MANUAL DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS. COMPLIANCE. COMPLIANCE OFFICER

Indice

Artículo 31 bis. 2
Penas que se podrán imponer a las personas jurídicas 4
Responsabilidad penal de las personas jurídicas 7
¿Qué es el programa de cumplimiento? 17
Norma ISO 19600 19
Sistema de Gestión de Compliance 21
Planificación 37
Apoyo 39
Evaluación del desempeño 49
Mejora 59
El Compliance Officer 61

ARTÍCULO 31 BIS.

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:

1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;

2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;

3.ª los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y

4.ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª

En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.

4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado

eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.

5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

Artículo 31 ter.

1. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el artículo anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.

2. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el artículo siguiente.

Artículo 31 quater.

1. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:

a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.

b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos.

c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito.

d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.

Artículo 31 quinquies.

1. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas.

2. En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33. Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

PENAS QUE SE PODRÁN IMPONER A LAS PERSONAS JURÍDICAS

Las penas que se podrán imponer a las personas jurídicas vienen detalladas en el Art. 33, apartado 7 del Código Penal, que señala:

"7. Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes:

a) Multa por cuotas o proporcional.

b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita.

c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.

d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.

e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años.

f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.

g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

La intervención podrá afectar a la totalidad de la organización o limitarse a alguna de sus instalaciones, secciones o unidades de negocio. El Juez o Tribunal, en la sentencia o, posteriormente, mediante auto, determinará exactamente el contenido de la intervención y determinará quién se hará cargo de la intervención y en qué plazos deberá realizar informes de seguimiento para el órgano judicial. La intervención se podrá modificar o suspender en todo momento previo informe del interventor y del Ministerio Fiscal. El interventor tendrá derecho a acceder a todas las instalaciones y locales de la empresa o persona jurídica y a recibir cuanta información estime necesaria para el ejercicio de sus funciones. Reglamentariamente se determinarán los aspectos relacionados con el ejercicio de la función de interventor, como la retribución o la cualificación necesaria.

La clausura temporal de los locales o establecimientos, la suspensión de las actividades sociales y la intervención judicial podrán ser acordadas también por el Juez Instructor como medida cautelar durante la instrucción de la causa."

Lo primero que debemos señalar es que la clausura temporal de los locales o establecimientos, la suspensión de las actividades sociales y la intervención judicial, además de penas a imponer por una sentencia judicial, también pueden ser acordadas por el Juez Instructor como medida cautelar mientras se realiza la investigación y se tramita el procedimiento, es decir, mucho antes de que exista sentencia; para evitar la continuidad de la actividad presuntamente delictiva y garantizar la eficacia del proceso.

Como puede verse, la pena común o general a imponer es la de multa, aunque también pueden imponerse cualquiera de las otras previstas.

En cuanto a los criterios para imponer la pena de multa, existen dos posibilidades, o imponerla por cuotas diarias (la fórmula de días-multa) o imponerla de forma proporcional.

Respecto de la multa por cuotas, el Art. 50.4 del Código Penal señala que la cuota diaria tendrá un mínimo de 30 y un máximo de 5.000 euros. Señala la norma también que, a efectos de cómputo, cuando se fije la duración de la pena de multa por meses o por años, se entenderá que los meses son de treinta días y los años de trescientos sesenta.

En cambio, para los casos en los que el Código prevé imponer una pena de multa para las personas jurídicas en proporción al beneficio obtenido o facilitado, al perjuicio causado, al valor del objeto, o a la cantidad defraudada o indebidamente obtenida, se impondrá la misma conforme al cálculo en base a tales conceptos.

Pero si no es posible llevar a cabo dicho cálculo, el Art. 52.4 del Código Penal señala que el Juez o Tribunal motivará la imposibilidad de proceder a tal cálculo y las multas previstas se sustituirán por las siguientes:

a) Multa de dos a cinco años, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.

b) Multa de uno a tres años, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años no incluida en el inciso anterior.

c) Multa de seis meses a dos años, en el resto de los casos.

EJEMPLO

Si la sentencia impone a la Sociedad "PEPITO.S.L" una pena de multa de 4 años, con una cuota diaria de 500 euros, la empresa vendrá obligada a abonar la cantidad total que resulte de abonar 500 euros al día durante 4 años (computados como de 360 días)

360 días x 4 años = 1.440 días

1.440 días x 500 euros cuota al día = 720.000 euros.

La empresa "PEPITO.S.L" habría sido condenada, en definitiva a una multa de 720.000 euros.

Como hemos visto, las penas a imponer pueden resultar muy elevadas (hasta de 9 millones de euros). Por ello, el Código Penal establece, en el Art. 53.5, que podrá fraccionarse el pago de la multa que se imponga a una persona jurídica, durante un período de hasta cinco años. Pero para ello habrá que demostrar que su cuantía pone probadamente en peligro la supervivencia de la persona jurídica o el mantenimiento de los puestos de trabajo existentes en la misma, o cuando así lo aconseje el interés general.

Además, si la persona jurídica condenada no paga, voluntariamente o por vía de apremio, la multa impuesta en el plazo que se le hubiera fijado, el Tribunal podrá acordar su intervención judicial hasta el pago total de la multa.

Por lo que se refiere al resto de penas distintas a la de multa, sólo podrán imponerse en aquellos casos en que el delito en cuestión lo prevea expresamente.

Los criterios para su imposición están establecidos en el Art. 66 bis y son los siguientes:

a) Su necesidad para prevenir la continuidad de la actividad delictiva o de sus efectos.

b) Sus consecuencias económicas y sociales, y especialmente los efectos para los trabajadores.

c) El puesto que en la estructura de la persona jurídica ocupa la persona física u órgano que incumplió el deber de control.

Para imponer las penas de suspensión de sus actividades, clausura de sus locales y establecimientos, prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito, inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social y de intervención judicial por un plazo superior a dos años será necesario que se dé alguna de las dos circunstancias siguientes:

a) Que la persona jurídica sea reincidente.

b) Que la persona jurídica se utilice instrumentalmente para la comisión de ilícitos penales (empresa pantalla o tapadera). Se entenderá que se está ante este último supuesto siempre que la actividad legal de la persona jurídica sea menos relevante que su actividad ilegal.

Asimismo, para imponer con carácter permanente las sanciones de disolución de la persona jurídica y de prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito, así como para imponer ésta última y la de inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social por un plazo, será necesario que se dé alguna de las dos circunstancias siguientes:

a) Que la persona jurídica imputada sea reincidente y haya sido condenada ejecutoriamente, al menos, por tres delitos comprendidos en el mismo título de este Código (Art. 66.1.5.ª).

b) Que la persona jurídica se utilice instrumentalmente para la comisión de ilícitos penales. Se entenderá que se está ante este último supuesto siempre que la actividad legal de la persona jurídica sea menos relevante que su actividad ilegal.

Finalmente, hay que señalar que la responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil en los términos establecidos en el artículo 110 del Código Penal de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos. (Art. 116.3 del Código Penal).

RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

I. Introducción. La reforma de la LO 5/2010

En Europa la responsabilidad de las personas jurídicas se ha extendiendo desde fines del siglo pasado, especialmente después de haber sido regulada en el Corpus Iuris (1997/2000) para la Protección de los Intereses Financieros de la UE (art.14).

La exigencia a las empresas de responsabilidad en el ámbito del derecho administrativo sancionador ha abierto la puerta a la exigencia de responsabilidad penal. No ha habido grandes problemas dogmáticos para admitir su responsabilidad penal ya que ambos tipos de sanciones, participan de similares principios por más que la jurisprudencia constitucional haya establecido algún matiz diferenciador (TCo 18/1981, 4-11-80, 14-6-89). La estructura de las normas y los criterios de imputación son similares de ahí que el reconocimiento de la responsabilidad penal de las personas jurídicas no constituya sino una consecuencia anunciada y previsible(1) y, además, la introducción de la responsabilidad penal ha sido más simbólica que real porque antes de su entronización el arsenal sancionatorio no era desdeñable (sanciones administrativas, consecuencias accesorias y responsabilidad civil).

En la Exposición de Motivos de la LO 5/2010 se justificó la introducción de esta cuestión por la demanda de los Convenios Internacionales suscritos por España y se afirmó haber optado por una doble vía de imputación.

a) La atribución de responsabilidad por la actuación delictiva del «representante legal, administrador de hecho o de derecho» por actos realizados «en nombre o por cuenta de la persona jurídica y en su provecho».

b) La transferencia de responsabilidad por defecto de control o «culpabilidad de organización» en el que se sanciona a la persona jurídica por los delitos cometidos por las personas que estén sometidas a la autoridad de los anteriores siempre que hayan podido realizar su acción «por no haberse ejercido sobre ellos el debido control, atendidas las circunstancias de cada caso».

En realidad el actual art.31 bis, que próximamente será derogado, establece dos sistemas de autoría, el de los directivos de la sociedad y el de los empleados, cuestión que para parte de la doctrina constituye una distinción desacertada e innecesaria al entender que la «deficiencia en la organización» debería ser una condición inexcusable de autoría en ambos casos por exigencias del principio de culpabilidad.
Algunos autores entienden incluso que la ubicación sistemática del art.31 bis , como una forma de autoría de delitos especiales propios no tenía justificación y que debiera haberse regulado en el marco general de la autoría (art.28).

En la LO 5/2010 se ha mantenido un sistema de responsabilidad penal accesoria del art.129 para todo tipo de delitos y para entes sin personalidad jurídica y otro de responsabilidad directa para las personas jurídicas (art.31 bis), limitado a cierto tipo de delitos. Al margen de esta distinción entre entes sin personalidad y personas jurídicas, que algunos entienden superada por la realidad en cuanto que lo determinante es la existencia de un patrimonio autónomo, lo cierto es que el art.129 CP ha de tener aplicación fundamentalmente para organizaciones delictivas cuya actividad central sea el delito, mientras que el art.31 bis se ha de aplicar a personas jurídicas que de modo ocasional se vean inmersas por la existencia de un delito cometido en su seno, por administradores o empleados.

Dado que la responsabilidad penal directa del art.31 bis CP puede exigirse aunque el autor material del hecho no haya sido identificado o no haya sido perseguido, este tipo de atribución requiere de la existencia del hecho punible, situación que, sin embargo, es insuficiente en el caso del art.129 CP que requiere inexcusablemente la declaración de responsabilidad penal de la persona física autora del delito.

Pues bien, el problema dogmático fundamental que ha planteado el art.31 bis , en su redacción de la LO 5/2010 , es que parte de la doctrina entiende que la deficiencia de organización debería ser un requisito de atribución de responsabilidad penal común, tanto en el caso de administradores y representantes legales

como en el de empleados, ya que aunque haya una actuación delictiva de cualquiera de éstos si el delito se ha cometido a pesar de la existencia de una estructura organizativa adecuada y de un sistema debido y eficaz de control, la persona jurídica no debería responder.

A este criterio se opuso la Fiscalía General del Estado recordando que el modelo instaurado por la LO 5/2010 no permitía juicio alguno a los Compliance Program en el ámbito de los delitos cometidos por los administradores.

La FGE afirmó en la Circular citada que los códigos éticos de las empresas no pueden modular la imputación de las personas jurídicas, que estos programas tienden a tratar de evitar la imputación de quienes dentro de las empresas ostentan el control y su dirección, que la posición que establece su relevancia obligaría a cambiar la ley y no es respetuosa con el contenido de la misma y que no es contrario al principio de culpabilidad establecer la imputación atribuyendo la responsabilidad penal de la persona jurídica como consecuencia de la actuación de sus directivos.

Sin embargo, la doctrina ha venido insistiendo en que la actuación del administrador debe producirse en el marco de unos poderes que le han sido confiados y su actuación fuera de ese marco constituye un supuesto de administración desleal lo que supone la paradójica situación de que la persona jurídica se convierte, a la vez, en sujeto activo y perjudicado de una misma acción punible. Por eso se ha propugnado la reforma de estos criterios de imputación y el establecimiento de criterios legales que determinen de forma concreta y expresa los deberes que incumben a las distintas personas encargadas de los distintos niveles de decisión dentro de la organización de la empresa a los efectos de concretar cómo y quién se constituye en la posición de garante para responder de las actuaciones de otro.

También ha sido objeto de polémica doctrinal el concepto de «acción provechosa». El art.31 derogado indicaba que la persona física que cometía el delito debía hacerlo «en provecho» de la persona jurídica para transferir a ésta la responsabilidad penal. El legislador no precisó ese concepto (beneficio económico evaluable, beneficio estratégico, beneficio en valores intangibles…) y se puede cuestionar que una actuación que se realice al margen de los sistemas de control preestablecidos por la sociedad con los riesgos consiguientes pueda entenderse como una actuación «provechosa».

Se ha cuestionado que la norma penal tampoco establezca regulación alguna de los deberes de control que corresponden a los administradores de las personas jurídicas para evitar la sanción penal.

