa que reduzca significativamente el riesgo de comisión de delitos, lo cual va a obligar al juez a efectuar un difícil juicio hipotético y retrospectivo.
10	MECANISMOS DE DETECCIÓN DE CONDUCTAS DELICTIVAS: CANALES DE DENUNCIAS	Los Programas de Cumplimiento tienen que tener una eficacia preventiva, pero además deben posibilitar la detección de conductas delictivas. Deben observar la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia de los Programas de Cumplimiento. Los canales de denuncia son por tanto uno de los elementos claves para la eficacia de los programas.
11	VERIFICACIÓN PERIÓDICA	Los Programas de cumplimiento deben contemplar un plazo y un procedimiento de revisión de forma expresa. Además, deben verificarse y revisarse si concurren circunstancias que puedan influir en el análisis del riesgo.
12	SUPERVISIÓN POR EL COMPLIANCE OFFICER O COMITÉ DE COMPLIANCE	Los Programas de Cumplimiento deben ser supervisados por la persona o el órgano encargado de esta función (Compliance Officer o Comité de Compliance), así como participar éstos en la elaboración de los programas, y asegurar su buen funcionamiento estableciendo sistemas de auditoría, vigilancia y control para verificar, al menos, la observancia de los requisitos de eficacia que establece la ley en el artículo 31 Bis 5 (un ejercicio insuficiente de sus funciones impedirá apreciar la exención).
13	CUMPLIMIENTO DE TODA LA LEGALIDAD, NO SOLO LA PENAL	Los Programas de Cumplimiento deben observar la legalidad en penal, pero no sólo ésta, sino que también deben observar la legalidad en general.
14	IMPORTANCIA EN LA TOMA DECISIONES	Es muy importante para valorar la eficacia de un Programa de Cumplimiento, no el sólo el mero hecho de que el programa sea eficaz, sino valorar la importancia de éste en la toma de decisiones de los dirigentes y subordinados, y ver en qué medida éste es una verdadera expresión de su cultura de cumplimiento.
15	CERTIFICACIONES Y ACREDITACIONES	Las certificaciones sobre la idoneidad del modelo son un elemento a tener en cuenta, pero no acreditan la eficacia del programa, cuyo juicio corresponde al juez. Serán considerados como un elemento adicional más de la observancia, pero en modo alguno sustituyen la valoración del juez o acreditan la eficacia del programa
16	FALTA DE COMPROMISO DE LA ALTA DIRECCIÓN	Es necesario el compromiso de la alta dirección, por lo que si un alto responsable participó o consintió el delito el programa se presumirá ineficaz por los fiscales.
17	DELITOS COMETIDOS EN BENEFICIO ÚNICAMENTE INDIRECTO DE LA PJ	Si los delitos son cometidos en beneficio propio del autor del delito con beneficio sólo indirecto para la persona jurídica, esto habrá de tenerse en cuenta por los fiscales.
18	COLABORACIÓN DE LA PERSONA JURÍDICA	Los fiscales concederán especial valor al descubrimiento de los delitos por la propia entidad y su puesta en conocimiento a la autoridad.
19	ANTECEDENTES DE LA PERSONA JURÍDICA	Los fiscales tendrán en cuenta la conducta en el pasado de la entidad en cuanto a compromisos éticos se refiere.
20	ACTUACIONES POSTERIORES A LA COMISIÓN DEL DELITO	Se evaluarán por los fiscales las actuaciones llevadas a cabo con posterioridad a la comisión del delito.

Figura 14. Criterios para evaluar un programa de compliance. Fuente: Instituto Español de Ética y Compliance, febrero 2016.

Es una propuesta muy interesante que agrupa los principales criterios incluidos en la Circular de la Fiscalía General del Estado. Sin embargo, no se trata de un *numerus clausus* y no es menos cierto que, en sentido estricto, estamos hablando de una propuesta que debe

ser valorada como tal, puesto que existen también otros criterios que pueden ayudar a valorar la eficacia de los programas de cumplimiento, por ejemplo los indicadores de cumplimiento y su evolución y control mediante la toma de decisiones tal y como se puede eventualmente acreditar mediante las actas de las reuniones del oficial de cumplimiento en sus reuniones con la dirección, el consejo de administración o el comité ético o de buenas prácticas.

