WORLD® COMPLIANCE ASSOCIATION

GUÍA COMPLIANCE EN EL TERCER SECTOR

Guía patrocinada por:

GA_P Gómez-Acebo & Pombo

Intedya International Dynamic Advisors

BUREAU VAN DIJK A Moody's Analytics Company

tirant lo blanch GRUPO EDITORIAL

tirant Compliancers®

Edición

Septiembre 2020

Coordinadores

Laura Gonzalvo Diloy

Guillermo González de la Torre

Lucía Gámez Henares

Diseño y maquetación

Departamento de Imagen WCA

Agradecimientos

A Laura Gonzalvo Diloy, Guillermo González de la Torre y Lucía Gámez Henares, por hacer posible este proyecto de muchos/as y, a la vez, de uno/a. Gracias por el trabajo de organización, coordinación y revisión, y gracias por vuestro apoyo durante todo el camino.

Gracias también a todos los autores y las autoras que habéis compartido vuestro conocimiento de forma desinteresada y que nos habéis acompañado en todo el proceso, aportando vuestro granito de arena a esta gran obra.

Orgullosos/as de formar esta asociación. Proud to be WCA.

Con la colaboración de las siguientes entidades

COLABORADORES

Iván Martínez López

DIRECTIVO Y EXPERTO EN SISTEMAS DE GESTIÓN Y ORGANIZACIÓN EMPRESARIAL EN ÁMBITOS NACIONALES E INTERNACIONALES CON ESPECIALIZACIÓN EN EL DESARROLLO DE NEGOCIOS Y LA GESTIÓN BAJO NORMAS Y ESTÁNDARES INTERNACIONALES.
EXPERTO EN GESTIÓN DEL COMPLIANCE, ISO19600 E ISO 37001.

Laura Gonzalvo Diloy

COMPLIANCE OFFICER ACREDITADA POR LA WORLD COMPLIANCE ASSOCIATION. LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS. MÁSTER EN "AUDITORÍA" Y EN "GESTIÓN Y DIRECCIÓN DE ENTIDADES NO LUCRATIVAS".
CHIEF ETHICS & COMPLIANCE OFFICER DE LA FUNDACIÓN AYUDA EN ACCIÓN.
COORDINADORA DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION Y MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA COORDINADORA DE ONGD.

Jorge Pelegrín Sáenz

LICENCIADO EN SOCIOLOGÍA. MÁSTER EN "CALIDAD Y MEDIOAMBIENTE" Y "DIRECCIÓN DE EMPRESAS";
CURSO DE EXPERTO EN "DELEGADO DE PROTECCIÓN DE DATOS".
TÉCNICO DE ORGANIZACIÓN Y CALIDAD DE CONFEDERACIÓN SALUD MENTAL ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Rocío López Escorial

LICENCIADA EN DERECHO Y ADMINISTRACIÓN DE EMPRESAS POR LA UNIVERSIDAD AUTÓNOMA DE MADRID.
MÁSTER EXECUTIVE EN DERECHO EMPRESARIAL EN EL CENTRO DE ESTUDIOS GARRIGUES.
ANALISTA Y RESPONSABLE DE NUEVAS ONG DE FUNDACIÓN LEALTAD.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Isabel Peñalosa Esteban

DOCTORA EN DERECHO.
DIRECTORA DE RELACIONES INSTITUCIONALES Y ASESORÍA JURÍDICA DE LA ASOCIACIÓN ESPAÑOLA DE FUNDACIONES.
POSGRADO EN COMPLIANCE UNIVERSIDAD CARLOS III DE MADRID.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Pilar Cervera Medina

LICENCIADA EN DERECHO Y RELACIONES INTERNACIONALES.
RESPONSABLE DE ASESORÍA JURÍDICA DE LA ASOCIACIÓN ESPAÑOLA DE FUNDACIONES.

Ana Martín

LICENCIADA EN GEOGRAFÍA E HISTORIA. MÁSTER (MSC) EN "POLÍTICA Y GESTIÓN CULTURAL".
POSTGRADO EN "MONITOREO Y EVALUACIÓN DE PROYECTOS". EXPERTA EN CALIDAD Y COACHING.
RESPONSABLE DE COMPLIANCE INSTITUCIONAL DE ACCIÓN CONTRA EL HAMBRE ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Patricia Fernández

LICENCIADA EN CIENCIAS ECONÓMICAS Y EMPRESARIALES.
RESPONSABLE DEL ÁREA ECONÓMICA Y FINANCIERA DE LA FEDERACIÓN DE ASOCIACIONES DE MEDICUS MUNDI.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION Y DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA COORDINADORA DE ONGD.

Guillermo González de la Torre Rodríguez

LICENCIADO EN PERIODISMO. MÁSTER EN "CALIDAD Y CONSULTORÍA" Y EN "DIRECCIÓN Y GESTIÓN DE ONG". COORDINADOR DE ESTRATEGIA Y CALIDAD DE MANOS UNIDAS. PRESIDENTE DE LA COMISIÓN DE SEGUIMIENTO DEL CÓDIGO DE CONDUCTA DE LA COORDINADORA DE ONGD Y MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO. MIEMBRO DEL CTN SOBRE ÉTICA DE AENOR, DEL OBSERVATORIO DE RESPONSABILIDAD SOCIAL CORPORATIVA Y DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION. DOCENTE DE POSGRADO EN EL INSTITUTO DE FORMACIÓN DE INTERVENCIÓN SOCIAL.

Albert Salvador

LICENCIADO EN CC ECONÓMICAS Y EMPRESARIALES.
AUDITOR INTERNO CERTIFICADO POR EL IIA (THE INSTITUTE OF INTERNAL AUDITORS).
ESPECIALISTA EN FRAUDE INTERNO, FORENSIC Y PREVENCIÓN DE BLANQUEO DE CAPITALES.
SECRETARIO GENERAL Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA WORLD COMPLIANCE ASSOCIATION.

Juan Arrese Romero-Rato

ABOGADO COMPLIANCE CORPORATIVO Y DE DIVERSIDAD, ÁRBITRO DE LA ASOCIACIÓN EUROPEA DE ARBITRAJE A.E.A, ASOCIADO A LA WORLD COMPLIANCE ASSOCIATION Y MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR, CONSEJERO DE ENTIDAD TERCER SECTOR ENVERA EMPLEO. CONSULTOR EN COMPLIANCE Y POLÍTICAS DE IGUALDAD Y DIVERSIDAD.

Vanessa Fernández

LICENCIADA EN DERECHO POR LA UNIVERSIDAD SAN PABLO-CEU, MADRID Y MÁSTER EN ABOGACÍA Y ESPECIALIDAD EN DERECHO PRIVADO POR EL INSTITUTO DE ESTUDIOS SUPERIORES SAN PABLO CEU-MADRID. SOCIA DEL ÁREA PENAL Y COORDINADORA DEL ÁREA CORPORATE COMPLIANCE DE GÓMEZ-ACEBO & POMBO ABOGADOS, S.L.P. MIEMBRO DE LA SUBCOMISIÓN DE PREVENCIÓN DEL BLANQUEO DE CAPITALES DEL CONSEJO GENERAL DE LA ABOGACÍA Y DEL COMITÉ DEL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Sandra Soler

FUNDADORA DE SOLER COMPLIANCE. CO FOUNDER DE PLAY COMPLIANCE. LICENCIADA EN DERECHO POR LA UBA. ASESORÍA Y GESTIÓN TRIBUTARIA POR ESADE. DIRECCIÓN Y ADMISTRACIÓN DE EMPRESAS. EN EUNCET BUSSINES SCHOOL. DIPLOMADA TÉCNICO ESPECIALISTA EN RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA. AUDITOR JEFE/LÍDER DE SISTEMAS DE GESTÍON DEL COMPLIANCE ISO 19600.

María Alvear García

LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS POR LA UNIVERSIDAD CARLOS III DE MADRID. POSGRADO DE GESTIÓN ECONÓMICA FINANCIERA DE ENTIDADES NO LUCRATIVAS. MÁSTER EN ESTRATEGIAS, AGENTES Y POLÍTICAS DE COOPERACIÓN. DIRECTORA DE ANÁLISIS DE FUNDACIÓN LEALTAD.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION.

Mónica Varela Gil

LICENCIADA EN DERECHO. DIPLOMA DE ESTUDIOS AVANZADOS EN DERECHO INTERNACIONAL PÚBLICO Y ESPECIALIZACIÓN EN DERECHOS HUMANOS.
TÉCNICO JURÍDICO EN LA FUNDACIÓN SAVE THE CHIDREN.
MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA COORDINADORA DE ONG DE DESARROLLO.

Elena Hidalgo Gaviria

LICENCIADA EN ECONÓMICAS Y EMPRESARIALES. ESTUDIOS DE POSGRADO EN ECONOMÍA REGIONAL Y EN GESTIÓN DE ENTIDADES NO LUCRATIVAS.
RESPONSABLE DE FINANCIACIÓN, PROYECTOS Y TRANSPARENCIA DE LA COORDINADORA DE ONG DE DESARROLLO.
MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA COORDINADORA DE ONG DE DESARROLLO.

Te invitamos a formar parte de la **Red Mundial para el Cumplimiento.**

La World Compliance Association (WCA) es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del compliance. La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La pertenencia a la WCA muestra por sí misma un interés y un compromiso real con el mundo del compliance. Está abierta a personas y organizaciones con interés en participar, impulsar y ampliar su conocimiento y red de trabajo y colaboración en el mundo del compliance corporativo.
Además nuestro socios profesionales están cubiertos por un Seguro de Responsabilidad Civil en sus actividades como compliance officer, consultor y/o auditor de compliance.

01 | CONTENIDOS EXCLUSIVOS

02 | PARTICIPACIÓN PRIVILEGIADA

03 | CRECIMIENTO PROFESIONAL

04 | PRIVILEGIOS EXCLUSIVOS

Y VENTAJAS ADICIONALES PARA ASOCIADOS CORPORATIVOS

CUOTA DE ADHESIÓN

Categoría Socio	Profesional		Corporativo
	Fuera de España	España (seguro RC)	
Cuota Semestral	70 €	110 €	195 €
Cuota Anual	120 €	195 €	295 €

WORLD® COMPLIANCE ASSOCIATION

WCA Internacional
Paseo Castellana 79, 7ª Planta (Lexington Center)
28046 Madrid - España Tlf: +34 917 91 66 16
info@worldcomplianceassociation.com
www.worldcomplianceassociation.com

WCA está acreditada por IAS para la certificación de ISO 37001:2016

ÍNDICE

ABREVIATURAS

Código Penal:	**CP**
Tribunal Supremo:	**TS**
Ley de Sociedades de Capital:	**LSC**
International Organization for Standarization:	**ISO**
Asociación Española de Normalización:	**UNE**
Sistema de Gestión de Compliance:	**SGC**
Agencia Española de Protección de Datos:	**AEPD**
Ley Orgánica Prot Datos y Garantía Derechos Digitales:	**LOPDGDD**
Ciclo Plan, Do, Check, Act:	**PDCA**

PRÓLOGO

IVÁN MARTÍNEZ LÓPEZ

DIRECTIVO Y EXPERTO EN SISTEMAS DE GESTIÓN Y ORGANIZACIÓN EMPRESARIAL EN ÁMBITOS NACIONALES E INTERNACIONALES CON ESPECIALIZACIÓN EN EL DESARROLLO DE NEGOCIOS Y LA GESTIÓN BAJO NORMAS Y ESTÁNDARES INTERNACIONALES.
EXPERTO EN GESTIÓN DEL COMPLIANCE, ISO19600 E ISO 37001.

PRESIDENTE INTERNACIONAL DE LA WORLD COMPLIANCE ASSOCIATION.
CEO DE INTEDYA INTERNACIONAL.
CEO DE PREVENSYSTEM.

En España se estima que operan más de 30.000 entidades dedicadas a cubrir y a asistir las necesidades de los más vulnerables. Resulta redundante exponer la tremenda labor social que realizan este tipo de entidades en favor de los más desfavorecidos, llegando en muchos casos donde los mecanismos "oficiales" de asistencia no pueden, no saben o no tienen la capacidad de llegar.

Desde un primer momento, en la WCA, entendimos el reto que supone para un sector que implica a más de dos millones de personas, entre voluntarios y profesionales, gestionar los enormes riesgos que rodean a su actividad, siendo a su vez uno de los grandes pilares de la cohesión social, lo cual convierte este reto en un objetivo en el cual todos debemos trabajar.

Sin entrar en el detalle de lo que ha supuesto la reforma de 2010 (L.O. 5/2010) introduciendo la responsabilidad penal corporativa, así como la reforma de 2015 (L.O. 1/2015) incorporando la adopción de los modelos de prevención de delitos en las organizaciones, cuestión sobre la cual disertarán magníficamente el resto de autores/as de esta guía, todos somos conscientes de cuál es quizás el mayor riesgo que afrontan la mayoría de las organizaciones del sector, el cual no está en la consecuencias derivadas de una posible condena penal. El mayor riesgo puede ser, y de hecho lo ha sido ya en muchas ocasiones, mucho más rápido e implacable, el riesgo reputacional.

En un sector en el cual el nivel de confiabilidad trasmitido a donantes, patronos, colaboradores/as, voluntarios/as y similares resulta fundamental para la capacidad de estas entidades para desarrollar plenamente su labor social, no han sido pocos los casos recientes en que el comportamiento inadecuado, delictivo o poco ético de unas pocas personas ha puesto en tela de juicio la increíble y necesaria labor que realizan estas entidades.

En un contexto como el que vivimos, la era de la hiper comunicación (lo cual no siempre es sinónimo de información), una conducta inadecuada de una sola persona pone en riesgo a miles. La adopción de medidas de control y prevención por parte las organizaciones de este sector no es solo una medida de protección legal, al contrario, en mi opinión eso es una consecuencia cuasi accesoria, más bien es un elemento estructural fundamental para alcanzar los fines sociales de la organización de forma sostenible, ayudando a prevenir conductas o incidentes que tiren por los suelos la buena labor de miles de personas.

El *compliance*, como herramienta para la prevención de riesgos en organizaciones del tercer sector, es un camino seguro para la introducción paulatina de políticas y proceso formales que incrementen sus niveles de transparencia, confiabilidad y control, dotándolas de mayor solidez y capacidad y, por tanto, mejorando la esencia del objeto asistencial que las fundamenta.

Ante todo, quiero agradecer al magnífico equipo de personas que han participado de forma totalmente altruista en este proyecto, todos/as ellos/as son profesionales de gran experiencia

y trayectoria contrastada y sus recomendaciones y guías tienen un valor incalculable y no puedo menos que agradecer públicamente su dedicación.

Esta guía pretende ser un documento de uso eminentemente práctico, huyendo en todo momento de reflexiones paradigmáticas o de disertaciones excesivamente técnicas. Desde luego que muchas de las cuestiones que plantea esta guía podrían ser "atacadas" desde otros puntos de vista o con otras fórmulas, pero sin embargo marcan un camino práctico, efectivo y sencillo que cualquier organización del sector puede tomar, navegando hacia un puerto seguro para iniciar la construcción de su programa de cumplimiento dotando de mayor seguridad y confianza a la entidad.

Cuando, en el año 2017, fundamos la World Compliance Association, uno de los valores fundacionales fue (y sigue siendo) ser un vehículo de intercambio de conocimientos, de ideas y de opiniones, en el que todos/as los/as profesionales, organizaciones e interesados/as en este complejo y amplio universo del cumplimiento se sintieran cómodos/as para expresarse y compartir, para aprender y enseñar, y es que en un mundo como en el que nos ha tocado vivir, aquellos/as que piensen que no tienen nada que aprender, serán rápidamente absorbidos por una realidad en la que cada día, incluso cada hora, hay novedades, nuevas herramientas, tecnología, legislación noticas, incidentes, etc. Me enorgullece como representante de la WCA haber impulsado y apoyado este proyecto que esperamos que sea útil para miles de organizaciones del tercer sector en España y en todo el mundo.

Para muchas entidades del tercer sector este documento aspira a ser un primer paso formal en el mundo del cumplimiento, un paso para quitarles decenas de dudas y cuestionamientos, y también un paso para restar temores. Si estás leyendo esta guía, ya has dado un excelente primer paso para tu organización. Quizás tus primeros pasos y tus primeras acciones para diseñar e implementar tu programa de *compliance* no sean perfectos, pero un primer paso en materia de prevención y ética siempre será mejor que vivir en la ignorancia. No tengas duda de que, cuando finalices la lectura de esta guía, tendrás la oportunidad de que tu organización sea más sólida y fuerte y, sobre todo, sirva mejor a los propósitos asistenciales de su existencia. De eso trata el cumplimiento, no de llenar a las organizaciones de papeles, de trabas y burocracia, sino de integrar en su día a día y en la normalidad de sus procesos y actividades, medidas naturales de prevención y control ante posibles riesgos que pueden terminar con la vida de una organización y arruinar los esfuerzos y el futuro de muchas personas.

Espero que disfrutes de esta guía, pero sobre todo que te resulte útil. Si conseguimos darte, aunque tan solo sea una buena idea que apliques en el día a día de tu organización y en tu actividad, ya habrá valido la pena el esfuerzo realizado por el espectacular equipo de profesionales que te han dedicado su tiempo.

Iván Martínez López

PRÓLOGO

LAURA GONZALVO DILOY

COMPLIANCE OFFICER ACREDITADA POR LA WCA.
LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS .
MÁSTER EN AUDITORÍA Y EN GESTIÓN DE ENTIDADES NO LUCRATIVAS .
CHIEF ETHICS & COMPLIANCE OFFICER DE LA FUNDACIÓN AYUDA EN ACCIÓN.
COORDINADORA DEL COMITÉ TÉCNICO DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA Y
MIEMBRO DEL GRUPO DE TRABAJO DE BUEN GOBIERNO Y TRANSPARENCIA DE LA CONGD.

El tercer sector difiere en muchos aspectos de otros sectores y es su compleja realidad la que determina las peculiaridades y dificultades a las que se enfrentan las organizaciones que lo componen a la hora de diseñar e implementar un programa de *compliance*.

Entre sus particularidades, destaca el hecho de ser un sector muy atomizado dada la diversidad de las organizaciones que lo integran -fruto de las necesidades sociales y humanitarias a las que dan respuesta-, el ámbito geográfico y de actuación en el que operan y la población destinataria de su intervención. De ahí que los riesgos inherentes a los que estará expuesta cada entidad varíen al estar condicionados por un contexto organizacional tan dispar.

Los limitados recursos humanos, técnicos y económicos con los que cuentan la gran mayoría de las organizaciones del tercer sector, y aún más los específicos para las labores de *compliance*, también determinan su capacidad en este sentido. La razón es que dichos recursos se destinan eminentemente a la propia intervención de las organizaciones, por una cuestión de coherencia institucional y también por ser una demanda social. Sin embargo, es importante plantear la importancia de ampliar los recursos que se destinan al cumplimiento normativo, ya que invertir en *compliance* es sinónimo de confianza y rigor en el desempeño de nuestra misión.

A la limitación de recursos se suma un marco legislativo cada vez más restrictivo con nuestro sector, lo que nos condiciona a dar respuesta a nuevas obligaciones, en ocasiones formuladas desde un plano muy teórico y que no atiende a nuestras diferentes realidades, con las complicaciones y dificultades que ello conlleva de cara a la gestión.

Por último, cabe destacar el elevado impacto que tiene sobre la reputación del tercer sector de forma generalizada cualquier escándalo asociado a una organización concreta, debido al "efecto dominó" que genera. Y es que, la tolerancia de la ciudadanía sobre este tipo de comportamientos es infinitamente menor a la que mostraría ante otros sectores; una cuestión comprensible, si tenemos en cuenta que la razón de ser de nuestras entidades se basa en valores éticos.

Ante este contexto, en 2019 un grupo de profesionales decidimos crear un comité técnico dentro de la World Compliance Association que albergara a personas y organizaciones del tercer sector, o próximas a este, con experiencia en el ámbito del *compliance*. El objetivo era construir un espacio de encuentro donde compartir nuestro conocimiento para, entre todos y todas, dar respuesta a las inquietudes y necesidades de las organizaciones del tercer sector, dotándolas de recursos y mecanismos. Así, trabajamos por fortalecer la cultura de cumplimiento en un sector cuya existencia radica en las personas que confían en nuestras organizaciones como agentes de cambio y, por tanto, a las que nos debemos.

La presente guía tiene como objetivo servir de hoja de ruta para aquellas entidades que

quieren afrontar el reto de diseñar e implementar un programa de eficaz, el cual no se delimita únicamente a los riesgos penales, puesto que existen riesgos de otra índole que también tienen un alto impacto. Es decir, un programa de *compliance* integra el modelo de prevención penal, pero no al contrario.

Este documento es el resultado del esfuerzo, compromiso y profesionalidad demostrados por todas las personas que han colaborado en su creación, a quienes quiero mostrar mi máximo agradecimiento y reconocimiento. Todos ellos, desde su experiencia en el Tercer Sector, han dotado a esta guía de un enfoque eminentemente práctico y adaptado a nuestra realidad.

La mayoría de las organizaciones cuentan con protocolos, más o menos formales, para asegurar una gestión rigurosa de sus recursos. Afrontar este reto, servirá para fortalecer su compromiso, poniendo el foco en los aspectos prioritarios desde un enfoque de riesgos y priorizando nuestros propios recursos.

La labor realizada por las organizaciones del tercer sector es indudable. Son un actor clave en cualquier sociedad, garantes de la defensa y protección de los derechos humanos y, en no pocas ocasiones, llegan a lugares, personas y cubren necesidades que ni las propias instituciones son capaces. Por todo ello, resulta transcendental su continuidad, mientras la situación así lo amerite, siendo fundamental contar con la confianza y respaldo social que garanticen su legitimidad. Implantar un programa de *compliance* nos ayudará a fomentar dicha sostenibilidad desde la defensa de los derechos e intereses de todas las partes implicadas.

Laura Gonzalvo Diloy

CAPÍTULO 1.
LA IMPORTANCIA DEL COMPLIANCE EN EL TERCER SECTOR.

JORGE PELEGRÍN SÁENZ

LICENCIADO EN SOCIOLOGÍA.
MÁSTER EN "CALIDAD Y MEDIOAMBIENTE" Y "DIRECCIÓN DE EMPRESAS".
CURSO DE EXPERTO EN "DELEGADO DE PROTECCIÓN DE DATOS".
TÉCNICO DE ORGANIZACIÓN Y CALIDAD DE CONFEDERACIÓN SALUD MENTAL ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

QUÉ ES EL TERCER SECTOR

A la hora de definir lo que es el tercer sector debemos distinguir entre las asociaciones y fundaciones que persiguen un fin humanitario o social y las entidades como cooperativas, mutualidades, sociedades laborales o empresas sociales que persiguen una economía solidaria. En el primer caso podemos encontrar organizaciones que se dedican a la acción social, la cooperación al desarrollo, el medio ambiente, la paz, los derechos humanos, la investigación o la promoción cultural o deportiva. En el segundo caso, cabe hacer referencia al término de economía social[1] . A grandes rasgos, es la economía que no está definida dentro del sector privado ni del sector público, aquella que, a través de entidades sociales, intenta llevar a cabo las funciones de producción, distribución, circulación y adquisición de bienes y servicios, aplicando la participación, cooperación, solidaridad, autogestión, la integración social y la democracia para la toma de decisiones, teniendo en cuenta que, por encima de todo, está el trabajo, y no el capital.

Es imprescindible, también, hacer referencia a la Ley 5/2011, de 29 de marzo, de economía social, que configura el marco jurídico en el que se encuentran las entidades del tercer sector y que tiene como objeto el reconocimiento y mejor visibilidad de la economía social, otorgándole una mayor seguridad jurídica por medio de las actuaciones de definición de la economía social, estableciendo los principios que deben contemplar las distintas entidades que la forman[2]. También son de su aplicación otras leyes básicas como la Ley 1/2002, de 22 de marzo, de Asociaciones; la Ley 50/2002, de 26 de diciembre, de Fundaciones; o la Ley 49/2002, de 23 de diciembre, de Régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.

Hechas estas aclaraciones iniciales, no se puede obviar el peso de las organizaciones que conforman el tercer sector en España. Para dar respuesta a las demandas de la población española, se estima que unas 30.000 entidades activas trabajan para garantizar los derechos sociales y cubrir las necesidades de las personas y colectivos más vulnerables. El colectivo que trabaja para que esas entidades cumplan con sus objetivos es de unos dos millones de personas, de los cuales un 58% del total son personal voluntario y el 32% restante, profesionales contratados[3]. Todo ello para intentar dar respuesta a las necesidades de 12,8 millones de personas que se encuentran en riesgo de pobreza y exclusión en España.

RETOS EN EL TERCER SECTOR

Las entidades del tercer sector se enfrentan a una serie de retos que determinarán la supervivencia de estas. La **Fundación PwC** diferencia entre retos relacionales e internos[3]. Entre los primeros, está la colaboración entre las entidades del propio sector con entidades públicas y privadas, el buen gobierno y la transparencia, así como la salvaguardia de su propia reputación. Entre los retos internos, destaca la atracción y retención del talento, la digitalización, el cumplimiento de la normativa y los controles internos y medir y comunicar el impacto de sus programas.

POR QUÉ ES IMPORTANTE UN PROGRAMA DE COMPLIANCE

Al margen de que las entidades del tercer sector se muevan entre el sector privado y el público, o de cuál sea el objeto para el que se hayan creado, debemos tener en cuenta principalmente que estamos hablando de personas jurídicas. Como se indica en el manual *Programa de cumplimiento normativo para centros educativos*[4], son aquellas que no podían cometer delitos y, por tanto, no podían ir a la cárcel ya que, según el Código Penal de nuestro ordenamiento jurídico, las personas jurídicas no podían tener responsabilidad penal y, por tanto, sólo podían ser condenadas por responsabilidad civil. Esta situación cambió con la reforma del Código Penal en el año 2010 y sus sucesivas modificaciones.

Posteriormente al año 2010, se incorporaron al ordenamiento jurídico los programas de *compliance* como herramienta que ayudará a eludir o atenuar la responsabilidad penal a la que se sometían las personas jurídicas. Así, la Ley 1/2015, de 30 de marzo, indica la posibilidad de eximirse de la responsabilidad penal o atenuarla si la entidad con personalidad jurídica ha adoptado un modelo de organización y gestión[5] con medidas de vigilancia y control que ayuden a prevenir o reducir el riesgo de comisión de los delitos anteriormente detallados, aspecto que está debidamente desarrollado en el capítulo 2 de la presente guía.

Llegados a este punto, estamos en disposición de establecer con cierto sentido cuál es la importancia de desarrollar un programa de *compliance* dentro de una entidad del tercer sector. El sentido común nos invitará a establecer una primera premisa: eludir la responsabilidad penal, evitar la cárcel. El error de esta premisa es que estamos dando por sentado que algo se va a hacer mal. El objetivo de un programa de *compliance* debe ser detectar aquellas actividades de la entidad que conllevan un riesgo, desde un sentido más amplio y no únicamente penal (ver mayor desarrollo sobre las posibles categorías de riesgo en el tema 5 de la presente guía) y establecer las medidas necesarias para evitarlo. Solo si las entidades demuestran haber

actuado con la diligencia debida en cuanto a la vigilancia y el control de aquellas actividades susceptibles de comisión de alguno de los delitos penales tipificados, estarán mostrando, cuanto menos, un correcto desempeño en cuanto a cumplimiento legal, lo que viene a ser tener integrada en la organización una auténtica **cultura de cumplimiento.**

Por otro lado, los programas de *compliance* que enfatizan la conducta responsable y permiten crear oportunidades para que los trabajadores practiquen y demuestren la ética, tienen mayor probabilidad de tener un impacto positivo y a largo plazo que los programas basados solo en la vigilancia y el control. Asimismo, la Circular 1/2016 de la Fiscalía General del Estado señala que los modelos de organización y gestión no tienen por objeto evitar la sanción penal de la empresa, sino promover una cultura de *compliance* o cultura de cumplimiento que citamos en el párrafo anterior. Es por esta razón, por la que esta guía va a plantear un sistema de prevención que vaya más allá de los riesgos penales e incluya todos los riesgos que puedan comprometer los objetivos estratégicos de una organización. Es un enfoque completo y más amplio que aquel que solo contempla la prevención de delitos, el cual deberá distinguir entre falta contra procedimientos o normativa propia; incumplimiento del código ético o de conducta; o vulneración de la ley, penal o no.

Hasta aquí hemos hablado de la importancia del cumplimiento de los requisitos legales o no, independientemente de que se trate de una entidad privada, pública o del tercer sector. No menos importante es considerar un programa de *compliance* como una herramienta poderosa en cuanto a **hacer más eficiente nuestro sistema de gestión.** Así, la norma UNE 19601:2017 indica en su introducción que "esta norma UNE facilita diseñar o evaluar sistemas de gestión de *compliance* penal, que permitan generar o mejorar una adecuada cultura organizativa sensible a la prevención y detección penal y opuesta a las malas praxis que toleran o amparan conductas ilícitas en el seno de las personas jurídicas. [...]. A los efectos anteriores, una organización sensibilizada con tales propósitos deberá disponer de un sistema de gestión que le permita alcanzar sus objetivos y su compromiso de integridad. La política, los objetivos, los procesos y los procedimientos conforman el núcleo de un sistema de gestión para la prevención, detección y gestión de riesgos penales proyectado en el ámbito de la organización, evitando así posibles daños económicos, reputacionales o de otra índole"[6] .

