



Guía para la implementación de un **sistema de compliance** en las PYME

Grupo de investigación Contabilidad,
Cambio y Sociedad (ERGO)
Universidad de Burgos

Coordinador del Documento:
Enrique Mesa Pérez

1	Introducción	5
----------	---------------------------	----------

2	¿Qué es el compliance?	6
	¿Qué supone la Responsabilidad Penal de las personas jurídicas?	7
	¿Cómo evitar que responda penalmente la persona jurídica?	8
	¿Si responde la persona jurídica no responde la persona física?.....	9
	¿Qué delitos conllevan Responsabilidad Penal para mi PYME?	9
	¿Qué penas puede recibir mi empresa o asociación?	11

3	¿Qué es un sistema de compliance?	13
	¿Cómo se elabora y qué herramientas debe incluir un sistema de compliance?	13
	¿Cómo mantener el sistema de compliance una vez implementado? .	17

4	¿Puedo verificar o certificar mi sistema de compliance?.....	18
	¿Cómo se realiza el aseguramiento o verificación de un sistema de compliance?	18
	¿Es necesario asegurar el sistema de compliance de mi PYME?	19
	¿Quiénes son los proveedores de aseguramiento?	19
	¿Qué estándares de aseguramiento se siguen para verificar el sistema de compliance?	20

5	Páginas web de interés donde encontrar más información:	22
----------	--	-----------

01

Introducción

Desde la introducción de la Responsabilidad Penal de las personas jurídicas en 2010 en el ordenamiento jurídico español, la incertidumbre sobre cómo se deben gestionar los riesgos penales e implementar los sistemas de compliance para evitarla está siendo un desafío constante para las empresas. Entre las pequeñas y medianas empresas (de aquí en adelante, PYME) esta incertidumbre ha sido aún mayor, debido a que el principio de proporcionalidad que establece el Código Penal y la posterior Directiva 1/2016 de la Fiscalía General del Estado no definen criterios claros que permitan determinar el nivel de proporcionalidad adecuado al diseñar e implementar el sistema de compliance.

La presente guía, financiada a través del proyecto “Contabilidad y transformación de la gobernanza empresarial como contribución al desarrollo sostenible” de la Junta de Castilla y León (BU058P17), tiene como objetivo aclarar las implicaciones de la Responsabilidad Penal de las personas jurídicas para las PYME y aportar las pautas básicas que éstas deben seguir en la implementación de un sistema de compliance para gestionar dicha responsabilidad.

Esta guía no pretende ser sustitutiva de la labor que un profesional pueda desarrollar al aconsejar sobre el diseño e implementación de un sistema de compliance, pero sí permitirá conocer qué herramientas deben implantarse y qué conductas, protocolos o procedimientos pueden ponerse en funcionamiento para evitar que la persona jurídica sea imputada penalmente.

La presente guía se estructura en tres apartados. El primero introduce el origen de la Responsabilidad Penal para las personas jurídicas y las consecuencias que puede tener para una PYME. El segundo apartado describe qué es un sistema de compliance y qué mínimos debe cumplir para ser efectivo. Finalmente, el tercer apartado explica cómo se puede verificar el correcto funcionamiento del sistema y los principales estándares existentes para ello.

02

¿Qué es el compliance?

El compliance, también conocido como Cumplimiento Normativo, adquiere relevancia en Estados Unidos a raíz de la promulgación de la Ley Sarbanes-Oxley en 2002 como herramienta para prevenir nuevos escándalos financieros. El origen en España del “compliance” data de 2010, cuando el Parlamento aprobó la reforma del Código Penal la cual in-



corporó por primera vez la Responsabilidad Penal de las personas jurídicas al ordenamiento jurídico español. La Responsabilidad Penal es una responsabilidad superior, en gravedad, a la civil y su objetivo no es resarcir un daño cometido, sino imponer una pena a la persona física que cometa un delito, pudiendo conllevar una privación de libertad, patrimonio u honor. A través de las reformas del Código Penal en 2010 y 2015, así como de la Circular 1/2016 de la Fiscalía General del Estado, se reconoce que las personas jurídicas también pueden ser condenadas penalmente, estableciéndose penas específicas para ellas.

