

Gestión del riesgo de *Compliance* y su control

Óscar LÓPEZ RODRIGUEZ

Abogado

Director de UBT Compliance

1. DEFINICIÓN DE RIESGO DE COMPLIANCE

Dice el poeta que el mayor riesgo de la vida es «no hacer nada» y si una organización encuentra su sentido en el desarrollo de unas actividades que le permitan obtener sus objetivos, al igual que las personas, el «no hacer nada» en relación a ciertas exigencias legales puede acarrear riesgos, al igual que hacerlo, aunque de heterogéneas características, eso sí.

El riesgo empresarial, entendido como aquel elemento de inestabilidad o efecto de la incertidumbre que pone en peligro la competitividad, logro de objetivos o satisfacción de necesidades o intereses públicos ha requerido siempre, en el marco de unas buenas prácticas de gestión empresarial, un control y seguimiento continuo. El término «Riesgo de *Compliance*» o de «incumplimiento normativo», para entendernos mejor, pone el foco en las consecuencias que puede acarrear a la organización no cumplir con las «obligaciones de *Compliance*», en el sentido más amplio de este término, y que sean de aplicación a dicha organización²⁶¹.

El respeto al marco legal exigible a una organización, a reglamentos, instrucciones internas, políticas, procedimientos, exigencias contractuales o estatutarias, guías de comportamiento, códigos de conducta o buenas prácticas reconocidas de aplicación general en el sector de que se trate o incluso en grupos de interés, puede conllevar riesgos por acción o in-

261. Obligación de *Compliance* según la norma UNE-ISO 19600:2015. Apartado 3.16 que incluye “requisito legal de *Compliance*” (3.14) o “compromiso (voluntario) de *Compliance*” (3.15).

acción que una conducta de *Compliance*, de ética y respeto a la ley debe controlar.

Así, un término válido de «riesgo de *Compliance*» podría ser «*aquel riesgo que potencialmente puede afectar a una organización, atendiendo a su contexto, por «dejar de hacer» o «hacer», siendo esto contrario a lo exigido o prohibido en alguna norma o compromiso a ella aplicable».*

Por consiguiente, una obligación o una prohibición pueden conducir a un riesgo de *Compliance*.

La norma UNE-ISO 19600:2015, marco de referencia en el establecimiento de un Sistema de Gestión de *Compliance*, define como riesgo de *Compliance* (apartado 3.12) el «efecto de la incertidumbre en los objetivos (apartado 3.9) de *Compliance*», estos últimos como resultados a lograr²⁶², y entendida la Incertidumbre como algo que puede que nunca ocurra.

Este concepto, en mi opinión, no aclara mucho desde un punto de vista práctico, pero si recuerda, quizás, la necesidad de tener en cuenta que los objetivos empresariales, comerciales, operativos y estratégicos de la organización deben estar alineados con una cultura de cumplimiento y respeto a las obligaciones de *Compliance* y que el riesgo debe gestionarse porque tiene un efecto negativo en la imagen de una organización que desea basar su cultura en la ética.

2. LA GESTIÓN DEL RIESGO DE COMPLIANCE

El objetivo a perseguir, por tanto, en el marco de una Cultura de cumplimiento, es gestionar el riesgo legal de manera eficaz porque, sin duda, contribuye de manera indudable a conseguir los objetivos estratégicos y operativos de la compañía, a mejorar el desempeño en lo referente al cumplimiento y el respeto a las obligaciones de *Compliance* y redunda en la buena imagen corporativa. Para ello, será preciso identificar, analizar y evaluar los riesgos de forma que el resultado permita clasificar y establecer prioridades en cuanto la designación de recursos y la toma de decisiones oportunas.

262. NOTA I UNE-ISO 19600:2015. (3.12) El riesgo de *Compliance* se puede caracterizar por la probabilidad de que ocurra y las consecuencias de los incumplimientos de *Compliance* (3.18) respecto a las obligaciones de *Compliance* (3.16) de una organización.