A todos estos problemas pretende dar solución la nueva reforma del Código Penal en esta materia, si bien es cierto que los problemas han sido más dogmáticos que reales dado que la responsabilidad penal de las personas jurídicas, implantada en 2010, ha sido de muy escasa aplicación. Los casos de condenas son hoy por hoy muy poco numerosos pese a lo cual esta materia suscita mucho interés y tiene consecuencias prácticas muy destacables debido a la necesidad de implementar costosos sistemas de prevención para evitar posibles condenas penales, con los riesgos económicos y reputacionales que pueden comportar.

II. Novedades introducidas por la LO 1/2015

a) Descripción de la reforma

La reforma que es objeto de comentario modifica fundamentalmente el art.31 bis ya que el resto de preceptos mantiene su redacción original con leves modificaciones.

• En el art.31 bis 1, aptdo. a) y b) , de nueva redacción y que sustituye al antiguo art.31 bis 1), se modifican los criterios de transferencia de responsabilidad entre la persona física y la jurídica.

• En el art.31 bis 2 , de nueva redacción, se establecen los criterios de exención en el caso de personal «directivo» (pongo comillas porque el concepto no es pacífico ni claro) haciendo referencia a los requisitos en base a los cuales pueden tener eficacia los «Compliance Programs».

• En el art.31 bis 3 se especifica esta misma cuestión en relación con las empresas de pequeñas dimensiones, aquellas que según la legislación mercantil están autorizadas a presentar cuentas de pérdidas y ganancias de forma abreviada.

• En el art.31 bis 4, de nueva redacción, se establecen los criterios de exención en el caso de empleados.

• En el art.31 bis 5 , de nueva redacción, se establecen los requisitos que han de cumplir los requisitos que han de cumplir los "Compliance Programs" para entender que son eficaces e idóneos.

• En el art.31 ter se reproduce el anterior art.31 bis, apartados 2 y 3 sin modificaciones. En el art. 31 ter 1 se posibilita el castigo de la persona jurídica aunque la persona física no haya sido individualizada o no se haya podido seguir el procedimiento contra ella. También se regula la necesaria proporcionalidad en las multas caso de condena conjunta. En el art.31 ter 2 se establece la autonomía entre persona física y jurídica en orden a circunstancias que afecten a la culpabilidad del acusado o que agraven su responsabilidad, así como a que la persona física haya fallecido o se hubiere sustraído a la acción de la justicia, lo que no impedirá la persecución y castigo de la persona jurídica.

• En el art.31 quarter, referido a las circunstancias atenuantes, se reproduce el antiguo art.31 bis.4 sin modificaciones.

• El art.31 quinquies reproduce el art.31 bis 5 pero añade un aptdo. 2, referido a las sociedades mercantiles públicas a quienes se les limita las penas de posible imposición salvo que «el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o empleados con el propósito de eludir una eventual responsabilidad penal» (levantamiento del velo).

• En el art.66 se establece una limitación temporal de dos años en las penas establecidas en las letras c) a g) del aptdo.7 del art.33 CP (Suspensión de sus actividades, clausura de locales y establecimientos, prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito, inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores) cuando se imponga la responsabilidad penal a la persona jurídica por los actos de los «directivos» derivada del incumplimiento de los deberes de vigilancia y control que no tenga carácter grave.

b) Críticas generales a la reforma legislativa

Muchas de las críticas al nuevo texto se hayan contenidas en el interesante informe elaborado por el Consejo de Estado en el año 2013, de obligada lectura. A continuación algunas de las críticas más comunes de los distintos estudios que han visto a la luz en los últimos meses.

Para Quintero Olivares, desde una posición muy crítica con la nueva orientación legislativa, la reforma no tiene su justificación en problemas interpretativos previos sino en hacer casi imposible la imputación de las personas jurídicas y en favorecer la implantación de sistemas de prevención o de buenas prácticas con el beneficio consiguiente para los profesionales dedicados a este tipo de actividad.

Dopico Gómez-Alleri considera que la reforma es un injerto extraño, un plagio legislativo de la ley italiana, con los problemas que genera ese tipo de técnica legislativa; que no estaba incluida en el primigenio Anteproyecto que el Gobierno remitió a las Cortes Generales, por lo que no ha informado previamente ni por el Consejo General del Poder Judicial ni el Consejo Fiscal; que incurre en un excesivo reglamentismo al incorporar una regulación en exceso prolija de los programas de Compliance que debería haber sido residenciada en la legislación mercantil y que contiene una inadmisible inversión de la carga de la prueba. Sobre esta cuestión afirma que como la norma contiene como requisito para imponer la responsabilidad penal no la infracción de un deber de control sino simplemente que el sistema de prevención no sea idóneo, desplaza la carga de probar la idoneidad y, en general, los demás requisitos establecidos en la ley penal a la empresa.

González Cussac estima que la reforma no tiene su fundamento en dudas interpretativas o en recomendaciones de organismos internacionales porque la responsabilidad penal de las personas jurídicas ha tenido una aplicación escasísima y porque el marco normativo internacional no ha cambiado.

III. Estudio del contenido de la reforma

1. Cambio en la definición de las personas físicas cuya actuación posibilita la responsabilidad penal de la persona jurídica

En el Código Penal la responsabilidad penal de la persona jurídica es vicarial en el sentido de que ésta responde penalmente por la actuación de otra persona, directivo o empleado, siempre que concurran determinados presupuestos. Se trata de un supuesto de responsabilidad por hecho ajeno ya que una persona física vinculada con la persona jurídica debe haber cometido un delito. Por lo tanto, para la exigencia de esta clase de responsabilidad penal se tiene que probar que la persona física ha cometido un delito y que se cumplen los presupuestos de transferencia de responsabilidad a la persona jurídica.

Las personas físicas que tienen que cometer el delito para que se produzca la transferencia son los directivos o empleados, y en cada caso se establece un sistema de transferencia distinto. El primer aspecto que hemos de analizar es el cambio legislativo en la determinación o individualización de los directivos.

En el art.31 bis 1 a) derogado se refiere a ellos como «representantes legales o administradores de hecho o de derecho». En el texto reformado se habla de «representantes legales o aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma».

En la nueva norma no se modifica el término «representantes legales», que suele plantear el problema de delimitar su ámbito en los casos de apoderados singulares o de colaboradores externos con poder (abogados etc.). Se modifica la expresión «administrador de hecho y de derecho» por «aquellos que de actuando individualmente o como miembros de un órgano de la persona jurídica «están autorizados para a tomar decisiones en nombre de la persona jurídica».

La nueva redacción parece dirigida, por tanto, a suprimir el tradicional concepto «administrador de hecho» por otro más técnico. Esta modificación fue criticada por el Consejo de Estado(12) ya que el sistema de definición anterior (administrador de hecho), si bien daba lugar a problemas interpretativos, era utilizado ampliamente en el ámbito mercantil y sigue utilizándose penalmente en el marco de los delitos societarios.

Como señala Dopico Gómez-Aller la técnica empleada para el fin propuesto es defectuosa. De un lado, en los instrumentos internacionales que se refieren a la cuestión siempre identifican al administrador o responsable de la empresa como persona «con poder de mando». En el texto reformado no se hace referencia e esa expresión de forma que la persona jurídica respondería por los actos de personas autorizadas a tomar decisiones, aunque no tengan poder de mando, en relación con el hecho concreto que se enjuicie, y también respecto de los actos de personas que tengan facultades en la organización y control de la empresa, también sin tener que tener necesariamente poder de mando.

Se amplía notablemente el ámbito de aplicación de la responsabilidad penal, porque cualquier apoderado podría encajar en esta descripción tan amplia, aunque no participe en la gestión ordinaria de la empresa y sus actos estén sujeto a aprobación del órgano de gestión y , de otro, no resuelve el problema de los administradores de hecho. Así, el administrador de hecho carece formalmente de autorización para tomar decisiones y no ostenta facultades de organización y control, pese a lo cual tiene el poder real de la empresa. Tampoco soluciona el problema en caso de holdings de determinar la autoría en los supuestos de decisiones tomadas por la empresa matriz.

Este tipo de problemas parecía estar superado a través del concepto «administrador de hecho», que, conforme a reiterada jurisprudencia(14) es aquel que sin ostentar formalmente la condición de administrador de la sociedad, ejerza poderes de decisión de la sociedad y asuma los poderes de un administrador de derecho; es la persona que, en realidad manda en la empresa, ejerciendo los actos de administración, aunque formalmente sean realizadas por otra persona que figure como su administrador.

La nueva redacción de la LO 1/2015 abre interrogantes que habrán de ser objeto de una cuidadosa interpretación. A mi juicio, la determinación del autor deberá seguir realizándose a partir de los criterios de «dominio del acto» y de «poder de dirección» referidos a la situación concreta que se examine. Como señaló la Circular de la Fiscalía General del Estado antes citada, no debería hablarse de responsabilidad penal de la persona jurídica si la persona física que comete el delito no es alguien del órgano de gobierno o controlable por el órgano de gobierno. Lo relevante debería ser «la dirección de facto y no el concreto título o circunstancia de la que derive la potestad de actuar».

2. Responsabilidad penal por los actos de los directivos

2.1 Requisitos

La responsabilidad penal de las personas jurídicas por los actos de los «directivos», comprendiendo en este concepto la compleja definición a que antes nos hemos referido, requiere de los siguientes presupuestos:

• Que el directivo haya cometido un delito actuado en nombre o por cuenta de la persona jurídica. Este presupuesto se mantiene inalterado.

• Que haya actuado en beneficio directo o indirecto de la persona jurídica. En este particular este presupuesto sustituye al anterior de actuar «en provecho» de la persona jurídica.

• La persona jurídica quedará exenta de responsabilidad criminal si se cumplen las siguientes condiciones:

a) Que el órgano de administración haya adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyan las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión.

b) Que se haya confiado la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica.

c) Que los autores individuales que cometan el delito hayan eludido fraudulentamente los modelos de organización y de prevención y

d) Que no se haya producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª.

En cuanto a la actuación en nombre o por cuenta de la persona jurídica, la expresión hace referencia al contexto material de actuación del directivo y se refiere al contenido formal y material del mandato o representación del directivo en cada caso. Cabe plantear como supuestos excluyentes los casos en que haya existido una extralimitación manifiesta aún cuando no debe determinarse ese contexto de acuerdo con las atribuciones formales del directivo en cuestión. Las reglas civiles o mercantiles no deben ser determinantes porque habrá de indagarse en el poder real para determinar si el directivo ha actuado dentro de la esfera de sus atribuciones para evitar zonas indeseables de impunidad.

La sustitución de «en provecho de» por «en beneficio directo o indirecto de la persona jurídica» ha merecido una valoración positiva en el informe del Consejo de Estado antes mencionado. La eliminación de la expresión «en provecho», que tenía muchas posibilidades interpretativas y la inclusión de la expresión «en beneficio directo o indirecto» permite concluir que la actuación del directivo ha de tener como objetivo la obtención de un beneficio o ventaja de cualquier tipo. Sigue siendo necesario recordar que se trata de una conducta tendencial que no precisa de un resultado concreto y que debe valorarse de forma objetiva y ex ante(17). En cualquier caso no se incluyen en este presupuesto los delitos cometidos por los directivos exclusivamente en beneficio propio o de terceros ajenos a la persona jurídica.

2.2 Programas de prevención penal (Compliance programs)

La exención de la responsabilidad penal de una persona jurídica pasa por la existencia de un programa de prevención de delitos. Se pretende instaurar una nueva cultura en las empresas, a fin de que de forma proactiva eviten la comisión de delitos. Se pretende la instauración de criterios de organización preventivos. La autorregulación y una nueva cultura corporativa respetuosa con las normas es la finalidad última de esta reforma, de ahí que se dé una relevancia incuestionable a los programas de prevención y detección de delitos.

Se requiere la adopción y ejecución eficaz de un modelo de organización y gestión que contenga medidas de prevención y control idóneas para prevenir el delito de que se trate o para reducir de forma significativa el riesgo de su comisión.

Para valorar la relevancia de un programa de prevención se precisa:

a) Idoneidad. Determinar la idoneidad entre el programa y del delito, lo que supone que el programa haya valorado como posible el riesgo de comisión del delito y haya establecido medidas abstractamente eficaces para prevenirlo o para reducir el riesgo de su comisión.

En este particular resulta especialmente importante que el programa cumpla con las previsiones del art.31 bis 1.5 , que «identifique las actividades en que se ha cometido el delito como actividad susceptible de prevención». Se trata de un análisis general de prevención, abstracto y ex ante. Si la idoneidad no es total debería apreciarse la atenuación prevista en el art.31 bis 2.4, párrafo 2º. De todas formas el concepto de idoneidad no creo que deba identificarse al de idoneidad absoluta.

b) Ejecución eficaz. Se debe valorar que el programa haya sido adoptado antes de la comisión del delito y que se está ejecutando con eficacia. No basta un simple papel para salir del paso.

Es preciso que sea un sistema de prevención real y eficaz, lo que se acreditará ordinariamente por el cumplimiento de los requisitos establecidos en el art.31 bis 5 , a saber: Establecimiento de protocolos operativos de gestión e información, modelo de gestión de recursos financieros, flujos de información hacia el órgano de control y establecimiento de un régimen disciplinario.