Por tanto, existen una serie de ventajas de las que las entidades del tercer sector y los colectivos a los que van dirigidas sus acciones, se pueden beneficiar. Son ventajas indirectas resultado de la implantación de un buen programa de *compliance*. Una de las más evidentes es la **mitigación de la responsabilidad penal,** tal como se indica en el artículo 31 bis del Código Penal; pero no menos importante es la **defensa de los intereses de los grupos de interés** significativos de las organizaciones y, especialmente, la de sus personas beneficiarias directas y donantes, puesto que el desarrollo de la actividad de la organización en los términos de seguridad, excelencia y transparencia que supone la implantación de un programa de *compliance*, repercutirá, indudablemente, en dichos grupos de interés.

La **reputación y la imagen** de las entidades del tercer sector también se beneficiarán del desarrollo de estos programas, pues denota un esfuerzo por cumplir con los requisitos propios y externos, legales o normativos, y con los compromisos adoptados con sus personas beneficiarias, donantes y, con la sociedad en general, lo que en última instancia ayuda a **consolidar la confianza** depositada por terceros en nuestras organizaciones como agentes de cambio.

Y, para terminar, si hablamos de operatividad, el desarrollo de una planificación en la que se integre el análisis de los riesgos, así como un correcto control de los mismos, permitirá identificar aquellas malas praxis que puedan llegar a cometerse por las personas vinculadas a las organizaciones, independientemente de su puesto o categoría, contribuyendo a la **mitigación de la probabilidad de ocurrencia de actos ilícitos.**

1. Economía social - ¿Qué es?, principios, características y tipos. (2020). Retrieved 7 January 2020. https://enciclopediaeconomica.com/economia-social/

2. BOE.es - Documento BOE-A-2011-5708. (2020). Retrieved 7 January 2020. https://www.boe.es/eli/es/l/2011/03/29/5

3. Radiografía del Tercer Sector Social en España: retos y oportunidades en un entorno cambiante. (2018). Retrieved 7 January 2020. https://www.pwc.es/es/publicaciones/tercer-sector/fundacion-pwc-tercer-sector-social-2018.pdf

4. Muñoz de Priego Alar, J. (2019). PROGRAMA DE CUMPLIMIENTO NORMATIVO PARA CENTROS EDUCATIVOS (pp. 5, 6). Madrid: Escuelas Católicas.

5. Nº 77, Sec. I, Pág. 27089. (2015). Retrieved 7 January 2020. https://www.boe.es/eli/es/lo/2015/03/30/1/dof/spa/pdf

6. Asociación Española de Normalización. (2017). Sistemas de gestión de *Compliance* penal. Requisitos orientación para su uso. (pp. 6, 7). Madrid.

CAPÍTULO 2.
RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA.

ROCÍO LÓPEZ ESCORIAL

LICENCIADA EN DERECHO Y ADMINISTRACIÓN DE EMPRESAS POR LA UNIVERSIDAD AUTÓNOMA DE MADRID.
MÁSTER EXECUTIVE EN DERECHO EMPRESARIAL EN EL CENTRO DE ESTUDIOS GARRIGUES.
ANALISTA Y RESPONSABLE DE NUEVAS ONG DE FUNDACIÓN LEALTAD.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

Hasta el año 2010, en España las personas jurídicas no podían ser responsables penalmente por los delitos cometidos en su seno, sino que eran declaradas responsables las personas físicas a las que les fueran imputables los delitos cometidos. Esto era así porque el derecho penal español, hasta ese año, recogía el aforismo del derecho romano *"societas delinquere non potest"*, según el cual una persona jurídica no puede cometer un delito.

La reforma del Código Penal Español en el año 2010 introdujo un gran cambio en este aspecto, al prever en su artículo 31 bis la posibilidad de que las personas jurídicas fueran declaradas responsables penalmente por los delitos cometidos en su seno.

REQUISITOS PARA QUE LA PERSONA JURÍDICA RESPONDA PENALMENTE

El artículo 31 establece determinados requisitos para poder considerar responsables penalmente a las personas jurídicas:

- Los delitos han de ser cometidos en nombre o por cuenta de la persona jurídica, es decir, la persona jurídica no responderá penalmente de cualquier delito cometido, por ejemplo, por una persona representante, sino que sólo responderá de aquellos delitos cometidos cuando esta persona actúe como representante de la persona jurídica y en el marco de sus funciones.

- Los delitos han de ser cometidos en beneficio, directo o indirecto, de la persona jurídica. Para que la persona jurídica pueda ser declarada penalmente responsable, el delito cometido ha de ser en provecho de la entidad. Este beneficio puede ser directo o indirecto. Por ejemplo, la obtención de un ahorro de coste. Es importante remarcar, como hace la Circular 1/2011 de la Fiscalía General del Estado, que no es necesario que el beneficio sea efectivo finalmente, es decir, la persona jurídica podrá ser declarada penalmente responsable independientemente de que finalmente el beneficio no se produzca.

QUIÉN PUEDE COMETER UN DELITO PARA QUE LA PERSONA JURÍDICA SEA DECLARADA PENALMENTE RESPONSABLE

El artículo 31 bis determina quién puede cometer estos delitos que podrían desencadenar la responsabilidad penal de una persona jurídica. El Código Penal en este aspecto prevé dos supuestos:

- Delitos cometidos por las personas representantes legales de las personas jurídicas o por aquellas que, actuando individualmente o como integrantes de un órgano de la persona jurídica, estén autorizados a tomar decisiones o tengan facultades de control y organización. Es decir, las entidades serían responsables por los delitos cometidos por cualquier persona representante legal, cualquier miembro de los órganos de gobierno (patronato o junta directiva) o cualquier persona que tenga control sobre la organización y/o poder de decisión, como la persona que ocupe el cargo de dirección en la entidad.

- Delitos cometidos por una persona que esté sometida a la autoridad de cualquiera de las personas nombradas anteriormente, siempre y cuando haya habido un incumplimiento grave de los deberes de vigilancia y control de la actividad. Es decir, la persona jurídica podría ser declarada responsable por un delito cometido por cualquier persona trabajadora siempre y cuando haya habido un incumplimiento en los deberes de vigilancia de las personas encargadas de su supervisión. Este supuesto podría aplicar a cualquier persona trabajadora de una fundación o asociación, pero también a una persona voluntaria que colabore con la entidad y cometiera un delito en beneficio de la persona jurídica, siempre y cuando haya existido un incumplimiento grave de los deberes de supervisión de las personas encargadas de la vigilancia de las actividades del voluntario. Este incumplimiento grave de los deberes de supervisión es un asunto crucial que se abordaría con la implantación de un programa de *compliance* cuyo contenido se explica a continuación.

¿ES POSIBLE QUE LA PERSONA JURÍDICA QUEDE EXENTA DE RESPONSABILIDAD?

Tras la reforma del año 2015, el Código Penal prevé la exención de responsabilidad de las personas jurídicas siempre que exista un programa de *compliance* y se den una serie de condiciones. En el caso de que solamente se puedan probar parcialmente alguno de los requisitos, esta circunstancia será valorada como atenuante a la hora de declarar la responsabilidad de la persona jurídica. A la hora de describir las condiciones que deben darse para la exención de responsabilidad penal, el Código Penal distingue entre los delitos cometidos por los órganos de gestión o gobierno (patronato, personal directivo, etc.) y los delitos cometidos por las personas dependientes de ellos (personal contratado, personal voluntario, etc.).

En el caso de un delito cometido por el órgano de gobierno, dirección o algún miembro del mismo, la entidad podría quedar exenta de responsabilidad siempre que se cumplan y prueben los siguientes **requisitos**:

- Existencia de un modelo de prevención: antes de la comisión del delito debe existir un

modelo de organización y gestión que incluya las medidas de vigilancia y control para prevenir delitos o para reducir el riesgo de cometerlos, el cual haya sido adoptado y ejecutado por el órgano de gobierno

- Nombramiento de un órgano encargado de la supervisión del funcionamiento y cumplimiento del modelo de prevención: debe existir un órgano con poderes autónomos de iniciativa y control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica. En el caso de personas jurídicas de pequeñas dimensiones, es decir, aquellas autorizadas a presentar cuentas abreviadas, este órgano puede ser el órgano de gobierno.

- Elusión fraudulenta del modelo de prevención: las personas autoras del delito deben haber cometido el citado delito eludiendo fraudulentamente los modelos de prevención de la entidad.

- No negligencia en la supervisión: no debe haber existido omisión o ejercicio insuficiente de las funciones de supervisión, vigilancia y control por parte del órgano supervisor.

En caso de que el delito fuera cometido por una persona sometida a la autoridad de los órganos de gestión de la entidad, por ejemplo, una persona contratada o personal voluntario, la persona jurídica quedaría exenta siempre que antes de la comisión del delito existiera un modelo de prevención adecuado para prevenir o reducir el riesgo de comisión del delito cometido. En definitiva, la ley establece que la entidad podría quedar exenta en caso de que una persona contratada cometiera un delito simplemente cumpliendo el primero de los requisitos mencionados, es decir, contar con un modelo de prevención eficaz.

REQUISITOS DEL MODELO DE PREVENCIÓN PENAL

La Circular 1/2016 de la Fiscalía General del Estado recalca la importancia de que los programas de prevención deben ser claros, precisos, eficaces y plasmarse por escrito. En este sentido, no basta con que exista un modelo de prevención, sino que la entidad debe acreditar que dicho modelo es adecuado para prevenir el delito concreto que se ha cometido, por ello es tan importante que el modelo de prevención esté perfectamente adaptado a la entidad concreta y no sea genérico.

El artículo 31 bis Código Penal establece una serie de requisitos que debería cumplir un modelo de prevención eficaz para lograr atenuar o eximir de responsabilidad a las entidades. De este modo, los modelos de prevención deberán:

- Identificar las **actividades** en cuyo ámbito puedan ser cometidos los delitos: es preciso que la entidad elabore un mapa de riesgos en el que identifique aquellas actividades en las que podría tener lugar la comisión de un posible acto ilícito, ya que el riesgo penal al que están sujetas las organizaciones varía en función de su contexto, de ahí la importancia de definirlo de forma previa.

- Establecer **protocolos o procedimientos** para la toma de decisiones y acuerdos y ejecución de los mismos: se deben establecer procedimientos que garanticen altos estándares éticos que regulen la toma de decisiones.

- Disponer de modelos adecuados de **gestión de los recursos financieros:** se deben disponer de un conjunto de medidas que en su conjunto configuren un entorno de control adecuado para la prevención de posibles conductas delictivas

- Imponer la obligación de **informar de posibles riesgos e incumplimientos** al órgano encargado de la vigilancia: la obligación de informar de las posibles conductas que puedan ser inadecuadas no solamente logra prevenir la comisión de delitos, sino que también es eficaz a la hora de detectar conductas que puedan derivar en la comisión de delitos. En este punto, toma especial relevancia el canal de denuncias, como medio de comunicación entre cualquier persona y la entidad, al cual hemos destinado un capítulo específico de la presente Guía

- Establecer un **sistema disciplinario**: es preciso diseñar un sistema disciplinario, para lo cual es necesario que exista previamente un código de conducta en el que se establezcan claramente las obligaciones de todas las personas a las cuales les resulta de aplicación dicho código.

- Establecer **revisiones periódicas** del modelo: es preciso verificar periódicamente la eficacia del modelo a través de la realización de auditorías internas y/o externas de forma periódica. El propio modelo de prevención debería establecer el plazo de revisión adecuado para que el modelo resulte eficaz. Además, el modelo deberá ser revisado inmediatamente si concurre alguna circunstancia que pueda provocar un cambio sustancial en el mismo

Los detalles de este modelo de prevención eficaz son precisamente aquellos que se abordan en esta guía, más en concreto los referidos a los capítulos de mapa de riesgos y de delitos, política de *compliance*, órgano de cumplimiento, código de conducta y canal de denuncias, que serían de algún modo como los grandes componentes de ese modelo, añadiéndole la formación.

En definitiva, el Código Penal prevé la posibilidad de que las personas jurídicas puedan ser penalmente responsables por los delitos cometidos por las personas que tengan un determinado poder de decisión en la entidad o por cualquier persona dependiente de las misma. Así como, prevé la forma de mitigar y prevenir esta responsabilidad a través de la elaboración de un programa de *compliance* eficaz que no solamente sea adecuado para prevenir la comisión de delitos, evadir la responsabilidad penal y evitar así la sanción penal, sino que debe promover una verdadera cultura ética y reafirmar una cultura interna de respeto a la ley.

CAPÍTULO 3. RESPONSABILIDAD CIVIL Y PENAL DE LOS MIEMBROS DE LOS ÓRGANOS DE GOBIERNO.

ISABEL PEÑALOSA ESTEBAN

DOCTORA EN DERECHO.
DIRECTORA DE RELACIONES INSTITUCIONALES Y ASESORÍA JURÍDICA DE LA ASOCIACIÓN ESPAÑOLA DE FUNDACIONES.
POSGRADO EN COMPLIANCE UNIVERSIDAD CARLOS III DE MADRID.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

PILAR CERVERA MEDINA

LICENCIADA EN DERECHO Y RELACIONES INTERNACIONALES.
RESPONSABLE DE ASESORÍA JURÍDICA DE LA ASOCIACIÓN ESPAÑOLA DE FUNDACIONES.

RESPONSABILIDAD CIVIL DE LOS PATRONOS Y MIEMBROS DE LA JUNTA DIRECTIVA U ÓRGANO RECTOR DE LA ASOCIACIÓN

Todas las fundaciones, así como las asociaciones inscritas, son entidades con personalidad jurídica propia, por lo que pueden adquirir y poseer bienes de todas clases, así como contraer obligaciones, respondiendo con su propio patrimonio de las obligaciones y deudas contraídas (art. 38 del Código Civil, en adelante "CC").

Como se recoge en el art. 1.089 CC, las obligaciones pueden surgir como consecuencia de las relaciones contractuales de la propia fundación o asociación (responsabilidad contractual), o pueden derivar de las actuaciones u omisiones que hayan causado un daño o perjuicio a otro (responsabilidad extracontractual). Pueden, incluso, existir supuestos en los que se dan ambas de forma simultánea.

Aunque la responsabilidad de la fundación y de la asociación, como personas jurídicas, es independiente de la de los patronos o miembros de la junta directiva u órgano rector, estos, en determinados supuestos, podrán incurrir en una responsabilidad personal que les puede obligar a resarcir el daño causado a la fundación o a terceros en el ejercicio de su cargo, con su patrimonio personal, siempre que se den los supuestos legalmente establecidos para ello.

FUNDACIONES

La Ley 50/2002, de 26 de diciembre, de Fundaciones ("LF"), señala en el art. 17 que los patronos deberán desempeñar su cargo con la **diligencia de un representante leal**, debiendo responder solidariamente frente a la fundación de los daños y perjuicios que causen por los actos que realicen contrarios a la ley o a los estatutos o por aquellos realizados sin el nivel de diligencia exigido para el desempeño de su cargo.

La propia LF establece determinados supuestos de **exención de responsabilidad** para:

- los patronos que hayan votado en contra del acuerdo; y
- los patronos que prueben que, no habiendo intervenido en su adopción y ejecución, desconocían su existencia, o conociéndola, hicieron todo lo conveniente para evitar el daño o, al menos, se opusieron expresamente a aquel.

La responsabilidad es **solidaria**, por lo que todos los miembros del patronato, o del órgano que adoptó el acuerdo, serán responsables salvo que prueben que no intervinieron en la adopción

del mismo. La acción podrá interponerse contra todos los patronos, o contra alguno de ellos, pudiendo reclamar a los demás la parte que corresponda.

La **acción de responsabilidad** se entablará ante la autoridad judicial y en nombre de la fundación:

- por el propio órgano de gobierno de la fundación, previo acuerdo motivado del mismo y en cuya adopción no participará el patrono afectado,
- por el Protectorado;
- por el o los patronos disidentes o ausentes; o
- por el fundador cuando no fuera patrono.

Esta acción, también denominada **acción fundacional de responsabilidad o acción en interés de la fundación**, se ejerce contra los patronos que hayan causado un daño al patrimonio de la fundación y su objetivo es la reparación íntegra del perjuicio causado a la fundación.

La LF no se refiere a la posible responsabilidad en la que pudieran incurrir los patronos de la fundación, de forma colectiva o individual, frente a **terceros**, pero esta se deriva, como se ha señalado, del propio Código Civil. Es claro, tal y como acepta la doctrina y la jurisprudencia, que la responsabilidad de los patronos no se limita a la reparación de los daños y perjuicios causados a la fundación, sino que incluye los causados a terceros, siempre que se den, de nuevo, la falta de diligencia o la actuación antijurídica que conecten con ese daño o perjuicio causado.

La LF no recoge, a diferencia de la Ley de Sociedades de Capital ("LSC"), la legitimación subsidiaria de los acreedores para el ejercicio de la acción social (art. 240 LSC) y tampoco hace ninguna mención a la **acción individual** de responsabilidad iniciada por terceros que han visto lesionados sus intereses por los actos de los administradores (art. 241 LSC). La discusión de la doctrina se centra en dilucidar si la legitimación de estos debe reconducirse a la legislación mercantil, por analogía, o bien por aplicación del Código Civil, tanto para los acreedores como para cualquier tercero afectado. La jurisprudencia se decanta, en general, por esta última. La diferencia estribaría, en esencia, en los plazos de prescripción de la acción.

Algunas normas autonómicas de fundaciones sí prevén expresamente, junto a la acción en interés fundacional, la existencia de una acción individual por daños contra los patronos que puede ser ejercitada por terceros (ej. art. 332.11.5 Código Civil Catalán).

ASOCIACIONES

En cuanto a las asociaciones, la Ley Orgánica 1/2002, de 22 de marzo, reguladora del derecho de asociación ("LODA"), tras señalar que las asociaciones inscritas responden de sus obligaciones con todos sus bienes presentes y futuros, añade que los asociados no responden personalmente de las deudas de la asociación. En las fundaciones, a diferencia de las asociaciones, no existen socios, por lo que no se plantea su responsabilidad.

La LODA señala en su artículo 15 que los miembros o titulares de los órganos de gobierno y representación, y las demás personas que obren en nombre y representación de la asociación, responderán ante esta, ante los **asociados** y ante **terceros** por los daños causados y las deudas contraídas por actos dolosos, culposos o negligentes. Las personas a que se refiere el apartado anterior responderán civil y administrativamente por los actos y omisiones realizados en el ejercicio de sus funciones, y por los acuerdos que hubiesen votado, **frente a terceros, a la asociación y a los asociados.**

Cuando la responsabilidad no pueda ser imputada a ningún miembro o titular de los órganos de gobierno y representación, responderán todos **solidariamente** por los representantes de la asociación – frente a la asociación o frente a terceros -, a menos que puedan acreditar que no han participado en su aprobación y ejecución o que expresamente se opusieron a ellas.

La ley de asociaciones sí se refiere por tanto a la responsabilidad frente a la entidad y frente a terceros, pero nada dice de la legitimación para ejercer la acción de responsabilidad, ya sea en interés de la asociación o individual, si bien parece clara dicha legitimación al mencionar a los asociados y a cualquier tercero.

En conclusión, l**a responsabilidad civil de los patronos y de los miembros de la junta directiva u órgano rector de las asociaciones es una responsabilidad por daños,** que solo es exigible si se produce un daño o perjuicio a la fundación o a terceros, por actos negligentes, dolosos o culposos, siempre que exista una conexión entre su actuación y el daño causado, que ha de determinarse judicialmente y es solidaria, salvo que se pruebe la responsabilidad individual de todos o algunos de los miembros. La acción de responsabilidad puede ser "social", si el perjudicado es la asociación o fundación, o individual, si el afectado es otra persona.

RESPONSABILIDAD CIVIL Y DILGENCIA DEBIDA: EL COMPLIANCE COMO MITIGADOR DE RIESGOS CIVILES

La influencia del derecho de sociedades de capital en el derecho de fundaciones y asociaciones

se manifiesta particularmente en el ámbito de determinación de la responsabilidad de los patronos y miembros del órgano rector, pues el criterio para su valoración es la diligencia en el desempeño de sus funciones.

La LF establece la obligación genérica de desempeñar el cargo con la diligencia de un representante leal y la LODA se refiere simplemente a la diligencia debida, pero ninguna de las dos se refiere a la diligencia de un ordenado empresario como hace la regulación mercantil.

Si bien el cargo de patrono de una fundación o miembro del órgano rector de una asociación no participa de la misma naturaleza que la de administrador de una sociedad, sí que tiene ciertas similitudes, en la medida en que la actuación de los patronos debe desarrollarse bajo el mandato genérico de desempeñar el cargo con la diligencia de un representante leal, lo que pone de manifiesto la transcendencia de sus funciones como representante de intereses ajenos y la relevancia de su actuación. Esto, unido a la gratuidad del cargo de patrono y a la gratuidad, en muchos casos, del cargo de miembro de la junta directiva u órgano rector, hacen que ese estándar de diligencia se considere menor, en general, por la jurisprudencia, que señala que el cargo de administrador y el de patrono no participan exactamente de la misma naturaleza. Uno es un profesional, podría decirse, mientras los segundos siguen participando de un carácter voluntario y altruista.

Sin embargo, la doctrina señala que es preciso analizar los parámetros de diligencia en función de las circunstancias objetivas de cada caso. Asimismo, no puede perderse de vista el papel que las organizaciones del tercer sector han ido adquiriendo como operadores económicos, siendo muchas de ellas organizaciones prestadoras de bienes y servicios en el mercado, en competencia muchas veces con las empresas. Además, las fundaciones y asociaciones trabajan en muchos casos con colectivos vulnerables, por lo que cabe esperar un especial celo en el desempeño de sus funciones.

Si la legislación examinada no ofrece demasiadas pistas para delimitar el estándar de diligencia, sí lo hacen otras normas. Entre estas, el Código Penal, al regular la responsabilidad penal de las personas jurídicas, establece unos supuestos de exoneración de la responsabilidad ligados a la actuación diligente o negligente de los órganos de administración de fundaciones y asociaciones: si una persona jurídica es condenada penalmente puede suponerse que las obligaciones de vigilancia, control y supervisión a que se refiere el artículo 31, bis han fallado, o que la entidad y, por tanto, sus representantes, no habían adoptado las decisiones conducentes a contar con un modelo de prevención de riesgos penales efectivos, lo que ha producido perjuicios evidentes para la organización.

Independientemente de la responsabilidad civil derivada del delito a que pudiera dar lugar un procedimiento penal frente a la asociación o fundación, ¿podría dar lugar al ejercicio de una acción de responsabilidad civil en interés fundacional o asociativo frente a los patronos o

miembros del órgano rector por los daños y perjuicios causados a la entidad?

No hay una opinión clara al respecto, pero parece razonable concluir que los programas de *compliance* contribuirán a mejorar la gestión, a formalizar los procesos internos y de toma de decisiones y a reforzar esa diligencia, esa responsabilidad in vigilando y, en definitiva, el deber fiduciario de los patronatos y juntas directivas, contribuyendo a reducir los riesgos penales y de otra índole en los que puede incurrir la fundación o asociación, protegiéndola a esta y a sus representantes también en el ámbito de la responsabilidad civil.

RESPONSABILIDAD PENAL DE LOS PATRONOS Y DE LOS MIEMBROS DE LA JUNTA DIRECTIVA U ÓRGANO RECTOR DE LA ASOCIACIÓN

Desde el año 2010, y en virtud de la aprobación de la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal ("CP"), las personas jurídicas pueden ser penalmente responsables. Esta novedad se ha consolidado con la reforma en 2015 del CP, pues a través de la Ley Orgánica 1/2015, de 30 de marzo, se ha desarrollado la responsabilidad penal de las entidades, en los términos desarrollados en el capítulo 2 de la presente guía.

No obstante, deben distinguirse dos situaciones, aquellos supuestos en los que los patronos o administradores de hecho o de derecho puedan resultar penalmente responsables, por ejemplo, de determinados delitos societarios, y otros en los que la fundación pueda resultar penalmente responsable.

- Respecto a la responsabilidad penal de los administradores, hay que señalar que los principios básicos que rigen nuestro derecho para poder responsabilizar penalmente a una persona son: culpabilidad, esto es, que haya actuado con dolo. Hay excepciones en los que la normativa penal contempla expresamente la culpa para determinar este factor; y

- responsabilidad personal, pues solo se responde penalmente por hechos propios – como autor o cómplice -.

La responsabilidad penal de las personas jurídicas del art. 31 bis CP no excluye la responsabilidad penal de la persona física, pudiendo concurrir ambas, aunque son autónomas la una de la otra.

Recuérdese que la comisión de un delito genera la obligación de indemnizar los daños y perjuicios causados por dicho delito. A este respecto, cuando, por los mismos hechos se condene a una persona física y a la persona jurídica, de conformidad con lo dispuesto en el art. 116.3 CP, ambas serán responsables solidarias del pago del importe de la responsabilidad civil derivada del delito cometido.

En todo caso, conviene tener presente que, para aquellos tipos penales en los que no está prevista la responsabilidad penal de las personas jurídicas, se puede aplicar el art. 120 CP, que establece la responsabilidad civil subsidiaria de la persona jurídica respecto de los daños y perjuicios derivados de un delito cometido por sus representantes o empleados, si bien esta no será una responsabilidad civil de patronos y miembros de órganos rectores.

“Nuestra estrategia, el Desarrollo Competitivo.”

El entorno legislativo en el que la empresa desarrolla sus actividades es cada vez más complejo. El nivel de exigencia de las autoridades y organismos regulatorios es cada vez mayor, y el impacto de la legislación es más intenso que nunca.

Por ello, y por los recientes escándalos societarios y el innegable incremento de la sensibilidad social respecto de la ética de los negocios, **un mayor número de organizaciones públicas y privadas integran estándares éticos y legales como protocolos de buen gobierno de obligado cumplimiento.**

Curso de Experto Universitario **Compliance Officer**

Modalidad > 450 horas, e-Learning
Titulación > Experto Universitario Compliance Officer emitido por la Universidad de San Jorge. Compliance Officer Certificado por la World Compliance Association. Experto Compliance Officer emitido por Intedya

Curso Universitario de Protección de Datos **Data Protection Officer**

Modalidad > 200 horas, e-Learning
Titulación > Curso Universitario de Protección de Datos – Data Protection Officer.

Data Protection Officer & Compliance Officer

Modalidad > 650 horas, e-Learning
Titulación > Experto Universitario Compliance Officer + Compliance Officer Certificado por la World Compliance Association. Curso Universitario de Protección de Datos – Data Protection Officer

Más información en:

T. 984 395 152 | info@intedya.com | www.intedya.com

WORLD COMPLIANCE ASSOCIATION
CURSOS ACREDITADOS

universidad SANJORGE
GRUPO SANVALERO

Intedya
International Dynamic Advisors

CAPÍTULO 4.
CONTEXTO ORGANIZACIONAL.

ANA MARTÍN

LICENCIADA EN GEOGRAFÍA E HISTORIA.
MÁSTER (MSC) EN "POLÍTICA Y GESTIÓN CULTURAL".
POSTGRADO EN "MONITOREO Y EVALUACIÓN DE PROYECTOS".
EXPERTA EN CALIDAD Y COACHING.
RESPONSABLE DE COMPLIANCE INSTITUCIONAL DE ACCIÓN CONTRA EL HAMBRE ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

JORGE PELEGRÍN SÁENZ

LICENCIADO EN SOCIOLOGÍA.
MÁSTER EN "CALIDAD Y MEDIOAMBIENTE" Y "DIRECCIÓN DE EMPRESAS".
CURSO DE EXPERTO EN "DELEGADO DE PROTECCIÓN DE DATOS".
TÉCNICO DE ORGANIZACIÓN Y CALIDAD DE CONFEDERACIÓN SALUD MENTAL ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

PATRICIA FERNÁNDEZ

LICENCIADA EN CIENCIAS ECONÓMICAS Y EMPRESARIALES.
RESPONSABLE DEL ÁREA ECONÓMICA Y FINANCIERA DE LA FEDERACIÓN DE ASOCIACIONES DE MEDICUS MUNDI.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WORLD COMPLIANCE ASSOCIATION Y DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA CONGD.

Conocer los beneficios que reporta tener un programa de *compliance* será fundamental para integrarlo en la gestión de las entidades. De ahí, que hayamos preparado un cuestionario que permite identificar las fortalezas y debilidades de cada organización en materia de *compliance*, fase fundamental a la hora de enfrentarse a este gran reto, para así dar los próximos pasos, los cuales se desarrollan a lo largo de la presente guía. Dicho cuestionario está disponible en la página Web de la **World Compliance Association**, en la sección "*Compliance* – Cuál es tu nivel de *Compliance*".

http://www.worldcomplianceassociation.com/173/nivel-compliance-compliance-en-el-tercer-sector.html#submenuhome

Este cuestionario, dividido en cuatro bloques, está compuesto por preguntas sencillas que ayudarán a las organizaciones a valorar algunos aspectos importantes en el diseño e implementación de un programa de *compliance*, además de permitir tener una primera opinión sobre los aspectos más relevantes antes de proceder con su diseño. La mayoría de las organizaciones cuentan con diversos protocolos, algunos más formales que otros, por lo que el punto de partida suele ser más avanzado del esperado inicialmente; de ahí la importancia de tomar conciencia de todo el camino recorrido, y el que aún queda por recorrer.

- El **bloque 1** hace referencia a preguntas sobre el **contexto de la organización**, es decir, a cómo se está preparando para iniciar el programa de *compliance*.
- El **bloque 2**, vinculado con el **liderazgo**, factor clave para la eficacia de cualquier programa de *compliance*, son preguntas relacionadas con el compromiso de la alta dirección para facilitar el despliegue de dicho programa.
- El **bloque 3** es el de **planificación** y contiene preguntas básicas sobre el proceso y efecto de organizar con un método que nos ayude a alcanzar los objetivos que nos hemos trazado.
- Y, por último, el **bloque 4** es el **operacional**, que está formado por preguntas relacionadas con un conjunto de tareas y procesos enfocados a la mejora continua de las organizaciones, con el fin de aumentar su capacidad para conseguir los propósitos de sus políticas y sus diferentes objetivos operativos.

