COMPLIANCE 360

Programa formativo en materia de compliance para entidades del tercer sector

BLOQUE 6

MAPA DE RIESGOS Y DEMÁS PROCEDIMIENTOS Y POLÍTICAS

Sesión 10 (13 de noviembre de 2024): **Identificación de políticas, procedimientos y protocolos necesarios en un programa de compliance.**

Sesión impartida por: Miguel Gadea (DLA Piper) y Víctor Caballero (Centro de Estudios Garrigues)

1. INTRODUCCIÓN A LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

Para comprender la relevancia que supone para las personas jurídicas la aprobación y aplicación de políticas así como a elaboración de un mapa de riesgos, es preciso referirnos al régimen de la responsabilidad penal de las personas jurídicas.

La Ley Orgánica 5/2010 de 22 de junio introdujo la responsabilidad penal de las personas jurídicas lo que supuso el cambio más relevante de la dogmática penal en el último siglo toda vez que se dejaba sin efecto el dogma "societas delinquere non potest" (*las sociedades no pueden delinquir).*

Las sociedades sí que pueden cometer los delitos que expresamente contemplen la responsabilidad penal de la persona jurídica. Su responsabilidad es separada e independiente de la propia persona jurídica hasta el punto que las mismas son responsables del delito cometido incluso si no se ha logrado identificar a la persona física que ha cometido el delito.

El artículo que regula la responsabilidad penal de la persona jurídica es el art. 31 bis del Código Penal. Los presupuestos para que opere la responsabilidad penal de las personas jurídicas son:

- Que los delitos sean cometidos en nombre o por cuenta de las mismas y en su beneficio directo o indirecto.

- Los delitos sean cometidos por su "*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*". También pueden ser cometidos por aquellos que *"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".*

Las personas jurídicas están expuestas a severas penas. El elenco de penas que pueden ser impuestas se recoge en el art. 33.7 del CP

"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."

No obstante, el art. 31 bis 2 permite la exoneración y la mitigación de las penas si 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".* Estas medidas de "vigilancia y control" es lo que comúnmente denominamos "compliance penal".

A este respecto, el art. 31 bis 5 establece las condiciones que un programa de compliance debe reunir para ser considerado eficaz:

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

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

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

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

6.° 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."

Como podemos comprobar, el primer apartado se refiere claramente a los mapas de riesgos y los siguientes apartados requieren de la elaboración de políticas y procedimientos para poder alcanzar los objetivos que indica este precepto legal.

2. ANTECEDENTES Y DERECHO COMPARADO

A pesar de las reformas operadas en el Código Penal en los años 2010 y 2015 y de la creación jurisprudencial y consuetudinaria de las propias empresas, nos encontramos con la base normativa conformada por las Normas ISO y UNE y los marcos integrados de COSO y el derecho comparado.

i) Las normas ISO y UNE

Juegan un papel fundamental en el marco del compliance, estableciendo estándares y directrices para la implementación de sistemas de gestión de cumplimiento normativo en las organizaciones.

a) Normas ISO en el marco del compliance

Las normas ISO (International Organization for Standardization) son estándares internacionales que proporcionan directrices y requisitos para sistemas de gestión en diversos ámbitos. En el contexto del compliance, destaca:

- **UNE-ISO 37301:** Esta norma establece los requisitos y orientaciones para implementar, evaluar, mantener y mejorar un sistema de gestión de compliance eficaz en las organizaciones. Es certificable a nivel internacional, lo que otorga homogeneidad al sector normativo

b) Normas UNE en el marco del compliance

Las normas UNE (Una Norma Española) son estándares nacionales desarrollados por la Asociación Española de Normalización (UNE). En el ámbito del compliance, destacan:

- **UNE 19601**: Esta norma establece los requisitos para implementar, mantener y mejorar un sistema de gestión de compliance penal en las organizaciones. Está alineada con la Ley Orgánica 1/2015 de reforma del Código Penal español y puede ayudar a atenuar o exonerar la responsabilidad penal de las personas jurídicas
- **UNE 19602**: Se enfoca en la gestión del compliance tributario, estableciendo requisitos para un sistema que ayude a prevenir y gestionar riesgos tributarios.
- **UNE 19603**: Esta norma reciente se centra en sistemas de gestión de compliance en materia de libre competencia.