En concreto, la persona jurídica responderá penalmente cuando una persona física perteneciente a la misma cometa un delito cumpliéndose una serie de circunstancias específicas. No obstante, aunque una persona física cometa un delito dentro de la organización, tanto la reforma del Código Penal primero, como la Circular 1/2016 después, reconocen la posibilidad de que la persona jurídica no sea responsable penalmente si tiene implementado un modelo de supervisión, vigilancia y control, el cual se conoce como Sistema de Cumplimiento o Compliance. Por tanto, a través de este sistema, la persona jurídica debe controlar el comportamiento de empleados y directivos para evitar la Responsabilidad Penal. Este sistema incluye políticas, procedimientos y medidas correctoras para dotar a la organización de un debido control sobre las actividades que realicen los empleados y directivos por las cuáles la persona jurídica pueda ser penalmente imputable, creando así una cultura ética empresarial.

¿Qué supone la Responsabilidad Penal de las personas jurídicas?

La Responsabilidad Penal de las personas jurídicas pone fin al precepto jurídico “*societas delinquere non potest*”, por el cual las personas jurídicas no pueden responder penalmente por los delitos cometidos por sus empleados y/o directivos. El fin de la aplicación de este precepto supone la adopción de penas específicas aplicables a las personas jurídicas. Estas penas se imponen a las personas jurídicas con base en el artículo 31 bis del Código Penal, que establece la posibilidad de transferir la Responsabilidad Penal de los delitos cometidos por los empleados y directivos de la empresa a la persona jurídica. En concreto, se distingue dos tipos de delitos cometidos por personas físicas transferibles a las personas jurídicas:

- a) Los delitos cometidos en nombre o por cuenta de éstas, 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) 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.

En el caso del apartado a), la Fiscalía General del Estado hace hincapié en tres grupos de personas:

- Los representantes legales: La representación orgánica y la voluntaria (en este último caso en referencia a autorizados a tomar decisiones en nombre de la persona jurídica) que corresponde únicamente a los administradores por los actos comprendidos en el objeto social de la actividad de la persona jurídica. De acuerdo con el artículo 157 de la Ley de Sociedades de Capital son administradores: “los directivos o las personas con poder de representación de la sociedad”.
- Quiénes actúen individualmente o como integrantes de un órgano de la persona jurídica: Administradores de derecho, en autoría única o colegiada, ejerciendo funciones de administración en virtud de un título jurídicamente válido. En aquellas sociedades de capital en las que el administrador de derecho sea una persona jurídica, se considera que será la persona física nombrada para el ejercicio de las funciones propias del cargo (art. 212 bis LSC) quién cometa el delito.

- Quiénes ostenten facultades de organización y control: Cargos y mandos intermedios que tengan atribuidas facultades de vigilancia y control para prevenir delitos.

En el caso del apartado b), el Código Penal hace referencia a cualquier empleado de la organización sometido a “supervisión, vigilancia y control” por parte de los integrantes del apartado a) del mismo artículo. Todas las personas jurídicas, con independencia de tamaño u objeto social, salvo la Administración General del Estado y las empresas públicas necesarias para el correcto funcionamiento del país (por ejemplo, AENA o ADIF), pueden ser procesadas penalmente. Sin embargo, el legislador establece el principio de proporcionalidad para reducir la complejidad y sofisticación de los modelos de supervisión, vigilancia y control en función del tamaño de la persona jurídica. De modo que el sistema de compliance de una PYME sea más simple que el de una gran empresa.

¿Cómo evitar que responda penalmente la persona jurídica?