CAPÍTULO 5.
RIESGOS HABITUALES EN EL TERCER SECTOR.

GUILLERMO GONZÁLEZ DE LA TORRE RODRÍGUEZ

LICENCIADO EN PERIODISMO.
MÁSTER EN "CALIDAD Y CONSULTORÍA" Y EN "DIRECCIÓN Y GESTIÓN DE ONG".
COORDINADOR DE ESTRATEGIA Y CALIDAD DE MANOS UNIDAS.
PRESIDENTE DE LA COMISIÓN DE SEGUIMIENTO DEL CÓDIGO DE CONDUCTA DE LA COORDINADORA DE ONGD Y MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO.
MIEMBRO DEL CTN SOBRE ÉTICA DE AENOR, DEL OBSERVATORIO DE RESPONSABILIDAD SOCIAL CORPORATIVA Y DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.
DOCENTE DE POSGRADO EN EL INSTITUTO DE FORMACIÓN DE INTERVENCIÓN SOCIAL.

LAURA GONZALVO DILOY

COMPLIANCE OFFICER ACREDITADA POR LA WCA.
LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS.
MÁSTER EN AUDITORÍA Y EN GESTIÓN DE ENTIDADES NO LUCRATIVAS.
CHIEF ETHICS & COMPLIANCE OFFICER DE LA FUNDACIÓN AYUDA EN ACCIÓN.
COORDINADORA DEL COMITÉ TÉCNICO DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA Y MIEMBRO DEL GRUPO DE TRABAJO DE BUEN GOBIERNO Y TRANSPARENCIA DE LA CONGD.

Una **organización del tercer sector** es una asociación o fundación de iniciativa privada y sin ánimo de lucro que aborda necesidades sociales o humanitarias. Estas causas pueden ser diversas y van desde la promoción de la salud, la cultura, el arte, el deporte o la paz, hasta la protección de la naturaleza, el respeto de los derechos humanos o la lucha contra el hambre, la pobreza y la desigualdad, entre otras. Estas organizaciones en general trabajan para alcanzar sus fines a través de la sensibilización y la denuncia, así como de la captación de fondos para la ejecución de sus proyectos, tanto en España como en aquellos otros países en los que opera. Asimismo, dentro del tercer sector también se encuentran aquellas entidades de la economía social, como cooperativas, mutualidades, sociedades laborales o empresas sociales, que persiguen una economía solidaria

Por tanto, y resumiendo mucho, los problemas más graves que puede sufrir una organización de este tipo se pueden agrupar en tres grandes temáticas:

- La escasez de fondos económicos.
- La ejecución inadecuada de proyectos.
- El descenso de voluntarios/as, activistas y seguidores/as que apoyen su causa.

DIFERENCIAS ENTRE RIESGO, PROBLEMA Y ERROR

Es importante distinguir desde el principio entre riesgo y problema, puesto que son conceptos muy diferentes que se confunden a menudo. En ese sentido, un **problema** es un hecho cierto que ya afecta negativamente a una organización. Si el listado anterior perteneciera a una organización, sería entonces una realidad que sus ingresos están acumulando un descenso continuado, por lo que esta deberá encontrar la manera de revertir dicha situación. Sin embargo, un **riesgo** es un evento, ya sea motivado por factores externos como internos, que aún no ha ocurrido pero que, si sucediera, dificultaría o impediría la consecución de los objetivos estratégicos de la organización. Un riesgo, en ese sentido, podría ser que, derivado de una crisis social y política, la actividad de una organización tuviera que ser paralizada temporalmente para no poner en riesgo la seguridad física de sus personas beneficiarias y personal contratado, o que una sentencia judicial suspendiera la ejecución de una convocatoria de subvención pública que ya le habían adjudicado.

Asimismo, es también importante distinguir entre el riesgo y el error. El **error** es una mala ejecución de algo que ya estaba previsto. Es una falta de diligencia y de profesionalidad al no prestar un servicio en los términos que se habían acordado. Es materia pura de calidad. Un ejemplo podría ser el envío de los certificados de desgravación a las personas socias a direcciones incorrectas.

CONTRIBUCIÓN DE LA GESTIÓN DE RIESGOS A LOS PROCESOS Y LOS OBJETIVOS DE LA ORGANIZACIÓN

Para resolver los grandes problemas que identificamos al inicio, se requieren metodologías más propias de la planificación, como son la reflexión estratégica o la identificación de prioridades organizativas. Resultado de las mismas, una organización debería ser capaz de poner en marcha un plan que persiga objetivos estratégicos como los siguientes:

- Incrementar los ingresos que se reciben y abrir nuevas vías de captación de fondos.
- Diseñar proyectos pertinentes y de calidad e identificar socios competentes e idóneos, así como hacer un debido monitoreo para asegurar la trazabilidad de los fondos y el impacto generado.
- Aumentar las acciones de sensibilización, comunicación, marketing y participación ciudadana.

Estos objetivos, después de que se asignen responsables, recursos y plazos, se sumarán a las grandes actividades que ya realizan las áreas de la organización, las cuales forman parte de sus procesos. Por tanto, para que la organización funcione correctamente y sea sostenible en el tiempo, podemos decir que cada área deberá contribuir al cumplimiento de los objetivos estratégicos que son de su competencia, así como gestionar sus propios procesos con un elevado nivel de calidad.

Pues bien, es aquí donde la gestión de riesgos puede ser una herramienta fundamental, porque ayuda a que esos objetivos y esos procesos se desarrollen adecuadamente. Al ser capaz de predecir eventos negativos que aún no han ocurrido, podría evitar que se ponga en peligro la realización de las actividades referidas a esos objetivos y procesos. A modo de ejemplo, citamos algunos posibles eventos, como que un/a directivo/a cometa una agresión sexual contra un/a trabajador/a de la organización, o que el sistema informático sufra un ciberataque, o que un proyecto de una escuela se derrumbe con víctimas mortales, entre otros muchos.

Para visualizar la correlación que existe entre **objetivo estratégico, proceso operativo y riesgos**, podríamos hacer una primera aproximación con el siguiente ejemplo:

OBJETIVO ESTRATÉGICO	Lograr un incremento del 25% de personas socias domiciliadas, con una cuota promedio de 10 euros al mes, a través de una campaña de telemarketing sobre las 5.000 interesadas, apoyado en una campaña de publicidad programática sostenida durante 4 semanas en 5 de los principales medios de comunicación del país, según perfil de consumidor seleccionado.
PROCESO ORGANIZATIVO	Para lograr que aumenten nuestros ingresos de donativos y personas socias domiciliadas, debemos captar la atención de la sociedad y transmitirles confianza a través de información sobre los proyectos que realizamos y las garantías de trazabilidad de los fondos, de realizar campañas intensas de marketing en medios tradicionales y digitales y de movilizar a nuestras masas sociales para que aumente la llegada de nuestros mensajes.
RIESGOS	▪ Las sedes territoriales de la organización se oponen a la campaña de telemarketing por considerarla intrusiva (riesgo organizativo). ▪ La agencia de comunicación que elaboró el perfil de consumidor no realizó un trabajo exhaustivo ni competente (riesgo de gestión de contratos). ▪ El 20% de la base de datos de personas interesadas contiene datos incompletos tras la migración de la información al nuevo sistema. Además, un 25% adicional de dichos datos no cuenta con el consentimiento requerido para el tratamiento de los mismos, por lo cual no es legítimo su uso y custodia (riesgo de transformación digital y de cumplimiento en materia de protección de datos personales). ▪ Días antes del lanzamiento de la campaña tiene lugar una crisis sanitaria sin precedentes en el país (riesgo político).

ÉXITO FRENTE A CONFIANZA EN ENTORNOS TURBULENTOS

El **éxito**, entendido como ejecutar tal cual lo que una organización se plantea y lograr todos sus objetivos, es un propósito que hoy se antoja excesivo porque los eventos externos son cada vez más numerosos, impactantes y difíciles de prever. Por esta razón, debemos advertir que la gestión de riesgos no asegura el éxito, algo en lo que entran en juego otros factores ajenos a la materia que nos ocupa. Pero sí asegura la **confianza**, un elemento, en cambio, que es imprescindible para poder operar en un entorno tan cambiante como es el de hoy en día, caracterizado por su volatilidad, incertidumbre, complejidad y ambigüedad.

Para responder a este entorno turbulento, las principales tendencias de gestión apuntan a que se debe planificar más a corto plazo y con un manejo exquisito, abundante y continuo de la información. Esto permitirá que las organizaciones sean ágiles y gestionen la incertidumbre, así como que se anticipen al futuro más inmediato para transformarse y adaptarse

continuamente a él. Es más, una de las reglas para que el enunciado de un riesgo sea correcto es que sea realista, algo que cobra la máxima importancia en estos entornos. Eso quiere decir que el plan de acción que quieras definir en tu organización para gestionar un riesgo, con el fin de establecer unas medidas que puedan prevenirlo o mitigarlo cuando ocurra, debe aludir a acciones que formen parte de tus capacidades.

El ejemplo de un riesgo de ese tipo lo estamos teniendo precisamente en la actualidad con la crisis global sin precedentes que está causando la pandemia del Covid-19. Seguramente, la mayoría de las organizaciones no tendrían contemplado este posible riesgo en sus modelos de gestión, porque era un evento que se escapaba de nuestra imaginación, pero una vez se ha materializado, deberán incorporarlo siendo conscientes de la capacidad que tenemos para poder gestionarlo. Al estar motivado por factores completamente externos a la organización, tenemos nula capacidad para reducir su probabilidad de ocurrencia en el futuro, pero sí que la tenemos a la hora de mitigar el impacto en nuestra organización. ¿Cómo? Diseñando un plan de contingencia para situaciones de esta índole donde se definan los protocolos a seguir internamente con el fin de asegurar la continuidad de la actividad y de velar por la seguridad de nuestros/as empleados/as, voluntarios/as y beneficiarios/as, entre otros.

IDENTIFICACIÓN DE RIESGOS

El presente capítulo de la guía se ocupa de la **identificación de riesgos**, fase fundamental en el proceso de gestión de riesgos, ya que la calidad con la que esta se haga determinará la eficacia del resto del proceso, de modo que aquellos riesgos que no sean contemplados inicialmente serán asumidos por la organización.

Para que la identificación de riesgos sea útil y efectiva, es fundamental llevar a cabo un análisis previo del contexto de la organización, fase debidamente desarrollada en el anterior capítulo de la guía. Asimismo, para su correcto diseño, los riesgos deben ser específicos, medibles, realistas, ubicados en el tiempo y, lo más importante, alineados con los objetivos estratégicos de la organización. Para el debido levantamiento de la taxonomía de riesgos, cada uno deberá ir acompañado de una breve descripción de cómo podría materializarse el riesgo en cuestión, las causas y los agentes generadores internos y/o externos, así como el efecto sobre la organización. Así, un ejemplo de riesgo bien enunciado podría ser el siguiente:

"Una persona contratada del socio local "X" con el que colaboramos para la ejecución de un proyecto de la AECID por importe de 430.000 euros en Guatemala, importe que supone el 20% de los ingresos de nuestra organización, ha sustraído parte o la totalidad de esos fondos. Sin embargo, las personas máximas responsables del socio local no asumen ninguna responsabilidad dado que no hemos firmado ningún contrato entre las partes que contemple dicha situación, ni tampoco solicitamos en

su día documentación que acreditara la titularidad real de la cuenta bancaria a la cual estábamos transfiriendo los fondos".

En este ejemplo, el riesgo sería "una indebida gestión del socio local, desde la formalización de la relación hasta el debido seguimiento a realizar". La causa sería "no haber identificado antes la titularidad real de la cuenta bancaria a la que transferir los fondos, ni haber firmado un contrato con el socio local donde se recojan sus obligaciones". El evento sería la "comisión del fraude por parte de la persona contratada del socio local". El impacto sería la "devolución de 430.000 euros, lo que supone el 20% de los ingresos de la organización, al no poder demostrar la trazabilidad de los fondos ante la AECID, lo que tendría un elevado impacto en nuestro presupuesto, así como la pérdida de imagen y credibilidad ante dicho organismo para futuras convocatorias".

El riesgo es específico porque alude a actividades concretas como documentos y controles a realizar en una *due diligence*, referidos a un socio local determinado, así como a proyectos e importes de dinero determinados. Es medible porque se podría establecer un indicador y una fuente de verificación que comprobaría cuánto ha ocurrido de aquello que se pretende prevenir. Es atribuible porque la titularidad real y el contrato los puede exigir la organización como condición para la aprobación del proyecto y la asignación de los fondos correspondientes. Es realista porque las capacidades que hay que poner en juego son asumibles por las entidades implicadas. Y, por último, es atribuible en el tiempo porque hace referencia a la fase anterior a que se le envíen los fondos a ese socio local.

A continuación, presentamos a modo de ejemplo algunos de los riesgos más habituales y críticos en el tercer sector, organizados según la clasificación propuesta en el capítulo anterior de la guía. Sin embargo, cada organización puede clasificarlos y/o definirlos de acuerdo a sus propias necesidades:

Riesgos estratégicos		
Riesgo	**Descripción**	**Justificación**
Posicionamiento estratégico	Ausencia de actividades de promoción tanto por inexistentes como por irrelevantes y/o inadecuadas, que permitan obtener una ventaja con el resto de organizaciones del tercer sector.	El tercer sector se caracteriza por su atomización, existiendo numerosas organizaciones con fines muy similares, por lo que crear una marca y un valor diferencial del resto de organizaciones es fundamental.
Innovación	Dificultad de transformación y/o adaptación a los cambios en el entorno, lo que repercutiría en una pérdida de oportunidades o de posicionamiento.	Teniendo en cuenta el contexto tan dinámico y competitivo en el que operamos, una indebida gestión del cambio para adaptarse a la evolución del mercado y de las expectativas de los grupos de interés puede llevar a una organización a una situación muy crítica.

Riesgos estratégicos		
Riesgo	**Descripción**	**Justificación**
Organizativo	Falta de alineación de la estructura organizativa y/o de las personas a las prioridades estratégicas de la organización, a una inadecuada y/o insuficiente gestión y acompañamiento de las personas, y/o a una falta de liderazgo por parte de responsables de la gestión de la organización.	En gran parte de las organizaciones del tercer sector, los recursos humanos tienden a estar tensionados con el fin de mantener una ratio razonable entre el porcentaje de financiación destinada a la intervención y el destinado a la estructura de la propia organización. Por ello, es fundamental que exista una debida gestión de las personas, para que estén motivadas y alineadas con los objetivos estratégicos, así como para asegurar que cuentan con las competencias técnicas y personales requeridas para el perfil. En el caso de organizaciones con delegaciones en diferentes territorios, tanto nacionales como internacionales, también es relevante un debido seguimiento para tratar de minimizar las discrepancias que puedan surgir y que impidan una correcta y eficaz implementación de los planes y medidas corporativas.
Económico	Dificultad para la consecución de los objetivos financieros debido a una menor capacidad económica de nuestros actuales y/o potenciales donantes, así como a una reducción de convocatorias y/o incremento de las exigencias vinculadas a las mismas por organismos públicos y/o privados a nuestra causa.	Los entornos en los que nos movemos son muy volátiles, siendo fundamental la capacidad de reacción de las organizaciones para adaptar su modelo de financiación a los procesos, personas y objetivos estratégicos, ya que los factores externos que pueden motivar una reducción de los ingresos son múltiples: cambios de políticas públicas o aumento de la tasa de desempleo, entre otras.

Riesgos operativos		
Riesgo	**Descripción**	**Justificación**
Ciberseguridad	Ataques externos a la seguridad de los sistemas que supongan el acceso no autorizado a información confidencial o incapacidad para el correcto funcionamiento de los mismos.	Teniendo en cuenta el uso exponencial que hacemos de la red, son cada vez más los ataques de seguridad que se están produciendo con un impacto directo en la continuidad de la operativa de las organizaciones y que pueden generar brechas de seguridad en lo que se refiere a los datos personales que tratamos.

Riesgos operativos		
Riesgo	**Descripción**	**Justificación**
Atención a terceros	Inadecuada gestión de las consultas, sugerencias, quejas y/o denuncias remitidas por un tercero y/o ausencia de canales de comunicación eficaces que permitan una adecuada canalización y resolución de éstas.	La criticidad de este riesgo viene más bien determinada por la pérdida de oportunidad de identificar conductas inadecuadas y/o contrarias a los estándares éticos de la organización, si tenemos en cuenta que un canal de denuncias eficaz es la herramienta más potente para la detección de este tipo de conductas.
Formulación y seguimiento de los proyectos	No alcanzar el impacto deseado con nuestra intervención y/o que no sea sostenible en el tiempo, bien porque los proyectos no respondan a las necesidades reales de las comunidades, o bien porque no estén adaptados a la cultura local, no cuenten con su respaldo y/o apropiación y/o no se haya realizado el monitoreo adecuado.	Conocer las necesidades y expectativas de las personas beneficiarias, así como las particularidades del entorno, es fundamental para asegurar que la intervención que estamos llevando a cabo es eficaz y genera cambios en el entorno. Adicionalmente, un debido monitoreo de los proyectos permite anticiparse y/o gestionar imprevistos que pudieran condicionar la consecución de logros planificados.
Entorno político	Sucesos graves que alteran el normal funcionamiento de un país, como pueden ser conflictos armados, revueltas políticas, terrorismo local o fenómenos naturales como inundaciones, terremotos, sequías, incendios o pandemias, lo cual afectaría total y/o parcialmente a la continuidad de las actividades.	Este riesgo adquiere mayor relevancia en aquellas organizaciones que trabajan en el ámbito de la cooperación al desarrollo y/o la ayuda humanitaria, por su presencia en países en los que el contexto económico, político y social es altamente dinámico. Además, su criticidad también está condicionada a que suele estar motivado por factores externos para los que nuestro nivel de gestión suele ser muy limitado.
Seguridad física y laboral	Exposición incrementada en el terreno de los/as trabajadores/as en términos de riesgos laborales, así como también de seguridad al trabajar en contextos peligrosos (daños, robos, amenazas, secuestros y otras acciones perjudiciales a la integridad física).	Igual que en el riesgo anterior, este adquiere mayor relevancia en aquellas organizaciones que trabajan en el ámbito de la cooperación al desarrollo y/o la ayuda humanitaria, ya que su personal está expuesto a contextos muy frágiles, siendo fundamental disponer de protocolos que aseguren su salvaguarda.
Identificación y monitoreo de socios locales	Ausencia de procedimientos que aseguren la idoneidad de las organizaciones con las colaboramos, así como el debido monitoreo de las obligaciones y/o compromisos alcanzados.	Gran parte de las organizaciones colaboran con terceros para implementar la intervención, siendo fundamental realizar una due diligence de forma previa para evitar una gestión inadecuada o no alineada a nuestras prioridades estratégicas, así como disponer de mecanismos que permitan hacer un monitoreo periódico de su gestión.

Riesgos operativos		
Riesgo	**Descripción**	**Justificación**
Transformación digital	Ineficiencia en los procesos y/o cuestionamiento sobre la fiabilidad de la información, derivada del empleo de tecnologías de información y comunicación que no responden a las necesidades de la organización, a un mal uso de las mismas y/o a la existencia de procesos manuales.	En nuestras organizaciones manejamos una gran cantidad de datos, bien para rendir cuentas a terceros, o bien para sustentar la toma de decisiones, siendo la calidad de los mismos cuestionable si los sistemas que usamos no son adecuados, lo que puede tener implicaciones de diferente índole. La limitación de recursos nos lleva a contar con procesos excesivamente manuales o a disponer de sistemas que no se adecúan a nuestras necesidades.
Cumplimiento		
Riesgo	**Descripción**	**Justificación**
Gestión de contratos	Incumplimiento de las obligaciones y/o compromisos que hemos adquirido con terceros (donantes, organismos públicos, empresas colaboradoras, proveedores, voluntariado, socios locales, etc.), así como de estos frente a nuestra organización, con motivo de una inadecuada gestión de los recursos, selección y/o monitoreo posterior de los terceros.	El incumplimiento de nuestras obligaciones y compromisos puede derivar en sanciones, multas y/o tener un impacto directo en la imagen de nuestra organización. Por ejemplo, si no rendimos cuentas en los términos requeridos por una empresa que nos ha concedido una subvención y/o no cumplimos con nuestros compromisos, esta nos podría solicitar la devolución de los recursos y se verían muy mermadas nuestras posibilidades de ser la organización seleccionada en una futura convocatoria. Esta situación podría venir motivada por un incumplimiento de los plazos por parte de un proveedor, ya que dicho proyecto se centraba en la construcción de unos pozos, los cuales no han sido finalmente construidos en tiempo y/o con una calidad aceptable.
Marco regulatorio	Asociado a la incertidumbre de los posibles cambios regulatorios en los países donde las organizaciones están presentes, los cuales suelen estar expuestos a una elevada fluctuación, y el consiguiente incumplimiento de las obligaciones a las que estamos sujetos bien por desconocimiento y/o falta de recursos.	Es importante que las organizaciones estén al día de las disposiciones legales a las que están sujetas, ya que podría generarse un efecto disruptivo de la organización, con especial atención a las leyes más recientes.

Cumplimiento		
Riesgo	**Descripción**	**Justificación**
Gobernanza y ética	Comportamientos no éticos y/o ilícitos por parte de terceros vinculados a la organización.	Ninguna organización se exime de este riesgo, tanto por conductas por parte de colectivos a nivel interno (plantilla, voluntariado, prescriptores, etc.) como a nivel externo (empresa colaboradora, plataforma a la que pertenecemos, socio local, etc.). Por ello, es fundamental contar con medidas de prevención para reducir la probabilidad de que este riesgo se materialice -cobrando especial importancia los procesos de selección-, así como para reducir su impacto, dotando a la organización de recursos que le permitan adoptar medidas disciplinarias con estos terceros, para así proteger su reputación.
Protección de la infancia	Incumplimiento de la normativa local en materia de protección de la infancia y/o los principios recogidos en la "Convención sobre los Derechos de la Niñez", así como la comisión de delitos relacionados con menores de edad por parte de personas vinculadas a la organización.	Aunque este riesgo podría englobarse dentro del anterior, su importancia amerita tener un espacio propio principalmente en aquellas organizaciones que trabajan en infancia ya que, en estas, contar con protocolos internos para proteger el interés superior del menor es un deber.

Riesgos reputacionales		
Riesgo	**Descripción**	**Justificación**
Imagen global de las ONG	Comportamientos no éticos y/o la comisión de delitos por parte de otras organizaciones y que repercuten en la imagen del tercer sector.	En el tercer sector este riesgo adquiere una criticidad especial dado el efecto dominó al que estamos expuestos, por la debilitación de manera generalizada de la confianza de terceros hacia la gestión de las organizaciones del tercer sector y por el menor nivel de gestión que podemos asumir al estar motivado por factores externos a la propia organización.
Trasparencia y rendición de cuentas	Insatisfacción y/o desconocimiento por parte de los grupos de interés de la organización con motivo de una rendición de cuentas que no tiene en cuenta sus expectativas y/o necesidades.	En nuestro sector, como en cualquier otro, es fundamental la comunicación interna y externa, es decir, ser capaces de transmitir qué y cómo lo hacemos para así conectar con nuestros grupos de interés y lograr movilizarlos.

CAPÍTULO 6.
MODELO DE GESTIÓN DE RIESGOS INTEGRAL. MAPA DE RIESGOS Y CONTROLES.

ALBERT SALVADOR

LICENCIADO EN CC ECONÓMICAS Y EMPRESARIALES.
AUDITOR INTERNO CERTIFICADO POR EL IIA (THE INSTITUTE OF INTERNAL AUDITORS).
ESPECIALISTA EN FRAUDE INTERNO, FORENSIC Y PREVENCIÓN DE BLANQUEO DE CAPITALES.
SECRETARIO GENERAL Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA WCA.

LAURA GONZALVO DILOY

COMPLIANCE OFFICER ACREDITADA POR LA WCA.
LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS .
MÁSTER EN AUDITORÍA Y EN GESTIÓN DE ENTIDADES NO LUCRATIVAS .
CHIEF ETHICS & COMPLIANCE OFFICER DE LA FUNDACIÓN AYUDA EN ACCIÓN.
COORDINADORA DEL COMITÉ TÉCNICO DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA Y
MIEMBRO DEL GRUPO DE TRABAJO DE BUEN GOBIERNO Y TRANSPARENCIA DE LA CONGD.

"El mapa de riesgos es un elemento clave en el sistema de gestión de compliance de las organizaciones y nos ayuda en el seguimiento de riesgos, controles y planes de acción"

QUÉ ES UN MAPA DE RIESGOS

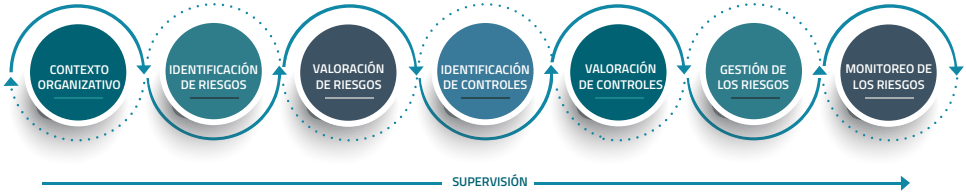
Un mapa de riesgos es una herramienta que ayuda a las organizaciones a identificar y priorizar aquellos riesgos a los que está expuesta, teniendo en cuenta el contexto de la organización y que este es dinámico en el tiempo.

Así, el primer paso es tomar conciencia de los riesgos a los que nos enfrentamos y, el segundo, es poner la atención en la gestión de aquellos riesgos que sean más críticos y que puedan cuestionar la consecución de nuestros objetivos estratégicos y, por tanto, nuestro fin misional, ya que la capacidad y recursos de la organización son limitados.

La representación gráfica de la priorización se suele realizar a través de un mapa de riesgos o un mapa de calor, en el que quede reflejada la importancia de cada riesgo en función de la probabilidad y el impacto o daño que tendría para la organización en caso de que el riesgo se materializase.

CONSEJOS SOBRE CÓMO HACERLO

Las fases establecidas para la elaboración de un mapa de riesgos se pueden clasificar en:



A continuación, se definen cada una de estas fases:

1. DEFINICIÓN DEL CONTEXTO

Entendemos por contexto todos aquellos aspectos internos y externos de los que depende que una organización pueda desarrollar su propia actividad, siendo entre otros:

Estructura de la organización. En este punto se recomienda la elaboración de un **mapa de procesos**, entendiendo por procesos al conjunto de actividades mutuamente relacionadas que utilizan entradas para proporcionar un resultado previsto, en el que un cliente interno o externo va secuencialmente recibiendo esos resultados. Se diferencia de la estructura funcional porque no es vertical, sino horizontal, y porque, respetando el organigrama de áreas y departamentos, va más allá de él. Cabe distinguir entre:

- Procesos estratégicos: constituyen guías y directrices para los procesos misionales y de apoyo. Ejemplos: planificación estratégica, relaciones institucionales, filantropía, financiación pública, alianzas estratégicas y rendición de cuentas, entre otros.

- Procesos misionales: responden a la misión o fin de la organización y tienen impacto en el destinatario final. Ejemplos: gestión de proyectos de desarrollo, de acción social y/o de ayuda humanitaria, entre otros.

- Procesos de apoyo: dan soporte a los procesos misionales. Ejemplos: selección y gestión del personal contratado y voluntariado, gestión de las finanzas y la contabilidad, asesoría jurídica y sistemas, entre otros.

Adicionalmente, se deberá asignar una persona responsable de cada proceso organizativo, quienes tendrán un rol fundamental en la gestión de riesgos.

Objetivos estratégicos de la organización, ya que la gestión de riesgos debe estar totalmente alienada con los mismos.

Grupos de interés de la organización, tanto internos como externos, con el fin de determinar cuáles son sus expectativas y necesidades respecto a nuestra organización.

Entorno competitivo y geográfico en el que opera la organización

Marco legislativo al que está sujeto la organización.

2. IDENTIFICACIÓN DE RIESGOS

Esta fase consiste en llevar a cabo una identificación de los riesgos significativos que pudieran afectar el logro de los objetivos estratégicos de la organización y, por tanto, de su fin misional, así como los agentes generadores del riesgo, las causas y los efectos en caso de materializarse.

Para ello, se deben utilizar metodologías de recolección de información, siendo de gran utilidad las entrevistas individuales y grupales con las personas responsables de los procesos organizativos, en las que poder realizar lluvias de ideas e indagar sobre riesgos materializados en el pasado.

La identificación de los riesgos debe realizarse con una periodicidad mínima anual, para así actualizar la taxonomía y poder confirmar aquellos que siguen siendo significativos, eliminar los que ya no apliquen e incorporar los nuevos emergentes, puesto que, como ya se remarcó al principio, el contexto en el que opera la organización y sus necesidades son dinámicos.

RIESGO INHERENTE Y RIESGO RESIDUAL

Asimismo, es conveniente distinguir desde el principio entre el concepto de inherente y el de residual. Los riesgos son sucesos que aún no han ocurrido pero que se identifican previamente y de forma regular con el fin de gestionarlos adecuadamente para, o bien prevenir su ocurrencia, o bien en el caso de que se materialicen, reducir su impacto en la consecución de nuestros objetivos estratégicos. En ese sentido, todas las organizaciones por el hecho de existir tienen riesgos. La cuestión es ser consciente de cuáles son para así priorizarlos. Esos riesgos varían según sea el tipo de organización, bien por la naturaleza de su actividad, por su presencia geográfica o por el volumen y la complejidad de sus operaciones, entre otras. Estos riesgos de base, que se identifican antes de considerar cualquier control, son los que se llaman inherentes.