ii) COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Es un marco de referencia fundamental en materia de compliance y control interno para las organizaciones. Este marco proporciona directrices y estándares para implementar, evaluar y mejorar los sistemas de control interno y gestión de riesgos. Por ejemplo, en EEUU para poder obtener un registro de entidad ante la Securities Exchange Commission (SEC) la entidad ha de seguir los Marcos Integrados de COSO.

iii) Derecho comparado

La función del compliance en las empresas surgió en la década de los 70 en EE.UU, como una respuesta a las exigencias legales y regulatorias establecidas por el legislador en respuesta a la incapacidad de las empresas para autorregularse y evitar una mala praxis. En 1977 se promulgaría una Ley sobre Prácticas Corruptas en el Extranjero. Más adelante en 1986, como consecuencia de las múltiples alegaciones de fraude entre los contratistas de defensa se creó el órgano para la Defensa de la Iniciativa Industrial (The Defense Industry Initiative).

3. MAPA DE RIESGOS PENALES

Son documentos que sirven de compendio de los riesgos penales que pueden afectar a una organización. Los mapas de riesgos no son exclusivos del compliance penal sino que también son utilizados en otro tipo de ámbitos del derecho (fiscal, regulatorio, laboral, etc.).

Los mapas de riesgos son de libre configuración pero, a nuestro juicio, el contenido mínimo que debe tener, a nuestro juicio, es el siguiente:

- Riesgos: se debe reflejar nominalmente qué riesgo se está analizando y qué norma legal prevé el mismo.
- Valoración del riesgo: esto requiere de un procedimiento que se expondrá a continuación.
- Áreas afectadas: qué departamentos o responsables están más expuestos.

- Controles aplicados: qué controles ayudan a mitigar el riesgo.

La valoración del riesgo, en la práctica forense, se suele realizar aplicando la siguiente fórmula:

Impacto X probabilidad = riesgo inherente – controles = riesgo residual

Las variables anteriores se pueden calcular de la siguiente manera:

- **Impacto:** el impacto es el grado de afectación que pueden traer las consecuencias penales derivadas de la eventual comisión del delito. Se establece una graduación de qué consecuencias podría traer a la sociedad las distintas penas que pudieran imponerse. Ej. Multas de hasta €50K reciben el grado "1", entre €50-100 K grado "2", riesgo reputacional grado "3" etc.
- **Probabilidad:** se trata de reducir a una valoración cuantitativa en qué grado es posible o esperable la comisión del delito. Para ello habrá que valorar el grado de exposición de la sociedad, antecedentes, etc.
- **Riesgo inherente:** es producto del impacto y la probabilidad. Es el riesgo "bruto" de la actividad de la persona jurídica.
- **Controles:** Medidas internas/externas que ayudan a mitigar el riesgo. También se someten a graduación en función de la calidad de los controles.
- **Riesgo residual:** Es el riesgo neto que tiene la persona jurídica de cara a la responsabilidad penal que le pudiera ser aplicable. También esta sujeto a graduación para poder medir el resultado final.

4. PROCEDIMIENTOS Y POLÍTICAS

Las políticas de empresa son principios, pautas a seguir, formas de pensar y de actuar que emanan de la dirección de la empresa. Las políticas ofrecen a los miembros de una organización una guía sobre como actuar en un determinado ámbito.

Las políticas y procedimientos sirven para mitigar la arbitrariedad y el desvío de poder dentro de las organizaciones.

Las políticas, para ser eficaces, deben ser coherentes y claras. Ser aceptadas y cumplidas por todos los integrantes de la organización o, al menos, las personas involucradas en el ámbito que regula la política. Deben responder al objeto para el cual ha sido diseñada, es decir, no deben ser irrelevantes o que generen una burocracia inútil para los objetos que se están persiguiendo. Deben reunir el mayor consenso de la compañía para generar adhesión entre los miembros de la organización que deben hacerla valer. Por último deben ser acordes a los valores y cultura de la persona jurídica.