Existen varios estándares nacionales e internacionales de gestión de riesgos que pueden facilitar el establecimiento de una metodología práctica:

- Se puede seguir la metodología COSO²⁶³ II, que tiene en cuenta algunos aspectos o componentes fundamentales a destacar como el «Ambiente de control» en cuyo capítulo se tratan los valores y los principios éticos de la organización, influyendo necesariamente en la visión de los trabajadores ante los riesgos y las actividades de control de los mismos y que se exige la definición de un Código ético, código de conducta y la Política de *Compliance* de la organización y el compromiso de la organización por la integridad y valores éticos. Otro componente relevante y que es motivo de este capítulo, es la exigencia de llevar a cabo una «evaluación de Riesgos» que permita la identificación y análisis de los riesgos relevantes para la consecución de los objetivos. Para ello, la organización debe especificar sus objetivos con suficiente claridad para permitir la identificación y valoración de los riesgos relacionados a los objetivos. Por último, se destaca la necesidad de dar una respuesta y determinar las acciones y medidas oportunas frente a los riesgos identificados, como puedan ser el establecimiento de Políticas y procedimientos internos, la asignación de responsabilidades internas y la supervisión y vigilancia cumplimiento de dichas acciones y controles internos.
- Otra de las metodologías más reconocidas es el sistema APPCC (Análisis de Peligros y Puntos Críticos de Control)²⁶⁴ de aplicación en industria alimentaria aunque también se aplica en la industria farmacéutica, cosmética y en todo tipo de industrias que fabriquen materiales en contacto con los alimentos. Esta metodología persigue identificar, evaluar y prevenir todos los riesgos de contaminación de los productos a nivel físico, químico y biológico.

263. COSO (Committee of Sponsoring Organizations of the Treadway) es una Comisión voluntaria constituida por representantes de cinco organizaciones del sector privado en EEUU.

264. Documento obligatorio y exigido por el Real Decreto 640/2006, de 26 de mayo, por el que se regulan determinadas condiciones de aplicación de las disposiciones comunitarias en materia de higiene, de la producción y comercialización de los productos alimenticios. En la actualidad el Reglamento 852/2004, obliga a estas empresas a que cuenten con un plan autocontrol según el APPCC.

gico a lo largo de todos los procesos de la cadena de suministro, estableciendo medidas preventivas y correctivas para su control, tendientes a asegurar la inocuidad.

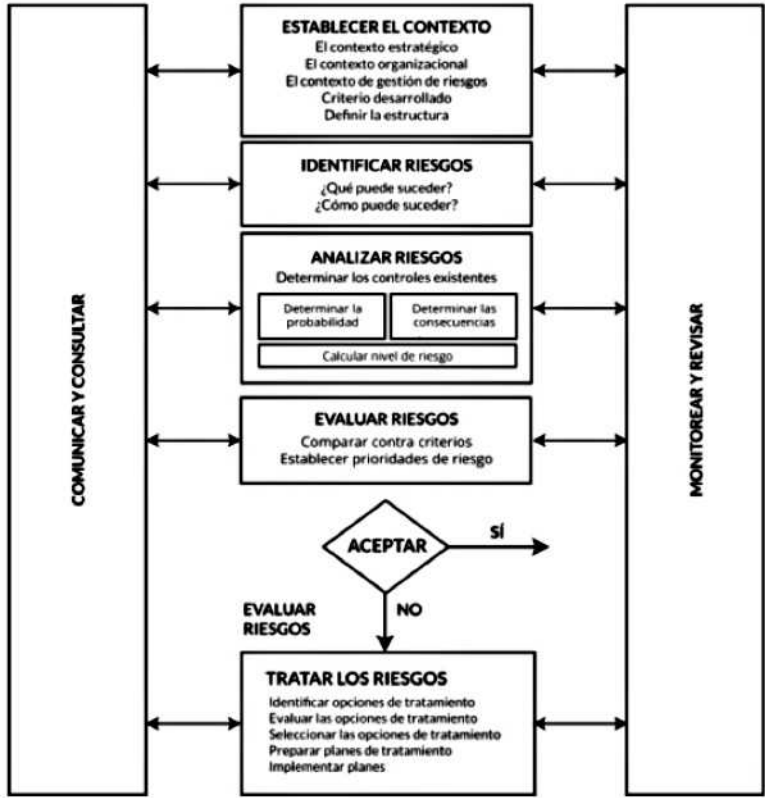
- El Sistema de Administración de Riesgo Operativo (conocido por las siglas S.A.R.O) marco regulador expedido por la Superintendencia Financiera de Colombia para la gestión de riesgos especialmente en el ámbito financiero²⁶⁵ y exigido mediante la circular externa 052 del año 2002, en el marco del Comité de Basilea es otro de los sistemas de gestión de riesgos a destacar. Así, dentro de los principios básicos propuestos por el Comité de Basilea, se definió la necesidad de dictar esquemas de administración de riesgo operativo por parte de los entes reguladores los cuales deben ser observados y aplicados por las compañías vigiladas, enunciando que las organizaciones están en la obligación de entender y medir el riesgo, determinar los niveles aceptables de exposición, implantar el control apropiado y monitorear su efectividad.
- Este sistema S.A.R.O. define una serie de tipos de riesgos entre los que se encuentra riesgo legal que lo define como «la posibilidad de incurrir en pérdidas derivadas del incumplimiento de normas legales, de la inobservancia de disposiciones reglamentarias, de códigos de conducta o normas éticas en cualquier jurisdicción en la cual opere la entidad. Igualmente puede derivar de situaciones de orden legal que pueden afectar la titularidad de los activos, o la efectiva recuperación de su valor».
- Otra herramienta que establece una serie de principios para la implementación de un Sistema de Gestión de Riesgos en las empresas dirigida a identificar, evaluar, tratar y monitorizar los riesgos asociados a una actividad, función o proceso es el estándar internacional ISO 31000:2009.