Por otro lado, el riesgo residual será el resultado de restar, al riesgo inherente, el efecto de los controles que tiene la organización en ese momento implantados, siendo el principal objetivo que dicho nivel de riesgo se sitúe por debajo del máximo nivel de riesgo que está dispuesta a asumir la organización (tolerancia al riesgo).

A lo largo de este capítulo, explicaremos cómo calcularemos el riesgo residual asociado a cada uno de los riesgos inherentes que previamente hemos identificado, en base a una metodología muy específica.

CATÁLOGO DE RIESGOS

Para definir la taxonomía de riesgos inherentes de una organización, se puede hacer en base a diferentes categorías, ya que no existe una estandarizada. A continuación, se muestra una posible clasificación:

- **Riesgos estratégicos:** asociados con los objetivos clave a largo plazo y que surgen derivados de la posición estratégica que la organización toma en el entorno en que desarrolla su actividad. Por tanto, pueden surgir de las acciones de otros grupos de interés, de las decisiones estratégicas y de los cambios en el entorno competitivo.

- **Riesgos operativos:** asociados con las operaciones habituales que se llevan a cabo en el desarrollo de la actividad de la organización.

- **Riesgos financieros:** relacionados con fluctuaciones adversas en los mercados financieros o con los procesos, técnicas e instrumentos utilizados para la gestión de las finanzas de la organización, cosa que revierte en el manejo eficiente y transparente de los recursos financieros y que podría conllevar problemas en la estructura financiera de la organización.

- **Riesgos de cumplimiento:** incertidumbre sobre el cumplimiento de los requisitos legales, contractuales y del propio marco normativo interno de la organización.

- **Riesgos reputacionales:** asociados a la imagen y reputación de la organización, consecuencia de actuaciones poco éticas en el seno de esta o de terceros con los que se relaciona.

3. VALORACIÓN DE LOS RIESGOS

Para la valoración de los riesgos, nos apoyaremos en una matriz de riesgos de doble entrada:

- Probabilidad/frecuencia.

- Impacto/severidad.

Las matrices más utilizadas son las de 3x3 y las de 5x5, siendo estas últimas las que se usan con más frecuencia.

PROBABILIDAD INHERENTE

Se entiende por probabilidad inherente la probabilidad de que el riesgo se concrete en un suceso cierto antes de considerar cualquier control o acción mitigadora. Para ello, se considerarán factores como la ocurrencia en la organización de ese riesgo en el pasado, su frecuencia en las organizaciones del tercer sector, la complejidad del riesgo y el número de personas involucradas en la revisión y aprobación del proceso, entre otros factores.

Evaluada la probabilidad de ocurrencia, esta se categoriza en función de la matriz utilizada. En una matriz de 5x5, tendríamos los siguientes tramos, los cuales pueden ser adaptados a las necesidades de la organización:

Tramo	Descripción
Severo	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad de que se materialice (90% a 100%).
Probable	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre un 66% a un 89% de seguridad de que se materialice.
Posible	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre un 31% a un 65% de seguridad de que se materialice.
Improbable	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre un 11% a un 30% de seguridad de que se materialice.
Rara	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene una seguridad por debajo del 11% de que se materialice.

IMPACTO INHERENTE

Se entiende por impacto inherente al daño que supondría para los objetivos estratégicos de la organización que el riesgo se concretara en un suceso cierto, antes de considerar cualquier control o acción mitigadora.

Para ello, se considerarán los diferentes tipos de impacto, tales como económicos (reducción

de ingresos, aumento de gastos y/o sanciones por incumplimientos legales), operacionales (reducción del rendimiento de la actividad y/o retrasos en la misma) y reputacionales (deterioro del valor de la marca, y/o pérdida de la imagen y confianza).

Al igual que con la probabilidad de ocurrencia, una vez evaluado el impacto de que un riesgo se materialice para cada una de las tipologías previamente definidas, este se categoriza.

En una matriz de 5x5 tendríamos los siguientes tramos, los cuales pueden ser adaptados a las necesidades de la organización:

Tipo de impacto	Tramo	Descripción
Económico	Severo	Impacto superior a XX euros.
	Mayor	Impacto entre XX y XX euros.
	Moderado	Impacto entre XX y XX euros.
	Menor	Impacto entre XX y XX euros.
	Insignificante	Impacto entre XX y XX euros.
Operacional	Severo	Implicaría el incumplimiento, retraso o cancelación de más del 10% de nuestras actividades y proyectos planificados en el ejercicio.
	Mayor	Implicaría el incumplimiento, retraso o cancelación de entre un 5 y un 10% de nuestras actividades y proyectos planificados en el ejercicio.
	Moderado	Implicaría el incumplimiento, retraso o cancelación de entre un 2,5% y un 5% de nuestras actividades y proyectos planificados en el ejercicio.
	Menor	Implicaría el incumplimiento, retraso o cancelación de entre un 1% y un 2,5% de nuestras actividades y proyectos planificados en el ejercicio.
	Insignificante	Implicaría el incumplimiento, retraso o cancelación de menos de un 1% de nuestras actividades y proyectos planificados en el ejercicio.
Reputacional	Severo	Deterioro de la imagen de la organización que reduce significativa y permanentemente la captación de fondos de forma global.
	Mayor	Deterioro de la imagen de la organización que reduce significativamente y de forma temporal la captación de fondos de forma global.
	Moderado	Deterioro de la imagen de la organización que reduce de forma puntual la captación de fondos de forma global.
	Menor	Deterioro de la imagen de la organización que reduce de forma puntual la captación de fondos en una zona geográfica concreta.
	Insignificante	Deterioro puntual de la imagen de la organización que provoca una reducción de la captación de fondos de forma muy residual en una zona geográfica concreta.

Adicionalmente, la organización puede optar por ponderar cada uno de los tipos de impacto en función de sus prioridades estratégicas.

En base a estas consideraciones, el cálculo del **impacto inherente global (IIG)** para cada uno de los riesgos identificados se formularía de la siguiente manera, teniendo en cuenta las ponderaciones que detallamos a continuación:

Adicionalmente, la organización puede optar por ponderar cada uno de los tipos de impacto en función de sus prioridades estratégicas.

En base a estas consideraciones, el cálculo del impacto inherente global (IIG) para cada uno de los riesgos identificados se formularía de la siguiente manera, teniendo en cuenta las ponderaciones que detallamos a continuación:

IIG= valor impacto económico x 50% + valor impacto operacional x 25% + valor impacto reputacional x 25%

Finalizada esta fase, obtendremos el **riesgo inherente** que, en función de la probabilidad e impacto, y usando la matriz de riesgos, lo podremos clasificar en: muy bajo, bajo, medio, alto o crítico.

Riesgo inherente = probabilidad inherente x impacto inherente global

PROBABILIDAD							
	5	CASI CIERTO	MEDIO	ALTO	ALTO	CRÍTICO	CRÍTICO
	4	PROBABLE	BAJO	MEDIO	ALTO	ALTO	CRÍTICO
	3	POSIBLE	BAJO	MEDIO	MEDIO	ALTO	ALTO
	2	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	1	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
			INSIGNIFICANTE	MENOR	MODERADO	MAYOR	SEVERO
			1	2	3	4	5
			IMPACTO				

(GRÁF.1)

En cualquier caso, cabe destacar que las categorías de impactos y su ponderación, así como las categorías de tramos y definición de los mismos, se adaptarán a las necesidades y características de la organización.

4. IDENTIFICACIÓN DE CONTROLES

De manera análoga a la fase de identificación de riesgos, mediante el conocimiento y análisis de la organización, preferiblemente a través de sus procesos documentados, se procede a la identificación de los controles. Estos controles permitirán, en última instancia, o bien reducir la probabilidad de ocurrencia de un suceso o, si este se produce, minimizar su impacto.

Estos controles son muy variados y se ajustan mucho a las características y necesidades de cada riesgo, pero, en general, consisten en pautas de trabajo vinculadas a los procesos de la organización, que deseablemente deberían estar recogidas en protocolos o procedimientos internos, con el fin de asegurar su debido funcionamiento.

Un ejemplo podría ser, para prevenir y/o mitigar el posible riesgo de fraude al que está expuesta una organización, disponer de, entre otros:

- Unos criterios de selección de personas vinculadas a la organización que garanticen altos estándares éticos, atendiendo a criterios de idoneidad y de honorabilidad.

- Un código de conducta que recoja los estándares éticos que se esperan de las personas vinculadas a dicha organización y que incluya un régimen disciplinario al que poder acogerse en caso de identificar una conducta contraria al mismo.

- Un canal de denuncias realmente eficaz y accesible a todos nuestros grupos de interés como herramienta fundamental para destapar este tipo de conductas.

En esta fase, es importante únicamente considerar los controles que la organización ya tiene implementados, de forma que una vez se concluya el análisis y prioricemos los riesgos críticos sobre los que centrar nuestra gestión, será el momento de identificar controles adicionales y/o planes de acción que se van a tener que diseñar e implementar en el futuro para reducir el nivel de riesgo hasta un nivel aceptable por la organización.

5. VALORACIÓN DE CONTROLES

Una vez identificados los controles, se determinará el nivel de gestión de la organización, es decir, se evaluará la eficacia de los mismos en base a los siguientes tramos, que pueden ser adaptados a las necesidades de la organización:

- **Insuficiente:** los controles existentes son inadecuados o no es posible el control del riesgo, al estar condicionado en su totalidad por factores externos.

- **Medio:** los controles existentes son adecuados, pero no suficientes, ya que son mejorables.

- **Suficiente:** los controles existentes son suficientes.

Así, el grado de efectividad del control determinará el grado de reducción que proporciona ese control sobre un determinado riesgo. Es decir, si al valorar un control existente en la organización vemos que es insuficiente, eso significará que tiene poca efectividad para reducir la probabilidad de ocurrencia y/o el impacto de dicho riesgo.

VULNERABILIDAD

El nivel de vulnerabilidad determina el factor reductor considerado por la implantación y aplicación de los controles previamente identificados, pudiendo oscilar su valor entre 0 y 1. Por tanto, a mayor nivel de gestión, es decir, de control del riesgo, menor nivel de vulnerabilidad.

De esta manera, se definirá el criterio a aplicar para uno de los tramos, los cuales pueden ser adaptados a las necesidades de la organización, pudiendo ser los siguientes:

- Cuando el nivel de gestión sea insuficiente, se mantendrá el impacto y la probabilidad inherente del riesgo, es decir, se multiplicará por 1.

- En el caso de que el nivel de gestión sea medio, se corregirá el impacto y/o la probabilidad un 20%, es decir, se multiplicará por 0,8.

- En el caso de que el nivel de gestión sea suficiente, se reducirá el impacto y/o la probabilidad un 40%, es decir, se multiplicará por 0,6.

De esta forma, volveremos a calcular el riesgo al que está sometida la organización, pero esta vez considerando el nivel de vulnerabilidad actual una vez valoremos los controles disponibles en la organización, obteniendo de esta forma el **riesgo residual**.

Riesgo residual = riesgo inherente global * nivel de vulnerabilidad

6. GESTIÓN DE LOS RIESGOS

Las fases previas de valoración de los riesgos y controles deben realizarse con una periodicidad mínima anual, siendo recomendable que sean realizadas por las personas responsables de los procesos organizativos, en base a un cuestionario cuyos resultados serán posteriormente agregados y analizados por el órgano de cumplimiento de la organización, de forma que la valoración sea lo menos sesgada posible y trasversal a toda la organización.

PRIORIZACIÓN

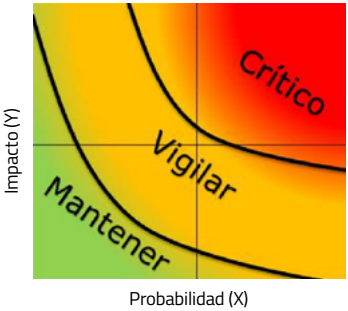
Una vez calculado el riesgo residual de todos los riesgos que forman parte de nuestro catálogo inicial, se determinará la importancia del riesgo (criticidad) utilizando la siguiente fórmula:

$$\textbf{Criticidad} = \sqrt{\text{Impacto residual x Probabilidad residual}}$$

En base a los resultados arrojados, los riesgos podrán ser clasificados según los siguientes tramos, que podrán ser adaptados a las necesidades de cada organización:

Categoría	Valor	Descripción
Riesgo crítico	Criticidad superior a 6	Aquellos cuyo impacto y probabilidad residual se sitúan en el rango más alto de evaluación, superando la tolerancia al riesgo establecido, o aquellos que considere oportuno el órgano de gobierno, por su especial relevancia en la operativa de la organización.
Riesgo a vigilar	Criticidad entre 4 y 6	Aquellos cuyo impacto y probabilidad residual se sitúen en un nivel intermedio de evaluación, cercano a la tolerancia máxima permitida.
Riesgo a mantener	Criticidad inferior a 4	Aquellos cuyo impacto y probabilidad residual se sitúen en el nivel más bajo de evaluación, dentro del nivel de tolerancia al riesgo establecido.

La representación gráfica de la priorización se realiza a través de un **mapa de riesgos** o un mapa de calor que refleja la importancia o criticidad de cada riesgo:



En base a esta categorización, el órgano de gobierno deberá seleccionar aquellos riesgos en los que enfocar el correspondiente monitoreo, con el fin de optimizar los recursos en la gestión de aquellos riesgos más críticos.

Una vez estos hayan sido seleccionados, se deberá asignar una **persona propietaria del riesgo**, siendo esta la responsable del proceso al que está mayoritariamente relacionado.

RESPUESTA A LOS RIESGOS

Las opciones para el tratamiento de los riesgos evaluados pueden consistir en:

- Aceptar el riesgo, lo que implica no hacer nada, ya sea porque no se puede dado el carácter del riesgo o porque este se encuentra dentro de los niveles aceptables.
- Evitar el riesgo, es decir, no proceder con la actividad que genera el riesgo.
- Reducir el riesgo, lo que implica implementar acciones dirigidas a reducir el impacto o la vulnerabilidad del riesgo hasta un nivel aceptable.
- Transferir el riesgo a terceros, cambiando la responsabilidad sobre el mismo hacia un externo a la organización.

El tratamiento de riesgos se define en un **plan de acción**, donde se detalla la respuesta a dar a los riesgos que se han priorizado, así como las medidas para que se mantengan en umbrales aceptables y, por tanto, no superen el apetito de riesgo establecido por el órgano de gobierno de la organización, entendiendo este como el riesgo que está dispuesto a asumir una organización en sus actividades.

En el plan de acción, se establecen los controles ya existentes y aquellas mejoras necesarias para mejorar el nivel de gestión, puesto que es posible que se identifiquen debilidades en nuestro entorno de control.

Para su correcta implementación, es importante la asignación de responsables para cada control, el establecimiento de un cronograma donde se defina la periodicidad de cada control y la planificación de los recursos humanos y técnicos necesarios para la implementación de las medidas.

De forma adicional, la organización debe definir, para aquellos riesgos que se han priorizado, indicadores cuantitativos y/o cualitativos (KPI de riesgo) que permiten monitorizar la posible materialización de los riesgos, para los cuales se establecerá una tolerancia. Así, en caso de que un indicador supere la tolerancia fijada, será el propietario del riesgo la persona que deberá analizar las causas y proponer un plan de contingencia para dar respuesta a dicha situación, informando debidamente al órgano de cumplimiento.

El plan de acción deberá ser elaborado por las personas propietarias de riesgos previamente asignadas, siendo estos debidamente reportados al órgano de cumplimiento para contar con una visión corporativa y ser aprobados por el órgano de gobierno de la organización.

7. MONITOREO DE LOS RIESGOS

El monitoreo de riesgos es una parte clave de cualquier plan de gestión de riesgos de toda organización, ya que valida el correcto funcionamiento del modelo. Para ello, las personas propietarias de los riesgos deberán reportar el plan de acción, al menos semestralmente, al órgano de cumplimiento para su supervisión.

8. ACTUALIZACIÓN

Para garantizar que el sistema de gestión de riesgos sea sólido y eficaz, la revisión se debe realizar al menos una vez al año, o con mayor frecuencia en caso de cambios significativos en la organización, en su entorno, etc. De esta forma, nos aseguramos que la gestión de riesgos que estamos llevando a cabo está adaptada al contexto actual de la organización.

9. SUPERVISIÓN

El órgano de cumplimiento, deberá informar al órgano de gobierno, con una periodicidad al menos anual, sobre el funcionamiento del sistema para la gestión de los riesgos, tanto en lo que se refiere al diseño como a la implementación y a la eficacia de los controles y demás acciones y planes puestos en marcha.

Para ello, será necesario que se lleven a cabo revisiones continuas que deberían estar recogidas en el plan de auditoría interna anual, cuyo alcance tenga en cuenta los aspectos mencionados anteriormente.

El alcance y funcionamiento de esta supervisión, y la propia composición de dicho órgano de cumplimiento se tratan con más detalle en los capítulos 8 y 10 de la presente guía.

CAPÍTULO 7.
POLÍTICA COMPLIANCE.

JUAN ARRESE ROMERO-RATO

ABOGADO COMPLIANCE CORPORATIVO Y DE DIVERSIDAD.
ÁRBITRO DE LA ASOCIACIÓN EUROPEA DE ARBITRAJE A.E.A.
ASOCIADO A LA WCA Y MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR.
CONSEJERO DE ENTIDAD TERCER SECTOR ENVERA EMPLEO.
CONSULTOR EN COMPLIANCE Y POLÍTICAS DE IGUALDAD Y DIVERSIDAD.

NOCIONES DE POLÍTICA DE COMPLIANCE

El ámbito de cumplimiento en las organizaciones afecta al conjunto de normas impuestas obligatoriamente en función de la actividad económica y/o mercado donde se opera, así como a las asumidas voluntariamente, configurando el término de ***compliance*** que se refiere, en general, al cumplimiento de la legislación aplicable y de la normativa interna de la propia organización.

Por tanto, un **programa de *compliance*** será el diseño, implantación y monitorización de la normativa y políticas internas que deben cumplir las organizaciones, con objeto de impulsar, prevenir y garantizar las prácticas de negocio y las estructuras organizativas que fomenten el respeto a las premisas de ética, equidad y legalidad, constituyendo la base del desarrollo y sostenibilidad del negocio, en términos legales, económicos y reputacionales.

El volumen y la complejidad de las normas donde se proyecta la actividad afectan directamente al modelo de negocio responsable de cada organización.

La pluralidad de normas de ámbitos diversos promueve la maximización de sinergias para coordinar y gestionar correctamente un programa de *compliance* y de prevención penal para la persona jurídica y diseñar uno que debe ser propio y que formará parte de los principios y valores organizativos, convirtiéndose este modelo en un objetivo estratégico a corto y medio plazo que configurará la cultura de la organización.

Tras la reforma del Código Penal en el año 2010 y, especialmente, tras la modificación operada por la Ley Orgánica 1/2015, surge la necesidad de que las organizaciones cuenten con modelos de prevención de riesgos penales y desarrollen un programa de *compliance* y prevención penal en línea con las consideraciones contenidas en la Circular 1/2016 de la Fiscalía General del Estado y los principios establecidos en la ISO 19600 y UNE 19601.

La **política de *compliance*** (en adelante la política) constituye el marco de referencia del programa de *compliance* y prevención penal.

La forma más adecuada de establecer un sistema de gestión de *compliance* (en adelante SGC) es el diseñar una política de *compliance*, que contemple en sus parámetros más representativos, los siguientes:

- Incorporar una cultura ética y de respeto a las leyes en la forma de actuar de las personas que integran la organización con la diligencia debida, como buenas prácticas de buen gobierno corporativo.

- Liderazgo y compromiso del órgano de gobierno o alta dirección (tone at the top), aprobando en acta el inicio del programa de *compliance* con el funcionamiento del SGC, para hacer más eficiente y efectivo el programa de *compliance* y observar una conducta ética y respetuosa con las normas, para que esta fluya a toda la organización.

- El deber de denunciar, por todos los agentes, internos o externos, las acciones o conductas irregulares de las que se tenga conocimiento, a través del canal de denuncias o líneas éticas que garanticen la confidencialidad.

- La autonomía e independencia del órgano de cumplimiento en la toma de decisiones y en sus propuestas a la organización, para evitar daños económicos y reputacionales.

- Establecer controles preventivos y detectivos para advertir de comportamientos ilícitos.

- Estimar la materialización de los riesgos e incorporar indicadores KPI, positivos y negativos, que midan la actividad y eficacia en las actividades de desarrollo del negocio.

La política debe definir por qué debe implantarse, quién la promueve y la aprueba, quien la diseña y qué objetivos o soluciones se pretenden conseguir con la aplicación de un modelo de prevención de riesgos penales.

Además, deben integrarse en el programa de *compliance* todas las políticas de la organización o bloques de obligaciones relativos a todos los contextos de los ámbitos de gestión (penal, defensa de la competencia, privacidad y protección de los datos personales, calidad, medioambiental y desarrollo sostenible, fiscal, laboral, seguridad y salud en el trabajo, responsabilidad social corporativa, diversidad, etcétera).

En la política, también pueden preverse otras cuestiones ajenas o relacionadas con el cumplimiento penal, como la regulación de regalos u obsequios, entre otros temas.

La política de *compliance* debe contemplar un mensaje rotundo de **tolerancia cero frente a la tipología de las conductas delictivas.**

Las buenas prácticas y el código de conducta deben ser el fiel reflejo y la total oposición de la organización a la comisión de cualquier acto ilícito, penal o de cualquier otra índole.

ESTRUCTURA DE UNA POLÍTICA DE COMPLIANCE

La política la conforman un conjunto de contextos específicos a medida de cada organización, ya que es la expresión formal de su voluntad e intenciones éticas. Por esta razón, no puede ser sustituida en ningún caso por modelos prediseñados.

Alcance, contenidos y detalle de la política:

1. INTRODUCCIÓN

- Descripción de la denominación, actividad y la aprobación en acta por el órgano de gobierno.
- Compromiso con los principios y buenas prácticas del *compliance* para la prevención de delitos.
- Referencias al marco jurídico y a las normativas legales donde se apoya jurídicamente.

2. OBJETIVOS

- Comunicar el mensaje de: "la firme oposición a la comisión de cualquier acto ilícito, penal o de cualquier otra índole", como muestra del compromiso de tolerancia cero por parte de la organización.
- Informar y comunicar que el órgano de gobierno pone en conocimiento de toda las personas trabajadoras, así como de los terceros que se relacionen con la organización, que en ningún caso está justificada la comisión de un delito, directa o indirectamente, por parte de la plantilla, ni aun cuando tal actuación produjese, aparentemente, un beneficio de cualquier clase, presente o futuro a la organización, y que, además, está dispuesta a combatir estos actos y a prevenir un eventual deterioro de su imagen y su valor reputacional.
- La prevención de delitos para la exención de la responsabilidad penal de la organización y evitar sanciones.

- La detección de conductas delictivas o de delitos.
- La reacción disciplinaria frente a conductas delictivas o hechos punibles de la persona responsable del incumplimiento normativo.

3. ÁMBITO DE APLICACIÓN Y RESPONSABILIDADES

- Vincula su aplicación al órgano de gobierno, a la alta dirección, personal directivo y, en general a toda la plantilla de la organización sin excepción y cualquiera que sea su cargo, responsabilidad, ocupación o ubicación geográfica.
- También relaciona a las personas que actúen en representación de la organización sin formar parte de la misma y que cumplirán con las disposiciones de la presente política y se esforzarán para promover su cumplimiento en las organizaciones a las que pertenezcan y desde las que representen a aquel.
- La responsabilidad penal de la persona jurídica se apoya en la transferencia de responsabilidad penal por la actividad de las personas físicas autoras materiales de la comisión de un delito contemplado en el código penal, delito cometido actuando en nombre o por cuenta de la persona jurídica y en su beneficio, ya sea este directo o indirecto.

4. ELEMENTOS GENERALES DEL COMPORTAMIENTO

- Cumplimiento de la legalidad y de la normativa interna.
- Independencia y transparencia en las relaciones con terceros
- Respeto a la imagen y reputación de la organización.
- Políticas y procedimientos adecuados a su actividad.
- Recursos humanos, financieros y tecnológicos suficientes para realizar las funciones de *compliance*.
- Supervisión y seguimiento continuo en materia de autocontrol y verificación de las políticas, procedimientos y protocolos.

- Deber de denunciar posibles conductas ilícitas. Aplicar, de forma proporcionada y ajustada, las sanciones previstas en el régimen disciplinario, respecto a las conductas ilícitas verificadas.

5. BASES DEL PROGRAMA DE COMPLIANCE

- El programa de *compliance* y prevención penal se constituye sobre el análisis, valoración e identificación de las actividades en cuyo ámbito pueden ser cometidos los delitos y priorizando los potenciales riesgos que pueden afectar a la organización, incorporándolos al mapa de riesgos y estableciendo los correspondientes controles destinados a prevenir, detectar y sancionar la comisión de tales ilícitos, especialmente los de carácter penal, por resultar de los más graves.

- En el marco del programa de *compliance* y prevención penal, se toman medidas organizativas y normativas de aplicación interna.

- La **formación** en materia de *compliance* se convierte en obligatoria para toda la plantilla, con la aprobación de la ISO/DIS 37301:2020 Sistema de gestión de cumplimiento, por lo que esta deberá ser apropiada, evaluada su eficacia y revisada regularmente.

6. PRINCIPIOS DEL PROGRAMA DE COMPLIANCE y PREVENCIÓN PENAL

- Prevención:

  Los elementos del programa de *compliance* y prevención penal destinados a prevenir la materialización de los riesgos de incumplimiento son los siguientes:

  - Modelo de gestión económico-financiero.
  - Órgano de cumplimiento.
  - Mapa de riesgos penales.
  - Código de conducta.
  - Manuales, políticas, procedimientos y protocolos.

Formación y difusión del código de conducta y del programa de *compliance* y prevención penal.

- **Detección**. El elemento fundamental del programa de *compliance* y prevención penal destinado a la comunicación de conductas irregulares es el canal de denuncias.
- **Reacción**. Un elemento del programa de *compliance* y prevención penal destinado a reaccionar frente a la materialización de los riesgos de incumplimiento es el régimen disciplinario.
- **Seguimiento**. Los elementos del programa de *compliance* y prevención penal destinados a su adecuado seguimiento y supervisión, así como verificación, son:
- **Plan de seguimiento, supervisión y monitorización** del programa de *compliance* y prevención penal.
- **Verificación** del programa de *compliance* y prevención penal.

7. APROBACIÓN, DIFUSIÓN Y REVISIÓN DE LA POLÍTICA

- La aprobación y su difusión constará del siguiente mensaje: "La presente política ha sido aprobada por la organización, en la correspondiente acta fechada y puesta a disposición de toda la plantilla, por los medios habituales de comunicación interna por los que se dará a conocer, completándose con acciones formativas y de sensibilización a todas las personas trabajadoras de la organización".
- La política, así como el programa de *compliance* y prevención penal, serán objeto de revisión y mejora continua, especialmente cuando las circunstancias normativas, sociales, empresariales o de cualquier otra índole así lo requieran, en todo caso, será objeto de revisión anual.

“Cuando la especialización e independencia **SON VALORES IMPRESCINDIBLES”**

Las certificaciones profesionales de la WCA son conformes con la **norma internacional ISO 17024 para organismos que realizan la certificación de personas**, aportando, un reconocimiento internacional a través del sistema de evaluación de la conformidad establecido y convirtiéndose en una herramienta para diferenciar los distintos niveles de capacitación de los profesionales.

Categorías de Certificaciones Profesionales:

01 | COMPLIANCE OFFICER.

02 | AUDITOR COMPLIANCE.

03 | EXPERTO EN PREVENCIÓN DEL FRAUDE.

04 | EXPERTO EN PROTECCIÓN DE DATOS (DPO).

05 | EXPERTO EN PREVENCIÓN DE BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO.

La alianza internacional para **la difusión de la ética y el cumplimiento** en las organizaciones.

WORLD® COMPLIANCE ASSOCIATION

WCA Internacional
Paseo Castellana 79, 7ª Planta (Lexington Center)
28046 Madrid - España Tlf: +34 917 91 66 16
info@worldcomplianceassociation.com
www.worldcomplianceassociation.com

WCA está acreditada por IAS para la certificación de ISO 37001:2016

CAPÍTULO 8.
ÓRGANO DE CUMPLIMIENTO.

JORGE PELEGRÍN SÁENZ

LICENCIADO EN SOCIOLOGÍA.
MÁSTER EN "CALIDAD Y MEDIOAMBIENTE" Y "DIRECCIÓN DE EMPRESAS".
CURSO DE EXPERTO EN "DELEGADO DE PROTECCIÓN DE DATOS".
TÉCNICO DE ORGANIZACIÓN Y CALIDAD DE CONFEDERACIÓN SALUD MENTAL ESPAÑA.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

LA VOLATILIDAD Y EL RIESGO

Como cualquier entidad de otros sectores, aquellas que desempeñan su actividad en el tercer sector se mueven, actualmente, en un entorno VUCA (volatile, uncertain, complex, ambiguous). Este entorno altamente volátil hace que nuestras entidades se enfrenten a una serie de retos estratégicos, económicos, relacionales e internos. Entre los últimos, hay que hablar del cumplimiento normativo y los controles internos[1].

En una encuesta realizada entre finales de noviembre de 2018 y enero de 2019 al alumnado en curso y a antiguos/as alumnos/as del Programa Formativo para Directivos de ONG de Esade, así como a directores y directoras de ONG participantes del programa Esade – PWC de Liderazgo Social, de los diez retos más importantes para el sector, se identificó en el primer puesto, con un 77% de votos, "una mayor orientación a resultados y medición de impacto", mientras que en último lugar, con un 13% de los votos, aparecía "la reputación de la entidad, legitimidad y confianza".