El Código Penal establece una serie de **condiciones que deben darse para que la persona jurídica no sea responsable penalmente**, aun cuando un directivo y/o empleado haya cometido un delito penalmente imputable. El primer requisito es que, como ya se ha mencionado, el sujeto activo, directivo y/o empleado de la PYME, cometa el delito **“por cuenta y provecho de la persona jurídica”**, es decir, que la realización del delito beneficie a la organización.

El segundo requisito está vinculado a la identificación del sujeto activo, es decir, **quién comete el delito** para dilucidar si la persona jurídica puede eximir su Responsabilidad Penal. Se deben diferenciar dos casos. En el caso de que el delito sea cometido por un directivo, la empresa responderá penalmente siempre que exista un beneficio en su favor. En el caso de ser cometido por un empleado, lo hará cuando, aparte de dicho beneficio, la actividad del empleado no haya sido sometida a supervisión, vigilancia y control por los mandos de la empresa (a través del sistema de compliance). Es decir, aunque la empresa se beneficie, si ésta controló debidamente a su empleado, no será responsable penalmente.

Surge pues la duda de saber cuándo se considera que la empresa ejerció una **supervisión, vigilancia y control debida**. La Fiscalía General del Estado a través de su Circular 1/2016 y el Tribunal Supremo a través de su Sentencia 154/2016 definen con más detalle el significado de un modelo de supervisión, vigilancia y control debidamente implementado, de modo que una persona jurídica no será responsable penalmente cuando:

1. Tenga implementado un **modelo de organización y gestión efectivo** (sistema de compliance).

2. Que dicho sistema cuente con un **órgano de vigilancia** que vele por su correcto funcionamiento (compliance officer).
3. Que el directivo o empleado que cometa el acto ilícito lo haga **eludiendo de forma fraudulenta el sistema**.
4. Que, una vez conocido el incumplimiento, la empresa **actúe diligentemente** sancionando al comitente y revisando el sistema para que no pueda producirse un nuevo acto similar (posible eximente).

La empresa podrá evitar ser condenada penalmente únicamente cuando se cumplan los requisitos indicados en los cuatro puntos anteriores.

¿Si responde la persona jurídica no responde la persona física?

No, la Responsabilidad Penal de las personas jurídicas no supone que la persona física no responda penalmente. Antes de la reforma, cuando una persona física cometía un delito penal, respondía penalmente por sus actos; mientras que la empresa lo hacía civilmente, es decir, restituyendo el bien jurídico lesionado o resarciendo el daño. Después de la reforma, la persona física seguirá respondiendo penalmente y la empresa responderá civil y penalmente cuando corresponda.

No obstante, no todos los delitos cometidos por empleados o directivos suponen Responsabilidad Penal para las personas jurídicas. Existen ciertos delitos que solamente pueden ser penalmente imputables a personas físicas. En estos casos, aunque la persona física comete el delito dentro de la organización y no se cumplan las eximentes establecidas en la Directiva 1/2016 y la STS 154/2016, la persona jurídica no responderá penalmente.

¿Qué delitos conllevan Responsabilidad Penal para mi PYME?

Aunque no existe una lista de delitos por los que pueden responder penalmente las empresas, se puede extraer una relación de delitos a partir del Código Penal. En este caso, siguiendo el listado que la ley digital publica en su web, los delitos por los que una persona jurídica puede ser condenada penalmente son:

- Tráfico de órganos humanos (Art. 156 bis CP)
- Trata de seres humanos (Art. 177 bis CP)