El presente gráfico recoge perfectamente los componentes del Sistema de Gestión de Riesgos propuesto por la norma ISO 31000:2009²⁶⁶

265. https://www.confianza.com.co/sites/default/files/adjuntos/cartilla_WEB_SARO.pdf

266. Acompañando a la ISO/IEC 31000:2009 y para complementarla se ha desarrollado la ISO/IEC 31010:2009 “Gestión del riesgo. Técnicas de evaluación de riesgos” que ofrece directrices para la aplicación de técnicas sistemáticas de evaluación de riesgos.

(o UNE–ISO 31000:2010 publicada en España), que nos puede servir de referencia para la gestión de riesgos de *Compliance*.



(Fuente norma UNE–ISO 31000:2010)

- Esta misma metodología de la gestión de los riesgos es la que se describe en la norma internacional ISO/IEC 27005:2011 relativo a la seguridad de información.

A través de este sistema de gestión se identifican los activos de información que se deben proteger y se valoran los riesgos desde una perspectiva de debilidades (vulnerabilidades) y amenazas a las que están expuestos proponiéndose controles de para tratar el riesgo reduciéndolo, aceptándolo, transfiriéndolo o incluso eliminándolo.

Todas estas metodologías para la implantación de un Sistema de Gestión de Riesgos aplicable a la gestión de riesgo de *Compliance* tienen elementos comunes que persiguen la definición de políticas que incluyan los objetivos de la organización en materia de *Compliance*, atendiendo a la estructura organizacional y su contexto, la identificación y evaluación de los riesgos y el establecimiento de procedimientos y mecanismos que permitan medir y controlar la ocurrencia del riesgo,

Si los objetivos de toda organización en cuanto a *Compliance* debe ser el respeto a la ley y el cumplimiento de todos los requisitos que le sean aplicables de cara a establecer un sistema de gestión de riesgos de *Compliance*, quizás haya que empezar por dar respuesta a las siguientes preguntas:

- ¿Sabe la organización como están gestionándose sus riesgos?
- ¿Tiene marcados la organización sus objetivos estratégicos y operacionales?
- ¿Tiene la organización capacidad de definir y cumplir sus objetivos de *Compliance*?
- ¿Tiene la organización definida una responsabilidad para la gestión de riesgos de *Compliance*?
- ¿Tiene la organización identificadas las obligaciones de *Compliance*, en un proceso de revisión y actualización continuo?
- ¿Esta la alta dirección implicada en apoyar, mantener y diseñar un sistema de gestión *Compliance*, para aprobar su implantación y la designación de las responsabilidades oportunas y dotar los recursos necesarios para ello?

3. ESTABLECIMIENTO DEL CONTEXTO

Partiendo de la base de que todas las organizaciones son distintas y los riesgos de *Compliance* a los que se enfrentan, por tanto, también, es preciso fijar el «contexto» de la Organización sobre la que se definirá el marco de actuación en la gestión de riesgos de *Compliance* y determinará su influencia en la evaluación de los riesgos.