Como vemos, la aceptación de los planes *compliance* está situada en los puestos más bajos en cuestión de importancia para los directivos y directivas del tercer sector y, por ello, va a ser muy importante su relativización entre los puestos que deben asumir las funciones de liderazgo. Se debe aprovechar el entorno VUCA a nuestro favor, ya que es ahora el mejor momento para diseñar y poner en marcha planes de gestión del riesgo para entender los riesgos a los que nos enfrentamos y, así, poder planificar estratégicamente y conseguir que nuestros financiadores públicos y privados confíen en que administramos eficazmente sus fondos. Asimismo, debemos buscar la sostenibilidad de nuestros programas y, en definitiva, aprender a gestionar el y en el riesgo.

ROLES EN MATERIA DE COMPLIANCE

Aunque, como indican Helena Prieto y Beatriz Bustamante en su artículo del diario Expansión[2] "*compliance* somos todos" el Código Penal, dentro de su ambigüedad, define al órgano de cumplimiento como *"el órgano de la persona jurídica con poderes autónomos de iniciativa y control que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica."*

Desde Esade – PWC, siguiendo la metodología elaborada y adoptada universalmente del Institute of Internal Auditors (IIA), nos proponen **tres líneas de defensa** frente al riesgo[3] (concepto en el que se profundizará en el tema 9 de la presente guía):

- **Direcciones y áreas de la organización:** deben asumir, instrumentar y poner en práctica la gestión del riesgo y los controles internos. Para ello, deben contar con un sistema de gestión adecuado a la naturaleza de su actividad. Este sistema está formado por el conjunto de procedimientos, normativa y controles que deben aplicar para el correcto funcionamiento de su dirección o área. Cuanto mejor y más actualizado esté ese sistema, menores serán los niveles de criticidad de los riesgos de su operativa.

- **Equipos de cumplimiento y gestión de riesgos:** deben coordinar el modelo de gestión asegurando el cumplimiento de políticas y estándares. Su función es prestar apoyo específico y especializado a los/as gerentes de las unidades operativas de una organización para que su dirección o área monitoree, vigile, detecte, aprenda, mitigue y mejore de forma constante la situación de sus riesgos. En este nivel debe trabajar personal especializado en esta materia, así como ser liderado por una unidad diferente a la dirección o área operativa.

- **Auditorías internas:** deben aportar supervisión, aseguramiento objetivo, buen gobierno, gestión de riesgos y cumplimiento. Asimismo, debe contemplarse la figura de la auditoría externa cuya función es la verificación del sistema y el reporte al órgano de gobierno que ayuden a asegurar la eficiencia y la efectividad de dicho sistema.

También debemos hablar del tipo de liderazgo que debe hacer que estas líneas de defensa calen en todas las áreas de nuestras entidades; un liderazgo enfocado en la reputación y la gestión de los riesgos para encarar los tres motivos por los que la reputación es importante en nuestro sector. Como indica Marie Gabrielle Cajoly[4], afecta directamente a los recursos financieros, amplía el impacto operativo y determina el poder de influencia.

Si enlazamos estos tres motivos con las preocupaciones mostradas en la encuesta realizada por Esade-PWC, podemos ver que damos solución a la inquietud mayoritaria de una "mayor orientación a resultados y medición de impacto", además de dar respuesta, también, a la última de sus preocupaciones, "la reputación de la entidad, legitimidad y confianza".

FUNCIONES Y RESPONSABILIDADES

Del anterior apartado, debemos asumir que la función principal del órgano de cumplimiento debe ser la supervisión del funcionamiento y cumplimiento del modelo de prevención de delitos penales que se haya articulado por mandato de los órganos de gobierno, a los que se debe tener informados periódicamente. Estos deben aprobar su constitución, otorgándole la autoridad debida, así como sus normas de funcionamiento.

Como indica Eduardo Pérez Fernández[5], entre las **funciones otorgadas al órgano de cumplimiento**, podemos encontrar las siguientes:

- Velar por el cumplimiento de las normativas internas, sectoriales y la legislación aplicable.
- Información y comunicación interna.
- Formación (diseño y revisión de la eficacia de esta).
- Seguimiento, evaluación y mejora del sistema de *compliance* de la entidad.
- Revisión anual de las actividades de *compliance*.
- Creación, evaluación y actualización del mapa de riesgos penales.
- Creación, comunicación, gestión y análisis de los canales de denuncia.
- Diseño, puesta en marcha y análisis del plan de mejora continua del sistema *compliance*.

¿UNIPERSONAL O COLEGIADO?

Helena Prieto y Beatriz Bustamante[6], en su artículo de Expansión, indican que dependerá, sobre todo, de la dimensión de la entidad y de su nivel de exposición a los riesgos penales, y se podría añadir la decisión de internalizarlo o externalizarlo, aunque esto vendrá decidido por la limitación de los recursos de la entidad.

Si hablamos de un órgano unipersonal, estaremos haciendo referencia sobre todo a la figura del *compliance officer*, una figura que deberá aunar conocimiento y experiencia en temas legales, recursos humanos, auditorías internas, financieros y de seguridad. En entidades de tamaño medio y/o grande, puede ser más recomendable constituir un órgano colegiado de cumplimiento conformado por aquellas personas que tengan formación en las áreas mencionadas, que además puedan dar opiniones distintas sobre la materia que tengan que tratar. Para entidades pequeñas entendiendo por éstas aquellas que puedan presentar cuenta de pérdidas y ganancias abreviadas, el Código Penal en el artículo 31.3 bis indica que, estas funciones podrán ser asumidas directamente por el órgano de administración, que, en el caso de las asociaciones y fundaciones, correspondería a la junta directiva u otro órgano que asuma las funciones de gobierno, gestión y representación de la entidad.

Una de las dudas que pueden plantearse las entidades del tercer sector es si debemos externalizar o no la figura del *compliance officer*, ya sea colegiado o unipersonal. Helena Prieto y Beatriz Bustamante indican que podemos inferir, del propio legislador, que esta función debe desarrollarse desde la propia entidad, cuyo conocimiento interno será siempre más profundo y cualificado.

En cuanto a la investigación de las irregularidades detectadas, sí que puede ser recomendable su externalización, ya que así se podrá garantizar la confidencialidad, objetividad, imparcialidad y la no adopción de represalias, puesto que no debemos olvidar que el órgano de cumplimiento debe velar por que se garantice el respeto a la normativa de protección de datos de carácter personal, la confidencialidad y la ausencia de represalias.

En cualquier caso, **existe tal variedad de situaciones desde el punto de vista de las organizaciones, que el diseño de este órgano de cumplimiento será también variado y personalizado, atendiendo al tamaño, capacidad, recursos, volumen, impacto y complejidad de su actividad.** Pero lo que siempre deberá respetarse, siguiendo las indicaciones de la Circular 1/2016 de la Fiscalía General del Estado, es que este órgano cuente con poderes autónomos de iniciativa y control.

Las indicaciones de la Fiscalía son determinantes y serán las que marquen la posibilidad de realizar un diseño u otro. Más allá de su obligatoriedad legal, esto también es así porque el riesgo de una organización va más allá de la prevención de delitos, ya que se debe instaurar una cultura de cumplimiento y eficaz. Es por eso que hay que velar para que el órgano de cumplimiento cuente con independencia, autonomía y acceso a los órganos de gobierno de la organización que, en el caso del tercer sector, serían el Patronato, la Asamblea o una Comisión que actúe en nombre de los mismos. De ese modo, cuando el órgano de cumplimiento detecte que no se están cumpliendo los procedimientos y controles clave de la organización o se esté cometiendo algún delito, pueda informar directamente a ese órgano de gobierno, o bien a través de un reporte sistemático que resulte de la revisión anual del mapa de riesgos de la entidad, o bien a través de un informe puntual y a demanda que surja de una denuncia recibida e instruida por el canal de denuncias.

En ese sentido, será necesario asegurar que el o los miembros del órgano de cumplimiento cuenten con un conocimiento completo y demostrado de la actividad de la organización, posean cierta autonomía jerárquica, se les dote de recursos, autoridad y de reconocimiento hacia el interior de la organización y, sobre todo, no exista la posibilidad de conflictos de intereses. Intentando cumplir con estos requisitos, y atendiendo a la estructura de la organización, se pueden valorar distintas opciones.

Esta función, por ejemplo, se le podría asignar a una persona que ya exista o a un equipo de personas que ya existan, a los que se les debería liberar del trabajo directo que tengan dentro

de una dirección o área específica. Pero si fuera posible según sea el tamaño o recursos de la organización, esa persona o equipo deberían seleccionarse de entre aquellos o aquellas que ya asumen tareas transversales y de apoyo relacionadas con la auditoría y el control interno, la asesoría jurídica o la calidad y los procesos. Dentro de esta primera opción también podríamos separar las tres principales funciones del programa de *compliance*, que son el seguimiento del modelo, la gestión del canal de denuncias y el funcionamiento del propio órgano de cumplimiento, y asignarles esas funciones a personas diferentes, buscando la manera de que el último sea lo más autónomo e independiente posible.

Pero también se podría contratar expresamente a una persona para que asuma internamente la función del órgano de cumplimiento o incluso externalizar dicha función, tal como ya se ha dicho antes. Asimismo, la dotación de autonomía y de control se pueden lograr modificando el organigrama y colocando la función del órgano de cumplimiento fuera de la estructura directiva y dependiendo del órgano de gobierno, de un modo similar al que se emplea para establecer los comités de auditoría o los comités éticos.

1. Cordobés, M., Carreras, I., & Sureda, M. (2019). ¿Hacia dónde va el liderazgo social? Nuevas tendencias y competencias. (p. 14). Instituto de la Innovación Social de Esade - PWC.

2. Prieto, H., & Bustamante, B. (2018). La función de '*compliance officer*' gana peso en las organizaciones. Retrieved 19 March 2020. https://www.expansion.com/juridico/opinion/2018/11/20/5bf454b7e5fdeadb1a8b469a.html

3. Cordobés, M., Carreras, I., & Sureda, M. (2019). ¿Hacia dónde va el liderazgo social? Nuevas tendencias y competencias (p. 78). Instituto de Innovación Social de Esade - PWC.

4. Cajoly, M. (2020). Are NGOs up to the reputation challenge? Retrieved 19 March 2020. https://www.linkedin.com/pulse/ngos-up-reputation-challenge-marie-gabrielle-cajoly

5. Fernández Pérez, E. (2020). Órganos de gobierno de *Compliance*. (Artículo del Comité Jurídico de la World Compliance Association). Retrieved 19 March 2020. http://www.worldcomplianceassociation.com/1477/articulo-rganos-de-gobierno-de-compliance-articulo-del-comite-juridico-de-la-world-compliance-association.html

6. Prieto, H., & Bustamante, B. (2018). La función de '*compliance officer*' gana peso en las organizaciones. Retrieved 19 March 2020. https://www.expansion.com/juridico/opinion/2018/11/20/5bf454b7e5fdeadb1a8b469a.html

CAPÍTULO 9.
COMPLIANCE COMO EJE TRANSVERSAL A LA GESTIÓN.

VANESSA FERNÁNDEZ

LICENCIADA EN DERECHO POR LA UNIVERSIDAD SAN PABLO-CEU, MADRID Y MÁSTER EN ABOGACÍA Y ESPECIALIDAD EN DERECHO PRIVADO POR EL INSTITUTO DE ESTUDIOS SUPERIORES SAN PABLO CEU-MADRID.
SOCIA DEL ÁREA PENAL Y COORDINADORA DEL ÁREA CORPORATE COMPLIANCE DE GÓMEZ-ACEBO & POMBO ABOGADOS, S.L.P.
MIEMBRO DE LA SUBCOMISIÓN DE PREVENCIÓN DEL BLANQUEO DE CAPITALES DEL CONSEJO GENERAL DE LA ABOGACÍA Y DEL COMITÉ DEL TERCER SECTOR DE LA WCA.

INTRODUCCIÓN

Los programas de cumplimiento normativo o de *compliance* (en adelante, "**programas de *compliance***") se configuran como una herramienta que sirve a las organizaciones, entre las que se encuentran las asociaciones y fundaciones, para (i) establecer o mejorar una cultura ética y de respeto por la legalidad; (ii) alinear la actividad de la organización y de sus miembros con los estándares éticos más elevados, y (iii) prevenir la asunción de riesgos de cumplimiento normativo en el desarrollo de su actividad.

El correcto funcionamiento de estos programas implica la participación e involucración de todos los miembros de la organización, es decir, cada uno de ellos tendrá unos deberes y obligaciones para con el programa de *compliance* y, por tanto, unas funciones que desempeñar para lograr la eficacia del programa y una verdadera cultura ética y de cumplimiento normativo en la organización.

Los programas de *compliance* son utilizados por las organizaciones como mecanismos para garantizar el cumplimiento de las leyes aplicables y las mejores prácticas éticas, así como para detectar y prevenir la asunción de riesgos normativos y, en su caso, su posterior gestión, mitigación y seguimiento. No obstante, el objetivo no debe ser únicamente la elusión o atenuación de la responsabilidad penal, como riesgo, en principio, más grave al que se enfrenta una organización, **su eficacia reside realmente en la incidencia que los programas tienen en todos los miembros de la organización a la hora de tomar decisiones y si estas están alineadas con una verdadera cultura de cumplimiento, de forma que el programa de *compliance* se integre como un elemento fundamental y transversal en la gestión de la organización.** Cuanto más alineados estén los miembros de la organización mayor será la eficacia del programa de *compliance*[1].

MODELO DE TRES LÍNEAS DE DEFENSA

A través de los programas de *compliance*, se realiza la gestión de, entre otros, los riesgos normativos, estratégicos, operativos e incluso reputacionales, a los que la organización y sus miembros pueden estar expuestos en el desempeño de sus funciones profesionales. Estos riesgos pueden ser laborales, penales, regulatorios, de protección de datos y administrativos, entre otros.

Para realizar correctamente dicha gestión, las organizaciones pueden implementar el denominado modelo de tres líneas de defensa[2] (concepto introducido en el tema 8 de la

presente guía), pudiendo distinguir tres grupos diferenciados que participan en la gestión de riesgos:

- **1ª línea de defensa:** áreas de negocio de la organización. Está compuesta por cada una de las áreas de negocio que componen la organización, ya que gestionan directamente los riesgos que pueden surgir en el desarrollo de la concreta actividad empresarial.

  Las áreas de negocio son las encargadas de identificar y prevenir la asunción de riesgos y de implementar los procedimientos necesarios para detectarlos, evitarlos y mitigarlos en el desarrollo de su actividad profesional diaria.

- **2ª línea de defensa:** áreas de cumplimiento y control. Se trata de funciones que controlan los riesgos como pueden ser el área de cumplimiento normativo, de prevención del blanqueo de capitales y de la financiación del terrorismo –en caso de ser sujeto obligado por la normativa sectorial–, de asesoría jurídica y financiera, o de calidad, entre otras áreas de control.

  Son responsables de controlar los riesgos de la organización gestionados por las áreas de negocio y de supervisar el cumplimiento de las políticas, procedimientos, controles e, incluso, instrucciones u otras normas internas o legales de obligado cumplimiento, así como de garantizar que las obligaciones de cumplimiento se integren en las políticas y procedimientos, ayudar a las áreas de negocio a definir e identificar la exposición al riesgo y evaluar el riesgo de cumplimiento, entre otras actividades de control del riesgo.

- **3ª línea de defensa:** áreas de supervisión o auditoría. Su propósito es evaluar y mejorar el programa de *compliance* en su conjunto, así como la eficacia de los procesos de gestión y control de riesgos. Por tanto, se trata de la función designada por la organización para realizar auditorías a intervalos planificados del programa de *compliance* para asegurar su buen funcionamiento.

  Esta auditoría interna podría ser llevada a cabo por una función independiente (por ejemplo, el área de auditoría interna) o por una persona en la organización designada para realizar este proceso, siempre y cuando no exista un conflicto de interés en la ejecución de esta auditoría.

Destacar que la supervisión externa de los programas de *compliance* realizada por **auditores/as externos/as, reguladores/as y otros entes externos** podría considerarse como una **4ª línea de defensa**, ya que establecen requerimientos con la intención de fortalecer los controles de una organización y realizan una función de vigilancia independiente y separada de los auditores/as internos/as.

EL PAPEL DEL ÓRGANO RECTOR Y LA ALTA DIRECCIÓN EN LOS PROGRAMAS DE COMPLIANCE Y LA GESTIÓN DE RIESGOS

Aunque ni el órgano rector[3] ni la alta dirección forman, per se, parte de las tres mencionadas líneas de defensa, ambos tienen una responsabilidad y un rol fundamental en los programas de *compliance*[4]: **promover y fomentar de forma visible y consistente la implementación, cumplimiento y mejora continua del programa de *compliance*,** así como las obligaciones de cumplimiento de la organización, para que sea capaz de gestionar los riesgos a los que la organización se ve expuesta en su actividad diaria.

Emana del órgano rector y la alta dirección el compromiso de establecer una cultura ética y de cumplimiento normativo. Entre otras funciones, son responsables de garantizar que el programa de *compliance* y sus elementos fundamentales se implementen de forma adecuada, de la promoción de la mejora continua del programa, de garantizar la disponibilidad de los recursos necesarios (tanto económicos como humanos) para la ejecución eficaz del programa y de velar por que este logre los resultados previstos.

A su vez, algunas organizaciones pueden constituir un **órgano de cumplimiento** que, sin perjuicio de las responsabilidades del órgano rector y la alta dirección, sea el encargado, entre otras cuestiones, de impulsar y supervisar de manera continua la implementación y eficacia del programa de *compliance* para que su correcto funcionamiento permita mitigar la asunción de riesgos.

Aquellas organizaciones que no cuentan con un área específica de cumplimiento normativo o de control, si tienen designado, en cumplimiento de los requisitos previstos en el artículo 31 bis del Código Penal, un órgano –unipersonal o colegiado- que desarrolla las funciones propias de las áreas de control de la mencionada 2ª línea de defensa, se podrá considerar a este órgano como 2ª línea de defensa en la gestión de riesgos. Es decir, que una organización podrá crear un órgano de cumplimiento y asignarle a él todas las funciones de control del cumplimiento por la entidad en las diferentes áreas organizativas (2ª línea de defensa) como el seguimiento del programa de *compliance* (órgano de cumplimiento).

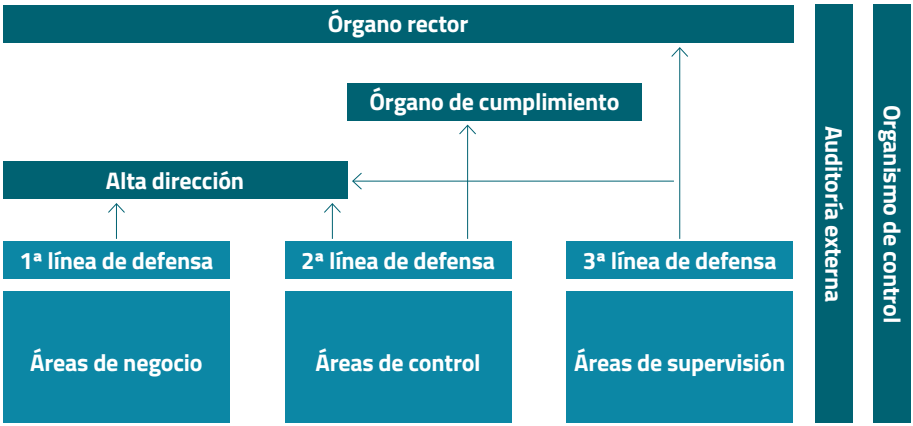
Con carácter general, las áreas que componen las tres líneas de defensa deben reportar la oportuna gestión de riesgos; en concreto la 1ª y 2ª línea reportarán a la alta dirección y la 3ª, de forma habitual al órgano rector. Y ello, sin perjuicio de que el programa establezca siempre la posibilidad de comunicación directa al máximo órgano de representación de la organización en determinados casos como, por ejemplo, la existencia de un conflicto de interés.

En el caso de que una organización haya establecido que las áreas de control reporten primero a la alta dirección y al órgano de cumplimiento, esas áreas de control podrán y deberán

reportar o informar directamente al órgano rector en el caso de que exista un conflicto de interés cuyo ejemplo más visual podría ser el que un directivo de la organización (a quien con carácter habitual se debiera reportar) estuviera implicado en un conflicto por incumplimiento grave de los procedimientos o del código de conducta o en un posible delito. Lógicamente, no se puede reportar a quien debe ser objeto de investigación por el órgano de cumplimiento, con el fin igualmente de procurarle todos los mecanismos de defensa pertinentes. Es por ello que esa área de control deberá ser dotado de poderes autónomos de iniciativa y control y sus responsabilidades estarán claramente delimitadas en un protocolo o estatuto de funcionamiento o similar aprobado por el órgano rector y que la dirección y todos los miembros de la organización (incluido el órgano de cumplimiento) deberán comprometerse a respetar.

Si fuera el caso de que no exista esa área de control porque se tratara de una organización que solo tuviera un órgano de cumplimiento para asumir esas tareas, tal como señalamos anteriormente, entonces ese órgano deberá reportar primero a la alta dirección excepto en aquellos casos en los que, de nuevo, exista por ejemplo un conflicto de interés, en los que se habilitará el mecanismo para informar directamente al órgano rector, debiéndose igualmente recoger sus competencias y responsabilidades en un protocolo o estatuto de funcionamiento aprobado por el máximo órgano rector de la organización y asumido por todos sus miembros.

El órgano rector y la alta dirección han de garantizar que el programa de *compliance* se implemente de forma adecuada y eficaz y se revise periódicamente, para que la actividad de la organización se desarrolle en todo momento cumpliendo las obligaciones de cumplimiento y evitando y, en su caso, mitigando la asunción de riesgos.



1. UNE 19601 Sistemas de gestión de *compliance* penal (apartados 5.1., 5.6. y 7).
2. Las tres líneas de defensa para una efectiva gestión de riesgos y control – Institute of Internal Auditors Inc, enero 2013.

3. Por ejemplo, se considerará órgano rector, en el caso de las asociaciones, a la asamblea general o junta directiva u órgano análogo, si así se prevé en los estatutos, y, en el caso de las fundaciones, al patronato, sin perjuicio de la delegación de facultades que se lleve a cabo de conformidad a la legislación aplicable y a los estatutos de la fundación.

4. La ISO 19600 sobre Sistemas de Gestión de *Compliance*, la UNE 19601 sobre Sistemas de Gestión de *Compliance* Penal, así como la ISO 37001 sobre Antibribery-management systems establecen en su punto 5 Liderazgo el rol y responsabilidades del órgano rector y de la alta dirección con respecto a estos sistemas.

Así mismo, la Circular de la Fiscalía 1/2016 determina en su punto 5.6. "Cualquier programa eficaz depende del inequívoco compromiso y apoyo de la alta dirección de la compañía. El comportamiento y la implicación del Consejo de Administración y de los principales ejecutivos son claves para trasladar una cultura de cumplimiento al resto de la compañía. Por el contrario, su hostilidad hacia estos programas, la ambigüedad, los mensajes equívocos o la indiferencia ante su implementación traslada a la compañía la idea de que el incumplimiento es solo un riesgo que puede valer la pena para conseguir *un mayor beneficio económico*. Si los principales responsables de la entidad incumplen el modelo de organización y de prevención o están recompensando o incentivando directa o indirectamente a los empleados que lo incumplen, difícilmente puede admitirse que exista un programa eficaz, que refleje una verdadera cultura de *respeto a la ley en la empresa*."

CAPÍTULO 10. SENSIBILIZACIÓN Y RENDICIÓN DE CUENTAS.

SANDRA SOLER VIDAL

SOCIA EN SOLER COMPLIANCE & ASOCIADOS Y FORMA COMPLIANCE.
LICENCIADA EN DERECHO POR LA UNIVERSIDAD DE BARCELONA.
TITULADA EN ASESORÍA Y GESTIÓN TRIBUTARIA POR ESADE.
DIPLOMADA POR LA ASOCIACIÓN ESPAÑOLA DE MEDIACIÓN ASEMED COMO TÉCNICO ESPECIALISTA EN RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA, COMO MEDIADORA EN MATERIA CIVIL MERCANTIL, PENITENCIARIA Y MEDIACIÓN ORGANIZACIONAL Y ÁRBITRO JUDICIAL.
DIPLOMADA POR THOMSON REUTERS-ARANZADI COMO TÉCNICO ESPECIALISTA EN RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS.
AUDITOR JEFE/LÍDER DE SISTEMAS DE GESTIÓN DEL COMPLIANCE ISO 19600.
MIEMBRO DE LA JUNTA DIRECTIVA DE LA WORLD COMPLIANCE ASSOCIATION Y PRESIDENTA DEL COMITÉ DE CERTIFICACIONES DE LA WCA Y MIEMBRO DEL COMITÉ DE TRABAJO COMPLIANCE Y PYMES DE LA WCA Y DEL TERCER SECTOR.

"LO QUE NO SE COMUNICA, NO EXISTE" (GABRIEL GARCÍA MÁRQUEZ)

FORMACIÓN A PERSONAL CONTRATADO

Diseñar e implementar un programa de *compliance* es importante, sobre todo para mitigar riesgos legales, financieros y reputacionales. Pero no tiene ningún efecto si la dirección y el personal contratado no lo compran, si no lo conocen y lo ven como algo útil y ventajoso para ellos y para la organización[1].

Es fundamental que todas las partes implicadas con la entidad conozcan la implantación del *compliance* en ésta. De poco servirá tener el mejor programa de *compliance* si las partes no conocen los principios básicos en los que se sustenta dicho programa y los valores y principios éticos de la entidad con la que se relacionan, y lo aplican en su día a día.

Es necesario, en consecuencia, evidenciar desde un inicio la implantación del programa de *compliance* de forma efectiva, cosa que hace esencial la comunicación del mismo a todas las partes. Todas las acciones que se realizan mediante **formación, concienciación y sensibilización** persiguen el cambio efectivo en las operativas y en la conciencia de los que se relacionan con la entidad, lo que supone mayor seguridad corporativa. Junto a la finalidad de concienciación, se encuentra la finalidad probatoria de la diligencia debida.

La formación tiene por objeto dar cumplimiento a lo establecido en las disposiciones nacionales e internacionales en materia de *compliance*, en particular, la ISO 19600, la UNE 19601:2017 y la Circular de la Fiscalía General del Estado 1/2016, en lo que a formación se refiere. La norma internacional ISO 19600 dedica un apartado específico a la formación, señalando que el objetivo de un programa de formación es "*asegurar que todos los empleados son competentes para cumplir con su rol profesional de forma consciente con la cultura del compliance de la organización y con el compromiso que tiene con el compliance*".

Por su parte, la UNE 19601:2017 sobre *Sistemas de Gestión de Compliance Penal* dedica un amplio apartado a la formación en materia de *compliance* y resalta su importancia en los siguientes términos: "*La organización debe fomentar que los miembros de la organización se conciencien, se formen adecuada, eficaz y proporcionalmente respecto de los riesgos penales, con la finalidad de evitarlos, detectarlos o saberlos gestionar conforme al sistema de gestión de compliance penal*".

Finalmente, la Circular 1/2016 de la Fiscalía General del Estado resalta la importancia de la formación de personal directivo y contratado en los modelos de organización y gestión y dispone que serán más eficaces cuanto mayor sea su nivel de externalización.

PRESENTE Y FUTURO DE LA FORMACIÓN

Este año nos traerá una de las novedades más relevantes en la escena internacional del *compliance* con la publicación del estándar ISO 37301 sobre *Compliance Management Systems*. Permitirá, no sólo el diseño, sino también la evaluación de la conformidad (certificación) de los sistemas de gestión de *compliance* transversales, es decir, de aquellos modelos que procuran el cumplimiento de las normas más relevantes de cada organización. Relevará a la norma ISO 19600 que, siendo el primer estándar internacional sobre *compliance*, se vio eclipsada por la inmediatamente posterior sobre sistemas de gestión anti soborno, la norma ISO 37001.

La ISO 37301 establece que la formación deberá cumplir los siguientes **requisitos**:

- Ser apropiada en relación a las funciones que desarrollan los diferentes grupos de la plantilla y a los riesgos de cumplimiento a los que están expuestas todas las personas trabajadoras.
- Estar planificada tanto inicial como periódicamente.
- Evaluar su efectividad.
- Estar documentada.
- Hacer reentrenamiento ante los incumplimientos.
- Garantizar que se implementan procedimientos que aborden la concienciación de cumplimiento y la formación para terceros que actúen en nombre de la propia organización.

CONTINUIDAD FORMATIVA

Se ha detectado que el gran problema, y por tanto el campo donde centrar el esfuerzo, es el olvido. L**os conceptos nuevos son fugaces en la memoria.** En dos días, se recuerda sólo el 30% y, tiempo después, cae al 10% de lo estudiado. Esto se debe a que un único impacto formativo no consigue resultados, no capacita para la aplicación práctica de los conocimientos tratados.

La solución está en la consolidación de los conocimientos. Repitiendo impactos de los nuevos conceptos a intervalos crecientes de tiempo y haciendo que los mensajes se procesen

mentalmente en cada revisión se consigue atenuar la pendiente de la curva de olvido, hasta llegar a consolidarse en la memoria. Es básico diseñar un plan formativo dirigido a todos los miembros de la plantilla y que sea de aplicación continuada a los efectos de ir consolidando conceptos relacionados con *compliance* y que la ética se integre en el ADN de la organización.