- Delitos relativos a la prostitución y la corrupción de menores (Art. 187, 188, 189 CP)
- Delitos contra la intimidad y allanamiento informático (Art.197, 197 bis y 197 ter CP)
- Estafas y fraudes (art. 248, 249, 250 y 251 CP)
- Frustración de la ejecución (Art. 257, 258, 258 bis CP)
- Insolvencias punibles (Arts. 259, 259 bis, 260 y 261 CP)
- Daños informáticos (Arts. 264, 264 bis y 264 ter CP)
- Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores y de corrupción privada (Arts. 270, 271, 273, 274, 275, 277, 278, 279, 280, 281, 282, 282 bis, 283, 284, 285, 285 bis (nuevo a partir del 13-3-2019), 285 quater (nuevo a partir del 13-3-2019), 286, 286 bis, 286 ter y 286 quater CP)
- Receptación y blanqueo de capitales (Art. 301 CP)
- Financiación ilegal de partidos políticos (Art. 304 bis CP)
- Delitos contra la Hacienda Pública y la Seguridad Social (Arts. 305, 306, 307, 307 ter, 308 y 310 CP)
- Delitos contra los derechos de los ciudadanos extranjeros (Art. 318 bis CP)
- Delitos de construcción, edificación o urbanización ilegal (Art. 319 CP)
- Delitos contra el medio ambiente (Arts. 325, 326, 326 bis y 330 CP)
- Delitos relativos a la energía nuclear y a las radiaciones ionizantes (Art. 343 CP)
- Delitos de riesgo provocado por explosivos (Art. 348 CP)
- Delitos contra la salud pública en la modalidad de práctica ilícita con medicamentos, productos sanitarios y adulteración de alimentos o de aguas potables (Arts. 359, 360, 361, 362, 362 bis, 362 ter, 362 quinquies, 363, 364 y 365 CP)
- Delitos contra la salud pública en la modalidad de tráfico de drogas (Art. 368 y 369 CP)
- Falsificación de moneda (Art. 386 CP)

- Falsificación de tarjetas de crédito y débito y cheques de viaje (Art. 399 bis CP)
- Cohecho (Arts. 424 y 427 CP)
- Tráfico de influencias (Arts. 429 y 430 CP)
- Malversación (Arts. 432 a 434 CP)
- Incitación al odio y a la violencia (Art. 510 CP)
- Organizaciones y grupos criminales (Arts. 570 bis y ter CP)
- Delitos de terrorismo (Arts. 571 a 580 CP)
- Ciertos casos de contrabando (Art. 2 LO 12/1995, de represión del contrabando)

Aunque no de forma directa, el Código Penal también incluye penas accesorias a los delitos cometidos por la persona física en los siguientes casos:

- Manipulación genética (Art. 159, 160, 161 CP)
- Alteración de precios en concurso y subastas públicas (Art. 262.1 CP)
- Negativa a actuaciones inspectoras (Art. 294 pfo 1º CP)
- Delitos contra los derechos de los trabajadores (Arts. 311, 311 bis, 312, 313, 314, 315, 316, 317 CP)
- Falsificación de moneda (Art. 386 CP)
- Asociación ilícita (Art. 515 CP)

Si el delito cometido por el empleado o directivo no se encuentra entre los anteriores la persona jurídica no responderá penalmente, aunque sí pueda hacerlo civilmente.

¿Qué penas puede recibir mi empresa o asociación?

De acuerdo con el artículo 33.7 del Código Penal, los jueces y tribunales podrán imponer unas penas específicas para las personas jurídicas. Éstas dependerán de la gravedad del delito cometido, pudiendo ser :

- Disolución de la persona jurídica en los casos más graves.
- Suspensión de su actividad por un período inferior a 5 años.
- Clausura de locales o establecimientos por un período inferior a 5 años.
- Prohibición de realizar la actividad por la que se cometió el delito de forma temporal (máximo 15 años) o definitiva.
- Inhabilitación para obtener subvenciones, ayudas públicas o contratar con el sector público por un período inferior a 15 años.
- Intervención judicial para salvaguardar los derechos de trabajadores, accionistas y acreedores por un período inferior a 15 años.

Estas penas aquí enumeradas son de aplicación para delitos de gravedad. Para aquellos delitos menos graves, se establecerán las penas pecuniarias correspondientes que serán de mayor cuantía a la multa civil que hubieran recibido de no existir la Responsabilidad Penal de las personas jurídicas.

03

¿Qué es un sistema de compliance?