Contextualizar es situar algo en un determinado contexto y establecer el contexto en el marco de la gestión de riesgos de *Compliance* resulta no solo necesario sino tremendamente eficaz porque nos va a encuadrar y determinar los límites y el alcance de nuestro Sistema de Gestión de *Compliance*.

El art. 38.1 de La Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito recoge que las entidades de crédito deberán disponer de una unidad u órgano que asuma la función de *gestión de riesgos proporcional a la naturaleza, escala y complejidad de sus actividades*, independiente de las funciones operativas, que tenga autoridad, rango y recursos suficientes, así como el oportuno acceso al consejo de administración.

El art. 24 del reglamento general de protección de datos (Reglamento (UE) 2016/679) del Parlamento Europeo y del Consejo de 27 de abril de 2016 recoge que, *teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad* para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.

Estas son dos muestras de cómo el ordenamiento jurídico está integrando la gestión de riesgos de *Compliance* y el concepto de «contexto», como elemento necesario para la gestión eficaz de responsabilidades y la supervisión del deber de diligencia debida en las organizaciones.

Es obligatorio, por tanto, entender bien la organización y su «contexto» antes de proceder a gestionar los riesgos y para ello hay que tener en cuenta todos aquellos factores internos y externos que puedan afectar a la misma como, por ejemplo, entre otras:

- Países y entorno organizativo en los que la organización opera y desarrolla sus actividades, especialmente si la organización es parte de otra organización más amplia en una zona determinada.
- Las actividades que constituyan su objeto social, sus objetivos y competencias, productos y servicios y canales de comercialización, suministro o fabricación, incluyendo el volumen de operaciones y la variedad de servicios.
- El contexto regulatorio, social y cultural en el que opera la organización (por ejemplo, entidades privadas que desarrollan su actividad en sectores económicos intervenidos por las Administraciones Públicas sometidos a autorizaciones, concesiones y demás permisos necesarios en dichos sectores).
- La situación económica y los flujos de gestión de cobros y pagos.
- La estructura societaria, organizativa, funcional y operativa y de los órganos de representación y dirección en la gestión de responsabilidades.

- Los procesos de gestión y las políticas internas y los procedimientos ya establecidos y los recursos disponibles.
- Las llamadas «partes interesadas» que incluirá a los accionistas o socios, empleados, proveedores y clientes, consumidores o destinatarios de los productos y servicios.

4. IDENTIFICACIÓN DE LOS RIESGOS DE COMPLIANCE (UNIVERSO DE LOS RIESGOS DE COMPLIANCE)

Una vez «contextualizada» la organización, los **riesgos de Compliance** asociados al negocio o actividad en cuestión juegan un papel fundamental en la asignación de los recursos. Las organizaciones dotan recursos operativos y económicos al desarrollo de las funciones precisas para la consecución de sus objetivos por lo que se hace necesario, por tanto, identificar claramente los riesgos legales asociados al particular «Compliance» de cada organización.

Como se indica, en materia de *Compliance*, las fuentes de riesgos derivan de las obligaciones de *Compliance* y de la incertidumbre de su incumplimiento.

Las organizaciones deberán identificar los riesgos de *Compliance* relacionando sus obligaciones con sus actividades, productos, servicios y aspectos relevantes de sus operaciones en los países en los que opera, con objeto de identificar situaciones en las que pueden ocurrir incumplimientos de *Compliance*. Al mismo tiempo y posteriormente, las organizaciones deberán identificar y valorar las causas y las consecuencias de los incumplimientos de *Compliance*.

Se identificarán y documentarán como requisitos legales y compromisos:

- Toda la normativa aplicable atendiendo al contexto de la organización.
- Las actividades sometidas a permisos, licencias o autorizaciones.
- Las obligaciones contractuales con terceros.
- Las órdenes, reglas o guías de las autoridades regulatorias, supervisores o asociaciones sectoriales.

Cuanto más regulado sea el sector donde la Organización opera o presta servicios, más elevado será este riesgo y más peso tendrá en la consideración de un programa de gestión de riesgos.

En términos generales, y título de ejemplos, a continuación, se indican las siguientes fuentes de obligaciones y requisitos legales que deben ser consideradas, como «factores de riesgo» más significativos:

Riesgos relacionados con la gestión del gobierno corporativo:

- Códigos de conducta.
- Controles internos.
- Políticas de Responsabilidad Social Corporativa.