Se trata de que el programa sirva para prevenir delitos, para reducir de forma significativa el riesgo de su comisión. El adverbio «significativamente» que utiliza el precepto es abierto, general y de difícil determinación. Habrá de valorarse su cumplimiento caso por caso en el bien entendido que la propia existencia del delito en el caso concreto supone de facto un fracaso del programa, lo que no ha de excluir la exención de responsabilidad penal si el programa puede ser calificado de eficaz e idóneo desde una perspectiva amplia.

Se encomienda al juez una difícil tarea, evaluar la eficacia de una plan de prevención. Al parecer, no están plenamente desarrollados programas de evaluación de los Compliance Programs y, sin embargo, se encomienda al juez la difícil tarea de hacer esa evaluación caso por caso. No cabe duda que será una cuestión que complicará la instrucción de las causas y su enjuiciamiento, que puede dar lugar a abundante prueba y documentación y en la que serán muy relevantes las pruebas periciales.

Por esa razón en el derecho anglosajón se han desarrollado acuerdos de suspensión del proceso (deferred prosecution arrangements) para evitar el enjuiciamiento, previa la asunción de multas o medidas de otro tipo.

c) Órgano de control del programa autónomo. Es un requisito que depende en buena medida de la cultura corporativa y del tamaño de la empresa. Algunos piensan que es una ingenuidad pensar que el órgano de administración de una empresa va a ceder poderes y permitir que un órgano autónomo permita tomar decisiones en este campo sin la previa aprobación por el órgano de administración tanto en lo que se refiere a medidas operativas, como a medidas financieras (art.31 bis 5 3º).

d) La actuación del directivo ha de sortear fraudulentamente el plan de prevención aprobado por la persona jurídica. La falta de precisión normativa permite que cualquier tipo de conducta fraudulenta pueda ser tomada en consideración.

e) Se precisa, por último, que el órgano de control no haya incurrido en omisiones o en el ejercicio insuficiente de sus facultades de supervisión, vigilancia y control. Este requisito está vinculado con la eficacia del programa. Se precisa un cumplimiento diligente por parte del órgano de control.

f) En el caso de personas jurídicas de pequeña dimensión se atribuye al administrador las funciones de supervisión, lo que no excluye que se deba implementar un plan de prevención pero sin órgano de control ajeno a la dirección (art.31 bis 3).

g) Requisitos del plan de prevención (art.31 bis 5).

• 1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

• 2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

• 3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

• 4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

• 5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

• 6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.»

3. Responsabilidad penal por los actos de los empleados

En el caso de empleados habrá responsabilidad penal de la persona jurídica cuando se haya podido cometer el delito «por haberse incumplido gravemente por aquéllos (-las personas físicas definidas en el artículo 31 bis1 a-) los deberes de supervisión, vigilancia y control de sus actividades, atendidas las circunstancias del caso».

Con la nueva redacción se reduce notablemente la exigencia de responsabilidad penal de la persona jurídica ya que no todo incumplimiento conlleva esa responsabilidad. Tiene que tratarse de un incumplimiento grave. Esta previsión normativa es razonable desde la perspectiva del principio de intervención mínima, pero se trata de un criterio flexible e indeterminado.

El Consejo de Estado con buen criterio afirmó que la regulación de los sistemas de supervisión, vigilancia y control deberían desarrollarse en la legislación mercantil con reformas inmediatas y paralelas a la reforma del Código Penal.

Dejando al margen la existencia de una incorrección terminológica puesta de relieve también por el Consejo de Estado y que no se ha corregido(19), la reforma complica sobremanera la declaración de responsabilidad penal por delitos cometidos por empleados ya que, de un lado, es preciso determinar de acuerdo con la abundante normativa extrapenal los deberes de supervisión, vigilancia y control en las actividades en cuyo ámbito se ha producido el delito y, de otro, determinar qué facultades corresponden individualmente a los administradores, puesto que la responsabilidad penal de la persona jurídica en este caso no surge por un defecto de control o por la inadecuación de los modelos de organización y control de

la propia sociedad sino por el incumplimiento de las obligaciones personales atribuidos a las personas físicas.

Como señala González Cussac lo que subyace a esta cuestión es el fundamento de esta responsabilidad pues se puede establecer en el «defecto de control» de la propia organización o en una forma de "culpa in vigilando" de los administradores o responsables de la persona jurídica.

Esto tiene importancia, como señala el autor citado, porque si de lo que estamos hablando es de «defecto de control de la propia organización», el establecimiento de un sistema eficaz de prevención sería un modo de excluir la responsabilidad y a ello parece referirse el art.31 bis, aptdo. 2 y 4 , relativos a la eficacia exculpante de los planes de prevención. Pero si de lo que hablamos es de la responsabilidad penal por la infracción de los deberes personales de las personas físicas dotadas de representación, decisión o control, los planes de prevención son meramente indicativos. Ciertamente constituyen un parámetro relevante, junto a las normas sectoriales, para determinar si la persona física ha efectuado el control debido, pero no actúan como un factor eximente de la conducta.

Se aprecia, por tanto, una cierta contradicción en la forma en que se ha regulado esta responsabilidad. De un lado, se afirma que su fundamento es la falta de diligencia de los directivos en el control de los empleados y, de otro, sin ser coherente con esa afirmación, se afirma que si la sociedad, al margen de la actuación concreta de sus directivos ha implementado un sistema de prevención, quedará exenta de responsabilidad penal sin establecer condiciones adicionales como en el caso de los directivos. A buen seguro esta cuestión será polémica. Se discutirá si, además del plan de prevención, es necesario que no haya habido por los directivos responsables una falta de vigilancia sobre el empleado. Lo cierto es que el art.31 bis 4 no exige este presupuesto, a diferencia de lo que acontece con los directivos en que, además del plan de prevención, se exige que no haya habido falta de vigilancia por parte del órgano encargado de la supervisión del plan (art.31 bis 2.4).

4. Atenuación de responsabilidad penal

La nueva norma dispone la atenuación de la pena, sin indicar cuantitativamente la consecuencia de la rebaja punitiva. En el caso de directivos procederá la atenuación si sólo se acredita parcialmente el cumplimiento de las condiciones previstas en el art.31 bis 2 y, en el caso de empleados, si se ha establecido o ejecutado un plan de prevención que no cumpla totalmente las exigencias para la exención de responsabilidad penal.

Tanto el Consejo de Estado como la doctrina critican la técnica del reconocimiento de esta atenuante ya que no la vinculan a la falta de cumplimiento de los requisitos de exención sino a la falta de prueba y no es la falta de prueba lo que determina la atenuación sino la inexistencia de un programa de prevención totalmente idóneo y ejecutado eficazmente.

¿QUÉ ES EL PROGRAMA DE CUMPLIMIENTO?

"Un programa de compliance analiza el riesgo para evitar que ocurran irregularidades en la empresa y para que, si se dan, sean descubiertas, investigadas y sancionadas, exonerando así a la organización diligente"

Hacíamos mención a los aspectos generales que suponen la irrupción del nuevo sistema legal de responsabilidad penal de las empresas, el cual no establece una regulación concreta sobre el contenido del programa de cumplimiento o auditoria penal. El modelo optado por el legislador español se ha inspirado en gran medida en el derecho norteamericano, el cual lleva instaurándose en diversos países europeos siendo habitual que los informes oficiales y doctrinales españoles, como los emitidos por la Fiscalía General del Estado y el Consejo General del Poder Judicial, se funden exclusivamente en estándares de cumplimiento normativo como las "Sentencing Guidelines" de los Estados Unidos, país al que debemos acudir para describir los códigos de autoregulación, también llamados "**compliance program**", término que en España entendemos que vendrá a denominarse **"auditoría penal"**.

La ausencia de dicha auditoría penal por parte de la empresa supone el primer incumplimiento del deber de control que le exige el legislador en el nuevo artículo 31 bis del código penal, habida cuenta que no existirá el control debido en la actividad empresarial. Dicho programa de cumplimiento efectivo tiene una función principal, aunque no única: eximir o atenuar la responsabilidad penal de la persona jurídica ante un eventual juicio. Dicha exención o atenuación puede manifestarse en tres estadios procesales distintos:

Con anterioridad al inicio del proceso penal: El Juez observará si la persona jurídica tenía implantado un programa de cumplimiento efectivo, valorando la calidad de dicho programa así como otros factores que condicionaran la eventual imputación de la persona jurídica.

Antes de dictar sentencia: El Juez Penal, puede valorar el programa de compliance como una prueba más en el proceso penal ya sea para evitar que la persona jurídica sea declarada penalmente responsable o bien atenuar su responsabilidad penal.

Una vez dictada la sentencia: Según está previsto en el derecho norteamericano, una vez la persona jurídica ya ha sido condenada, si ha resarcido el daño causado y, consecuentemente, ha tomado las medidas necesarias para impedir que se vuelva a cometer la conducta delictiva, se pueden mitigar los efectos de la pena.

Al empresario y a su empresa, se le suman actualmente los incumplimientos penales, además de los ya tradicionalmente regulados incumplimientos derivados del derecho civil, el derecho administrativo, el derecho mercantil, el derecho tributario, el derecho al trabajo y a la Seguridad Social y el derecho al medioambiente. Con ello, ya no sólo se expone a la imposición de sanciones sino a la pérdida de prestigio y reputación.

El **Programa de Cumplimiento** tiene como función establecer los mecanismos de prevención de cualquier actividad ilícito-penal en el marco de la persona jurídica. Por otra parte es un mecanismo de control efectivo sobre la acciones individuales de los empleados y en consecuencia el programa de compliance puede ahorrar mucho dinero a la empresa:

1.Si la persona jurídica resulta condenada, se expone, por un lado, a lo que la doctrina estadounidense llama "hard costs", que incluyen desde la multa impuesta por el Juzgado, hasta la responsabilidad civil, el pago de honorarios del abogado y del procurador, costas del proceso…

2.Los llamados "soft costs", consistentes en la pérdida de productividad por parte de los empleados, el descenso de la moral, la interrupción en las operaciones comerciales mientras dure el proceso….

3.La existencia de una auditoria penal supone la difusión de una ética empresarial corporativa positiva, ya que el programa actúa como un potente disuasor de conductas ilícitas por parte de los empleados.

Está previsto, nuevamente, una reforma del Código Penal que concretará y pulirá conceptos y términos que hasta el momento no estaban claros, así como añadirá nuevos preceptos. De entre las novedades que incluye la reforma, las más destacables son las siguientes:

1. Concreción de los requisitos, en cuanto a contenidos y ejecución que deben contener los protocolos de prevención de riesgos penales de las empresas (compliance), a fin de quedar exentas de responsabilidad penal. Es decir, que aquellas empresas que aún no hayan adoptado una compliance deberán hacerla con adecuación a dichos requisitos; y aquellas empresas que ya hayan adoptado su programa de compliance deberán verificar que el mismo se adecua a los futuros requisitos. Dichos requisitos en cuanto al contenido son:

- Identificar las actividades de riesgo.
- Establecer los protocolos de adopción de decisiones y de ejecución.
- Disponer de recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.
- Imponer la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.
- Establecer un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.
- Verificar de forma periódica dicho contenido, así como su eventual modificación, cuando se detecten infracciones relevantes o se produzcan cambios importantes en la organización, en la estructura del control o en la actividad de la sociedad.

Además, la supervisión del funcionamiento y del cumplimiento del programa de prevención debe estar confiado a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control, distinto al órgano de administración. En la práctica, dicho órgano sea posiblemente el de prevención de riesgos

laborales, que pasará a serlo también de riesgos penales. Se hace una excepción para las personas jurídicas de pequeñas dimensiones, donde dichas funciones podrán ser asumidas por el propio órgano de administración.

2. Configuración de un nuevo tipo penal que castigará con pena de prisión o multa a los órganos de administración que, ya sea con dolo o por imprudencia, omitan la adopción de dicho protocolo, luego de que se haya cometido un delito en su empresa que habría sido evitado o, al menos, seriamente dificultado, si se hubiera empleado la diligencia debida. Es decir, la compliance deja de ser una opción libre a manos del administrador que quiera atenuar la responsabilidad de su empresa, y pasa a ser obligatoria, del mismo modo que lo son los programas preventivos de riesgos laborales.

En conclusión la compliance no sólo introduce la ética en la empresa sino que debe en cierta forma intimidar o prevenir la comisión de delitos al establecer fórmulas que eleven las posibilidades de descubrimiento de las conductas irregulares. Ante la comisión del delito el programa de cumplimiento servirá de elemento de defensa, ya que acreditado el delito de la persona física en las condiciones del artículo 31 bis del Código Penal, será la empresa quién tendrá que probar su diligencia para resultar exonerada de responsabilidad penal.

NORMA ISO 19600

El Cumplimiento Normativo o Compliance es un tema en boga en España, una materia que está deshaciéndose de un cierto halo de concepto etéreo y mera importación (una más) del mundo anglosajón, para mostrar su capacidad y su necesidad en las empresas de todo tipo y tamaño de cara a identificar, prevenir y gestionar sus riesgos legales.