Los sistemas de compliance tienen como objetivo fomentar una cultura ética de cumplimiento mediante (i) la definición de unas pautas de comportamiento que los empleados y directivos deberían seguir en el desarrollo de sus funciones y (ii) el establecimiento de mecanismos para denunciar y/o sancionar los incumplimientos de dichas pautas.



Antes de abordar la puesta en marcha de un sistema de compliance y las herramientas que contiene, es importante dilucidar el “Principio de proporcionalidad” que recoge la Directiva 1/2016. Este principio tiene como objetivo que las empresas adapten los sistemas de compliance a su tamaño, de modo que su diseño e implementación no constituyan un esfuerzo económico que ponga en riesgo la viabilidad de la persona jurídica. Es especialmente relevante para las PYME, ya que no deberán implementar sistemas de compliance tan sofisticados como las grandes empresas.

¿Cómo se elabora y qué herramientas debe incluir un sistema de compliance?

Los sistemas de compliance permiten a las organizaciones ejercer el deber de supervisión, vigilancia y control. Entre las medidas de vigilancia y control se deben incluir medidas efectivas que ayuden a reducir el riesgo de comisión de delitos en el seno de la organización. Como indica la Circular 1/2016, no bastaría con disponer de un sistema de control estándar, sino que este sistema debe adaptarse a las características específicas de la empresa y probar una debida diligencia en la prevención de delitos penales.

Es importante que los sistemas de control no sean únicamente un conjunto de directrices de conducta o códigos éticos, sino que incorporen pautas que permitan la vigilancia, el control y la supervisión de los miembros de la empresa con una finalidad preventiva, de forma que el sistema solo pueda fracasar en caso de existir una elusión fraudulenta del mismo. Si el sistema permite la comisión del delito sin

elusión fraudulenta, significa que éste no incluía las pautas debidas de vigilancia, control y supervisión. De esta forma, se establecen **seis condiciones que deben satisfacer los sistemas de compliance**:

1. Identificación de las actividades en cuyo ámbito puedan cometerse delitos que deriven en Responsabilidad Penal para la organización.
2. Establecimiento de protocolos o procedimientos que determinen las funciones y los responsables a fin de que, en caso de comisión de un delito, se conozca al responsable.
3. Establecimiento de modelos de gestión de los recursos financieros para controlar los posibles casos derivados de los mismos.
4. Establecimiento de mecanismos que permitan a los empleados cumplir con la “obligación de informar” de riesgos o incumplimiento de la legalidad o del propio sistema de cumplimiento. El mecanismo más conocido es el “whistleblowing” o canal de denuncias interno.
5. Implementación de un sistema disciplinario, que sancione los incumplimientos del sistema de control, con el fin de castigar y corregir la infracción de las medidas preventivas.
6. Realización de una verificación periódica del funcionamiento del sistema y corrección de posibles deficiencias.

Mapa de riesgos

El primer requisito de los sistemas de compliance consiste en identificar los riesgos dentro de la actividad empresarial que pueden repercutir en Responsabilidad Penal. Los mapas de riesgos están compuestos por el análisis de los diferentes riesgos a los que se enfrenta la PYME, para ello se utiliza una herramienta conocida como “matriz de riesgos” en la que se contraponen el riesgo concreto de que un delito pueda materializarse en la persona jurídica con las consecuencias o impacto que puede tener para la persona jurídica de un modo similar al de la figura 1. La agrupación de las diferentes matrices da como resultado el mapa de riesgos.