Riesgos relacionados con la gestión de los órganos de administración:

- Obligaciones y responsabilidades.
- Independencia/conflictos de interés.
- Comités especiales.
- Obligaciones de los consejeros: diligencia, lealtad e incompatibilidades.

Riesgos relacionados con la gestión de operaciones societarias especiales:

- Fusiones y adquisiciones.
- «*Joint Ventures*».
- Alianzas estratégicas comerciales.

Riesgos relacionados con la gestión de las relaciones laborales:

- Conciliación de la vida familiar y laboral.
- Políticas de igualdad y no discriminación.
- Prevención de riesgos laborales.
- Pensiones y beneficios.
- Migración y movilidad.
- Visados y permisos de trabajo.
- Contrataciones de personal.
- Obligaciones frente a la Hacienda Pública y la Seguridad Social.
- Riesgo de infracción de obligaciones en materia de blanqueo de capitales.
- Pruebas de selección.
- Extinciones de la relación laboral y expediente de regulación de empleo.

- Ejercicio de la Libertad sindical.
- Incapacidad y discriminación acoso y represalias.

Riesgos relacionados con la gestión de información, protección de datos y uso de tecnología:

- Información privilegiada: confidencialidad.
- Revelación de secretos.
- Protección de menores.
- Tratamiento de Imágenes.
- Recogida, tratamiento y cesión de datos personales.
- Uso de software.
- Privacidad del correo electrónico.
- Acceso y uso de internet.

Riesgos relacionados con la gestión económica-financiera:

- Blanqueo de capitales.
- Pagos a agentes o facilitadores.
- Pagos y cobros de Comisiones.
- Pagos y cobros en metálico.
- Control de cambios.
- Inversiones extranjeras.
- Pagos de Impuestos.
- Precios de transferencia.
- Ajustes de precios.
- Pagos de Royalties y descuentos.
- Operaciones en Mercados de valores.
- Información y transparencia.

Riesgos relacionados con la gestión del diseño y la fabricación y producción:

- Impacto medioambiental.
- Emisiones de CO2.
- Vertidos.
- Sustancias toxicas.
- Derechos de propiedad intelectual.
- Patentes y marcas.

- Secretos industriales y comerciales.
- *Know how*.
- Gestión de la cadena de suministro.
- Seguridad en cadena suministro.
- Externalización y *Outsourcing*.
- Salud, seguridad e higiene.
- Autorizaciones.
- Registros.
- Seguridad del producto: Certificaciones y Etiquetado.
- Protección del consumidor.
- Etiquetado.

Riesgos relacionados con la gestión urbanística:

- Convenios.
- Licencias.
- Planeamiento.

Riesgos relacionados con la gestión comercial y distribución:

- Agentes y distribuidores.
- Franquicias.
- Trámites aduaneros.
- Transporte.
- Licencias comerciales de importación o exportación.
- Tratados internacionales.
- Contratación pública: Procedimientos abiertos, restringidos, negociados o adjudicación directa.

Riesgos relacionados con la gestión comercial y marketing:

- Defensa de la Competencia.
- Competencia desleal.
- Reparto de mercados.
- Fijación de precios.
- Participación en asociaciones sectoriales.
- Tratos con competidores.
- Publicidad y promoción.
- Publicidad desleal.

- Autocontrol.
- Ventas por internet.
- Marketing digital.
- Telemarketing.
- Ventas a distancia.
- Garantías de producto.
- Servicio postventa.

Los sectores más regulados elevan el número de fuentes de obligaciones de *Compliance* por lo que si nuestra organización pertenece a alguno de estos sectores la gestión de riesgos de *Compliance* se hace expresamente obligatoria:

- Sector bancario: Entidades de crédito, entidades de depósito (bancos, cajas de ahorro, cooperativas de crédito) y establecimientos financieros de crédito.
- Sector sanitario y farmacéutico: Sanidad y Salud Pública, seguridad alimentaria y nutrición, servicios y asistencia hospitalaria, asistencia y prestación farmacéutica, comercialización de productos sanitarios.
- Sector aeronáutico y aeroportuario, seguridad, circulación y navegación aérea.
- Sector energético: eléctrico, fotovoltaico, atómicos, gas, petróleo, carbón.
- Sector de las Telecomunicaciones.
- Sector asegurador.