REPORTING DEL PROGRAMA DE COMPLIANCE

De conformidad con lo dispuesto en la UNE 19601:2017 sobre *Sistemas de Gestión de Compliance Penal*, el órgano de gobierno, la alta dirección y el órgano de cumplimiento deben asegurarse de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión de *compliance* penal y de su mejora continua (apartado 9.1.7). Lo mismo cabría decirse del desempeño del sistema de *compliance* en general, que es aquel que contempla todos los riesgos de la organización, los cuales van más allá de la responsabilidad penal de la persona jurídica. A tal efecto, deberá elaborarse un informe en el que se incluyan aspectos tales como los incumplimientos, no conformidades relevantes, controles, acciones de mejora y cualquier otro aspecto relevante para el funcionamiento efectivo del sistema de gestión de riesgos, penales o no. En este sentido, la citada UNE 19601 insiste en que es obligación de las organizaciones **promocionar activamente una cultura de información completa y transparente.**

Por su parte, el borrador de la ISO 37301 establece que los órganos de gobierno deben revisar el programa de *compliance* para garantizar su idoneidad, adecuación y eficacia.

En conclusión, anualmente se debe reportar al órgano de gobierno acerca de todas las acciones realizadas en materia de cumplimiento, para garantizar así su idoneidad y eficacia

RENDICIÓN DE CUENTAS

Uno de los fundamentos más importantes de los programas de *compliance*, como hemos mencionado en un inicio, es que todas las partes implicadas con la organización conozcan la implantación del programa en la organización. De poco servirá tener el mejor programa de *compliance* si las partes, tales como personal contratado, voluntariado, donantes, socios locales, otros socios y aliados, proveedores, y colaboradores, entre otros, no conocen los principios básicos en los que se sustenta dicho programa.

«La comunicación es la verdadera tarea del Liderazgo»

Durante el proceso de implantación del programa de *compliance*, podemos diferenciar dos **fases esenciales de comunicación, tanto interna como externa.**

En esta primera fase, lo fundamental será dar a conocer a las partes implicadas del inicio del proyecto de *compliance* y de la intención por parte del órgano de gobierno de la organización de expandir una cultura de ética y buen gobierno corporativo. La manera efectiva de comunicar con los demás es «tomar conciencia a quien nos vamos a dirigir». Cada organización, dependiendo de su estructura organizativa deberá analizar de qué forma la comunicación es más efectiva, en el sentido de que llegue a todas las partes interesadas y cuál es el contenido de dicha comunicación, esto es, qué se quiere comunicar, qué se quiere transmitir. Se puede optar por el envío de una comunicación mediante correo electrónico, un anuncio en la Intranet de la organización, un anuncio en el tablón de anuncios interno o la entrega de la comunicación personalmente, entre otros diversos procedimientos.

Una vez implantado el programa de *compliance*, se procederá a la siguiente fase, donde diferenciaremos si la comunicación va dirigida a:

1. COMUNICACIÓN A NUEVOS/AS EMPLEADOS/AS y VOLUNTARIOS/AS

La comunicación se puede realizar con la entrega del **Pack de Bienvenida o Welcome Pack,** a través del cual se les debe trasladar de forma homogénea la información y formación necesaria en materia de *compliance*, haciendo así que se incremente el compromiso con la organización.

El contenido se divide en dos partes diferenciadas:

- **Información de carácter legal y ético de la organización.** Deberá entregarse con suficiente tiempo de antelación a la firma del contrato o acuerdo de vinculación, para que el/a nuevo/a empleado/a o voluntario/a, respectivamente, tenga la posibilidad de conocer de primera mano la cultura organizativa de la que formará parte. Los documentos principales de esta primera parte son el código de conducta, la política de *compliance*, los canales de denuncia y otros procedimientos internos de la organización, entre los que se encuentra el tratamiento de los datos personales.

  El objetivo es que ambas partes estén de acuerdo en los principales puntos del funcionamiento de la organización antes de formalizar la relación contractual.

- **Documento acreditativo del conocimiento y aceptación del marco normativo interno.** Deberá entregarse una vez el/la empleado/a o voluntario/a haya firmado el contrato laboral o acuerdo de vinculación, respectivamente, que le une a la organización.

2. COMUNICACIÓN A EMPLEADOS/AS y VOLUNTARIOS/AS VINCULADOS

No debemos de olvidar que cada organización tiene sus operativas de trabajo, y, por tanto, debe realizar dicha comunicación o sensibilización de la forma que considere más adecuada a su estructura organizativa. Una forma efectiva de transmitir la información es mediante la formación básica en *compliance* a todos/as los/as empleados/as y voluntarios/as, en la que se les entregue el código de conducta y un documento de aceptación del marco normativo interno que les resulte de aplicación.

En el supuesto de que se decida realizar la formación básica en *compliance* en una fase posterior, se les puede transmitir la información por correo electrónico. En este caso, resultará obligatorio recabar la evidencia de ello, así como su conservación mediante los logs de recepción (nombre usuario y fecha recepción). Para aquellos/as empleados/as y voluntarios/as que no dispongan de correo corporativo, la comunicación será en papel, por lo que resultará oligatorio recabar la aceptación del marco normativo interno por escrito.

3. COMUNICACIÓN A LAS PERSONAS BENEFICIARIAS

Uno de los principios de cualquier organización del tercer sector, es la acción sin daño, y para ello es fundamental que las personas beneficiarias conozcan sus derechos y cómo ejercerlos, dotándoles de recursos para poder hacerlo. Tal es así que es más apropiado emplear el término de titulares de derecho para referirnos a estas personas. Por ello, en este caso, se recomienda realizar jornadas de formación y sensibilización en las que dar a conocer el código de conducta de la organización, para que de este modo comprendan cuáles son las conductas esperadas por parte de las personas vinculadas a la organización, y cómo actuar en caso de que tengan indicios de sospecha. En este caso, se les dará a conocer el canal de denuncias accesible a este grupo de interés para ejercer sus derechos, primando en todo momento su protección.

Para dejar evidencia de ello, se deberá guardar documentación soporte de la jornada impartida, bien mediante material fotográfico y/o listados de asistencia.

4. COMUNICACIÓN A LAS PERSONAS DONANTES

En este caso se les puede informar a través de la web de la organización, de la newsletter o a través de cualquier otra comunicación periódica que reciben a modo de rendición de cuentas.

Adicionalmente, supone una buena práctica la publicación del código de conducta y del enlace al canal de denuncias en la página web de la organización de manera abierta y pública, así como de aquella otra documentación que se considere relevante de cara a terceros, como muestra de una gestión transparente y accesible.

5. COMUNICACIÓN A LOS PROVEEDORES y OTROS SOCIOS

La comunicación del *compliance* a nuevos proveedores y otros socios con los que colaboramos para desempeñar nuestra actividad, como entidades intermediarias o socios locales en los países de intervención, se puede realizar mediante la inclusión en el contrato de cláusulas de *compliance* y anexando el código de conducta como parte integrante del contrato. En el supuesto de proveedores y otros socios donde ya existía relación contractual, se les puede enviar el código de conducta por medios digitales para la acreditación de su comunicación y aceptación posterior, o bien mediante la firma de una adenda al contrato vigente.

1. Libro Blanco de la Formación (s.f.). (Foxize).

"Cuando la especialización e independencia **SON VALORES IMPRESCINDIBLES"**

Servicios internacionales de auditoría, evaluación y certificación de Sistemas de Gestión del Compliance.

Los organizaciones precisan dar evidencia de que aplican sistemas y/o programas de cumplimiento de acuerdo a los requisitos y/o recomendaciones de Normas y Legislaciones tanto nacionales como internacionales y el someter la evaluación de los mismos a una auditoría de tercera parte imparcial e independiente, además de una fuente de mejora para la seguridad de la propia organización, transmite un elevado nivel de confianza a los grupos de interés con los que la organización se relaciona.

- **ISO 37001:2016 Sistema de Gestión Contra el Soborno**
- **ISO 19600:2014 Sistema de Gestión del Compliance**
- **Planes/Programas de Prevención de Delitos en cumplimiento de legislaciones nacionales**
- **UNE 19601, Gestión del Compliance Penal (España)**
- **Programas de Compliance alineados con los requisitos de la FCPA**

La alianza internacional para **la difusión de la ética y el cumplimiento** en las organizaciones.

WORLD® COMPLIANCE ASSOCIATION

WCA Internacional
Paseo Castellana 79, 7ª Planta (Lexington Center)
28046 Madrid - España Tlf: +34 917 91 66 16
info@worldcomplianceassociation.com
www.worldcomplianceassociation.com

WCA está acreditada por IAS para la certificación de ISO 37001:2016

CAPÍTULO 11.
CÓMO MEDIR LA EFICIENCIA DE UN PROGRAMA DE COMPLIANCE.

ALBERT SALVADOR

LICENCIADO EN CC ECONÓMICAS Y EMPRESARIALES.
AUDITOR INTERNO CERTIFICADO POR EL IIA (THE INSTITUTE OF INTERNAL AUDITORS).
ESPECIALISTA EN FRAUDE INTERNO, FORENSIC Y PREVENCIÓN DE BLANQUEO DE CAPITALES.
SECRETARIO GENERAL Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA WCA.

Uno de los temas que genera más debate entre los profesionales del mundo del *compliance* es cómo poder medir el grado de cumplimiento de su organización y, por tanto, si el sistema de gestión de *compliance* es eficaz o no.

Unos de los elementos válidos para poder demostrar a un tercero, donante, proveedor, miembro del órgano de gobierno, fiscal o magistrado que un sistema de gestión de *compliance* es eficaz son los indicadores de *compliance* o **KCI (Key *Compliance* Indicators).**

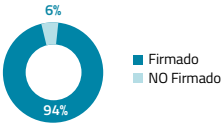
Una frase célebre en el mundo de la gestión de riesgos es: "***Lo que no se mide, no se puede mejorar***". En realidad, la frase corresponde a William Thomson Kelvin (Lord Kelvin), físico y matemático británico (1824 – 1907): ***"Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre ".***

Pues bien, aplicando este criterio válido para la gestión de riesgos en general, en esta guía se proponen, a nivel de ejemplo, 5 ***sencillos KCI*** que nos pueden servir para ***medir, mejorar y mantener*** un sistema de gestión de riesgos de *compliance* eficaz.

EJEMPLOS DE KCI

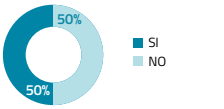
1 ACEPTACIÓN DEL CÓDIGO ÉTICO, MANUAL Y POLÍTICAS

Muestra el porcentaje de empleados que tiene firmado el código ético y las políticas.



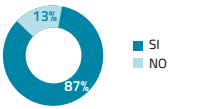
2 % RR > UMBRAL

Muestra el porcentaje de riesgos valorados que tienen el Riesgo Residual por encima del umbral de riesgo determinado.



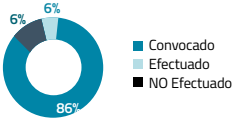
3 REALIZACIÓN DE CONTROLES

Muestra qué porcentaje de controles definidos en la matriz de riesgos están realizando, y qué % no se está realizando:



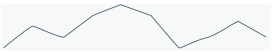
4 FORMACIÓN

Muestra qué porcentaje de realización de los cursos de formación convocados a sus empleados.



5 PLANES DE MITIGACIÓN

Muestra la situación de los planes de mitigación de la matriz de riesgos.



CÓMO CONSTRUIR UN KCI

Para poder construir un KCI, necesitamos tener registros con los datos necesarios.

Vamos a analizar la construcción del primer KCI propuesto de *"aceptación del código ético, manual y políticas"* el cual muestra el porcentaje de empleados/as que tienen firmado el código ético y las políticas. Para ello, necesitamos tener un registro vivo, con los datos de los/as empleados/as y la situación al respecto de la aceptación o no del código ético, manual y políticas:

Empleado	Situación
Juan López	Firmado
Manolo García	No Firmado
Juan López	...
Javier Fernández	Firmado

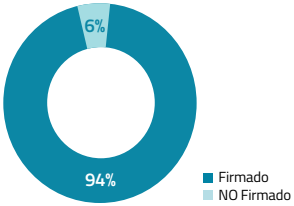
Es importante poder tener una foto mensual y guardar esos datos históricos, para poder construir la evolución de este indicador:

Año	Mes	% firmado	% No firmado
2020	01	66	33
2020	02	70	30
...	...	...	...
2020	04	94	6

La evolución nos va a permitir establecer una tendencia de cumplimiento de cada indicador, siendo este un dato útil para su gestión:

1 **ACEPTACIÓN DEL CÓDIGO ÉTICO, MANUAL Y POLÍTICAS**

Muestra el porcentaje de empleados que tiene firmado el código ético y las políticas.



Por último, establecer para cada indicador un **umbral de riesgo** con el fin de poder valorar si se cumplen con las expectativas de cada organización.

Por ejemplo, para el KCI propuesto de "*aceptación del código ético, manual y políticas*", imaginemos que la organización ha establecido un umbral de riesgo del 90%, es decir, que el 90% de los/as empleados/as ha de tenerlo firmado:

Dado que el porcentaje de cumplimiento (94%) es superior al umbral (90%), el color de la circunferencia es verde. Si el porcentaje de cumplimiento estuviera por debajo del 90%, el color de la circunferencia tendría que ser amarillo, naranja o rojo, en función del grado de desviación existente. A modo orientativo se proponen los siguientes tramos:

Color	Significado
Verde	El valor obtenido está por encima del umbral de riesgo.
Amarillo	El valor obtenido está por debajo del umbral de riesgo, hasta un máximo del 10% sobre el umbral. En el ejemplo sería entre el 81%-90%.
Naranja	El valor obtenido está por debajo del umbral de riesgo, hasta un máximo del 20% sobre el umbral. En el ejemplo sería entre el 72%-81%.
Rojo	El valor obtenido está por debajo del umbral de riesgo, por debajo del 20% del umbral. En el ejemplo sería por debajo de 72%.

Como podemos observar, se muestran de una manera visual y gráfica numerosos datos relevantes a este indicador y que, juntamente con el resto de KCI, nos ayudan tanto a medir la eficiencia del programa de *compliance* como a su gestión.

Para la creación de los otros KCI, usaremos el mismo criterio, teniendo en cuenta que los 5 KCI propuestos son meros ejemplos y que cada organización puede establecer otros diferentes.

CAPÍTULO 12.
CÓDIGO DE CONDUCTA.

SANDRA SOLER VIDAL

SOCIA EN SOLER COMPLIANCE & ASOCIADOS Y FORMA COMPLIANCE.
LICENCIADA EN DERECHO POR LA UNIVERSIDAD DE BARCELONA.
TITULADA EN ASESORÍA Y GESTIÓN TRIBUTARIA POR ESADE.
DIPLOMADA POR LA ASOCIACIÓN ESPAÑOLA DE MEDIACIÓN ASEMED COMO TÉCNICO ESPECIALISTA EN RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA, COMO MEDIADORA EN MATERIA CIVIL MERCANTIL, PENITENCIARIA Y MEDIACIÓN ORGANIZACIONAL Y ÁRBITRO JUDICIAL.
DIPLOMADA POR THOMSON REUTERS-ARANZADI COMO TÉCNICO ESPECIALISTA EN RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS.
AUDITOR JEFE/LÍDER DE SISTEMAS DE GESTIÓN DEL COMPLIANCE ISO 19600.
MIEMBRO DE LA JUNTA DIRECTIVA DE LA WORLD COMPLIANCE ASSOCIATION Y PRESIDENTA DEL COMITÉ DE CERTIFICACIONES DE LA WCA Y MIEMBRO DEL COMITÉ DE TRABAJO COMPLIANCE Y PYMES DE LA WCA Y DEL TERCER SECTOR.

"HAY QUE EVITAR QUE DESAPAREZCA
LO QUE TANTO TIEMPO LLEVA CONSTRUIR, LA REPUTACIÓN"

INTRODUCCIÓN

Todas las entidades sociales basan su actuación en una serie de principios y valores que contribuyen, a través del desarrollo de sus actividades y del cumplimiento de sus fines, a generar transformaciones sociales que mejoren la calidad de vida de las personas más vulnerables.

Uno de los pilares fundamentales de los programas de *compliance* es la elaboración de códigos éticos o de conducta que reflejen dichos principios y valores y que puedan orientar las actuaciones de las entidades del tercer sector y cómo se pueden organizar estas en las esferas internas y externas, así como las relaciones que se establecen con otras entidades no lucrativas, las personas, la sociedad y el entorno. El código ético o de conducta es la guía de comportamiento adecuado, junto con las normas y procedimientos de trabajo establecidos en las entidades, para garantizar lo correcto y que en su consecuencia lógica no se produzca ningún delito en la entidad, ni falta grave contra esos principios y valores

El código constituye una guía para todos los/as empleados/as y voluntarios/as en su desempeño profesional en relación con su trabajo cotidiano, los recursos utilizados y el entorno en el que se desarrolla. En este se ofrecen las directrices a seguir entre dichos profesionales, pero también a seguir por las personas beneficiarias o titulares de derecho, los socios locales, otras entidades no lucrativas, la sociedad y, en general, cualquier persona con interés directo o indirecto en la actividad que desarrolla la entidad.

La ética aplicada en una organización, en cualquier caso, es el ejercicio consciente que realiza el órgano de gobierno de la misma para identificar aquellos requisitos de actuación que van más allá de la ley, basados en esos principios y valores, cuyo cumplimiento exige a todos sus grupos de interés. Son los límites que se impone a sí misma para operar con normalidad en el ámbito de su actividad.

La ética, entendida como un conjunto de reglas de juego, no se debe emplear solo de forma reactiva cuando se ha detectado alguna tropelía a través de canales y comités que instruyen una posible vulneración del código de conducta y lo sancionan en caso de que se pruebe dicha vulneración, sino que se necesita también durante la rutina de una organización puesto que conecta su actividad con un sentido que la trasciende y la defiende de posibles abusos. Un código ético o de conducta es un seguro y una protección contra comportamientos inadecuados que ayuda prevenir o dificultar esas conductas entre las personas que forman parte de la organización, así como ayuda a las personas con responsabilidad y poder en la misma a generar y orientar debates a la hora de tomar decisiones. Por último, cabe puntualizar que no toda conducta contraria al código de conducta de una organización será ilícita, pero

sí toda conducta ilícita será no ética. De ahí, que dicho código debe recoger las conductas éticas esperadas de las personas vinculadas a una organización, las cuales estarán siempre alineadas con los principios y valores de la entidad.

ELEMENTOS ESENCIALES DE UN CÓDIGO DE CONDUCTA

1. ÁMBITO DE APLICACIÓN

Las directrices establecidas en los códigos deben ser de aplicación, no solo al personal propio y en todos los niveles de la entidad, sino también en esferas externas, relaciones que se establecen con otras entidades no lucrativas, las personas, la sociedad y el entorno.

2. PRINCIPIOS DE COMPORTAMIENTO ÉTICO

Los principios de comportamiento ético fundamentales que deben regir las entidades del tercer sector son principalmente entre otros[1]:

- **Buena fe.** Todas las actuaciones deben ajustarse a los principios de lealtad y buena fe con la entidad, con superiores, compañeros y compañeras, personas beneficiarias o titulares de derechos, socios, donantes y colaboradores con los que nos relacionamos. Se deben supeditar los objetivos personales a los generales de la entidad.

- **Honestidad.** Todos los miembros de la entidad se deben comprometer a declarar cualquier relación personal o profesional que pudiera condicionar el comportamiento como empleado/a de la entidad, y por tanto puedan cuestionar su imparcialidad e independencia en la toma de decisiones. Queda prohibida la aceptación de compensaciones o ventajas indebidas. Se debe inculcar la honestidad y ética profesional en las relaciones profesionales habituales en el desempeño del trabajo. No está permitido ofrecer regalos ni tratos de favor indebidos a terceros, ya sean de carácter público o privado, con el fin de obtener una ventaja. Se debe promover la confianza para declarar los regalos o ventajas que se puedan obtener de terceros y ponerlos a disposición de la entidad.

- **Respeto.** Todos y cada uno de nosotros y nosotras somos responsables de generar un ambiente de cordialidad y amabilidad en nuestro entorno. Se debe potenciar el respeto

y confianza entre las personas. Se debe apreciar la diversidad en opiniones, formación y cultura como fuente de conocimiento y ventaja competitiva. Se debe cuidar el lenguaje que se utiliza al hablar de terceros y propiciar la no existencia de pautas y comentarios difamatorios dentro y fuera de la entidad. Se debe promover el respeto a la igualdad real de oportunidades entre hombres y mujeres. Ninguna persona debe ser discriminada en el ámbito profesional por raza, discapacidad o capacidad diversa, religión, edad, nacionalidad, orientación e identidad sexual, sexo, opinión política u origen social. Se debe respetar el medio ambiente y colaborar con el desarrollo sostenible de la sociedad, así como ser respetuosos y sensibles con las costumbres y culturas propias de los territorios donde intervienen las entidades del tercer sector.

- **Confidencialidad.** Es obligatorio abstenerse de proporcionar, interna o externamente, datos confidenciales sobre las personas y/o las actividades desarrolladas en la entidad. Se deben evitar conductas contrarias a la libre competencia, o que supongan un acto de competencia desleal. En campañas publicitarias, se debe ofrecer la información de forma clara y veraz. Es obligatorio cumplir con la normativa de protección de datos de carácter personal.

3. PRINCIPIOS Y VALORES DE COMPORTAMIENTO PROFESIONAL

En este apartado se dividen los comportamientos profesionales en los que se podrían basar las entidades del tercer sector en 3 bloques de principios y valores: i) principios centrados en las personas, ii) principios centrados en las organizaciones, y iii) principios centrados en la sociedad.

Principios centrados en las personas		
Principio	**Valor**	**Recomendación**
Defensa de los Derechos Humanos	Compromiso	▪ Aplicar la Declaración Universal de Derechos Humanos y demás textos jurídicos internacionales sobre esta materia en sus actuaciones. ▪ Defender los derechos de las personas vigilando su cumplimiento y denunciando su vulneración. ▪ Apoyar a las personas en la reivindicación de sus derechos. ▪ Sustentar las reivindicaciones de los Derechos Humanos en acciones no violentas. ▪ Fomentar el empoderamiento de las personas y la autodefensa de sus derechos.
Dignidad humana	Igualdad	▪ Valorar y reconocer la diversidad. ▪ Impulsar medidas de acción positiva. ▪ Evitar actitudes que no conduzcan a la Justifica Social. ▪ Garantizar un trato digno, estableciendo las condiciones necesarias para ello. ▪ Incluir la perspectiva de género y de diversidad en la estrategia y las actuaciones. ▪ Garantizar un trato digno hacia las personas.
	Libertad	▪ Facilitar oportunidades y medios para que las personas puedan expresarse por sí mismas. ▪ Fomentar la autonomía y la autoestima de las personas. ▪ Garantizar el respeto a las decisiones de las personas. ▪ Promocionar prácticas que muestren respeto por las ideas y opiniones y creencias de las personas.

Principios centrados en las organizaciones		
Principio	**Valor**	**Recomendación**
Promoción de la implicación	Participación	■ Fomentar la participación e integración de las personas beneficiarias y voluntarias. ■ Velar por el cumplimiento de los procesos participativos. ■ Habilitar canales adecuados de participación. ■ Establecer criterios de funcionamiento democrático en la toma de decisiones y la elección de cargos en los órganos de gobierno. ■ Mantener una actitud de escucha y observación, centrada en las personas.
Cumplimiento de la misión	Responsabilidad	■ Dar respuesta a las necesidades de las personas. ■ Orientar la gestión de la organización en base a criterios de eficiencia y excelencia, y buen uso de los recursos. ■ Entender la labor como un servicio a la comunidad.
Principios centrados en la sociedad		
Principio	**Valor**	**Recomendación**
Confianza	Transparencia	■ Desarrollar su actuación bajo los principios de transparencia y buen gobierno. ■ Garantizar la transparencia en la elección de cargos de los órganos de gobierno, y en la gestión de personas en general. ■ Garantizar la transparencia económico-financiera
	Rendición de resultados	■ Informar de los acuerdos tomados y trabajos realizados, publicando la información relevante. ■ Ser transparente en la demanda de recursos económicos. ■ Promover el control externo de la gestión económico-financiera.
	Honestidad	■ Rechazar fórmulas especulativas y de riesgo en la gestión de los fondos. ■ Ser austeros en la utilización de los medios disponibles. ■ Velar por la independencia de las organizaciones. ■ Actuar de forma equilibrada y coherente cumpliendo con la legalidad vigente. ■ Rechazar y evitar recibir dádivas y el lucro personal.
Responsabilidad social	Responsabilidad	■ Colaborar activamente con otras entidades del sector. ■ Promover el desarrollo comunitario. ■ Procurar el conocimiento profundo de las demandas del colectivo que representa. ■ Dar respuesta e informar a/de las demandas de las personas vulnerables.
	Compromiso	■ Actuar como agentes de cambio social promoviendo la innovación social. ■ Contribuir a la sostenibilidad medioambiental actuando responsablemente en su ámbito. ■ Trasladar una imagen ajustada de las personas vulnerables.
	Solidaridad	■ Desarrollar políticas de colaboración e intercambio. ■ Impregnar la gestión de respeto y solidaridad hacia las personas y colectivos más vulnerables. ■ Fundamentar la toma de decisiones en el diálogo y la reflexión. ■ Fomentar el trabajo en equipo. ■ Extender la solidaridad a otras organizaciones del sector.

4. CUMPLIMIENTO Y RÉGIMEN DISCIPLINARIO

El artículo 31 bis, 5.5° del Código Penal establece que los modelos de organización y gestión exigidos para conseguir la exención de la responsabilidad penal de la persona jurídica establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo. La ley, tanto por la redacción dada en el año 2010 como la del 2015, impone a las organizaciones tener un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que impone el modelo de prevención penal.

La Circular 1/2016 de la Fiscalía General del Estado establece que los modelos o planes de prevención deben ser completos y eficaces y que no son un mero papel mojado, sino verdaderos instrumentos de concienciación de la cultura de cumplimiento. Las entidades deben asegurarse de que sus empleados/as y sus voluntarios/as entiendan que violar las políticas y procedimientos de la organización tendrá como consecuencia la adopción de **acciones disciplinarias** que pueden variar desde sanciones leves a muy graves, entre las que se distinguirán aquellas que solo afecten al personal contratado, como la terminación de su relación laboral con la organización, de aquellas otras que solo afecten al personal voluntario, como la expulsión de la organización.

Las medidas adoptadas por la entidad tras la comisión de un delito o de una falta grave contra el código de conducta, pueden acreditar el compromiso de sus dirigentes con el programa de cumplimiento. Por ejemplo, la imposición de medidas disciplinarias a las personas autoras o la inmediata revisión del programa para detectar sus posibles debilidades, la restitución y la reparación inmediata del daño, la colaboración activa con la investigación si la hubiere o la aportación al procedimiento de una investigación interna, sin perjuicio del valor atenuante que pueda tener alguna de estas actuaciones.

Sin embargo, debe existir un régimen disciplinario que no solo contemple las infracciones de tipo penal y que sea independiente de otros sistemas sancionadores, administrativos, laborales o civiles, por cuanto trae causa y justificación otra norma que no es otra que la ley penal. En consecuencia, se debe establecer un procedimiento sumario, rápido, pero con todas las garantías y que sea compatible con cualquier otro régimen, como lo son el laboral, el civil o el administrativo, sin que la sanción implique una duplicación de la sanción correspondiente.

5. DENUNCIA DE LAS IRREGULARIDADES

Un canal ético o **canal de denuncia es el más efectivo y eficaz control** de entre los que, según

prevé el Código Penal, deben formar parte de los modelos de *compliance*, a fin de prevenir y evitar la responsabilidad penal de las personas jurídicas. En este sentido, la Circular 1/2016 de la Fiscalía General del Estado se refiere a los canales de denuncia del modo siguiente: *"La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención".* Recordemos además que el término ilícito es amplio porque va más allá de lo penal pero también es preciso porque hace referencia a todo aquello que vaya en contra de la norma propia y de la ley.

Si una persona contratada, colaboradora y, en general, cualquier persona con interés directo o indirecto en la actividad que desarrolla la entidad identifica una conducta prohibida, es obligatorio comunicarlo de forma confidencial al órgano de cumplimiento a través del canal de denuncias. En el código ético es requisito obligatorio establecer la vía o vías o procedimientos para comunicar dichas irregularidades.

6. EXISTENCIA DEL ÓRGANO DE CUMPLIMIENTO

Se debe identificar la figura o área de referencia que será la persona encargada del cumplimiento del programa de *compliance*, aspecto en el que abundará con más detalle el tema 8 de la presente guía.

7. ACTUALIZACIÓN Y DISPONIBILIDAD DEL CÓDIGO

El código ético debe ser actualizado periódicamente cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la entidad, en la estructura de control o en la actividad desarrollada que lo hagan necesario.

8. ACEPTACIÓN DEL CÓDIGO

El código ético debe ser aceptado y aprobado por todos los miembros de la entidad y partes interesadas que les resulte de aplicación a través de un documento justificativo de conocimiento y contenido del mismo. A continuación, se presenta un ejemplo de modelo a seguir:

Declaro haber leído y comprometerme a cumplir el código de conducta de la Fundación XX.
Lugar y fecha.....
Firmado ..... (trabajador)
Firmado ..... (director o responsable)

En conclusión, el objeto de los modelos de organización y gestión no es solo evitar la sanción penal de la empresa, sino **promover una verdadera cultura ética a nivel organizativo**, de tal modo que su verdadera eficacia resida en la importancia que tales modelos tienen en la toma de decisiones de las personas directivas y contratadas, y en la medida en que constituyen una verdadera expresión de su cultura de cumplimiento. A tal efecto, el documento normativo de mayor categoría en una entidad y de obligado cumplimiento y donde se deben reflejar las pautas y comportamientos a seguir, así como las conductas intolerables, es en el código ético o de conducta.