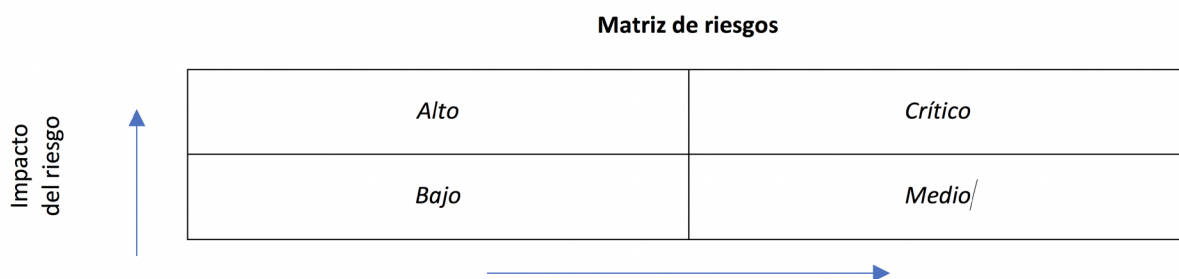


Figura 1 - Matriz de riesgos, elaboración propia

Las matrices de riesgos se elaboran de acuerdo con dos criterios: la probabilidad de que dichos delitos pudieran hacerse realidad y el impacto que la materialización del riesgo puede tener sobre una PYME para ser condenada penalmente. Por ejemplo, en una PYME de distribución de productos de papelería, tanto la probabilidad como el impacto de que un delito de manipulación genética se materialice es insignificante al no estar relacionado de ningún modo con su actividad, por lo que su riesgo es bajo. Sin embargo, en el mismo caso, un delito contra la Hacienda Pública es posible si, por ejemplo, la persona encargada de presentar las declaraciones no tiene la formación precisa o proporciona un asesoramiento inadecuado; en este caso, si las cuantías exceden ciertos límites, el riesgo que entraña un acta de inspección puede tener ser alto. La persona jurídica debe valorar estas circunstancias en el mapa de riesgos.

Una vez identificados los riesgos que tienen una mayor probabilidad de materialización e impacto sobre la PYME, se deben analizar en profundidad para confeccionar el “Mapa de riesgos”. En este mapa se analizan las amenazas en términos de probabilidad y se priorizan los riesgos para determinar a cuáles destinar más recursos para su control.

Política o manual de compliance

Este documento, generalmente interno, es el documento fundamental para probar la existencia de un modelo de supervisión, vigilancia y control en la PYME. Los resultados del mapa de riesgos deberán plasmarse en el manual de compliance, diferenciando qué delitos suponen un mayor o menor riesgo. Además, el documento debe describir las políticas, procedimientos y controles establecidos para prevenir, detectar y gestionar los riesgos identificados en función de su probabilidad e impacto y así evitar que los delitos puedan materializarse, salvo infracción flagrante del sistema de compliance por parte de algún integrante de la PYME.

La identificación de riesgos, y la consecuente actualización del sistema de compliance está muy relacionados con el requisito de la Circular 1/2016 de verificación periódica del sistema. Una vez detectados los riesgos e implementadas las políticas y protocolos para evitarlos, es clave que la revisión periódica del funcionamiento del sistema sea eficaz y permita identificar nuevos riesgos o, si fuera necesario, implementar medidas correctivas que mejoren el sistema de control de los riesgos ya identificados.

El manual de compliance también deberá hacer referencia a las herramientas empleadas con tal fin, como pueden ser los códigos éticos o los canales de denuncia. El manual se archivará en un sistema documental que recopile el mapa de riesgos, cualquier herramienta empleada, como puede ser el código ético, y un archivo dónde se incluyan las revisiones periódicas del sistema y cualquier modificación de este.

Código ético

La Asociación Española de Compliance (ASCOM) define en su Libro Blanco sobre la función del Compliance al Código Ético como el documento esencial “a los efectos de promover una cultura de cumplimiento” (pg. 31). Este documento define los principios que deben guiar el comportamiento y la conducta de los empleados y directivos en su trabajo para evitar la materialización de los principales riesgos identificados en el mapa de riesgos.

El código ético también debe informar y describir los canales a disposición de los empleados para realizar comunicaciones confidenciales o resolver dudas al respecto del funcionamiento del sistema de compliance en general o el código ético en concreto, así como las sanciones que se impondrán a aquellos que cometan un delito.