Sin duda, la incorporación al Código Penal de la responsabilidad penal de las personas jurídicas, ha supuesto un hito importante en este sentido. El denominado Corporate Compliance, referido a tal responsabilidad, ha enfrentado a las empresas a la necesidad de tomar medidas para evitar las duras consecuencias que puede acarrear una sentencia en sede penal contra la propia compañía, más allá de la que pueda concurrir contra el autor de determinados hechos delictivos, en caso de que la misma incurra en alguno de los delitos susceptibles de ser "cometidos" por una sociedad (y se incluyen las comillas para obviar ahora el debate técnico y/o las carencias actuales en la Ley de Enjuiciamiento Criminal).

No obstante, cuando hemos de considerar como empresa qué es el Compliance, siempre surgen las mismas dudas iniciales: qué materias están en su alcance, quién se debe encargar del Cumplimiento Normativo, si el

Compliance Officer es una figura nueva o una competencia adicional de una ya existente, qué recursos requiere, qué impacto tiene en el IT de la compañía, qué herramientas deben soportar su gestión, cómo se debe integrar en el Negocio sin obstaculizarlo…

Este elenco de preguntas requiere de respuestas objetivas, claras y que superen ciertos localismos, incompatibles con una sociedad y una economía globales, donde las empresas actúan en espacios únicos que superan las nacionalidades y donde la comparación entre ellas debe basarse en métricas ajenas a fronteras, aunque no por ello desconocedoras de las normativas locales.

En este sentido, el pasado diciembre se produjo un hecho fundamental en materia de Compliance o Cumplimiento Normativo, con la publicación de la Norma ISO 19600:2014, Compliance management systems — Guidelines.

La Norma ISO 19600 pretende constituirse como una herramienta para ayudar a la función de Compliance en sus objetivos, entre los cuales debe de estar sin duda -y al menos- la detección y gestión de los riesgos por incumplimientos de sus obligaciones legales. Se trata de un documento internacional que establecerá un referente de buenas prácticas en materia de gestión de Compliance, más allá de fronteras, culturas y jurisdicciones.

La Norma ISO 19600 es aplicable a todo tipo de organizaciones, independientemente de su tamaño y actividad, aunque en la misma norma se asumen las grandes diferencias que puede haber entre unas y otras empresas en función de volumen de operaciones, dispersión geográfica, mercados de referencia, etc. El propio texto de la Norma reconoce que el alcance con el que deben aplicarse las recomendaciones de la guía depende del tamaño, estructura, naturaleza y complejidad de cada organización.

No se trata de hacer una norma rígida y ciega ante la diversidad de organizaciones. Antes bien, se trata de hacer una norma que articule una metodología común, medible y comparable, pero con capacidad de articular las necesidades del Compliance adaptadas a la operativa, distribución competencial, idiosincrasia, madurez y cultura de cumplimiento, momento económico, estrategia comercial, etc., de cada empresa y grupo de empresas.

El Cumplimiento Normativo no admite una incorporación a las organizaciones basada en modelos industralizados que no permiten más adaptación que la puramente nominal, ni acepta la clonación de experiencias y resultados, porque aunque todas las empresas pudieran parecer iguales (a la vista de un observador inexperto o que las observe desde la estratosfera), cada una es diferente de cualquier otra.

Es por ello que la Norma ISO 19600 recoge directrices para implantar, mantener y mejorar un sistema de gestión de Compliance eficaz y receptivo. Así, incluye recomendaciones sobre los elementos con los que una organización debería contar para asegurar que cumple su política de Compliance y que tiene capacidad para asumir sus obligaciones en este ámbito.

Entre estas recomendaciones, se incluyen las relativas a la formación continua en Compliance para los perfiles implicados en su gestión y para toda la organización en cuanto a su rol en el cumplimiento, la integración del desempeño en Compliance en la evaluación del desempeño de los empleados, o la supervisión de los acuerdos de contratación externa para asegurarse de que recogen obligaciones en materia de Compliance.

En definitiva, la Norma ISO 19600:2014, Compliance management systems — Guidelines permite contar ya con un marco de referencia claro, internacional y específico para la materia de Compliance o Cumplimiento Normativo.

SISTEMA DE GESTIÓN DE COMPLIANCE

Las organizaciones cuya meta es tener éxito a largo plazo necesitan mantener una cultura de integridad y de cumplimiento, así como tomar en consideración las necesidades y expectativas de las partes interesadas. Integridad y *compliance*, por tanto, no sólo son la base, sino también una oportunidad para una organización de éxito y sostenible.

Compliance es el resultado de que una organización cumpla con sus obligaciones, y se hace sostenible introduciéndola en la cultura de la organización y en el comportamiento y en la actitud de las personas que trabajan en ella. Mientras mantenga su independencia, es preferible que la gestión de *compliance* esté integrada con los procesos de gestión de finanzas, riesgos, calidad, medio ambiente y salud y seguridad, y en sus requisitos y procedimientos operacionales.

Un sistema de gestión de *compliance* eficaz y que abarque a toda la organización permite que la organización demuestre su compromiso de cumplir con la normativa, incluyendo los requisitos legales, los códigos de la industria y los estándares de la organización, así como con los estándares de buen gobierno corporativo, las mejores prácticas, la ética y las expectativas de la comunidad en general.

El enfoque ideal de una organización hacia *compliance* consiste en que su dirección aplique los valores fundamentales y los estándares de gobierno corporativo, de ética y de relaciones con la comunidad generalmente aceptados. El que se interiorice a *compliance* en el comportamiento de las personas que trabajan en una organización depende, sobre todo, de sus directivos, en todos los niveles, y de que existan unos valores claros en la organización, así como de la aceptación y aplicación de medidas que promuevan un comportamiento de cumplimiento. Si eso no sucede así en todos los niveles de la organización, existe riesgo de incumplimiento.

En varias jurisdicciones, a la hora de determinar la sanción a imponer por contravenir las leyes, los tribunales han tenido en cuenta el compromiso de cumplimiento de una organización a través de su sistema de gestión de *compliance*. Por ello, los organismos regulatorios y judiciales también se pueden beneficiar de tener esta norma internacional como punto de referencia.

Las organizaciones están cada vez más convencidas de que si aplican valores obligatorios y una gestión adecuada de *compliance*, pueden salvaguardar su integridad y evitar o minimizar los incumplimientos legales. Integridad y un *compliance* eficaz son, por tanto, elementos clave para llevar una buena y diligente gestión. *Compliance* también contribuye al comportamiento socialmente responsable de las organizaciones.

Esta norma internacional no especifica requisitos, sino que proporciona una guía para los sistemas de gestión de *compliance* y prácticas recomendadas. Se pretende que la guía que proporciona esta norma internacional sea adaptable, por lo que el uso de esta guía puede diferir de acuerdo con el tamaño y el nivel de madurez del sistema de gestión de *compliance* de una organización y de acuerdo con el contexto, la naturaleza y la complejidad de las actividades de la organización, incluyendo su política de *compliance* y sus objetivos.

El flujograma de la figura 1 es coherente con otros sistemas de gestión y está basado en el principio de mejora continua (Planificar-Hacer-Verificar-Actuar).

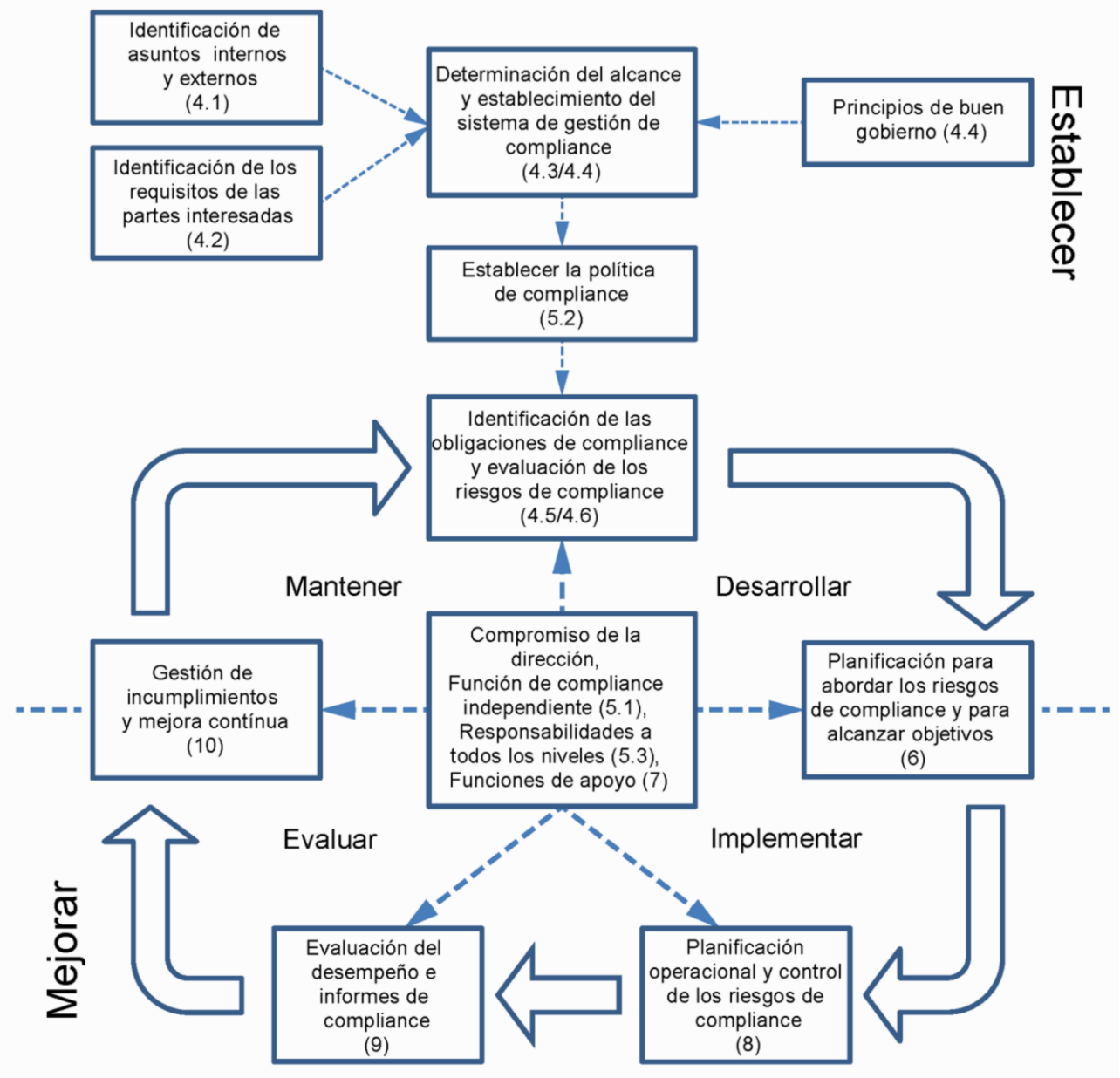

Figura 1 – Organigrama de un sistema de gestión de *compliance*

Esta norma internacional ha adoptado la "estructura de alto nivel" (es decir, secuencia de cláusulas, texto común y terminología común) desarrollada por ISO para mejorar el alineamiento entre sus normas internacionales para sistemas de gestión. Además de una guía genérica sobre un sistema de gestión de *compliance*, esta norma internacional también proporciona un marco para ayudar en la implementación de cuestiones relacionadas con *compliance* en cualquier sistema de gestión.

Las organizaciones que no hayan adoptado normas de sistemas de gestión o un marco de gestión de *compliance* pueden adoptar fácilmente esta norma internacional como una guía independiente en su organización.

Esta norma internacionales adecuada para mejorar los requisitos relacionados con *compliance* en otros sistemas de gestión y para ayudar a la organización a que mejore la gestión global de todas sus obligaciones de *compliance*.

Esta norma internacional puede combinarse con normas de sistemas de gestión existentes (por ejemplo, las Normas ISO 9001, ISO 14001, ISO 22000) y con guías genéricas (por ejemplo, ISO 31000, ISO 26000).

COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO

La organización debería determinar las cuestiones externas e internas que son pertinentes para su propósito, tales como las que se refieren a riesgos de *compliance*, y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de *compliance*. Para ello, la organización debería considerar un conjunto amplio de aspectos internos y externos, tales como el contexto regulatorio, social y cultural, la situación económica y las políticas internas, los procedimientos, los procesos y los recursos.

COMPRESIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La organización debería determinar:

- las partes interesadas que son pertinentes al sistema de gestión de *compliance*; y
- los requisitos de estas partes interesadas.

DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE *COMPLIANCE*

La organización debería determinar los límites y la aplicabilidad del sistema de gestión de *compliance* para establecer su alcance.

Cuando se determina este alcance, la organización debería considerar:

- las cuestiones externas e internas
- los requisitos

El alcance debería estar disponible como información documentada.

SISTEMA DE GESTIÓN DE *COMPLIANCE* Y PRINCIPIOS DE BUEN GOBIERNO

La organización debería establecer, implementar, mantener y mejorar continuamente un sistema de gestión de *compliance*, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta norma internacional, tomando en consideración los siguientes principios de gobierno:

- acceso directo de la función de *compliance* al órgano de gobierno;
- independencia de la función de *compliance;*
- asignación a la función de *compliance* de la autoridad correspondiente y de recursos adecuados.

El sistema de gestión de *compliance* debería reflejar los valores, objetivos, estrategia y riesgos de *compliance* de la organización.