1. Antonio Pascual P. C., & Antonio, P. C. (2016). El Plan de Prevención de Riesgos Penales Responsabilidad Corporativa. Barcelona: Wolters Kluwer.
RECOMENDACIONES ÉTICAS DEL TERCER SECTOR DE ACCIÓN SOCIAL. (s.f.).

CAPÍTULO 13.
GESTIÓN DE LAS DENUNCIAS.

MARÍA ALVEAR GARCÍA

LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS
POR LA UNIVERSIDAD CARLOS III DE MADRID.
POSGRADO DE GESTIÓN ECONÓMICA FINANCIERA DE ENTIDADES NO LUCRATIVAS.
MÁSTER EN ESTRATEGIAS, AGENTES Y POLÍTICAS DE COOPERACIÓN.
DIRECTORA DE ANÁLISIS DE FUNDACIÓN LEALTAD.
MIEMBRO DEL COMITÉ DE COMPLIANCE EN EL TERCER SECTOR DE LA WCA.

POR QUÉ UN CANAL DE DENUNCIAS

Un canal de denuncias es una vía de comunicación entre la entidad y sus grupos de interés mediante la cual puede conocer acciones delictivas o impropias que se estén produciendo en su seno. En el caso de las entidades del tercer sector, este canal de denuncias debe ser accesible no solo para los/as propios/as trabajadores/as de la organización, sino también para otros grupos de interés que puedan tener conocimiento de hechos denunciables, como pueden ser personas voluntarias, trabajadores/as de contrapartes o socios locales, personas beneficiarias, proveedores, otras entidades de la red, etc.

La Circular 1/2016 de la Fiscalía General del Estado (en adelante, FGE) sobre la responsabilidad penal de las personas jurídicas especifica que, uno de los elementos clave de los modelos de prevención, son los canales de denuncia. Por lo tanto, contar con un modelo de prevención penal que incluya medidas de vigilancia y control adecuadas podría suponer un eximente en la responsabilidad penal de la persona jurídica.

El hecho de contar con un canal de denuncias facilita que las organizaciones conozcan y se anticipen a actuaciones que puedan poner en riesgo a la entidad y su reputación, así como transmitir una cultura de transparencia y cumplimiento. Por lo tanto, la implementación del canal de denuncias no debe producirse de una manera aislada, sino que debe formar parte de una gestión idónea y transparente de la organización.

La implementación eficaz de un canal de denuncias debe estar sustentada por otros elementos que faciliten su uso y su integración en la organización, como son un código ético o de conducta, que permita dar a conocer la cultura organizativa y la normativa que le es propia y que, por lo tanto, facilita denunciar también actividades que son impropias de dicha cultura organizativa, o contar con un sistema disciplinario, que debe estar de acuerdo con la legislación en materia de derecho de las personas trabajadoras y ser negociado con las personas que las representen.

CARACTERÍSTICAS MÍNIMAS DE UN CANAL DE DENUNCIAS

- **Accesibilidad.** El canal de denuncias debe ser accesible, abierto y público en la página web de la organización y, además, se pueden utilizar otras vías para aquellos grupos de interés que no tienen fácil acceso a internet, como pueden ser buzones físicos, teléfono e incluso encuentros presenciales de la persona informadora con las personas responsables del canal o también con las personas representantes autorizadas del

canal, las cuales en el sector de la cooperación al desarrollo han venido a denominarse puntos focales. Es importante que cualquier medio que se utilice pueda garantizar la confidencialidad de la persona informadora.

- **Confidencialidad de la persona informadora.** Repercute en el buen uso y la eficacia del canal de denuncias, ya que su utilización depende de manera directa de la seguridad que sientan las personas a la hora de hacer uso de él. Es un factor determinante para que luego el canal sea utilizado o no como vía de denuncia.

  La Directiva Europea 2019/1937 relativa a la protección de las personas que informen sobre infracciones del derecho de la Unión establece, en su artículo 53, que *"siempre que se garantice la confidencialidad de la identidad del denunciante, corresponde a cada entidad jurídica individual del sector privado y público definir el tipo de canales de denuncia que se hayan de establecer. Más concretamente, los canales de denuncia deben permitir que las personas denuncien por escrito y que lo puedan hacer por correo, a través de un buzón físico destinado a recoger denuncias o a través de una plataforma en línea, ya sea en la intranet o en internet, o que denuncien verbalmente, por línea de atención telefónica o a través de otro sistema de mensajería vocal, o ambos. A petición del denunciante, dichos canales deben también permitir denunciar mediante la celebración de reuniones presenciales en un plazo razonable".* Es decir, si bien se pueden utilizar los medios que cada entidad decida, se debe poder garantizar la confidencialidad y, por lo tanto, que el sistema utilizado impida el acceso a terceras personas. Solo deberían tener acceso al canal de denuncias, independientemente del medio que se utilice, aquellas personas con competencias para ello, bien por razón de su cargo como pueden ser aquellas que lleven a cabo funciones de control interno o sean responsables de cumplimiento, o porque hayan sido designadas específicamente como personas encargadas de su recepción en aquellas organizaciones que no cuenten con un área de *Compliance* o similar. Esa persona o personas responsables del canal tendrán asimismo que firmar una cláusula de confidencialidad.

  Por su parte, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD) establece en su artículo 24 que los datos se podrán conservar en el sistema el tiempo imprescindible para realizar la investigación sobre los hechos denunciados, con un máximo de tres meses siempre que no haya razones que justifiquen un tiempo superior. Sin embargo, la ley establece también que, una vez transcurridos los tres meses, los datos podrán seguir siendo tratados para la investigación, pero no se conservarán en el propio sistema del canal de denuncias.

- **Independencia.** En todos los casos se debe garantizar la independencia e imparcialidad de todas las personas que participan en la gestión de las denuncias a la hora de emprender cualquier tipo de acción, pero esto cobra especial relevancia en el caso de que el canal de denuncias sea gestionado por personal de la propia organización, ya

que es donde mayores problemas pueden surgir.

Es imprescindible, por tanto, que la persona o personas designadas para cada una de las fases del proceso (recepción, investigación y resolución) puedan tomar decisiones de manera independiente, especialmente en aquellas entidades que no cuentan con la figura del *Compliance Officer*, al que se le presupone dicha independencia. Para ello, debe haber necesariamente un compromiso de los órganos de gobierno y dirección con la transparencia e importancia del canal de denuncias.

Ese compromiso se completará con un protocolo o estatuto de funcionamiento o similar que recogerá las responsabilidades que han asumido esas personas con la gestión del canal de denuncias, del mismo modo que se habrán establecido las responsabilidades de aquellas otras personas que hayan asumido la gestión de los demás componentes del sistema de *compliance*, en el caso de que no sean las mismas personas. Este protocolo o estatuto deberá ser aprobado por el órgano de gobierno para que así ese compromiso sea firme, y se configurará de tal manera que esas personas tengan poderes autónomos de iniciativa y control, tal como exige de la Circular de la FGE.

Asimismo, ese protocolo determinará cómo actuar en caso de que exista un conflicto de interés entre la persona encargada de esa parte del proceso y la denuncia recibida, bien sea designando a otra persona o derivando la denuncia a algún comité o empresa externa.

- **Anonimato.** El artículo 24 de la LOPDGDD prevé que "será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable". Por tanto, si así lo decide la organización, las denuncias podrán ser anónimas.

  La posibilidad de que las denuncias sean anónimas podría facilitar que la organización reciba información de personas que pueden tener miedo a represalias. No obstante, para evitar la posible recepción de denuncias de mala fe, es muy importante que el canal de denuncias permita mantener el diálogo con la persona informadora para poder solicitar y recibir información adicional que sea requerida para el proceso de investigación, manteniendo en todo momento el anonimato, por lo que además de plataformas anónimas en la web de la organización, también se podrán habilitar otros espacios o encuentros de intercambio.

  En cualquier caso, si la denuncia no prosperara porque falta información precisa y no

es posible el contacto con la persona informadora, la persona responsable del canal será consciente de la limitación de la instrucción o proceso de investigación que inicie, así como de la escasa posibilidad de fundamentar conclusiones finales al poder solo recabar información de la parte acusada pero no de la parte acusadora. Indistintamente del resultado final de esa investigación, esa información de origen anónimo se deberá registrar e incluso se podrá emplear y relacionar razonadamente si fuera necesario en futuros casos similares.

Tal como se señaló en el punto anterior de confidencialidad, para lograr la eficacia del canal, es primordial incentivar, ayudar y proteger a la persona informadora para que llegue el máximo número de denuncias posible. Eso se logra posibilitando tanto la confidencialidad como el anonimato. Al mismo tiempo, es importante que exista un único espacio donde se acaben registrando dichas denuncias y solo a partir de ese espacio se mantenga un histórico fiel y fiable.

Por todo esto, es fundamental que, en la gestión de toda denuncia, sea esta anónima o no, la entidad cuente con los mecanismos adecuados para que las personas informadoras tengan la seguridad de que se respetará la confidencialidad y se asegurará que no existirán represalias de ningún tipo, así como las garantías de protección de la persona denuncia o afectada sean idénticas. Por otra parte, es imprescindible la formación y sensibilización a todos los grupos de interés para que hagan un uso responsable del canal de denuncias.

- **Garantía de no represalias a las personas informadoras.** La Circular 1/2016 de la FGE recoge que *"[...] resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (whistleblower), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos, etc.) sin riesgo a sufrir represalias".* Por lo tanto, las organizaciones deberán abstenerse de tomar represalias contra una persona informadora que utilice de manera idónea el canal de denuncias.

- **Formación e información a los/as empleados/as y a otros grupos de interés.** Se deberá informar de los siguientes aspectos: existencia y funcionamiento del canal de denuncias, código ético o de conducta que rige en la organización, cómo presentar la denuncia, modo de tramitación y plazos de resolución, entre otros temas.

- **Garantizar que se respetan los derechos de la persona denunciada,** en caso de que la denuncia se refiera a una persona concreta. Para ello, se debe informar a la persona afectada, respetando tanto su presunción de inocencia como la normativa en materia de protección de datos personales. Esta comunicación se debe realizar en un plazo razonable para que pueda ejercer su derecho a la defensa, si bien dicho plazo se puede

reducir en caso de haber riesgo de destrucción de pruebas.

- **Revisión y actualización periódica del sistema.** De manera que se garantice el buen funcionamiento del mismo en todo momento.

ÓRGANO INSTRUCTOR

El órgano instructor es aquel designado para recibir las denuncias y llevar a cabo la investigación. Su nombramiento es uno de los puntos críticos para el buen funcionamiento del canal de denuncias y también para la confianza que puedan tener las posibles informadoras en él. Por lo tanto, el órgano instructor debe ser objetivo e imparcial. También es recomendable, para asegurar la objetividad e imparcialidad, que el órgano instructor sea diferente del órgano encargado de la resolución de las denuncias o de la imposición de sanciones si es necesario.

En ese sentido, cuando el órgano instructor finalice su investigación podrá elaborar un informe con el contenido más relevante de la misma, donde se identificará cuál es el artículo de la ley o el apartado concreto de la normativa interna y/o código de conducta de la organización que la persona informadora asegura que la persona denunciada o afectada incumple, se detallará cuál sería la sanción en caso de que fuera cierto, y se expondrán las evidencias aportadas por ambas partes. Ese informe podrá también contener un razonamiento donde el órgano instructor señale si existen indicios sobre si ha habido incumplimiento o no, pero lo hará solo a modo de recomendación, delegando esta conclusión al órgano que resuelve, el cual podrá ser el comité ejecutivo o directivo (alta dirección) y/o el órgano de gobierno de la organización.

La Ley Orgánica 3/2018 de LOPDGDD establece en su artículo 24 que el acceso a los datos *"quedará limitado a quienes desarrollen las funciones de control interno y de cumplimiento o a los encargados del tratamiento que se designen a tal efecto".* Se refiere, en este caso, tanto a órganos o personas de la propia organización como externas. No obstante, esta ley establece también que será lícita su comunicación a terceros *"cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan".* Es decir, además de prever la comunicación a las autoridades, se observa la posibilidad de facilitar el acceso a los datos de la denuncia al personal con funciones de gestión y control de recursos humanos si de la investigación se concluye una medida disciplinaria. No obstante, es imprescindible también, en estos casos, continuar protegiendo en la mayor medida posible la identidad de la persona informadora y evitar el riesgo de represalias.

La organización debe decidir entre los siguientes modelos de gestión de las denuncias:

- **Interno.** Dependiendo de la estructura y tamaño de la organización, puede estar

compuesto por el oficial de cumplimiento, personal de dirección, miembros del órgano de gobierno, etc. El número de personas dependerá del tamaño de la organización, pero en cualquier caso debe cumplir con las características de independencia, imparcialidad y autonomía. En el caso de entidades que no cuenten con un órgano de cumplimiento u oficial de cumplimiento, es recomendable que no sea encargada de la gestión ni una única persona ni varias personas de un mismo departamento, ya que eso dificultará la actuación en caso de un posible conflicto de interés con alguna de las denuncias recibidas. En cualquier caso, debe quedar definido el procedimiento a seguir en caso de que una o varias personas del órgano instructor estuvieran en conflicto de interés. Por ejemplo, en estos casos se puede establecer que sea el órgano de gobierno quien realice la investigación o, si se pudiera asegurar la consistencia de la misma, podría bastar con que esa persona implicada se inhibiera de la investigación y no participara en ella.

- **Externo.** Si bien la elección de un tipo u otro de gestión del canal de denuncias depende tanto del tamaño como de los medios de cada organización, la Circular 1/2016 de la FGE indica, como ventajas de la externalización de la gestión del canal de denuncias, la imparcialidad y objetividad del órgano externo. La contratación de un tercero para la gestión del canal de denuncias implica también que la organización debe garantizar la independencia, confidencialidad, protección de datos y secreto profesional.

PROCEDIMIENTO TRAS LA RECEPCIÓN DE UNA DENUNCIA

A continuación, se enumeran las posibles fases del proceso tras la recepción de una denuncia, sin que se pretenda que esta descripción sea exhaustiva, ya que cada organización deberá establecer su propio protocolo de gestión de las denuncias. Es importante que todo el proceso quede documentado de manera correcta, así como el cumplimiento de los plazos establecidos y la comunicación con la persona informadora sobre la fase en la que se encuentra. A modo de ejemplo, las fases de la investigación podrían ser:

- **Recepción de la denuncia por parte del órgano designado.** Se deberá hacer constar fecha de recepción, forma y contenido. Se abrirá, para cada denuncia recibida, número de expediente que permita su control y seguimiento.

- **Análisis de pertinencia.** Se analizarán los hechos denunciados para determinar si procede continuar la investigación, archivar la denuncia por no existir indicios de delito o de conducta inapropiada o si se traslada a otro órgano competente.

- **Designación del equipo investigador.** En caso de que así se considere, se abrirá un

expediente de investigación y se establecerán la persona o personas que realizarán la investigación. La designación del equipo investigador se realizará en función de la tipología o área de la denuncia, y se debe realizar siempre evitando posibles conflictos de interés.

- **Investigación.** Se realizarán entrevistas a las personas implicadas, solicitudes a otros departamentos, obtención de información de fuentes externas, etc. Este proceso debe respetar siempre, tanto el derecho a la defensa, en el caso de que exista una denuncia contra una persona concreta, como el principio de confidencialidad respecto a la identidad de la persona informadora y de la denunciada o afectada.

- **Resolución.** Una vez finalizada la investigación, se emitirá un informe con las conclusiones. Este informe se remitirá al órgano que deba resolver la denuncia y a cualquier otro órgano que se establezca en el proceso. Como ya se señaló antes, el órgano que resuelve podría ser el comité ejecutivo o directivo, pero también podría ser el órgano de gobierno. Pero, indistintamente de cuál sea el caso, podría existir la obligación de informar al órgano de gobierno de la organización.

- **Propuesta de sanción y/o cierre del proceso.** Si es pertinente, el órgano que resuelve efectuará una propuesta de sanción y, en el caso de que el hecho denunciado pueda ser constitutivo de delito, se propondrá ponerlo en conocimiento de la fiscalía o el juez. En el caso de organizaciones del tercer sector, lo recomendable es que el órgano de gobierno esté informado de las conclusiones del proceso de investigación. En ese sentido, y de forma anual, al órgano de gobierno se le debería remitir un breve informe donde se exponga el número de denuncias tramitadas, el número de investigaciones finalizadas y el número de denuncias que se han cerrado con sanción, así como clasificadas todas ella por tipologías, que bien podrían ser estableciendo la temática a la que alude, según la clasificación de riesgos que hemos propuesto en esta guía (financiero, estratégico, de reputación, etc.), o bien podrían ser estableciendo si es falta contra procedimientos o normativa propia; incumplimiento del código ético o de conducta; o vulneración de la ley, penal o no. Al ser el máximo órgano de gobierno, más allá de exigir esta rendición de cuentas interna, podrá también requerir mayor información sobre cualquier caso, si así lo fundamenta, y salvaguardando la confidencialidad pertinente.

CAPÍTULO 14.
MAPA DE DELITOS POR PROCESOS Y CONTROLES.

MÓNICA VARELA GIL

LICENCIADA EN DERECHO.
DIPLOMA DE ESTUDIOS AVANZADOS EN DERECHO INTERNACIONAL PÚBLICO Y ESPECIALIZACIÓN EN DERECHOS HUMANOS.
TÉCNICO JURÍDICO EN LA FUNDACIÓN SAVE THE CHIDREN.
MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA COORDINADORA DE ONG DE DESARROLLO.

ELENA HIDALGO GAVIRIA

LICENCIADA EN ECONÓMICAS Y EMPRESARIALES.
ESTUDIOS DE POSGRADO EN ECONOMÍA REGIONAL Y EN GESTIÓN DE ENTIDADES NO LUCRATIVAS.
RESPONSABLE DE FINANCIACIÓN, PROYECTOS Y TRANSPARENCIA DE LA CONGD.
MIEMBRO DEL GRUPO DE TRANSPARENCIA Y BUEN GOBIERNO DE LA CONGD.

INTRODUCCIÓN

El objeto de este capítulo es compartir la experiencia de la Coordinadora de ONG de Desarrollo y, en concreto, del Grupo de Trabajo de Transparencia y Buen Gobierno, en sus tareas de análisis normativo, en el ejercicio de abstracción de un mapa de riesgos en una ONG de Desarrollo. No hay que perder de vista que es un ejercicio de abstracción, pedagógico, con la intención de facilitar el camino a la elaboración y actualización del mapa de riesgos en las organizaciones. El verdadero trabajo será el que cada organización realice, con su proceso de reflexión interno, adaptado a su actividad y funcionamiento, y la revisión y/o elaboración posterior de los controles asociados que sirvan de prevención a la comisión de un delito.

Desde el Grupo de Transparencia y Buen Gobierno, nos parecía importante hacer este ejercicio, para animar a las organizaciones a plantear las preguntas y buscar sus propias respuestas, de manera que fuese un ejercicio práctico que sirviese de calentamiento antes de abordar el mapa de riesgo ad hoc en nuestras organizaciones.

Este trabajo no hubiera sido posible sin la colaboración pro bono del Centro de Responsabilidad Social del Ilustre Colegio de Abogados de Madrid, y de la mano de Ruth de Miguel Sedano, que nos puso en contacto con el despacho de abogados Garrigues y, en concreto, con Beatriz Bustamante y Laura Santiago, quienes nos apoyaron y guiaron durante todo este proceso de reflexión y aprendizaje[1].

POR QUÉ ES IMPORTANTE CONTAR CON UN MAPA DE DELITOS

En línea con lo recogido en el tema 1 de la presente guía, son numerosas las ventajas a la hora de disponer de un programa de *compliance*, y en este caso concreto, se detallan algunas específicas de la identificación y evaluación de los delitos en una organización:

- Permite analizar el trabajo de forma minuciosa e identificar eventos que pueden generar riesgos.
- Ayuda a actualizar y, en su caso, desarrollar protocolos y procedimientos de prevención ante esos eventos de riesgo.
- Constituye un elemento de confianza para nuestra base social, para las personas donantes, y para la sociedad en general.

- Permite dotar a las organizaciones de elementos que facilitan la toma de decisiones.

- Puede evitar penalizaciones por incurrir en alguno de los delitos recogidos en el Código Penal. A continuación, se detalla el catálogo de posibles penas, lo que hace una idea de la dimensión económica, operativa y reputacional que implica:

  - Multa por cuotas o proporcionales.

  - Disolución de la persona jurídica.

  - Suspensión de actividades (hasta 5 años).

  - Clausura de locales y establecimientos (hasta 5 años).

  - Prohibición de realizar actividades en cuyo ejercicio se haya cometido, favorecido, o encubierto el delito (temporal hasta 15 años o definitiva).

  - Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público, y gozar de beneficios e incentivos fiscales o de la Seguridad Social (hasta 15 años). De carácter obligatorio en delitos contra la Hacienda Pública y la Seguridad Social y cohecho.

  - Intervención judicial para salvaguardar los derechos de las personas contratadas o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de 5 años.

  - Para algunas organizaciones, es un esfuerzo difícil de asumir, ya que se cuenta con escasos recursos para abordar este análisis. Por eso, con este capítulo, queremos contribuir a facilitar un acercamiento a la elaboración de un mapa de delitos, a través del análisis de los principales eventos de riesgo y las posibles medidas de prevención que se pueden poner en marcha.

En todo momento, debemos tener en cuenta que, para que se produzcan estos delitos y se consideren como tal, tiene que producirse con ello un **beneficio directo y/o indirecto para la organización en cuestión.**

No obstante, cabe destacar desde el inicio que el ámbito de aplicación de esta guía no es solo el *compliance* penal, sino el *compliance* en sentido completo, que es aquel que incluye cualquier tipo de riesgo que pueda comprometer los objetivos estratégicos de la organización (ver capítulos 1, 5, 6 y 7). Por lo tanto, el enfoque de la guía es más amplio que este capítulo de mapa de delitos, aunque todo lo que se refiere aquí se podría trasponer sin problemas y contribuir así a crear una cultura ética y de cumplimiento.

QUÉ INFORMACIÓN DEBE CONTENER UNA MAPA DE DELITOS

A continuación, se detallan cada uno de estos elementos:

ARTÍCULOS	DELITOS	DEPARTAMENTOS IMPLICADOS						EVENTOS DE RIESGO Y EJEMPLOS	CONTROLES ASOCIADOS
		RRHH	Financiero/ Contable	Jurídico	Proyectos	Administración	Otros		

- **Artículos y delitos.** Listado de artículos y delitos correspondientes a la responsabilidad penal de las personas jurídicas y recogidos en el Código Penal.

- **Departamentos implicados.** Definir a qué departamentos, equipos o procesos de la organización afectaría cada uno de los delitos, esto es, dónde existe riesgo de que éste pueda cometerse. En la plantilla adjunta se plantea una propuesta, por lo que deberá adaptarse a la estructura propia de cada organización.

- **Eventos de riesgo y ejemplos concretos.** Con la participación de las personas responsables de los departamentos, equipos o procesos de la organización, se identificarán los eventos de riesgo asociados a los distintos delitos.

- **Controles asociados.** Por último, una vez detectados los eventos de riesgo, se deberá definir la batería de controles necesarios para prevenir y/o mitigar estos eventos, algunos de los cuales ya existirán u otros que será necesario diseñar.

ANÁLISIS DE PREVENCIÓN, DELITO A DELITO

A continuación, se detallan aquellos delitos que podrían tener lugar en una organización del tercer sector, pero que en cualquier caso se trata de una mera propuesta, por lo que cada organización debería hacer un análisis propio y específico:

- **Descubrimiento y revelación de secretos.** Art. 197 a 197 ter del Código Penal. Este delito está relacionado con la protección de datos y la seguridad[2]. Muchas circunstancias se dan en nuestras organizaciones y en varios departamentos, equipos o procesos que necesitan de controles y prevención. Nos podríamos hacer las siguientes preguntas: ¿cómo es el acceso a los sistemas informáticos?; ¿qué datos personales de las personas trabajadoras manejamos y cómo lo hacemos?; ¿tenemos datos personales de estudiantes, personas beneficiarias y proveedores?; cuando celebramos actos,

¿los grabamos?, ¿tomamos fotos? Esto nos hará hacernos con un mapa en torno a este delito y los eventos relacionados y plantearnos ciertas medidas, como el acceso restringido a ciertas carpetas del servidor, la creación de un sistema de manejo y actualización de contraseñas y el diseño, para todo ello, de una política de seguridad. Haríamos lo mismo con los datos personales, diseñando una política que recoja todas las medidas de seguridad técnicas y organizativas para garantizar la protección de los datos personales que trabaja la organización, desde su recogida hasta su custodia, incluidas las imágenes.

- **Delitos contra la Hacienda Pública y la Seguridad Social** (fraude a la Hacienda pública y supuestos agravados; fraude a la Seguridad Social, supuestos agravados y disfrute indebido de prestaciones del sistema de Seguridad Social; fraude de ayudas y subvenciones públicas; incumplimiento de obligaciones contables establecidas por ley tributaria). Art. 305 a 310 del Código Penal. Estos delitos conllevan la intencionalidad. Para su consumación, es necesario obtener el resultado buscado y solo podrán ser cometidos por los obligados tributarios, contribuyentes, titulares de las ventajas fiscales, solicitantes de subvenciones o pagos o los obligados a la llevanza de la contabilidad.

  Algunos ejemplos que pueden tener lugar en las organizaciones del tercer sector son: irregularidades en el ámbito tributario e incumplimiento de las obligaciones fiscales (impuestos, tasas, etc.), obligaciones frente a la Seguridad Social (cuotas, etc.) e irregularidades o incumplimiento de las obligaciones contables, al no reflejar las cuentas con exactitud la imagen fiel.

  Especial mención se debe dar al delito de fraude de ayudas o subvenciones públicas, el cual busca proteger el patrimonio de la Hacienda Pública, que ve menoscabados sus recursos destinados a fines prestacionales y la finalidad a la que atiende la actividad subvencionada que se ve alterada o frustrada por la aplicación de esos recursos a otros fines. Un ejemplo que se puede dar en las organizaciones es que se presente ante la Administración información o documentación incompleta o poco rigurosa y/o no respetar el fin de la concesión de la subvención o ayuda.

  Como controles asociados para evitar estos eventos de riesgo, podrían ser, entre otros, disponer de un código de conducta, establecer controles de supervisión para verificar el pago oportuno de cualquier tributo, y el correcto manejo de contabilidad. En este último control nos referimos al doble check de cierres contables, incluyendo conciliaciones bancarias, arqueos de caja y estados financieros, además de la realización de auditorías financieras externas y un plan de formación continua al equipo de contabilidad. En general, establecer controles de supervisión para verificar el destino de las donaciones obtenidas mediante herramientas que permitan la trazabilidad de los fondos, así

como disponer de procedimientos internos que los complementen y que orienten la justificación de los recursos.

- **Blanqueo de capitales y supuestos agravados.** Art. 301 a 302 del Código Penal. Se persiguen tres tipos de conductas: adquirir, poseer, utilizar, convertir o transmitir bienes conociendo que provienen de una actividad delictiva; realizar cualquier acto para ocultar o encubrir el origen delictivo de los bienes o para ayudar a la persona que haya participado en la infracción a eludir las consecuencias legales de sus actos; y ocultar o encubrir la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos, a sabiendas de que proceden de algún delito.

  La ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo[3] y su reglamento de desarrollo también deben ser cumplidas por las organizaciones del tercer sector. ¿Qué nos puede pasar en las organizaciones? No cumplir con suficiente diligencia las obligaciones emanadas de la ley arriba citada, que nos afecta directamente como sujetos obligados (artículo 2.1.x de la Ley). Este tipo de conductas podrían ser derivadas, por ejemplo, de no cumplir exhaustivamente con la obligación de identificar a los donantes o a las contrapartes, falta de documentación o de actualización de la documentación, etc.

  Para evitar este evento, nuestro control sería desarrollar y poner en práctica una política y procedimiento que emanen de la propia Ley 10/2010, y que, por tanto, cumplan con las obligaciones recogidas en el artículo 42 del Real Decreto 304/2014, contando con protocolos para garantizar la trazabilidad y el uso lícito de los recursos desde el origen al destino de los mismos.

- **Cohecho activo: cometido por particular a autoridades o personal funcionariado público; cometido por particular a autoridades, funcionariado públicos o agentes que trabajen en o para la Unión Europea, u otro país extranjero u organización internacional.** Art. 419 a 427 bis del Código Penal. Se protege el prestigio y eficacia de la Administración Pública garantizando la probidad e imparcialidad de su personal funcionariado y, asimismo, la eficacia del servicio público encomendado a estos. Puede ser cometido por una persona a autoridades o funcionariado público del gobierno español o que trabajen en o para la Unión Europea, u otro país extranjero u organización internacional.

  ¿Cómo puede una organización incurrir en este delito? Al no observar la transparencia e integridad en la relación con autoridades o funcionariado público, tratando de obtener con ello un trato favorable o indebido.

¿Cómo podemos prevenirlo? A través del código de conducta de la organización, de una política sobre anticorrupción/anti soborno, declaración de conflicto de intereses, cláusula en contrato/convenio con la entidad y registro y control de regalos recibidos y realizados.

- **Tráfico de influencias: cometido por particular a autoridad o funcionariado público.** Art. 428 a 430 del Código Penal. Se protege el principio de imparcialidad de la actuación de la Administración Pública.

  Una organización puede incurrir en este delito al no observar la transparencia e integridad debidas en la relación con autoridades o funcionariado público, tratando de obtener con ello un trato favorable o indebido.

  Para prevenir este evento, los controles asociados serán: código de conducta (incluye difusión, formación y canales de denuncia), procedimiento que regule los posibles conflictos de interés y política sobre anticorrupción/anti soborno.