Por lo tanto, en esta fase deberemos marcarnos como objetivos:

1. Identificar la fuente de las Obligaciones de *Compliance*.
2. Detallar las obligaciones y prohibiciones aplicables a nuestra organización.

5. ANÁLISIS Y EVALUACIÓN DEL RIESGO LEGAL

5.1. Introducción

Como ya se ha destacado, el riesgo es inherente a todo negocio y actividad, razón por la cual es fundamental que las organizaciones posean

adecuados sistemas de control interno. Un componente fundamental de todo sistema de gestión de riesgos de *Compliance* exige el análisis y la evaluación del riesgo legal.

La organización debería analizar los riesgos de *Compliance* considerando las causas de los incumplimientos de *Compliance*, así como la probabilidad de que ocurran los incumplimientos de *Compliance* y la gravedad de sus consecuencias. En términos generales las consecuencias pueden incluir, por ejemplo, pérdidas económicas, daño reputacional y responsabilidades administrativas.

El objetivo es establecer una valoración y priorización de los riesgos de incumplimientos de obligaciones de *Compliance* (requisitos legales y compromisos voluntarios asumidos por la organización) con el fin de clasificarlos de forma tal que permita a la organización la toma de decisiones y priorizar el establecimiento de acciones y controles preventivos.

Este es un proceso individual y sometido a valoraciones subjetivas que cada organización debe afrontar atendiendo a sus criterios particulares.

5.2. Método de evaluación del riesgo

El concepto de apreciación del riesgo esta intrínsecamente ligado al método que se utiliza para la evaluación y la valoración del riesgo.

Las organizaciones, a través de su responsable de *Compliance*, deberían trabajar con los distintos responsables de las áreas de gestión para identificar procesos y obligaciones de *Compliance* asociadas a los mismos.

Una vez identificados los riesgos legales, nos preguntaremos:

- ¿A qué área de responsabilidad y proceso de la organización afecta o impacta el riesgo?
- ¿Qué efectos tiene en la Organización?
- ¿Qué tiempo de reacción permite a la dirección paliar el riesgo?
- ¿Qué grado de complejidad o coste requieren las medidas?
- ¿Qué consecuencias implicará el no cumplir la Obligación de *Compliance*?

La Norma ISO 31000:2009 facilita una guía detallada sobre apreciación de riesgos y las normas complementarias ISO GUIA 73 e ISO/IEC 31010:2009 «Gestión del riesgo» establece técnicas de evaluación de riesgos que ofrece directrices para la aplicación de técnicas sistemáticas de

evaluación de riesgos, como el riesgo crediticio, operacional, tecnológico de mercado, de liquidez y, entre otros, el riesgo legal o de cumplimiento.

La extensión y el nivel de detalle de la apreciación de riesgos de *Compliance* dependen de la situación de riesgo, el contexto, el tamaño y los objetivos de la organización y puede variar para sub-áreas específicas (por ejemplo, ambiental, financiera, social).

Una práctica habitual en la evaluación de riesgos es generar matrices de Riesgo, que permiten presentar de manera gráfica el impacto (severidad o pérdida) y la probabilidad (probabilidad de ocurrencia) de factores de riesgo. Así, se destaca un gráfico en un plano cartesiano, en donde un eje identifica la probabilidad de ocurrencia del factor de riesgo de *Compliance* y otro eje identifica el impacto que este factor tiene sobre los objetivos estratégicos de *Compliance*.

El objetivo es poder medir, priorizar y tratar los Riesgos de *Compliance*. Las opciones del tratamiento de riesgos *Compliance* se deberán considerar en función de las necesidades y circunstancias particulares de cada organización siguiendo la siguiente jerarquía ²⁶⁷

- Eliminando el riesgo de *Compliance*, finalizando la actividad que lo provoca.
- Eliminando la fuente del riesgo.
- Modificando la probabilidad de ocurrencia.
- Modificando las consecuencias.
- Compartiendo el riesgo con otras partes (aseguramiento del riesgo).
- Manteniendo el riesgo en base a una decisión informada.