OBLIGACIONES DE COMPLIANCE

IDENTIFICACIÓN DE LAS OBLIGACIONES DE *COMPLIANCE*

La organización debería identificar sistemáticamente sus obligaciones de *compliance* y las implicaciones que éstas tienen para sus actividades, productos y servicios. La organización debería considerar estas obligaciones al establecer, desarrollar, implementar, evaluar, mantener y mejorar su sistema de gestión de *compliance*.

La organización debería documentar sus obligaciones de *compliance* de forma adecuada a su tamaño, complejidad, estructura y operaciones.

Las fuentes de las obligaciones de *compliance* deberían incluir requisitos de *compliance* y pueden incluir compromisos de *compliance*.

EJEMPLO 1 Ejemplos de requisitos de *compliance* incluyen:

- normas legales,
- permisos, licencias u otras formas de autorización,
- órdenes, reglas o guías emitidas por agencias regulatorias,

- sentencias de juzgados o de tribunales administrativos,
- tratados, convenciones y protocolos.

EJEMPLO 2 Ejemplos de compromisos de *compliance* incluyen:

- acuerdos con grupos de la comunidad u organizaciones no gubernamentales,
- requisitos organizativos, tales como políticas y procedimientos,
- principios voluntarios o códigos de prácticas,
- etiquetado voluntario o compromisos ambientales,
- obligaciones derivadas de acuerdos contractuales con la organización,
- normas y estándares relevantes para las organizaciones y la industria.

MANTENIMIENTO DE LAS OBLIGACIONES DE *COMPLIANCE*

Las organizaciones deberían disponer de procesos que identifiquen novedades y modificaciones en la legislación, los códigos y otras obligaciones de *compliance* para asegurar un cumplimiento continuo. Las organizaciones deberían tener procesos para evaluar el impacto de los cambios identificados y para implementar cualquier cambio en la gestión de las obligaciones de *compliance*.

EJEMPLO Ejemplos de procesos para obtener información sobre cambios en leyes y en otras obligaciones de *compliance* incluyen:

- estar en las listas de distribución de los reguladores relevantes,
- ser miembros de grupos profesionales,
- suscribirse a servicios de información relevantes,
- asistir a foros de la industria y seminarios,
- revisar las páginas web de los reguladores,
- mantener reuniones con los reguladores,
- llegar a acuerdos con asesores legales,
- revisar las fuentes de las obligaciones de *compliance* (por ejemplo, pronunciamientos regulatorios y sentencias judiciales).

IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS DE COMPLIANCE

La organización debería identificar y evaluar sus riesgos de *compliance*. Esta evaluación puede estar basada en una apreciación de riesgos formal o bien puede llevarse a cabo a través de enfoques alternativos. La apreciación de riesgos de *compliance* constituye la base para la implementación del sistema de gestión de *compliance* y para planificar la asignación de recursos y de procesos que sean adecuados y apropiados para gestionar los riesgos de *compliance* identificados.

La organización debería identificar los riesgos de *compliance* relacionando sus obligaciones de *compliance* con sus actividades, productos, servicios y aspectos relevantes de sus operaciones, con objeto de identificar situaciones en las que pueden ocurrir incumplimientos de *compliance*. La organización debería identificar las causas y las consecuencias de los incumplimientos de *compliance*.

La organización debería analizar los riesgos de *compliance* considerando las causas y las fuentes de los incumplimientos de *compliance* y la gravedad de sus consecuencias, así como la probabilidad de que ocurran los incumplimientos de *compliance* y las consecuencias asociadas. Las consecuencias pueden incluir, por ejemplo, daño personal y ambiental, pérdidas económicas, daño reputacional y responsabilidades administrativas.

La evaluación de riesgos incluye comparar el nivel del riesgo de *compliance* identificado durante el proceso de análisis con el nivel de riesgo de *compliance* que la organización puede y está dispuesta a aceptar. Basándose en esta comparación, se pueden establecer las prioridades como base para determinar la necesidad de implementar controles y la extensión de dichos controles (véase 6.1).

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-financieras, condiciones de mercado, pasivos y relaciones con los clientes;
- cambios en las obligaciones de *compliance*
- incumplimiento(s) de *compliance*.

NOTA 1 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).

NOTA 2 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/situaciones de compliance son objeto de seguimiento, corrección y acciones correctivas.

NOTA 3 La Norma ISO 31000 facilita una guía detallada sobre apreciación de riesgos.

LIDERAZGO Y COMPROMISO

La alta dirección debería demostrar liderazgo y compromiso con respecto al sistema de gestión de *compliance*:

a) estableciendo y defendiendo los valores fundamentales de la organización;

b) asegurando que se establezcan la política de *compliance* y los objetivos de *compliance* y que estos sean compatibles con la dirección estratégica de la organización

c) asegurando que se desarrollan e implementan las políticas, procedimientos y procesos para alcanzar los objetivos de *compliance*

d) asegurando que los recursos que se necesitan para el sistema de gestión de *compliance* están disponibles, distribuidos y asignados;

e) asegurando la integración de los requisitos del sistema de gestión de *compliance* en los procesos de negocio de la organización;

f) comunicando la importancia de una gestión de *compliance* eficaz y conforme con los requisitos del sistema de gestión de *compliance*;

g) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de *compliance*;

h) apoyando a otros roles de dirección relevantes a demostrar en sus correspondientes áreas su liderazgo en relación a sus responsabilidades en materia de *compliance*;

i) asegurando el alineamiento entre los objetivos operacionales y las obligaciones de *compliance*;

j) estableciendo y manteniendo mecanismos de contabilidad, incluyendo la información puntual de cuestiones relacionadas con *compliance*, incluyendo los incumplimientos de *compliance*;

k) asegurando que el sistema de gestión de *compliance* logre los resultados previstos;

l) promoviendo la mejora continua.

EJEMPLO Para que *compliance* sea eficaz se requiere un compromiso activo del órgano de gobierno y de la alta dirección que penetre en el conjunto de la organización. El nivel de compromiso se indica por el grado en el que:

- el órgano de gobierno y todos los niveles de la dirección, a través de sus acciones y decisiones, demuestran activamente su compromiso para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de *compliance* eficaz y que genera respuesta por parte de la organización,
- la política de *compliance* está formalmente aprobada por el órgano de gobierno,
- la alta dirección asume la responsabilidad de asegurar que el compromiso de *compliance* en la organización es plenamente eficaz,
- todos los niveles de la alta dirección transmiten a todos los empleados de forma consistente un mensaje claro (demostrado de palabra y acción) de que la organización cumplirá con sus obligaciones de *compliance*,
- el compromiso hacia *compliance* se comunica ampliamente en declaraciones claras y convincentes y apoyadas por actuaciones,
- se otorga a la función de *compliance* un nivel de autoridad que refleje la importancia de que *compliance* sea eficaz y se le da acceso directo al órgano de gobierno,
- se asignan recursos para establecer, desarrollar, implementar, evaluar, mantener y mejorar una cultura de *compliance* robusta a través de actividades de concienciación y formación,
- las políticas, procedimientos y procesos reflejan, no sólo los requisitos estrictamente legales, sino también códigos voluntarios y los valores fundamentales de la organización,
- la organización asigna y exige responsabilidades de *compliance* a la dirección en todos los niveles de la organización,
- se requieren revisiones periódicas del sistema de gestión de *compliance*, – el desempeño de *compliance* en la organización se mejora de forma continua, – se toman acciones correctivas.

POLÍTICA DE COMPLIANCE

GENERALIDADES

El órgano de gobierno y la alta dirección, preferiblemente tras consultar con los empleados, debería establecer una política de *compliance* que:

- sea adecuada al propósito de la organización;
- proporcione un marco de referencia para el establecimiento de los objetivos de *compliance*;
- incluya el compromiso de cumplir los requisitos aplicables; e
- incluya el compromiso de mejora continua del sistema de gestión de *compliance*.

La política de *compliance* debería definir:

- el alcance del sistema de gestión de *compliance*;
- la aplicación y el contexto del sistema en relación con el tamaño, la naturaleza y la complejidad de la organización y del entorno en el que opera;
- la medida en la que *compliance* va a estar integrada con otras funciones, tales como gobernanza, riesgos, auditoría y asesoría jurídica;
- el grado en el que *compliance* estará embebida en las políticas, procedimientos y procesos operacionales;
- el grado de independencia y autonomía de la función de *compliance*;
- la responsabilidad para gestionar e informar de cuestiones de *compliance*;
- los principios bajo los cuales se van a gestionar las relaciones con partes interesadas internas y externas;
- la norma/niveles exigida/exigibles de conducta y responsabilidad;
- las consecuencias de los incumplimientos de *compliance*.

La política de *compliance* debería:

- estar disponible como información documentada;
- estar escrita en un lenguaje sencillo de forma que los empleados puedan entender fácilmente los principios y su intención;
- estar traducida a otros idiomas en caso de ser necesario;
- comunicarse de forma clara dentro de la organización y estar fácilmente disponible para todos los empleados;
- estar disponible para las partes interesadas, según corresponda;
- actualizarse en caso de que sea necesario, asegurándose de que sigue siendo pertinente.

La política de *compliance* debería establecerse en línea con los valores, objetivos y estrategia de la organización, y debería ser respaldada por el órgano de gobierno.

La política de *compliance* establece los principios generales y el compromiso de acción de una organización para lograr *compliance*. Establece el nivel de responsabilidad y de desempeño que se requiere y establece las expectativas bajo las que se evaluarán las acciones. La política debería ser adecuada para las obligaciones de *compliance* de la organización que se derivan de sus actividades.

La política de *compliance* no debería ser un documento único sino que debería estar apoyado por otros documentos, incluyendo políticas, procedimientos y procesos operacionales.

DESARROLLO

Al desarrollar la política de *compliance*, se debería considerar lo siguiente:

a) obligaciones específicas internacionales, regionales o locales;

b) la estrategia, los objetivos y los valores de la organización;

c) la estructura y el marco de gobierno de la organización;

d) la naturaleza y el nivel de riesgo asociado a los incumplimientos de *compliance*;

e) otras políticas, normas y códigos internos.

ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

GENERALIDADES

La alta dirección debería asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización.

La alta dirección debería asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de *compliance* es conforme con los requisitos de esta norma internacional; e

b) informar a la alta dirección sobre el desempeño del sistema de gestión de *compliance*.

NOTA Las tareas específicas de la función de *compliance* no exoneran a otros empleados de las responsabilidades que puedan existir de informar sobre cuestiones de *compliance*.

ASIGNACIÓN DE RESPONSABILIDADES DE *COMPLIANCE* EN LA ORGANIZACIÓN

La involucración activa y la supervisión por parte del órgano de gobierno y de la alta dirección es una parte integral de un sistema de gestión de *compliance* eficaz. Lo anterior contribuye a asegurar que los empleados comprendan plenamente la política y los procedimientos operacionales de la organización y cómo se aplican en sus trabajos, así como a que las obligaciones de *compliance* se lleven a cabo con eficacia.

Para que un sistema de gestión de *compliance* sea eficaz, se necesita que el órgano de gobierno y la alta dirección prediquen con el ejemplo, adhiriéndose y apoyando activamente a *compliance* y al sistema de gestión de *compliance*.

Muchas organizaciones tienen una persona dedicada (por ejemplo, un responsable de *compliance* o *compliance officer*) responsable de la gestión de *compliance* en el día a día, y otras, tienen un comité de *compliance* multifuncional para coordinar *compliance* en toda la organización.

Algunas organizaciones- dependiendo de su tamaño- también tienen a una persona que tiene una responsabilidad general de la gestión de *compliance*, aunque también puede ser algo adicional a otros roles o funciones, incluyendo comités existentes, unidad(es) organizativas, o externalizar algunos elementos a expertos en *compliance*.

Esto no debería verse como una exoneración a otros niveles de la dirección de sus responsabilidades de *compliance*, ya que todos los directivos tienen un papel que jugar con relación al sistema de gestión de *compliance*. Es, por tanto, importante que se establezcan claramente sus respectivas responsabilidades y que se incluyan en sus descripciones de puesto de trabajo.

Las responsabilidades de *compliance* de los directivos variarán, necesariamente, en función de los niveles de autoridad, influencia y otros factores, tales como la naturaleza y tamaño de la organización. Sin embargo, es probable que algunas responsabilidades sean comunes a través de una variedad de organizaciones.

NOTA Esta norma internacional no distingue entre el concepto de responsabilidad y el de rendición de cuentas. Rendición de cuentas está implícito en el término "responsabilidad".