- **Estafa (estafa y circunstancias agravantes, estafa sobre cosa mueble o inmueble y contratos simulados)**. Art. 248 a 251 bis del Código Penal. La estafa se produce cuando, mediante engaño, se ataca el patrimonio privado ajeno.

  En nuestras organizaciones, pueden darse casos de estafa en diversas situaciones, afectando a distintos departamentos, equipos o procesos, por lo que debemos hacernos algunas preguntas para evitar este delito, tales como: ¿se está mostrando la información veraz o se altera algún dato o documentación con el fin de obtener la suscripción de un contrato o convenio, así como de cualquier tipo de bien, en beneficio o provecho de la propia organización o de un tercero?; ¿se contrasta la información financiera relevante de la organización?; ¿son transparentes las condiciones en la prestación de un servicio o la ejecución de una actividad?; ¿se permite suscribir cualquier tipo de contratos, convenios u ofertas públicas con terceros o con la Administración Pública, sin la certeza razonable de poder cumplir con las obligaciones asumidas?; ¿hay una ausencia de medidas de control sobre el uso de dinero o bienes recibidos?; ¿hay controles en la custodia de contratos?; ¿existen controles sobre los medios de pago?; ¿hay procedimientos sobre el control de poderes, la aprobación y la firma de transacciones?; ¿se llegan a transmitir por venta viviendas sin verificar que estén "libres de cargas"?

  Para evitar que en las organizaciones se den algunas de estas prácticas, es importante tener una política financiera clara, con unos controles, que no centralice una persona todas las decisiones y transacciones financieras. Un procedimiento de compras y una política de poderes ayudan a seguir unas indicaciones claras para todas las personas que forman la organización, sin que puedan darse interpretaciones equivocadas.

- **Daños informáticos.** Art. 264 a 264 quater del Código Penal. Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos de manera grave y sin autorización.

  Para evitar incurrir en este delito, se deben proteger los programas o documentos electrónicos ajenos, tanto elementos informáticos constitutivos del software como grabaciones analógicas o digitales contenidas en discos o cintas magnéticas tradicionales que puedan ser dañados. ¿Y qué podemos hacer en las organizaciones? Nos ayudará en la prevención de estos eventos elaborar e implantar una política de seguridad o procedimientos informáticos.

- **Delitos sobre la ordenación del territorio y el urbanismo.** Art. 319 del Código Penal. Es un delito que implica conocer la imposibilidad de construir en determinados espacios. Exige la modificación del mundo exterior a través de la construcción y sólo podrán ser considerados autores los promotores, constructores o técnicos directores.

  ¿Cómo puede una organización del tercer sector cometer este delito? Por ejemplo, al subcontratar la construcción de infraestructuras que garanticen servicios de educación y salud (escuelas, centros de salud, pozos, etc.) a empresas sin verificar su calificación urbanística o sin constatar que disponen de los permisos correspondientes. También, al iniciar una construcción en una finca o inmueble propiedad de la organización, sin constatar que dispone de los permisos y licencias correspondientes.

  ¿Qué controles asociados podríamos desarrollar? Un procedimiento de construcción y obras dentro de la política de compras, verificar que se cumple la normativa urbanística local y una cláusula dentro del contrato. Así como incluir a terceros en nuestra cultura de cumplimiento, mediante la adhesión a aquellas políticas que muestren su compromiso de cumplimiento y alineación con valores y principios, y estándares éticos de la organización.

- **Delitos contra los recursos naturales y el medio ambiente (emisiones y vertidos; traslado de residuos; explotación de instalaciones con actividades o sustancias peligrosas; dañar elementos de espacios naturales protegidos).** Art. 325 a 328 del Código Penal. Al castigar este delito, se protege el derecho de todas las personas a disfrutar de un medio ambiente adecuado para el desarrollo de la persona, así como el deber de conservarlo.

  Una organización puede incurrir en este delito, por ejemplo, al subcontratar una empresa de gestión de residuos sin constatar que están autorizados o certificados para dicha actividad; o al trasladar residuos sin haber cumplido con la notificación previa ni la autorización necesaria que exige la legislación europea; o incluso construir instalaciones

sin verificar su calificación urbanística (y descartar que se trate de un espacio natural protegido).

Como medida preventiva se podría desarrollar una cláusula dentro del contrato, incluyendo a terceros en nuestra cultura de cumplimiento, mediante la adhesión a aquellas políticas que muestren su compromiso de cumplimiento y alineación con valores y principios, y estándares éticos de la organización.

- **Delitos contra la salud pública.** Art. 359 a 370 del Código Penal. La finalidad de castigar este delito es garantizar el derecho a la salud, imponiendo a los poderes públicos la obligación de su promoción, además de garantizar los derechos de las personas consumidoras y usuarias, las cuales pueden resultar gravemente dañadas por estas conductas.

  Directamente pueden afectar a las organizaciones los siguientes tipos: el despacho o expedición de medicamentos deteriorados (por ejemplo, no poner la atención adecuada a los requisitos y restricciones exigidos por la normativa local en materia de medicamentos), alteración de medicamentos o sustancias beneficiosas para la salud (por ejemplo, la recepción, elaboración y/o distribución de medicamentos) y manipulación de alimentos (por ejemplo, la recepción, elaboración y/o distribución de alimentos).

  Para prevenir estos eventos de riesgo, podríamos desarrollar un procedimiento de control en la compra, recepción y distribución de medicamentos y alimentos, siempre en concordancia con la normativa aplicable, con el fin de garantizar la calidad técnica de los mismos.

- **Delitos relativos a la propiedad intelectual.** Art. 270 a 272 del Código Penal. La finalidad de sancionar este delito es proteger el derecho de autor en todas sus facetas (obra literaria, artística, científica, etc.).

  Las organizaciones debemos tener especial cuidado en el uso de materiales susceptibles de estar protegidos, no haciendo uso de los mismos si no se cuenta con la autorización expresa del autor, editorial, discográfica, etc. De la misma forma, las organizaciones deben reflexionar sobre el tipo de protección que quieren dar a los materiales producidos (documentos divulgativos, videos, informes, libros, videos, etc.), estableciendo un procedimiento sobre propiedad intelectual. En cualquier caso, será necesario registrar los materiales para que no se pueda hacer un uso indebido de los mismos; solicitar autorizaciones, por escrito, para obras con propiedad intelectual e incluso la firma de contratos con cláusula de cesión de derechos.

- **Delitos relativos a la propiedad industrial (patentes, modelos de utilidad y otros**

derechos, marcas, nombres comerciales y rótulos de establecimientos). Art. 273 a 277 del Código Penal. Se protegen el derecho de exclusiva a la utilización y explotación en el comercio de los objetos amparados por un título de propiedad industrial -patentes, modelos de utilidad, marcas, nombres comerciales, rótulos, etc.- de carácter exclusivamente patrimonial e individual y la dinamización de la competencia, mediante el fortalecimiento de la posición del titular de los derechos de propiedad industrial.

En nuestras organizaciones, ¿cómo se puede materializar este delito? Utilizando una patente o modelo de utilidad sin la autorización de su titular, empleando signos distintivos de otras organizaciones que infrinjan los derechos de su titular o incluso dar de alta un nombre o un logo parecido o confundible al de otra organización conocida para aprovechar su penetración o prestigio en la sociedad.

Para prevenir estos eventos de riesgo, será necesario comprobar que todo producto o metodología que use la organización tenga su correspondiente permiso; o con contrato y pago a un proveedor, o con autorización (por escrito) del titular de la patente, además de realizar en su caso una auditoría de proyectos y hacer las necesarias comprobaciones en el Registro de marcas y patentes (guardando la comprobación por escrito).

- **Apoderamiento, difusión, revelación, cesión, divulgación o utilización de secretos de empresa.** Art. 278 a 280 del Código Penal. Se protegen los intereses del mercado y de las personas consumidoras y, en concreto, la capacidad competitiva de la empresa, castigándose el espionaje industrial y protegiendo la información como valor económico de la empresa.

  En nuestras organizaciones, se puede dar este delito al emplear información de interés, sensible o confidencial perteneciente a otra organización con el fin de obtener ventaja competitiva.

  Como medidas de control, en este caso, se recomienda disponer de un código de conducta, un procedimiento de compras y relación con proveedores, así como incluir una cláusula fija de confidencialidad en los contratos laborales y en contratos de prestación de servicios, y poner en marcha un canal de denuncias accesible a los diferentes grupos de interés, entre otros a personas trabajadoras, personal voluntario, socios locales y proveedores. En la medida en que, a través del canal, se debe poner de manifiesto cualquier irregularidad o incumplimiento, esta es una medida de control que aplica para todos los riesgos penales y riesgos de cualquier tipo.

- **Publicidad engañosa.** Art. 282 del Código Penal. La finalidad de incluir este delito es proteger los intereses de las personas consumidoras y, en concreto, la información veraz. Se pretende evitar, por ejemplo, que las organizaciones realicen publicidad

ofreciendo información incompleta, no contrastada o poco rigurosa sobre lo ofrecido.

Para evitar estos eventos de riesgo, nuestros controles asociados provendrían de nuestro código de conducta, el desarrollo de un procedimiento de captación de fondos (incluiría compromiso público en la web, contratos e informes en los que se asume la obligación de respetar el destino de los fondos, especificarlo en las campañas, etc.), así como de un procedimiento de comunicación de información veraz y transparente.

- **Corrupción en los negocios (corrupción entre particulares y corrupción a funcionariado público en actividades económicas internacionales).** Art. 286 bis a 286 quater del Código Penal. Se sanciona este delito para proteger una competencia justa y honesta en el ámbito de los negocios privados. La corrupción puede ser activa (un beneficio o ventaja no justificados de cualquier naturaleza) o pasiva (reciba, solicite o acepte ese beneficio o ventaja). La corrupción puede ser entre particulares, o con autoridades o funcionariado público, y el tipo de beneficio puede ser regalos, dinero, ocio o entretenimiento, entre otros.

  Las organizaciones debemos tender a una tolerancia cero en este sentido, evitando situaciones que puedan llevar a la ilegalidad. Los controles asociados, además del código de conducta, serían el desarrollo de una política sobre anti corrupción/anti soborno, declaración de conflicto de intereses, cláusula en contratos y registro de gastos efectuados en regalos y de regalos recibidos. Las medidas preventivas para los dos delitos de corrupción en los negocios pueden ser comunes, simplemente tienen que abarcar tanto a las personas particulares o ámbito privado (primer delito), como a las autoridades y funcionariado público (segundo delito). Estas medidas también se podrían extender a la prevención de los delitos de cohecho y tráfico de influencias, detallados anteriormente.

- **Delitos contra los derechos de los ciudadanos extranjeros.** Art. 318 bis del Código Penal. En este delito se incluyen el tráfico ilegal y la migración clandestina de personas.

  ¿Cómo puede una organización ser responsable por este delito? Por ejemplo, facilitando la entrada en territorio español, desde otro país, sin comunicarlo a las autoridades y evitando cualquier identificación y control.

  Para ello, los controles asociados vendrán de la mano de nuestro código de conducta y del desarrollo, por ejemplo, de un procedimiento de visitas.

- **Falsificación de tarjetas de crédito, débito o cheques de viaje.** Art. 399 bis del Código Penal. Se trata del uso inapropiado de los datos de las tarjetas de crédito, débito o cheques de viaje.

En una organización se podría dar, por ejemplo, la duplicación de los datos contenidos en una tarjeta bancaria.

Para ello, además de nuestro código de conducta, como controles asociados podríamos desarrollar un procedimiento sobre uso/permiso de medios de pago, así como un sistema de verificación y control de pagos con tarjeta.

- **Fomento, promoción o incitación al odio, hostilidad, discriminación o violencia contra grupos.** Art. 510 del Código Penal. Se trata de proteger la dignidad de la persona. El discurso del odio es una conducta orientada hacia la discriminación frente a un determinado grupo o sus integrantes. No se sancionan las meras ideas u opiniones, sino las manifestaciones de odio que denotan un desprecio hacia otro ser humano, por el simple hecho de ser diferente.

  Los eventos de riesgo en una organización podrían ser utilizar canales de información y redes sociales no controlados; la falta de diagnóstico y análisis sobre las interpretaciones de los mensajes que se van a comunicar; y no revisar las comunicaciones de terceros en nombre de la organización.

  Para prevenir estos eventos de riesgo, podríamos desarrollar un código de conducta y un procedimiento de comprobación de la adecuación de los mensajes o comentarios que se efectúan en nombre de la organización antes de su emisión, publicación o difusión. También, contagiaremos a los terceros la cultura de cumplimiento de la organización, mediante la adhesión a aquellas políticas que muestren su compromiso de cumplimiento y alineación con valores y principios, y estándares éticos de la organización.

- **Medidas derivadas del artículo 129 del Código Penal:**

  - Delitos contra los derechos de las personas trabajadoras: condiciones laborales o de Seguridad Social lesivas, inmigrantes o menores, tráfico ilegal de mano de obra, emigración fraudulenta, discriminación en el empleo, limitación de la libertad sindical y derecho de huelga, omisión de medidas de seguridad y salud en el trabajo con infracción de normas de prevención de riesgos laborales. Se protegen los derechos reconocidos legalmente a las personas trabajadoras[4]:

    En una organización, se pueden dar las siguientes circunstancias: dificultar injustificadamente a un/a trabajador/a disfrutar de las vacaciones que legal o contractualmente le corresponden; no prestar la debida atención a los plazos que establece la Seguridad Social; imponer a los/as empleados/as condiciones laborales desfavorables; inducir a un/a empleado/a a desvincularse de la organización; contratar a personal extranjero o menores de edad, sin verificar la documentación exigida; contratar a personal extranjero sin haber tramitado debidamente su permiso

de trabajo; dar empleo en otro país sin comunicar a la Seguridad Social su contrato; no ser rigurosos en la aplicación de criterios objetivos en la relación con los/as empleados/as; dificultar a los/as empleados/as hacer uso de sus derechos sindicales; durante una huelga, dificultar o impedir a los/as empleados/as ejercitar su derecho a la misma.

Para prevenir estas situaciones deberíamos tener implantado un código de conducta (incluyendo su difusión, formación y canales de denuncia), así como contar con una política y procedimiento de personal (selección y contratación), con una política de igualdad y/o de no discriminación y garantizar que en los procesos de selección participan diferentes personas, siendo la valoración de cada una de ellas compartida con todo el equipo que participa en la selección. No se deberían permitir valoraciones individuales o secretas y sería importante contar con un Comité de Empresa.

» **Asociación ilícita.** Según el Código Penal *"son punibles las asociaciones ilícitas, teniendo tal consideración: las que tengan por objeto cometer algún delito o, después de construidas, promuevan su comisión, así como las que tengan por objeto cometer o promover la comisión de faltas de forma organizada, coordinada y reiterada; las que, aun teniendo por objeto un fin lícito, empleen medios violentos o de alteración o control de la personalidad para su consecución; las organizaciones de carácter paramilitar; las que promuevan la discriminación, el odio o la violencia contra personas, grupos o asociaciones por razón de su ideología, religión o creencias, la pertenencia de sus miembros o de alguno de ellos a una etnia, raza o nación, su sexo, orientación sexual, situación familiar o enfermedad o minusvalía, o inciten a ello."*

Puede darse, en las organizaciones, una falta de control interno sobre los objetivos misionales de la organización, o la inclusión de simbología, comentarios referentes a grupos u organizaciones criminales o terroristas, o, por ejemplo, no comprobar los mensajes oficiales que se realizan en nombre de la organización, o hacer uso de expresiones o justificaciones en apoyo del terrorismo en nombre de la organización en ponencias o cualquier evento público.

Para ello, además de disponer de un código de conducta, incluyendo su difusión, formación y canales de denuncia, deberíamos desarrollar una política de portavocía y verificar las relaciones con terceros (otras organizaciones, proveedores, etc.).

» **Organizaciones y grupos criminales y organizaciones y grupos terroristas y delitos de terrorismo.** Los eventos relacionados con este delito son, por ejemplo, la falta de verificación e identificación de los fondos recibidos y entregados y la falta de control interno sobre los objetivos misionales de la organización. Para prevenirlo, podemos contar, además de con un código de conducta, con un manual/protocolo

de prevención de blanqueo de capitales y financiación del terrorismo y verificar las relaciones con terceros.

- **Frustración de la ejecución: alzamiento de bienes, presentación de relación de bienes incompleta o mendaz y uso de bienes embargados sin autorización.** Art. 257 a 258 ter del Código Penal. La frustración de la ejecución es la conducta en la que una persona deudora oculta bienes, de forma que la acreedora no encuentre en su patrimonio medios económicos suficientes con los que pueda satisfacer sus créditos[5].

  En nuestras organizaciones, se puede materializar a través de la falta de atención, o atención incompleta, ante el requerimiento del juez sobre la situación patrimonial de la empresa; actos que supongan una disminución del patrimonio, realizados con anterioridad a la posible notificación de una sentencia que podría resultar condenatoria; falta de notificación formal interna en caso de embargo; ventas de bienes inmuebles sin atender las posibles deudas o derechos de crédito de las personas acreedoras; o la falta de atención de notificaciones de embargo relativas a los acreedores.

  Es importante que, en las organizaciones, exista un sistema de comunicación directa y transparente, en el que las personas que trabajan con la información directamente faciliten esos detalles, que pueden tener gran trascendencia, a las personas representantes de la organización.

- **Insolvencias punibles (disposición de bienes en situación de insolvencia y circunstancias agravantes, pago fraudulento a personas acreedoras y presentación de datos contables falsos en procedimiento concursal).** Art. 259 a 261 bis del Código Penal. Son tipos de disminución o destrucción de un patrimonio como consecuencia de una mala gestión en situaciones de insolvencia real.

  Las organizaciones deben actuar con la diligencia debida en la gestión de los asuntos económicos para no disminuir el patrimonio de la sociedad. En este sentido, es importante contar con una política de contabilidad y pagos que establezca los procesos a seguir dentro de la organización para no incurrir en este delito.

- **Financiación del terrorismo.** Art. 576 del Código Penal. Las conductas penadas son: recabar, adquirir, poseer, utilizar, convertir, transmitir o realizar cualquier otra actividad con bienes o valores de cualquier clase con intención de que se utilicen, o a sabiendas de que serán utilizados, para cometer cualquiera de los delitos de terrorismo o para hacerlos llegar a una organización o grupo terrorista.

- Una organización puede llegar a cometer este delito, por ejemplo, al no cumplir

exhaustivamente con la obligación de identificar a los proveedores, falta de documentación o de actualización de documentación, etc. Esta organización no está cumpliendo con suficiente diligencia las obligaciones emanadas de la Ley 10/ 2010 y el reglamento que la desarrolla, ambos citados previamente, que nos incumben como sujetos obligados.

Los controles asociados serían, disponer de un código de conducta (incluye difusión, formación y canales de denuncia) y el desarrollo de un manual/protocolo de prevención de blanqueo de capitales y financiación del terrorismo.

- **Financiación ilegal de los partidos políticos (donaciones o aportaciones).** Art. 304 bis del Código Penal. La finalidad de este artículo es proteger el buen funcionamiento del sistema democrático. Únicamente se contempla el riesgo para organizaciones vinculadas a partidos políticos, y un posible riesgo adicional para la financiación de partidos políticos en otros países (según los requisitos del Código Penal aplicables a delitos fuera de España).

  En este caso, los controles asociados podrían ser: elaborar y poner en práctica un procedimiento de compras y selección de proveedores, llevar contabilidad única y separada del partido político, identificación real de los donativos recibidos y servicios ofrecidos al partido político e incluir en la normativa interna (código de conducta, relaciones institucionales, etc.) la prohibición expresa de realizar cualquier donación o aportación que tenga como destinatario un partido político, federación, coalición o agrupación de electores.

- **Delitos de prostitución.** Art. 187 a 190 del Código Penal. Dentro del desarrollo de nuestras actividades, tenemos que detectar aquellas situaciones que pudiesen permitir el desarrollo de acciones, que pudieran contribuir a no respetar la libertad sexual de personas mayores de edad, menores de edad o con capacidades especiales. Ello debería quedar recogido en nuestro código de conducta y hacerse referenciar a la Declaración Universal de Derechos Humanos[6].

- **Tráfico ilegal de órganos humanos.** Art. 156 bis del Código Penal. Lo primero que tenemos que pensar es: ¿qué situaciones se dan en mi organización que puedan derivar en la comisión de este delito? Podrían ser eventos de riesgo, en este caso, aceptar un órgano para un trasplante, el traslado de los órganos desde el centro extractor al centro trasplantador o realizar intervenciones médicas que impliquen extracción de órganos. Un ejemplo de delito sería aceptar un órgano para trasplante sin comprobar su procedencia, aunque recordemos que, para que sea un delito, debe de darse un beneficio para la organización.

Continuando con nuestro análisis, tendríamos que identificar qué departamentos, equipos o procesos estarían implicados, para poder implantar las medidas de prevención. En este caso, podría involucrar a dirección, a administración, al personal sanitario de la organización y al comité ético, si existe. Por último, tenemos que recopilar y actualizar, si las tenemos, y desarrollar las medidas de control asociadas a estos eventos. Podrían ser el código de conducta, incluyendo su difusión, formación y establecimiento de canales de denuncia; la existencia de un departamento o mecanismo que vigile el cumplimiento y seguimiento de la normativa específica en la materia: Ley 30/1979, de 27 de octubre, sobre extracción y trasplante de órganos[7]; Real Decreto 1723/2012, de 28 de diciembre, por el que se regulan las actividades de obtención, utilización clínica y coordinación territorial de los órganos humanos destinados al trasplante y se establecen requisitos de calidad y seguridad[8], Directiva 2010/53/UE, del Parlamento Europeo y del Consejo, de 7 de julio de 2010, sobre normas de calidad y seguridad de los órganos humanos destinados al trasplante[9]; y desarrollar un protocolo de procedimientos sanitarios.

- **Trata de seres humanos.** Art. 177 bis del Código Penal. En nuestras organizaciones, trabajamos con personas de otros países, tenemos relaciones laborales, de voluntariado, externalizamos actividades. Es necesario controlar que en toda la cadena de intervención tenemos en cuenta los derechos humanos[10], y ello deberá quedar recogido en el código de conducta de nuestras organizaciones. Además, y dependiendo de cuál sea esta cadena de intervención, se requerirán controles específicos. Por ejemplo, para evitar la explotación laboral se deberá llevar un control y seguimiento del registro de horas del personal contratado.

CONCLUSIONES

Es importante que las organizaciones hagamos un análisis interno, profundo y realista de quiénes somos, con quién nos relacionamos, cómo trabajamos, dónde estamos, dónde queremos llegar y cómo lo vamos a hacer.

Después, debemos aterrizar los delitos en eventos que puedan darse en la organización, para hacer un mapa ajustado a nuestra actividad. Cada organización tiene unas características que la hacen diferente, por lo que un mapa de riesgos debe hacerse a la medida exacta de cada una. No se puede extrapolar el mapa de delitos de una organización a otra, pues no hay dos organizaciones iguales y, los eventos de riesgo de una, no van a coincidir con los de otra (algunos pueden coincidir, pero nunca será al 100%).

Las organizaciones debemos tener un código de conducta (o código ético, según la denominación en cada entidad) actualizado y alineado con la prevención de riesgos.

Este código se convertirá en el elemento central del que emanen otras políticas, protocolos o procedimientos que lo desarrollen. Además, el código de conducta deberá ser conocido, interiorizado y difundido por todos los miembros de la organización.

No debemos olvidarnos del trabajo de revisión y actualización periódica del mapa de delitos, pues pueden cambiar las circunstancias o ser necesaria una mejora de ciertos procesos, por riesgos que finalmente han sucedido, que nos obligarán a fortalecer e implementar otras medidas para evitar esos riesgos.

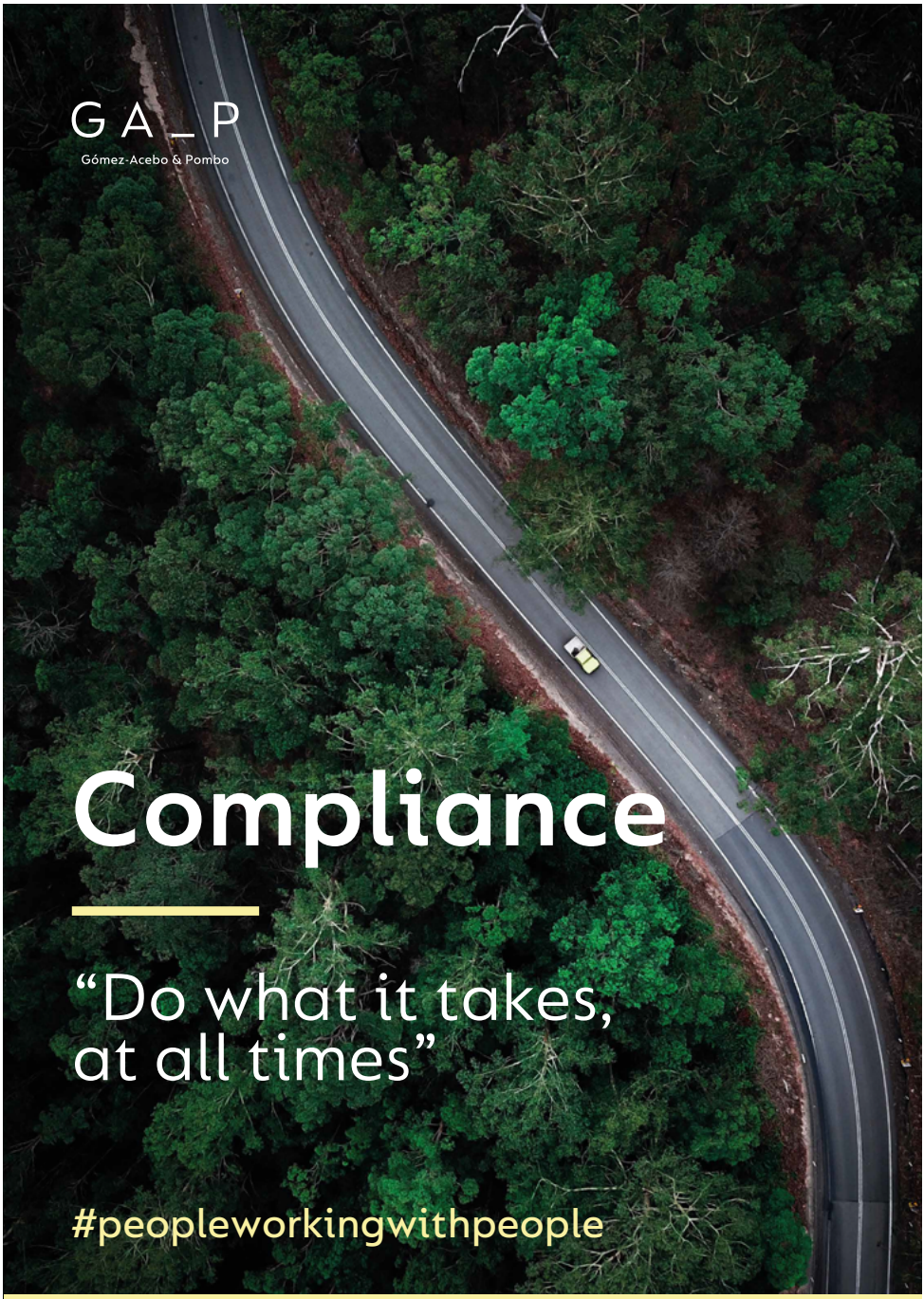
La dirección y el órgano de gobierno de la organización deben confiar, apoyar y promover un programa de *compliance*, convirtiendo el cumplimiento normativo y ético en un elemento más de la cultura de la organización, permeando a todos los niveles de la misma. En ese sentido, y tal como señalamos al principio, el *compliance* que debemos promover es aquel en sentido completo que incluye cualquier tipo de riesgo que pueda comprometer los objetivos estratégicos de la organización, más allá de lo estrictamente penal.

Ser mejores organizaciones hará que trabajemos mejor, que estemos más orgullosos y orgullosas de pertenecer a ellas, que nuestros financiadores y donantes confíen más en nosotros, que les demos más seguridad a nuestros beneficiarios o participantes, que tengamos proveedores de más calidad y que, en definitiva, la imagen que reflejemos sea una copia fiel de lo que somos.

1. Fruto de este trabajo fue la Guía práctica de auto diagnóstico y *compliance* para entidades sociales (Plataforma del Tercer Sector de Madrid, Universidad Complutense de Madrid, Ilustre Colegio de Abogados de Madrid) y las presentaciones de delitos elaboradas por el despacho de abogados Garrigues en el marco de la colaboración pro bono con La Coordinadora de ONGD.
Estas colaboraciones nos han servido de base y apoyo en la creación de este capítulo.

2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (https://www.aepd.es/es/informes-y-resoluciones/normativa-y-circulares).

3. https://www.sepblac.es/es/normativa/normativa-nacional/
4. https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430
5. https://guiasjuridicas.wolterskluwer.es/
6. https://www.un.org/es/universal-declaration-human-rights/
7. https://www.boe.es/eli/es/l/1979/10/27/30
8. https://www.boe.es/eli/es/rd/2012/12/28/1723
9. https://www.boe.es/buscar/doc.php?id=DOUE-L-2010-81418
10. https://www.un.org/es/universal-declaration-human-rights/


G A _ P
Gómez-Acebo & Pombo
Compliance
“Do what it takes, at all times”
#peopleworkingwithpeople
www.ga-p.com | gapcorporatecompliance@ga-p.com

Guía patrocinada por:

GA_P
Gómez-Acebo & Pombo

BUREAU VAN DIJK
A Moody's Analytics Company

Intedya
International Dynamic Advisors

tirant lo blanch
GRUPO EDITORIAL

tirant Compliancers®