El objetivo, por tanto, es priorizar los riesgos en función del impacto que tengan y la probabilidad de que ocurran, asignándole un nivel de riesgo y un objetivo de tratamiento

5.3. Documentación de los resultados. El registro de riesgos

Las buenas prácticas en la gestión de la seguridad de la información (norma UNE-ISO/IEC 27001:2014) definen como:

267. Norma UNE 19601:2017

- **Amenaza:** Aquel evento capaz de desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Por ejemplo, el desconocimiento de la ley.
- **Vulnerabilidad:** Aquel aspecto que influye negativamente en un activo y que posibilita la materialización de una amenaza. Por ejemplo, la falta de asignación de responsabilidades.
- **Riesgo:** La probabilidad de que suceda la amenaza o evento no deseado. Por ejemplo, la probabilidad de recibir una denuncia por incumplimiento de la actividad obligatoria o de desarrollo de una actividad prohibida.

El registro de los riesgos y su análisis y valoración nos permitirá gestionar los mismos con los responsables de la organización afectados por los mismos.

Se pueden elaborar unas fichas de riesgos que nos permitan trabajar y diseñar los controles oportunos para reducir la probabilidad de ocurrencia y las consecuencias, dentro de nuestra propia metodología de planificación y respuesta al riesgo.

(Ejemplo de modelo de fichas de riesgos)

Id	1.1
Norma aplicable (Oblig Compliance)	Contrato con clientes de mantenimiento de equipos, digitalización y gestión de archivo
Escenario de Riesgo	Incumplimiento contractual
Probabilidad	Medio
Impacto	Medio-Alto
Descripción	Incumplimiento los acuerdos de niveles de servicio asumidos por contrato
Afectados	Clientes
Indicadores	Reclamaciones de clientes
Id	1.2
Norma aplicable (Oblig Compliance)	Ley 31/95 de prevención de riesgos laborales
Escenario de Riesgo	Seguridad y la salud de los trabajadores
Probabilidad	Medio
Impacto	Alto
Descripción	ausencia de control de gestión de obligaciones de responsables en materia de prevención de riesgos laborales
Afectados	Trabajadores
Indicadores	Reportes periódicos

5.4. La evaluación del riesgo como un proceso dinámico permanente

Los riesgos de *Compliance* deberían reevaluarse periódicamente y en todo caso cuando haya actividades, productos o servicios nuevos o modificados; cambios en la estructura o en la estrategia de la organización; cambios externos significativos, tales como circunstancias económico-fi-

nancieras, condiciones de mercado, etc. o cambios en las obligaciones de *Compliance* exigibles a la organización.

La adecuada gestión de un sistema de gestión de *Compliance* requiere de una planificación y una documentación detallada de todas las tareas que integran el tratamiento de gestión de riesgos de *Compliance*. Uno de los puntos determinantes será planificar y documentar la evaluación de riesgos, definiendo como y cuando llevar a cabo las evaluaciones del riesgo, designando los responsables implicados en la supervisión y ejecución de los mismos

6. TRATAMIENTO DEL RIESGO: APETITO DE RIESGO Y ESTABLECIMIENTO DE CONTROLES

Todas las organizaciones, al igual que los particulares, tienen su propia percepción del riesgo.

Las actitudes frente al riesgo de la organización pueden verse afectadas por una serie de factores, los cuales pueden clasificarse a grandes rasgos en tres categorías:

- **Apetito de riesgo**, cantidad de riesgo que la organización acepta asumir en la consecución de sus objetivos.
- **Tolerancia al riesgo**, que es la desviación respecto al nivel de riesgo que la organización se siente cómoda.
- **Umbral de riesgo**, que se refiere al nivel máximo de riesgo o incertidumbre que la organización puede soportar. Por debajo de ese umbral de riesgo, la organización aceptará el riesgo. Por encima de ese umbral de riesgo, la organización no tolerará el riesgo.

La actitud frente al riesgo de una organización está en función de esos tres factores (apetito, tolerancia y umbral). Al mismo tiempo, la actitud hacia el riesgo de una organización también depende de su contexto, del sector en donde se desempeñe, del mercado en el que opera, de su madurez, y de la actitud hacia el riesgo de las personas que dirigen la organización.

Las organizaciones, en distintos ámbitos de la gestión (seguridad de la información, continuidad de negocio, medioambiente, calidad,) pueden establecer reglas para la asunción de riesgos o respecto a su apetito de riesgo pero una cultura organizativa de *Compliance* basada en la ética solo debe ser utilizada para facilitar determinar prioridades y para la atención y toma de decisiones.