Los criterios señalados, a su vez, pueden agruparse en distintos bloques: (1) la implicación de los directivos, que permite acreditar el compromiso y liderazgo vertical en pos del cumplimiento; (2) la participación de los trabajadores, proveedores y grupos de interés, acreditando el compromiso de la organización en su conjunto, incluidas las sesiones formativas y de prevención específica; (3) la coherencia entre las políticas y el código ético, entre los controles y el contexto de la organización, entre los mecanismos de comunicación, consulta, revisión y mejora continua, etc.; (4) la dotación de recursos personales, materiales y presupuesto adecuado y suficiente para diseñar, aplicar y monitorizar el programa, las políticas, los protocolos y los controles necesarios; (5) el respeto a la autonomía e independencia, la capacidad y formación, de los oficiales de cumplimiento y del órgano de cumplimiento; (6) la vigencia, renovación y revisión constante del sistema.

4.2. Los indicadores de cumplimiento normativo (Modelos)

Los indicadores de cumplimiento, como la propia palabra indica, advierten y ofrecen información muy relevante de forma muy visual y asequible. Los gráficos y la información permiten rápidamente visualizar los resultados de los controles desde la implementación del programa o sistema del cumplimiento normativo, evidentemente, con el detalle del histórico por etapas.

En este apartado me gustaría compartir simplemente algunos modelos y ejemplos de indicadores que permiten trasladar a la gerencia o dirección, o al consejo de administración, una idea mucho más comprensible del cumplimiento normativo, si bien lógicamente estos indicadores siempre estarán acompañados de los informes preceptivos, análisis pormenorizados y todo el trabajo documental que incluye políticas, protocolos y códigos.

En la Figura 15 se detalla un modelo de trabajo basado en indicadores relativos a la cuenta total de riesgos inherentes, clasificados por nivel, versus la cuenta total de riesgos residuales, también clasificados por nivel. Todo ello con detalle de las sedes o empresas del grupo (países en el caso del ejemplo) y por departamentos. Nada impide, además, hacer otros entregables o gráficos cuya información represente lo mismo, pero en relación con los procesos de negocio en lugar de los departamentos. Otra opción es incluir, además de lo anterior, gráficos lineales que muestren la evolución temporal (por meses o por años), observando el detalle de la evolución de la cuenta total de riesgos inherentes y riesgos residuales, o de la cuenta específica por departamentos de empresa o por procesos de negocio. Además, si se quiere aumentar la complejidad, pero también el nivel de detalle se puede desglosar todos los indicadores anteriores, pero introduciendo únicamente el nivel de probabilidad del riesgo o el nivel de impacto o gravedad, lo que permitirá observar la evolución singular de esos dos parámetros por sedes, departamentos, procesos y también en el plano temporal.

RIESGOS INHERENTES

Cuenta de Riesgo Inherente	Etiquetas de columna					
Etiquetas de fila	Riesgo Crítico	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Riesgo muy Bajo	TOTAL
ESPAÑA						
DIRECCIÓN		1	1	4		6
FINANCIERO	1	2		2		5
RRHH	1	2			1	4
DEPUTY MANAGER	1	4	1	2		8
ADMINISTRACIÓN	1	1		1		3
COMINICACIÓN	1	4	1	2		8
INGLATERRA						
DIRECCIÓN		1				1
COMINICACIÓN		1				1
TOTAL	5	16	3	11	1	36

RIESGOS RESIDUALES

Cuenta de Riesgo Residual	Etiquetas de columna				
Etiquetas de fila	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Riesgo muy Bajo	TOTAL
ESPAÑA					
DIRECCIÓN		2	4		6
FINANCIERO	1	1	2	1	5
RRHH	1	1		2	4
DEPUTY MANAGER	3	2	2	1	8
ADMINISTRACIÓN	1		1	1	3
COMINICACIÓN	3	2	2	1	8
INGLATERRA					
DIRECCIÓN	1				1
COMINICACIÓN	1				1
TOTAL	11	8	11	6	36