ROL Y RESPONSABILIDAD DEL ÓRGANO DE GOBIERNO Y DE LA ALTA DIRECCIÓN

El órgano de gobierno y la alta dirección deberían:

a) establecer una política de *compliance*;

b) asegurar que se mantiene el compromiso hacia *compliance* y que se gestionan adecuadamente los incumplimientos de *compliance* y los comportamientos contrarios a *compliance*;

c) incluir las responsabilidades de *compliance* en las declaraciones de posiciones de los altos directivos;

d) designar o nominar una función de *compliance* con:

1) autoridad y responsabilidad para el diseño, consistencia e integridad del sistema de gestión de *compliance*,

2) apoyo claro y sin ambigüedad del órgano de gobierno y la alta dirección y acceso directo a los mismos,

3) acceso a:

- tomadores de decisiones de alto nivel y oportunidad de contribuir en etapas tempranas de los procesos de toma de decisiones,

- todos los niveles de la organización,

- toda la información documentada y los datos necesarios para desarrollar las tareas de *compliance*,

- asesoramiento experto en legislación, códigos y normas organizativas relevantes,

4) la autoridad y capacidad de ejercer como contrapoder al mostrar cualquier consecuencia para *compliance* en los procesos de toma de decisión relevantes,

e) asegurar que la función de *compliance* tiene autoridad para actuar de forma independiente y que no se ve comprometida por otras prioridades que entren en conflicto, especialmente cuando *compliance* está integrado en el negocio.

La alta dirección debería:

- asignar recursos adecuados y apropiados para establecer, desarrollar, implementar, evaluar, mantener y mejorar el sistema de gestión de *compliance* y los resultados del desempeño;

- asegurar que se asignan las responsabilidades y autoridades para los roles relevantes y que son comunicadas a toda la organización;

- asegurar que hay sistemas de información y comunicación eficaces y puntuales;

- medirse contra baremos o resultados de desempeño clave de *compliance*;

- asignar la responsabilidad de informar sobre el desempeño del sistema de gestión de *compliance* al órgano de gobierno y a la alta dirección.

FUNCIÓN DE *COMPLIANCE*

No todas las organizaciones crearán una función de *compliance* separada, algunas pueden asignar esta función a una posición existente.

La función de *compliance*, trabajando conjuntamente con la dirección, debería ser responsable de:

a) identificar las obligaciones de *compliance*, con el apoyo de los recursos necesarios, y traducir esas obligaciones en políticas, procedimientos y procesos viables;

b) integrar las obligaciones de *compliance* en las políticas, procedimientos y procesos existentes;

c) proporcionar u organizar apoyo formativo continuo a la plantilla para garantizar que todos los empleados relevantes son formados con regularidad;

d) promover la inclusión de las responsabilidades de *compliance* en las descripciones de puestos de trabajo y en los procesos de gestión del desempeño de los empleados;

e) poner en marcha un sistema de información y documentación de *compliance*;

f) desarrollar e implementar procesos para gestionar la información, tales como las reclamaciones y/o comentarios recibidos de líneas directas, un canal de denuncias anónimas u otros mecanismos;

g) establecer indicadores de desempeño de *compliance* y supervisar y medir el desempeño de *compliance*;

h) analizar el desempeño para identificar la necesidad de acciones correctivas;

i) identificar los riesgos de *compliance* y gestionar aquellos riesgos que relacionados con terceras partes, tales como proveedores, agentes, distribuidores, consultores y contratistas;

j) asegurar que el sistema de gestión de *compliance* se revisa a intervalos planificados;

k) asegurar que hay acceso a un asesoramiento profesional adecuado para el establecimiento, implementación y mantenimiento del sistema de gestión de *compliance*;

l) proporcionar a los empleados acceso a los recursos de los procedimientos y referencias de *compliance*;

m) proporcionar asesoramiento objetivo a la organización en materias relacionadas con *compliance*.

NOTA La Norma ISO 10002 proporciona directrices para el tratamiento de las quejas.

Cuando se asigne la responsabilidad de la gestión de *compliance*, se debería considerar la forma de asegurar que la función de *compliance* no tiene conflictos de intereses y que ha demostrado:

– integridad y compromiso con *compliance*;

– habilidades de comunicación eficaz y de capacidad de influencia;

– capacidad y prestigio para que sus consejos y directrices tengan aceptación;

– competencia necesaria.

RESPONSABILIDADES DE LA DIRECCIÓN

La dirección debería ser responsable de *compliance* dentro de su área de responsabilidad. Esto incluye:

a) cooperar con y apoyar a la función de *compliance* y animar a los empleados a hacerlo de la misma forma;

b) cumplir personalmente, y que se le vea que cumple, con las políticas, procedimientos y procesos y atender y apoyar las actividades formativas de *compliance*;

c) identificar y comunicar los riesgos de *compliance* en sus operaciones;

d) llevar a cabo de forma activa y fomentar las actividades de orientación, entrenamiento y supervisión de empleados para promover un comportamiento de cumplimiento;

e) animar a los empleados a que planteen sus preocupaciones de *compliance*;

f) participar activamente en la gestión y resolución de incidentes y cuestiones relacionadas con *compliance*;

g) desarrollar la concienciación de los empleados sobre las obligaciones de *compliance* y dirigirlos a que completen los requisitos de formación y competencia;

h) asegurar que *compliance* se introduce en las descripciones de puestos de trabajo;

i) integrar el desempeño de *compliance* en las evaluaciones del desempeño de los empleados (por ejemplo, indicadores clave de desempeño, objetivos y criterios de promoción);

j) integrar las obligaciones de *compliance* en las prácticas y procedimientos de negocio existentes en sus áreas de responsabilidad;

k) junto con la función de *compliance*, asegurar que, una vez que se identifica la necesidad de una acción correctiva, ésta se implementa;

l) supervisar los acuerdos de externalización para asegurar que tienen en cuenta las obligaciones de *compliance*.

RESPONSABILIDAD DE LOS EMPLEADOS

Todos los empleados, incluso los directivos, deberían:

a) observar las obligaciones de *compliance* de la organización que son relevantes a su posición y obligaciones;

b) participar en la formación de acuerdo con el sistema de gestión de *compliance*;

c) usar los recursos de *compliance* disponibles como parte del sistema de gestión de *compliance*;

d) informar sobre preocupaciones, cuestiones o fallos de *compliance*.

PLANIFICACIÓN

ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

Al planificar el sistema de gestión de *compliance*, la organización debería considerar los principios de buen gobierno, las obligaciones de *compliance* y los resultados de la apreciación de riesgos de *compliance* para determinar los riesgos y oportunidades que es necesario tratar con el fin de:

- asegurar que el sistema de gestión de *compliance* pueda lograr sus resultados previstos;
- prevenir o reducir efectos indeseados;
- lograr la mejora continua.

La organización debería planificar:

a) las acciones para tratar estos riesgos y oportunidades; y

b) la manera de:

  - integrar e implementar las acciones en sus procesos del sistema de gestión de *compliance*,
  - evaluar la eficacia de estas acciones.

La organización debería conservar información documentada sobre los riesgos de *compliance* y sobre las acciones planificadas para gestionarlos.

OBJETIVOS DE COMPLIANCE Y PLANIFICACIÓN PARA LOGRARLOS

La organización debería establecer los objetivos de *compliance* en las funciones y niveles pertinentes.

Los objetivos de *compliance* deberían:

a) ser coherentes con la política de *compliance*;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos aplicables;

d) ser objeto de seguimiento;

e) comunicarse; y

f) actualizarse, según corresponda.

La organización debería conservar información documentada sobre los objetivos de *compliance*.

Cuando se hace la planificación para lograr sus objetivos de *compliance*, la organización debería determinar:

- qué se va a hacer;
- qué recursos se requerirán;
- quién será responsable;
- cuándo se finalizará;
- cómo se evaluarán los resultados, por ejemplo, de conformidad con las medidas y resultados clave de rendimiento de *compliance* identificados.

La organización debería conservar información documentada sobre los objetivos de *compliance* y sobre las acciones planificadas para alcanzarlos.

APOYO

RECURSOS

La organización debería determinar y proporcionar los recursos necesarios para el establecimiento, desarrollo, implementación, evaluación, mantenimiento y mejora continua del sistema de gestión de *compliance* de acuerdo con su tamaño, complejidad, estructura y operaciones.

La alta dirección y todos los demás niveles de dirección deberían asegurar que se despliegan los recursos necesarios de forma eficaz para asegurar que el sistema de gestión de *compliance* logra sus objetivos y que se consigue *compliance*.

Los recursos incluyen recursos financieros y humanos, así como el acceso a asesoramiento externo y a habilidades especializadas, infraestructura organizativa, material de referencia actual sobre gestión de *compliance* y obligaciones legales, desarrollo profesional y tecnología.

COMPETENCIA Y FORMACIÓN

COMPETENCIA

La organización debería:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño de *compliance*; y

b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

FORMACIÓN

El órgano de gobierno, la dirección y todos los empleados tienen obligaciones de *compliance* y deberían ser capaces de cumplirlas de forma eficaz. La obtención de esa capacidad se puede lograr de muchas maneras,

incluso las habilidades y conocimiento que se requieran, a través de educación, formación o experiencia profesional.

El objetivo de un programa de formación es asegurar que todos los empleados son competentes para cumplir con su rol profesional de forma consistente con la cultura de *compliance* de la organización y con el compromiso que tiene con *compliance*.

Una formación diseñada y ejecutada adecuadamente puede proporcionar una manera eficaz para que los empleados comuniquen riesgos de *compliance* que previamente no hubieran sido identificados.

La educación y formación de los empleados deberían:

a) estar hechas a medida de las obligaciones y los riesgos de *compliance* relacionados con los roles y responsabilidades del empleado;

b) cuando sea necesario, estar basadas en una evaluación de las carencias de conocimientos y competencias del empleado;

c) llevarse a cabo al comienzo de la relación del empleado con la organización y posteriormente de forma continua;

d) estar alineadas con el programa de formación corporativo e incorporadas en los planes anuales de formación;

e) ser prácticas y fácilmente comprensibles para los empleados;

f) ser relevantes para el trabajo diario de los empleados e ilustrativas de la industria, organización o sector de que se trate;

g) ser lo suficientemente flexibles como para que puedan ser impartidas por varias técnicas para acomodarse a las diferentes necesidades de las organizaciones y los empleados;

NOTA La formación interactiva podría ser la mejor forma de impartir formación si los incumplimientos de *compliance* pudieran tener consecuencias serias.

h) ser evaluadas por su eficacia;

i) ser actualizadas siempre que sea necesario;

j) ser registradas y conservadas.

Se debería considerar la necesidad de impartir formación adicional siempre que haya:

- cambios en la posición o en las responsabilidades;
- cambios en las políticas, procedimientos y procesos internos;
- cambios en la estructura organizativa;
- cambios en las obligaciones de *compliance*, en especial las relativas a requisitos legales o de las partes interesadas;
- cambios en las actividades, productos y servicios;
- cuestiones identificadas en el seguimiento, auditorías, revisiones, reclamaciones e incumplimientos, incluyendo las opiniones de los accionistas.

TOMA DE CONCIENCIA

GENERALIDADES

Las personas que realizan el trabajo bajo el control de la organización deberían tomar conciencia de:

a) la política de *compliance*;

b) su contribución a la eficacia del sistema de gestión de *compliance*, incluyendo los beneficios de una mejora del desempeño de *compliance*;

c) las implicaciones de no cumplir los requisitos del sistema de gestión de *compliance*.

COMPORTAMIENTOS

GENERALIDADES

Se deberían fomentar los comportamientos que generan y apoyan a *compliance* y no se deberían tolerar comportamientos que comprometen a *compliance*.

ROL DE LA ALTA DIRECCIÓN EN EL APOYO A *COMPLIANCE*

La alta dirección tiene una responsabilidad crucial para:

a) alinear los compromisos de *compliance* de una organización con sus valores, objetivos y estrategia para posicionar a *compliance* de forma adecuada;

b) comunicar su compromiso con *compliance* para sensibilizar y motivar a los empleados para que adopten el sistema de gestión de *compliance*;

c) animar a todos los empleados para que acepten la importancia de alcanzar los objetivos de *compliance* de los que son responsables;

d) crear un entorno en el que se fomenta que se informe sobre los incumplimientos y en el que se protege de represalias al empleado que informe;

e) animar a los empleados a que hagan sugerencias que faciliten la mejora continua del desempeño de *compliance*;

f) asegurar que *compliance* se incorpora en la cultura amplia de la organización y en las iniciativas de cambio cultural;

g) identificar los incumplimientos de *compliance* y actuar de forma inmediata para corregirlos o gestionarlos;

h) asegurar que las políticas, procedimientos y procesos de la organización apoyan y alientan a *compliance*;

i) asegurar que los objetivos y metas operacionales no comprometen un comportamiento adecuado.

CULTURA DE *COMPLIANCE*

El desarrollo de una cultura de *compliance* exige que el órgano de gobierno, la alta dirección y la dirección tengan un compromiso visible, consistente y sostenido con un estándar común y publicado de comportamiento que se requiere en todas y cada una de las áreas de la organización.

EJEMPLO Algunos ejemplos de factores que apoyarán el desarrollo de una cultura de *compliance* son:

- un conjunto claro de valores publicados,
- que se vea a la dirección implementando activamente y respetando los valores,
- consistencia en el tratamiento de acciones similares, con independencia de la posición,
- guiar, entrenar y predicar con el ejemplo,
- realizar evaluaciones adecuadas a los potenciales empleados antes de su contratación,
- un programa de iniciación u orientación adecuado que enfatice *compliance* y los valores de la organización,
- formación continua de *compliance*, incluyendo actualizaciones de la formación,
- comunicación continua de las cuestiones de *compliance*,
- sistemas de evaluación del desempeño que consideren la evaluación del comportamiento de *compliance* y que incluyan retribuciones del desempeño en base al logro de objetivos y parámetros clave de *compliance*,
- reconocimiento visible de los logros en la gestión de *compliance* y en sus resultados,
- medidas disciplinarias rápidas y proporcionadas en caso de infracciones de las obligaciones de *compliance* intencionadas o negligentes,
- una relación clara entre la estrategia de la organización y los roles individuales, que reflejen *compliance* como esencial para alcanzar los resultados de la organización,
- una comunicación abierta y adecuada sobre *compliance*.