Teniendo en cuenta lo anterior, las políticas se pueden categorizar en tres áreas distintas:

- Políticas que regulan aspectos económicos: ejemplo. Política de compras, política de homologación de proveedores, políticas de gestión de tesorería y de consolidación financiera. Política de donaciones.
- Políticas que regulan aspectos organizativos de la persona jurídica: Manual del empleado, política de higiene y seguridad en el trabajo, política de protección de datos, política de uso de equipos informáticos etc.
- Políticas que regulan aspectos éticos de la organización, código de conducta, manual de PBC/FT, políticas anticorrupción, conflicto de intereses, etc.

Para la elaboración de las políticas y procedimientos se han de tener en cuenta los siguientes aspectos:

- Capacidad de aprobación y revisión. Se han de considerar quien aprueba la política y quien se encarga de su revisión. Las políticas pueden ser confeccionadas por las personas más próximas a la realidad objeto de regulación pero requiere de su aprobación por parte del órgano de administración.
- Personas involucradas en la redacción. Como se han indicado anteriormente, lo idóneo es servirse de las personas que conocen la materia objeto de regulación pero también resulta conveniente involucrar a terceros que ofrezcan una visión objetiva que evite la perpetuación de vicios, malas prácticas, etc.
- Segregación de funciones. En la medida en que sea posible, se recomienda la aplicación del principio "cuatro ojos" que evite que las decisiones o los procedimientos sean dependientes de una sola persona.
- Tipos de controles a implementar: pueden ser de distinta naturaleza, límites cuantitativos, aplicaciones informáticas, aprobaciones, etc.
- Publicación y difusión: las políticas deben ser conocidas por sus aplicadores y deben estar disponibles para su consulta en intranet, carpetas comunes, etc.
- Archivo y revisión. Al hilo de lo anterior las políticas deben ser revisadas. Se recomienda incluir un cuadro de control de versiones en la que se refleje la fecha de revisión y qué elementos se han modificado.

Para concluir, recuérdese que el diseño de controles en el marco de la gestión de riesgos de compliance es un proceso fundamental para las organizaciones que buscan mantener un programa de cumplimiento efectivo. Como hemos expuesto anteriormente, este proceso se compone de tres etapas clave interrelacionadas: identificación, análisis y valoración de riesgos.

La **identificación de los riesgos** es el punto de partida crucial en el diseño de controles. En esta etapa, las organizaciones se dedican a:

- Descubrir, reconocer y registrar sistemáticamente los posibles incumplimientos que pueden ocurrir en cada actividad de la organización.

- Identificar situaciones específicas, causas subyacentes y fuentes potenciales de incumplimientos.

A continuación, el proceso avanza hacia el **análisis de los riesgos:**

- Examinar los controles existentes para determinar si tratan adecuadamente los riesgos identificados.
- Estimar la probabilidad de ocurrencia de los riesgos y la gravedad de sus consecuencias (impacto).
- Considerar diversos escenarios y cómo los controles actuales podrían responder a ellos.

La etapa final del proceso es la **valoración de los riesgos,** donde se toman decisiones críticas basadas en la información recopilada y analizada. Esta fase implica:

- Comparar el nivel de riesgo identificado y analizado con el apetito de riesgo de la organización.
- Determinar la estrategia de respuesta más apropiada para cada riesgo, que puede incluir aceptar, mitigar, transferir o evitar el riesgo.
- Priorizar los riesgos en función de su importancia relativa y la capacidad de la organización para gestionarlos.

En resumen, el compliance no debe verse como una mera obligación legal, sino como una inversión estratégica que aporta valor a largo plazo. Implementar y mantener un programa de compliance robusto es esencial para la sostenibilidad, el crecimiento y el éxito de las empresas en el panorama empresarial actual. Las organizaciones que lo adoptan de manera proactiva no solo se protegen contra riesgos, sino que también se posicionan para aprovechar oportunidades y destacar en un mercado cada vez más consciente de la importancia de la ética y el cumplimiento normativo.