Los canales de denuncias

Los “canales de denuncias” o “whistleblowing” son sistemas internos, normalmente incrustados en el sistema de gestión informático de las grandes empresas, que permiten a los empleados comunicar a los responsables de la organización sobre cualquier actividad ilícita o contraria al Sistema de Compliance.

Los canales de denuncias deben cumplir dos características fundamentales: (i) deben ser absolutamente confidenciales y anónimos, de forma que no se puedan tomar represalias contra los denunciantes; y (ii) deben estar disponibles para todos los miembros de la organización, debiendo el sistema notificar al responsable de su funcionamiento, quien deberá realizar un seguimiento de las denuncias y promover la confianza de su uso.

En el caso de las PYME, el canal de denuncias suele consistir en un procedimiento de comunicación directo entre los empleados y el gerente o responsable de cumplimiento, puestos que, en muchos casos, son desempeñados por la misma persona. Además, los canales de denuncias de las PYME no pueden estar soportados, generalmente, por un sistema informático, al no disponer de recursos suficientes para ello. Finalmente, el canal de denuncias puede ser una herramienta conflictiva puesto que las denuncias comunicadas a los directivos o gerentes pueden no ser tomadas en cuenta, o sufrir el empleado que presente la denuncia represalias por ello. En ambos casos, esto pondría de manifiesto la falta de cultura ética de la organización y redundaría en contra de la efectividad del sistema de compliance.

Compliance officer o responsable de compliance

El compliance officer o responsable de cumplimiento es la persona encargada de garantizar el cumplimiento de la ley en la organización. Normalmente, el cargo de compliance officer suele recaer en un experto legal o contable (en el caso de las grandes empresas son asesoradas por grandes auditoras o despachos de abogados). Esta persona tendría la responsabilidad de supervisar el sistema de com-

pliance implementado en la compañía. Sin embargo, debido al principio de proporcionalidad, dicha labor suele ser realizada por el propio gerente o propietario en las PYME. No obstante, las labores del compliance officer se deben realizar con la mayor independencia posible y se pueden resumir en:

1. Gestionar el modelo de previsión.
2. Supervisar el funcionamiento y cumplimiento del modelo.
3. Vigilar y controlar el personal sometido al mismo.
4. Informar y formar sobre el funcionamiento del sistema.
5. Revisar y modificar, si fuera necesario, el sistema.
6. Gestionar el canal de denuncias.

¿Cómo mantener el sistema de compliance una vez implementado?

La simple implementación de un sistema de compliance no es suficiente para evitar la Responsabilidad Penal, sino que se debe demostrar la vigencia de dicho sistema y su eficacia durante el desarrollo de la actividad empresarial. Es decir, se debe demostrar que el sistema de compliance es más que un documento y está en funcionamiento.

Por ello, los sistemas de compliance siguen el ciclo de mejora continua PDCE: Planificar, Hacer, Verificar y Actuar. Este ciclo viene recogido por la mayor parte de normas y estándares que regulan el funcionamiento de los sistemas de compliance. El objetivo es obtener la mejora continua en el funcionamiento de los sistemas de compliance.

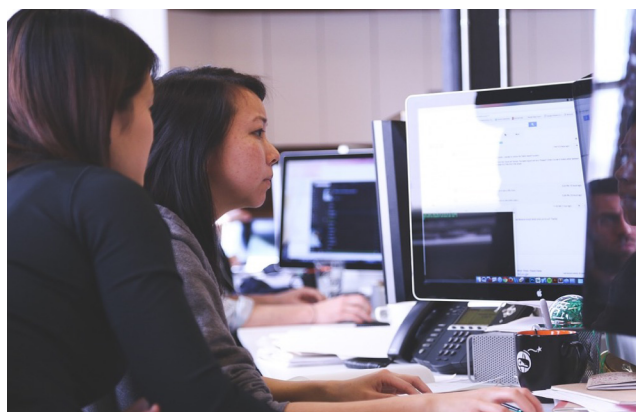
La siguiente tabla muestra un ejemplo del proceso adecuado a seguir por la herramienta del sistema de compliance para cada una de las etapas del ciclo PDCE:

Etapa	Herramienta
Planificar	Detección de riesgos, mapa de riesgos
Hacer	Manual de Compliance, procedimientos específicos
Verificar	Revisión periódica, infracción notificada a través del canal de denuncias
Actuar	Modificación del código ético

04

¿Puedo verificar o certificar mi sistema de compliance?