La existencia de una cultura de *compliance* se mide por el grado en que:

- se implementan los puntos señalados arriba;
- las partes interesadas (especialmente los empleados) creen que se han implementado los puntos señalados arriba;
- los empleados entienden la relevancia de las obligaciones de *compliance* relativas a sus propias actividades y a las de sus unidades de negocio;
- la remediación de los incumplimientos se asumen y se gestionan en todos los niveles de la organización cuando sea necesario;
- se valora el papel de la función de *compliance* y sus objetivos;

– se permite y se anima a los empleados a que comuniquen sus preocupaciones de *compliance* al nivel adecuado de la dirección.

COMUNICACIÓN

GENERALIDADES

La organización debería determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de *compliance*, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) cómo comunicar.

COMUNICACIÓN INTERNA

La organización debería adoptar métodos adecuados de comunicación para asegurar que el mensaje de *compliance* es escuchado y comprendido por todos los empleados de forma continua. La comunicación debería indicar claramente cuáles son las expectativas de la organización sobre los empleados y cuáles son los incumplimientos que se espera que sean escalados, en qué circunstancias y a quién.

COMUNICACIÓN EXTERNA

Se debería adoptar un enfoque práctico de comunicación externa, dirigido a todas las partes interesadas, de acuerdo con la política de la organización.

Las partes interesadas pueden incluir, pero no están limitadas a, organismos reguladores, clientes, contratistas, proveedores, inversores, servicios de emergencia, organizaciones no gubernamentales y vecinos.

Los métodos de comunicación pueden incluir páginas web y correos electrónicos, comunicados de prensa, anuncios y boletines periódicos, informes anuales (o con otra periodicidad), discusiones informales, jornadas de puertas abiertas, grupos de trabajo, diálogo con la comunidad, involucración en eventos de la comunidad y líneas telefónicas directas. Estos enfoques pueden apoyar el entendimiento y la aceptación del compromiso con *compliance* de una organización.

INFORMACIÓN DOCUMENTADA

GENERALIDADES

El sistema de gestión de *compliance* de la organización debería incluir:

a) la información documentada requerida por esta norma internacional;

b) la información documentada que la organización ha determinado como necesaria para la eficacia del sistema de gestión de *compliance*.

EJEMPLO Ejemplos de información documentada incluyen:

- la política de *compliance* de la organización,
- los objetivos, fines, estructura y contenido del sistema de gestión de *compliance*,
- la asignación de roles y responsabilidades de *compliance*,
- el registro de las obligaciones de *compliance* relevantes,
- los registros de los riesgos de *compliance* y la priorización del tratamiento basada en el proceso de apreciación de riesgos de *compliance*,
- el registro de los incumplimientos y de los conatos de incumplimientos,
- los planes anuales de *compliance*,
- los registros personales, incluyendo, pero no limitado a, los registros de formación.

NOTA 1 La información documentada puede incluir materias relacionadas con requisitos de información regulatorios.

NOTA 2 El extensión de la información documentada para un sistema de gestión de *compliance* puede ser diferente de una organización a otra, debido a:

- el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,
- la complejidad de los procesos y sus interacciones, y
- la competencia de las personas.

– la madurez del sistema de gestión de *compliance*.

CREACIÓN Y ACTUALIZACIÓN

Al crear y actualizar información documentada, la organización debería asegurarse de que lo siguiente sea apropiado:

– la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

– el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

– la revisión y aprobación con respecto a la idoneidad y adecuación.

CONTROL DE LA INFORMACIÓN DOCUMENTADA

La información documentada requerida por el sistema de gestión de *compliance* y por esta norma internacional se debería controlar para asegurarse de que:

a) esté disponible y adecuada para su uso, dónde y cuándo se necesite;

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debería tratar las siguientes actividades, según corresponda:

– distribución, acceso, recuperación y uso;
– almacenamiento y preservación, incluida la preservación de la legibilidad;
– control de cambios (por ejemplo, control de versión);
– retención y disposición final;
– el papel de terceras partes en la creación y el control de la información documentada.

La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de *compliance* se debería identificar, según sea adecuado, y controlar.

La información documentada se puede preparar con el propósito de obtener asesoramiento legal y, por tanto, puede estar sometida a privilegio legal.

NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización debería planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas mediante:

- la definición de los objetivos de los procesos;
- el establecimiento de criterios para los procesos;
- la implementación del control de los procesos de acuerdo con los criterios;
- el mantenimiento de información documentada en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.

La organización debería controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, según sea necesario.

ESTABLECIMIENTO DE CONTROLES Y PROCEDIMIENTOS

Se deberían implantar controles para gestionar las obligaciones de *compliance* identificadas y los riesgos de *compliance* asociados y para alcanzar el comportamiento deseado.

Se necesitan controles eficaces para asegurar que se cumplen las obligaciones de *compliance* y que se previenen, o se detectan y corrigen, los incumplimientos. Los tipos y niveles de controles deberían diseñarse con el rigor suficiente para facilitar el logro de las obligaciones de *compliance* específicas de las actividades de la organización y del entorno en el que opera. Cuando sea posible, dichos controles deberían estar embebidos en los procesos organizativos normales.

EJEMPLO Ejemplos de controles incluyen:

- políticas operativas, procedimientos, procesos e instrucciones de trabajo documentados, claros, prácticos y fáciles de seguir,

- sistemas e informes de excepciones,
- autorizaciones,
- segregación de roles y responsabilidades incompatibles,
- procesos automatizados,
- planes anuales de *compliance*,
- planes de desempeño de empleados,
- evaluaciones de *compliance* y auditorías,
- compromiso de la dirección demostrado y comportamiento ejemplarizante y otras medidas para promover un comportamiento cumplidor,
- comunicación activa, abierta y frecuente sobre el comportamiento esperado de los empleados (estándares y valores, códigos de conducta).

Estos controles se deberían mantener, ser evaluados y probados periódicamente para asegurarse de que continúan siendo eficaces.

Se deberían establecer, documentar, implementar y mantener procedimientos para apoyar la política de *compliance* y traducir las obligaciones de *compliance* a la práctica.

Al desarrollar estos procedimientos, se debería considerar lo siguiente:

a) integración de las obligaciones de *compliance* en procedimientos, incluyendo sistemas informáticos, formularios, sistemas de información, contratos y otra documentación legal;

b) consistencia con otras funciones de revisión y control de la organización;

c) seguimiento y medición continuos;

d) evaluación e información (incluyendo supervisión de la dirección) para asegurar que los empleados cumplen con los procedimientos;

e) disposiciones específicas para identificar, informar y escalar casos de incumplimientos y riesgos de incumplimientos.

PROCESOS EXTERNALIZADOS

La organización se debería asegurar que los procesos externalizados son controlados y se realiza seguimiento de los mismos.

Normalmente, la externalización de las operaciones de una organización no le libera de sus responsabilidades legales o sus responsabilidades de *compliance*. Si existe alguna externalización de las actividades de la organización, la organización necesita llevar a cabo una diligencia debida eficaz para asegurar que sus estándares y compromisos con *compliance* no son rebajados. También debería haber controles sobre los contratistas para asegurar que se cumple con el contrato de forma eficaz (por ejemplo, evaluaciones del desempeño de terceras partes).

La organización debería considerar los riesgos de *compliance* relacionados con otros procesos relacionados con terceras partes, tales como el suministro de bienes y servicios y la distribución de productos, y establecer controles según sea necesario (por ejemplo, introducir las obligaciones de *compliance* en cláusulas contractuales).

EVALUACIÓN DEL DESEMPEÑO

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

GENERALIDADES

La organización debería determinar:

a) a qué es necesario hacer seguimiento y qué es necesario medir;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

c) cuándo se deberían llevar a cabo el seguimiento y la medición;

d) cuándo se deberían analizar y evaluar los resultados del seguimiento y la medición.

La organización debería conservar la información documentada adecuada como evidencia de los resultados.

La organización debería evaluar el desempeño de *compliance* y la eficacia del sistema de gestión de *compliance*.

SEGUIMIENTO

Se debería hacer seguimiento del sistema de gestión de *compliance* para asegurar que se alcanza el desempeño de *compliance*. Se debería establecer un plan de seguimiento continuo, definiendo los procesos, programas y recursos del seguimiento y la información que se debe recoger.

El seguimiento de *compliance* es el proceso de recoger información con el objetivo de evaluar la eficacia del sistema de gestión de *compliance* y el desempeño de *compliance* de la organización.

El seguimiento del sistema de gestión de *compliance* típicamente incluye:

- eficacia de la formación;
- eficacia de los controles, por ejemplo, a través de los resultados de análisis sobre una muestra;
- asignación eficaz de responsabilidades para cumplir con las obligaciones de *compliance*;
- actualización de las obligaciones de *compliance*;
- eficacia en la gestión de fallos de *compliance* previamente identificados;
- casos en los que no se llevan a cabo según lo previsto inspecciones internas de *compliance*.

El seguimiento del desempeño de *compliance* típicamente incluye:

- incumplimientos y conatos (es decir, incidentes sin efectos adversos);
- casos en los que no se cumplen las obligaciones de *compliance*;

– casos en los que no se alcanzan los objetivos;

– estado de la cultura de *compliance*;

– indicadores predictivos y reactivos establecidos en 9.1.6.

FUENTES DE OPINIÓN SOBRE EL DESEMPEÑO DE *COMPLIANCE*

La organización debería establecer, implementar, evaluar y mantener procedimientos para buscar y recibir opiniones de su desempeño de *compliance* de una serie de fuentes, incluyendo:

– empleados, por ejemplo, a través de canales de denuncias, líneas de ayuda, buzones de opinión y de sugerencias;

– clientes, por ejemplo, a través de un sistema de gestión de reclamaciones;

– proveedores;

– reguladores;

– registros de control de procesos y registros de actividad (incluyendo tanto electrónicos como en papel).

EJEMPLO Ejemplos de opiniones sobre el desempeño de *compliance* incluyen:

– cuestiones de *compliance*,

– incumplimientos y preocupaciones relativas a *compliance*,

– cuestiones de *compliance* emergentes,

– cambios continuos regulatorios y organizativos,

– comentarios sobre la eficacia y el desempeño de *compliance*.

Las opiniones deberían servir como una fuente clave de mejora continua del sistema de gestión de *compliance*.

MÉTODOS DE RECOGIDA DE INFORMACIÓN

Existen muchos métodos para recoger información. Cada método que se relaciona más abajo es relevante en distintas circunstancias y se deberían seleccionar con cuidado las diferentes herramientas para que sean adecuadas al tamaño, escala, naturaleza y complejidad de la organización.

EJEMPLO Ejemplos de recogida de información incluyen:

- informes ad hoc de incumplimientos cuando aparecen o son identificados,
- información obtenida en líneas directas, reclamaciones y otras fuentes, incluyendo el canal de denuncias,
- discusiones informales, talleres de trabajo y grupos temáticos,
- pruebas integrales y por muestreo, tales como *mystery shopping*,
- resultados de encuestas de percepción,
- observaciones directas, entrevistas formales, visitas a las instalaciones e inspecciones,
- auditorías y revisiones,
- consultas a las partes interesadas, peticiones de formación y opiniones recogidas durante la formación (especialmente las de los empleados).

ANÁLISIS Y CLASIFICACIÓN DE LA INFORMACIÓN

Es fundamental hacer una clasificación y gestión eficaz de la información.

Se debería desarrollar un sistema para la clasificación, almacenamiento y recuperación de la información.

EJEMPLO Ejemplos de criterios de clasificación de información incluyen:

- fuente,
- departamento,
- descripción del incumplimiento,
- referencias de la obligación,

– indicadores,

– severidad,

– impacto real o potencial.

Los sistemas de gestión de la información deberían capturar tanto problemas como reclamaciones y permitir la clasificación y el análisis de aquellos que estén relacionados con *compliance*.

Una vez que la información ha sido recogida, necesita analizarse y evaluarse de forma crítica para identificar el origen y las acciones adecuadas que es necesario tomar. El análisis debería considerar los problemas sistémicos y recurrentes para proceder a su corrección o mejora ya que es probable que conlleven riesgos de *compliance* significativos para la organización y pueden ser más difíciles de identificar.

DESARROLLO DE INDICADORES

Es importante que las organizaciones desarrollen un conjunto de indicadores medibles que ayuden a la organización a medir el logro de sus objetivos (véase 6.2) y a cuantificar su desempeño de *compliance*. Este proceso debería tener en cuenta los resultados de la apreciación de los riesgos de *compliance* (véase 4.6) para asegurar que los indicadores estén relacionados con las principales características de los riesgos de *compliance* de la organización. La cuestión de qué y cómo medir el desempeño de *compliance* puede ser complejo en ocasiones, pero sin embargo es un factor vital para demostrar la eficacia del sistema de gestión de *compliance*. Además, los indicadores necesarios variarán a medida que la organización madure, así como con el ritmo y alcance de los programas nuevos y revisados que se implementen.