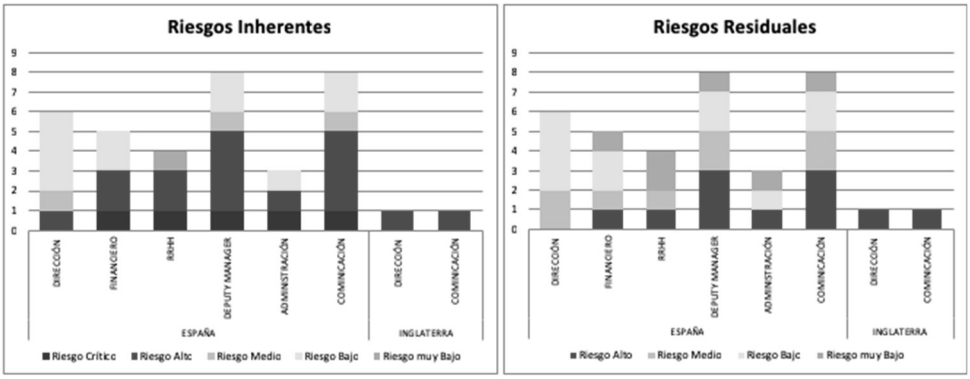

Figura 15, Indicadores utilizando la cuenta total de riesgos inherentes versus riesgos residuales. Fuente: Albert Salvador, secretario general de la World Compliance Association.

La Figura 16 corresponde a un indicador muy básico pero que también puede ser lineal y mostrar la evolución en el tiempo, que básicamente ofrece el porcentaje de empleados o trabajadores que han aceptado formalmente y firmado el código ético de la empresa, así como los manuales, políticas y protocolos internos.

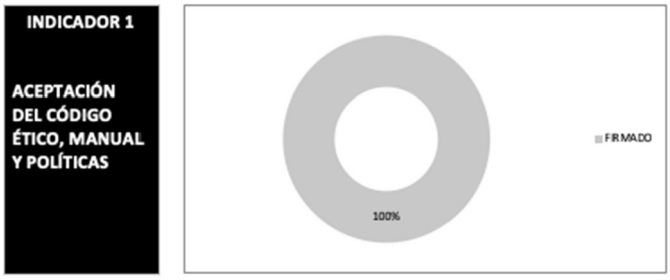

Figura 16. Indicador del % de empleados que han aceptado el código ético y firmado su compromiso con los manuales, políticas y protocolos de la empresa.

La Figura 17, por su parte, sitúa como indicador la confrontación o tensión entre el nivel final del riesgo residual, fruto de sumar y multiplicar los distintos parámetros que se empleen en función de la metodología concreta —normalmente probabilidad e impacto—, y el umbral de riesgo, esto es, el nivel de riesgo que la organización está dispuesta a aceptar. Este indicador, concretamente, en modo lineal y con inclusión de la evolución mensual resulta un indicador clave en la medida que permite observar todos aquellos riesgos que se sitúan más allá del límite aceptable que ha establecido el órgano de gobierno de la propia persona jurídica. Más concretamente, el detalle en versión histórico permite dar trazabilidad y acreditar la mejora, en su caso, de los sistemas, y ayuda a poner el foco en los procesos y escenarios de riesgo más acuciantes.

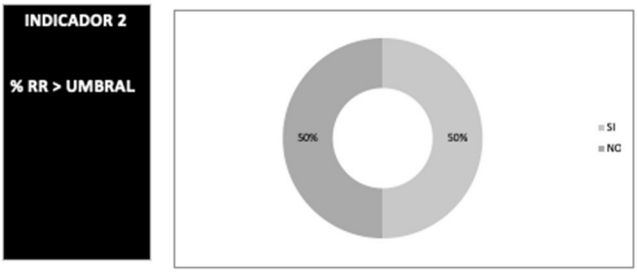

Figura 17. Indicador del % de riesgos residuales situados dentro del umbral.

La Figura 18, 19 y 20 hacen lo propio en relación con el grado y porcentaje de controles efectivos implementados, los programas de formación realizados y el estado del plan de mitigación, respectivamente.