Es importante matizar que el enfoque basado en el riesgo en la gestión de *Compliance* no significa que para situaciones de riesgo bajo de incumplimientos de *Compliance*, la organización acepte incumplimientos de *Compliance*. Sirve de ayuda a la organización para centrar la atención primaria y los recursos en los riesgos más elevados de forma prioritaria y, en última instancia, cubrirá todos los riesgos de *Compliance*. Todos los riesgos y situaciones de *Compliance* deben ser objeto de seguimiento, corrección y acciones correctivas²⁶⁸.

En una metodología basada en la gestión de riesgos, el concepto de riesgo residual, como aquel que asume la organización tras haber implantado las medidas y controles de prevención oportunos, puede entenderse aceptado, teniendo en cuenta que la mejora continua que nuestro sistema de evaluación de riesgos periódico nos permitirá ir reduciendo.

La siguiente fase en la gestión de riesgos de *Compliance* es la definición y el establecimiento de controles.

La gestión de riesgos de *Compliance* y la evaluación de riesgos debe:

- Permitir elegir que riesgos merecen ser tratados a fin de establecer prioridades para su tratamiento y control.
- Permitir designar propietarios de los riesgos en cada área, recordando que «la responsabilidad no se transfiere se comparte».
- Permitir abordar las medidas y controles oportunos atendiendo a los recursos disponibles para los riesgos según prioridades.
- Permitir adoptar decisiones para la eliminación del riesgo, la transferencia del riesgo o la minimización del mismo, posibilitando así la reducción de la probabilidad o el impacto de un riesgo sobre la organización.

Los controles los podemos clasificar en controles preventivos, reactivos y de detección²⁶⁹, atendiendo a varias líneas de actuación:

1. Políticas y procedimientos internos:
 - Procedimientos de gestión.
 - Política de regalos.

268. UNE-ISO 19600. Nota 2, Capítulo 4.6, «Identificación, análisis y evaluación de los riesgos de *Compliance*».

269. ENSEÑAT, SYLVIA. *Manual del Compliance Officer*. Thomson-Reuters, 2016.

- Política de compras.
- Conflictos de intereses y segregación de funciones.
- 2. Códigos de conducta dirigida a:
 - Consejeros y ejecutivos.
 - Empleados.
 - Proveedores.
- 3. Formación:
 - Principios éticos.
 - Integridad financiera.
 - Derecho de la competencia.
 - Relaciones laborales.
 - Compras.
 - Ventas.
 - Distribuidores/agentes.
 - Responsabilidad Social Corporativa.
- 4. Medidas reactivas:
 - Medidas disciplinarias.
 - Investigación interna o externa.
 - Incentivos.
- 5. Detección:
 - Líneas directas de denuncia.
 - Líneas directas de reporte y apoyo.
 - Procedimiento de denuncia.
 - Auditorias y análisis de riesgos.
 - Atención de reclamaciones e incidencias.
 - Monitorización.
 - Indicadores.

7. NECESIDAD DE CONTROLES ADICIONALES

El adecuado sistema de gestión e riesgos de *Compliance* nos debe facilitar la labor de establecer una serie de indicadores de control que nos permitan evaluar su diseño y eficacia que deberán ser convenientemente documentados.

El propio análisis de estos indicadores debe facilitar la revisión continua de los procesos y las actividades que permitan actualizar continuamente las medidas implantadas por la organización para la gestión de los riesgos asociados a las obligaciones de *Compliance* (como por ejemplo

cláusulas contractuales o procedimientos de gestión) que permitan así definir estándares de comportamiento a nivel global en las organizaciones.

Algunos indicadores clave de riesgos en *Compliance* que nos permita la monitorización de los riesgos más relevantes podrían ser:

- Modificaciones legislativas y requerimiento legales de aplicación a la organización.
- Requerimientos de autoridades de control.
- Número de recomendaciones o no conformidades resultantes de las auditorías periódicas.
- Porcentaje de reclamaciones, incidentes o denuncias reaccionadas con incumplimientos de *Compliance*.
- Porcentajes de reportes internos de cumplimiento incluyendo incidencias o propuestas de mejoras.
- Demandas o reclamaciones judiciales interpuestas contra la organización.