EJEMPLO 1 Ejemplos de indicadores de actividad incluyen:

– porcentaje de empleados a los que se haya impartido formación de forma eficaz,

– frecuencia de los contactos con los reguladores,

– utilización de mecanismos para obtener opiniones (incluyendo comentarios sobre el valor de dichos mecanismos por parte de sus usuarios),

– qué tipo de acción correctiva se tomó para cada incumplimiento.

EJEMPLO 2 Ejemplos de indicadores reactivos incluyen:

– cuestiones e incumplimientos identificados y comunicados, por tipo, área y frecuencia,

– consecuencias de los incumplimientos, que pueden incluir valoración del impacto que resulte de compensaciones monetarias, multas y otras sanciones, coste de remediación, pérdida de reputación o coste del tiempo de los empleados,

– la cantidad de tiempo utilizado para informar y adoptar acciones correctivas.

EJEMPLO 3 Ejemplos de indicadores predictivos incluyen:

– riesgos de incumplimientos, medidos como la pérdida/ganancia potencial de los objetivos (ingresos, salud y seguridad, reputación, etc.) a lo largo del tiempo,

– tendencias de incumplimientos (tasa de *compliance* esperada basada en tendencias pasadas).

INFORMES DE *COMPLIANCE*

El órgano de gobierno, la dirección y la función de *compliance* deberían asegurarse de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión de *compliance* de la organización y de su adecuación continua, incluyendo todos los incumplimientos relevantes, y promover activamente el principio de que la organización anima y apoya una cultura de información completa y franca. Las disposiciones relativas a la información interna deberían asegurar que:

a) se establecen criterios adecuados y obligaciones de información;

b) se establecen programas para la presentación periódica de informes;

c) existe un sistema de informes de excepciones que facilita información ad hoc sobre incumplimientos emergentes;

d) existen sistemas y procesos que aseguren la exactitud y completitud de los informes;

e) se facilita una información exacta y completa a las funciones o áreas de la organización apropiadas, para permitir que se adopten acciones preventivas, correctivas y remediadoras;

f) hay un proceso de firmas que confirmen la exactitud de los informes que se remiten al órgano de gobierno, incluyendo la firma de la función de *compliance*.

Una organización debería elegir un formato, contenido y periodicidad de sus informes internos de *compliance* que sean adecuados a sus circunstancias, a no ser que haya alguna especificidad legal en otro sentido.

Los informes de *compliance* deberían incorporarse en los informes normales de la organización.

Sólo se deberían preparar informes separados en caso de que hubiera incumplimientos graves y para cuestiones emergentes.

Todos los incumplimientos deben ser informados adecuadamente. Mientras que los informes de problemas sistémicos y recurrentes son particularmente importantes, un incumplimiento puntual puede ser igualmente preocupante si es grave o deliberado. Incluso un fallo pequeño puede indicar una gran debilidad en los procesos existentes y en el sistema de gestión de *compliance*. Si no se informa sobre él puntualmente, puede llevar a pensar que el fallo no importa y puede dar lugar a que dicho fallo se convierta en un problema sistémico.

Se debería animar a los empleados a que respondan e informen sobre incumplimientos de las leyes y otros incidentes de incumplimientos de *compliance* y para que vean dichos informes como una acción positiva y no amenazante, sin ningún temor a sufrir represalias.

Las obligaciones de informar deberían establecerse de forma clara en la política y procedimientos de *compliance* de la organización y reforzarse por otros métodos, tales como refuerzos informales de la dirección durante su trabajo del día a día con los empleados.

CONTENIDO DE LOS INFORMES DE *COMPLIANCE*

Los informes de *compliance* pueden incluir:

a) cualquier materia sobre la que la organización deba notificar a cualquier regulador o autoridad;

b) cambios en las obligaciones de *compliance*, en su impacto en la organización y las propuestas para cumplir con las nuevas obligaciones;

c) medidas del desempeño de *compliance*, incluyendo los incumplimientos y la mejora continua;

d) número y detalles de posible(s) incumplimiento(s) y su análisis subsiguiente;

e) acciones correctivas adoptadas;

f) información sobre la eficacia del sistema de gestión de *compliance*, sus logros y tendencias;

g) contactos, y desarrollo de las relaciones, con los reguladores;

h) resultados de las auditorías, así como de las actividades de seguimiento.

La política de *compliance* debería fomentar el informe inmediato de cuestiones materialmente significativas que surjan fuera de los periodos previstos para el informe periódico.

MANTENIMIENTO DE REGISTROS

Se deberían mantener registros exactos y actualizados de las actividades de *compliance* de la organización con objeto de ayudar en los procesos de seguimiento y revisión y para demostrar la conformidad con el sistema de gestión de *compliance*.

El mantenimiento de registros debería incluir el registro y clasificación de las reclamaciones, los conflictos y los presuntos incumplimientos y los pasos dados para resolverlos.

Los registros deberían almacenarse de manera que se asegure que permanecen legibles, fácilmente identificables y recuperables.

Estos registros deberían protegerse contra cualquier adición, borrado, modificación, uso no autorizado u ocultación.

Los registros del sistema de gestión de *compliance* de la organización pueden incluir:

a) información sobre el desempeño de *compliance*, incluyendo los informes de *compliance*;

b) reclamaciones, su resolución y comunicaciones de las partes interesadas;

c) detalles de los incumplimientos y acciones correctivas y preventivas;

d) resultados de los seguimientos y de las auditorías de los sistemas de gestión de *compliance* y las acciones adoptadas.

AUDITORÍA INTERNA

La organización debería llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de *compliance*:

a) cumple:

1) los requisitos propios de la organización para su sistema de gestión de *compliance*,

2) los requisitos de esta norma internacional,

b) se implementa y mantiene eficazmente.

Se pueden realizar auditorías adicionales en caso de que sea necesario.

La organización debería:

- planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deberían tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

- para cada auditoría, definir los criterios y el alcance de ésta;

- seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

- asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y

- conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

REVISIÓN POR LA DIRECCIÓN

La alta dirección debería revisar el sistema de gestión de *compliance* de la organización a intervalos planificados, para asegurarse de su idoneidad, adecuación y eficacia continuas.

La revisión por la dirección debería considerar:

a) el estado de las acciones desde anteriores revisiones por la dirección;

b) la adecuación de la política de *compliance*;

c) el grado en el que se han cumplido los objetivos de *compliance*;

d) la adecuación de los recursos;

e) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de *compliance*;

f) la información sobre el desempeño de *compliance*, incluidas las tendencias relativas a:

- no conformidades, acciones correctivas y tiempos para su resolución,
- seguimiento y resultados de las mediciones,
- comunicación de las partes interesadas, incluyendo las reclamaciones,
- resultados de la auditoría,

g) las oportunidades de mejora continua.

Las salidas de la revisión por la dirección deberían incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de *compliance*.

Debería incluir también recomendaciones sobre:

a) la necesidad de cambios en la política de *compliance* y en sus objetivos, sistemas, estructura y personal asociados;

b) cambios de los procesos de *compliance* para asegurar una integración eficaz con las prácticas operacionales y sistemas;

c) áreas sobre las que hacer seguimiento de incumplimientos futuros potenciales;

d) acciones correctivas respecto a los incumplimientos;

e) lagunas o carencias en los sistemas de *compliance* existentes e iniciativas de mejora continua a más largo plazo;

f) reconocimiento de un comportamiento de *compliance* ejemplar dentro de la organización.

La organización debería conservar información documentada como evidencia de los resultados de las revisiones por la dirección y se debería entregar una copia al órgano de gobierno.

MEJORA

NO CONFORMIDADES Y ACCIONES CORRECTIVAS

GENERALIDADES

Cuando ocurra una no conformidad, la organización debería:

a) reaccionar ante la no conformidad, y según sea aplicable:

   – tomar acciones para controlarla y corregirla, y

   – hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

   – la revisión de la no conformidad;

   – la determinación de las causas de la no conformidad; y,

   – la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas; y

e) si es necesario, hacer cambios al sistema de gestión de *compliance*.

La falta de prevención o detección de un incumplimiento puntual no significa necesariamente que el sistema de gestión de *compliance* no sea eficaz para prevenir y detectar los incumplimientos en general.

Las acciones correctivas deberían ser adecuadas a los efectos de las no conformidades encontradas. La organización debería conservar información documentada, como evidencia de:

- la naturaleza de las no conformidades y cualquier acción tomada posteriormente; y
- los resultados de cualquier acción correctiva.

La información obtenida del análisis de las no conformidades y/o de los incumplimientos puede usarse para considerar si:

- evaluar el rendimiento del producto y servicio;
- mejorar y/o rediseñar productos y servicios;
- cambiar las prácticas y procedimientos de la organización;
- repetir la formación de los empleados;
- reevaluar la necesidad de informar a las partes interesadas;
- proporcionar una alerta temprana de potenciales incumplimientos;
- rediseñar o revisar los controles;
- mejorar las etapas de notificación e información a niveles superiores (internos y externos).

ESCALADO DE INFORMACIÓN

Se debería adoptar y comunicar un proceso claro y puntual de información a niveles superiores, para asegurar que todos los incumplimientos se ponen de manifiesto, se reportan y eventualmente se escalan a niveles relevantes de la dirección, y que se informa a la función de *compliance* y ésta es capaz de apoyar esta información a niveles superiores. Cuando sea necesario, la información a niveles superiores se debería hacer a la alta dirección y al órgano de gobierno, incluyendo los comités relevantes. El proceso debería especificar a quién, cómo y cuándo se deben reportar los asuntos y los plazos para reportar interna y externamente.

Cuando se requiere por ley que las organizaciones informen sobre los incumplimientos, las autoridades regulatorias deben ser informadas de acuerdo con la legislación aplicable o según lo convenido.

Aun cuando la legislación no requiera que las organizaciones informen sobre los incumplimientos, deberían considerar hacer declaraciones voluntarias de los incumplimientos a las autoridades regulatorias para mitigar las consecuencias de los incumplimientos.

Un sistema de gestión de compliance eficaz debería incluir un mecanismo para que los empleados de la organización y/u otras personas informen sobre malas prácticas reales o sospechosas, o sobre violaciones de las obligaciones de *compliance* de la organización, de forma confidencial y sin temor a represalias.

MEJORA CONTINUA

La organización debería mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de *compliance*.

La información recogida, analizada y evaluada consecuentemente, e incluida en los informes de *compliance*, debería usarse como base para identificar las oportunidades de mejora del desempeño de *compliance* en la organización.

EL COMPLIANCE OFFICER

El compliance officer es una figura imprescindible para las empresas anglosajonas, especialmente para las estadounidenses. Y por suerte, esta figura, también conocida como resposable del cumplimiento normativo, está cada vez más presente en las empresas españolas. El entorno que regula a las empresas para asegurar el cumplimiento de la normativa y la transparencia es cada vez más complicado tanto a nivel nacional como internacional por culpa de los escándalos financieros y problemas contables que han surgido en los últimos años.

Y ahí es donde entra esta figura que ayuda a prevenir, supervisar, detectar riesgos y resolver determinados problemas poniendo en marcha medidas preventivas. La labor de compliance es imponer la cultura del cumplimiento normativo y el de la ética empresarial, asesorando a entidades y empresas para que no se salen ninguna normativa, desde el punto de vista legal, pero también desde el punto de vista ético. Porque una de las grandes diferencias del compliance officer con respecto a las asesorías jurídicas tradicionales es que en su trabajo también impera el punto de vista ético, ya que hay veces que una empresa puede cumplir las normas legales, aunque con métodos que podrían calificarse de inmorales.

Una labor especialmente importante, dado que en estos momentos, y desde la reforma del Código Penal, las penas pueden imponerse también a la empresa si un empleado comete un delito por no haber sido controlado por los administradores de la compañía. Es decir, el compliance tiene como objetivo evitar que un problema individual provocado por el mal proceder de un empleado, pueda terminar siendo un auténtico problema para la empresa.

En esta situación, en la que el administrador de una empresa puede ser condenado con elevadas penas por la acción de un empleado, o por desconocer la normativa de un país en el que se está trabajando, entra en juego la necesidad de tener un compliance officer que se encarge de cumplir la normativa legal y evitar que existan problemas. Pero para que el compliance pueda ser efectivo 100%, es importante que los responsables de controlar que se cumple la normativa vigente tengan autoridad, recursos, y por supuesto, independencia para poder desarrollar su trabajo.que n solamente es lograr la legalidad y la transparencia en la empresa, sino que también debe controlar a sus proveedores y subcontratas para asegurar que todos los aspectos que rodean a la compañía están cumpliendo con la normativa.

Y por supuesto, que su trabajo no quede relegado y aislado, sino que sea compartido por todos los departamentos de la empresa. De hecho, es fundamental que la plantilla de la compañía asuma que el compliace es tarea de todos, y que cada empleado sea responsable en su propio departamento o labor de cumplir la normativa legal y ética.