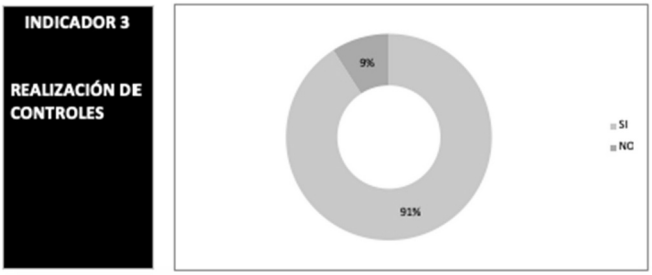

Figura 18. Indicador del % de controles efectivos.

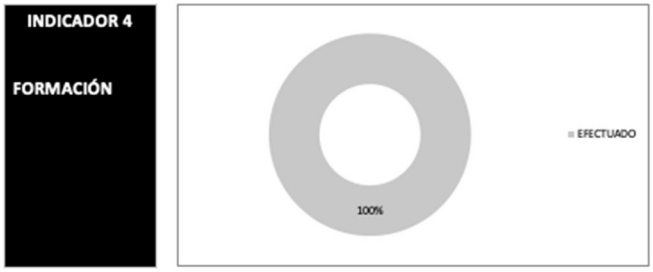

Figura 19. Indicador del % de empleados que han recibido formación.

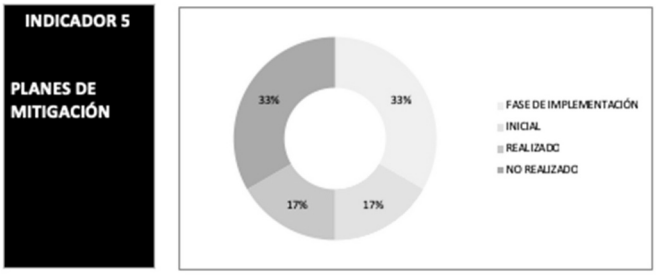

Figura 20. Indicador de la fase en la que se encuentran los controles previstos en los planes de mitigación y que ayudan a calcular el riesgo futuro.

5. Reflexiones finales

Este trabajo es el punto de partida de una obra colectiva cuyo principal objetivo es aunar teoría y práctica, y compartir con el lector las herramientas y métodos que permiten activar los sistemas y programas de cumplimiento, convirtiéndolos en elementos operativos y funcionales en el seno de la empresa. En este contexto, hemos estudiado como el mapa de riesgos penales se convierte en el principal recurso que permite visualizar el grado de exposición a las amenazas y su evolución, con trazabilidad y detalle de histórico de versiones.

En este capítulo hemos observado, en primer lugar, las profundas transformaciones que la nueva cultura de cumplimiento normativo ha proyectado sobre nuestro ordenamiento jurídico. Una realidad más propia de sistemas del derecho común anglosajón se ha acabado imponiendo también en nuestro modelo por razones de eficacia y de utilidad. Hemos introducido al lector así delimitando el concepto de cumplimiento normativo, estudiando su origen y evolución, para finalmente analizar su introducción en España con el nacimiento de la responsabilidad penal de las personas jurídicas y diferenciándolo, además, de figuras conexas como la autorresponsabilidad, la responsabilidad social corporativa, el gobierno corporativo, la ética empresarial, la auditoría interna y la asesoría jurídica.

En segundo lugar, hemos abordado el estudio de las fases del análisis y gestión de riesgos corporativos, empezando por la apreciación o identificación de riesgos, con detalle de las distintas técnicas a tal efecto, pasando por la evaluación en sentido estricto con los parámetros más habituales —probabilidad e impacto—, y acabando con la definición de los indicadores, controles y alertas que garantizan la mejora continua.

A continuación, nos hemos sumergido en el estudio de los métodos para el análisis y gestión del mapa de riesgos en la empresa. No existe un modelo único; son muchas las metodologías y criterios que pueden ser empleados, los parámetros y elementos que se pueden tener en cuenta. El oficial de cumplimiento debe conocerlos y dominarlos puesto que su papel como asesor y catalizador de procesos no puede llevarse eficazmente a cabo sin ese conocimiento específico que le permite trasladar a la dirección y al comité de buenas prácticas o al órgano de cumplimiento colegiado, en su caso, una opinión formada al respecto.

Finalmente, hemos compartido modelos de trabajo en base a indicadores que deberían ayudar a sustentar y defender, ante los tribunales, la existencia de programas y sistemas de cumplimiento normativo funcionales, eficaces y operativos, lo que en definitiva debería contribuir a eximir la responsabilidad penal de la persona jurídica en el caso concreto.

6. Bibliografía

ARJONA, A.; YUBERO, M. P.; MANZANEQUE, M. y BANEGAS, R. (2017). *Gobierno corporativo, control de riesgos y auditoría interna. El cambio y valor de las empresas del siglo XXI*. Valencia, Tirant lo Blanch.

ARTAZA VARELA, O. (2013). *La empresa como sujeto de imputación penal*. Barcelona, Marcial Pons.

AYALA DE LA TORRE, J. M. (2018). *Compliance. Claves Prácticas*. Madrid, Editorial Francis Lefebvre.

BAJO ALBARRACÍN, J.C. (2017). *Sistemas de gestión compliance. Guía práctica para el compliance officers*. Madrid, Editorial CEF.

BAJO FERNÁNDEZ, M.; FEIJOO SÁNCHEZ, B. J. y GÓMEZ JARA, C. (2016). *Tratado de responsabilidad de las personas jurídicas*. Cizur Menor, Civitas.

BONATTI, F. (2017). *Implementación y certificación de Sistemas de compliance penal conforme a la norma UNE 19601: 2017*. Madrid, Lefebvre El Derecho.

BRODOWSKI, D.; ESPINOSA DE LOS MONTEROS, M.; TIEDEMANN, K. y VOGEL, J. (2014). *Regulating Corporate Criminal Liability*. Múnich, Springer.

DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J. (Dirs.) (2013). *Responsabilidad penal de las personas jurídicas*. Cizur Menor, Aranzadi.

DE VICENTE REMESAL, J. (2014). «Control de riesgos en la empresa y responsabilidad penal», *Revista Penal,* 34.

ESTUPIÑÁN GAITÁN, R. (2016). *Administración de riesgos ERM y la auditoría interna*. Bogotá, ECOE Ediciones.

ESTUPIÑAN GAITÁN, R. (2017). *Control interno y fraudes con base en los ciclos transaccionales. Análisis del informe COSO I, II y III*. Bogotá, ECOE Ediciones.

GÓMEZ TOMILLO, M. (2010). *Introducción a la responsabilidad penal de las personas jurídicas en el sistema español*. Valladolid, *Lex* Nova.

KUHLEN, L.; MONTIEL, J. P. y ORTIZ DE URBINA GIMENO, I. (Eds.) (2013). *Compliance y teoría del derecho penal*. Madrid, Marcial Pons.

NIETO MARTÍN, A. (Coord.) (2013). *El derecho penal económico en la era compliance*. Valencia, Tirant lo Blanch.

NIETO MARTÍN, A. (Dir.) (2015). *Manual de cumplimiento penal en la empresa*. Valencia, Tirant lo Blanch.

PASCUAL, A. (2016). *El plan de prevención de riesgos penales y responsabilidad corporativa*. Barcelona, Editorial Bosch.

RIBAS, X. (2018). *Practicum Compliance*. Pamplona, Aranzadi; SAIZ PEÑA, C. A. (coord.). (2015). *Compliance. Cómo gestionar los riesgos normativos en la empresa (Gran Tratado)*. Pamplona, Aranzadi.

SIMÓN CASTELLANO, P. (2018). *El desempeño de las funciones de Delegado de Protección de Datos: gestión de procesos críticos y casos prácticos*. Madrid, Wolters Kluwer.

SIMÓN CASTELLANO, P. «El ejercicio de las funciones del delegado de protección de datos en la supervisión y gestión de procesos críticos», en SIMÓN CASTELLANO, P. y BACARIA MARTRUS, J. (Coords.) (2020*). Las funciones del delegado de protección de datos en los distintos sectores de actividad*. Madrid, Wolters Kluwer.

SIMÓN CASTELLANO, P. «La responsabilidad penal de las personas jurídicas y el nacimiento de los sistemas de compliance», en ABADÍAS SELMA, A. y BUSTOS, M. (coords.) (2020). *Una década de reformas penales*. Colección *Penalcrim*. Barcelona, J. M. Bosch.

THOMSON REUTERS. (2017). *Compliance. Guía Práctica de identificación, análisis y evaluación de riesgos*. Pamplona, Aranzadi.