El requisito básico para el desarrollo de un sistema de compliance es la necesidad de prevenir, detectar y gestionar los riesgos a los que se enfrenta la persona jurídica, adaptándose a las características propias de la organización en la que se implemente. Sin embargo, en caso de comisión de delito e imputación de la persona jurídica, será fundamental poder demostrar el correcto funcionamiento del sistema de compliance.



Para ello, muchas empresas recurren a la verificación o certificación del sistema de compliance, que proporciona una garantía del correcto funcionamiento del sistema en la PYME y de que el sistema cumple los requisitos establecidos. Sin embargo, pese a que la certificación es una práctica cada vez más extendida, verificar el correcto funcionamiento del sistema de compliance no evitará la Responsabilidad Penal de la persona jurídica de forma automática, ya que la certificación únicamente prueba el funcionamiento puntual del mismo, en el momento que se realizó, y se deberá probar que el sistema funciona de forma constante. Por ello, se recomienda que las organizaciones estén comprometidas con el sistema de compliance y su funcionamiento y que no destinen recursos a verificar o certificar un sistema como si de un sello de garantía se tratase.

¿Cómo se realiza el aseguramiento o verificación de un sistema de compliance?

Antes de comenzar el aseguramiento de un sistema de compliance, es necesario recopilar el manual de compliance y demás herramientas que lo componen (mapa de riesgos, código ético, etcétera). Una vez obtenida toda la información documental del sistema, se debe evaluar al comprobar que el sistema de compliance es sometido a una revisión periódica por parte de la propia organización. Esto es fundamental dado que permite la mejora continua en los procesos de control. Además, es

necesario comprobar que el funcionamiento del sistema tenga esté documentado y archivado para probar la buena fe y diligencia de la organización.

El proveedor de aseguramiento también deberá comprobar la existencia de revisiones programadas y sobrevenidas. Las primeras son de carácter normal y periódicas. Las segunda son aquellas que surgen cuando se producen infracciones relevantes en las disposiciones del sistema o cambios en la organización o en la estructura de control que hagan necesario los cambios. La organización debe archivar todas estas revisiones junto al manual de compliance en un sistema documental que recoja toda la información.

Para poder conocer si el sistema de compliance cumple con su función es necesario desarrollar pruebas sustantivas que permitan recoger el nivel de aplicación real y la consistencia del modelo. Estas pruebas también pueden conocerse como testeos, terminología propia del mundo de la auditoría. En función de las pruebas realizadas se obtendrán diferentes niveles de aseguramiento: un aseguramiento limitado, que verifica los controles aplicados, aunque con restricciones en el alcance de las pruebas; y un aseguramiento de opinión razonable, que permite un estudio más amplio de los controles del sistema.

¿Es necesario asegurar el sistema de compliance de mi PYME?

No es necesario asegurar el sistema de compliance de una PYME si la empresa no dispone de los recursos suficientes. El Código Penal exige que el sistema de compliance sea eficaz; por ello en las PYME es más importante tener unos procesos documentados, así como implementar las herramientas mencionadas en el capítulo dos que certificar el sistema. Es fundamental comprender que pese a tener certificado la correcta implementación y funcionamiento del sistema de compliance, ésta no deja de probar que en un momento puntual el sistema funcionaba correctamente. Es decir, no será sustitutivo de los eximentes establecidos por la Directiva 1/2016 o la STS 154/2016, ni evitará que la empresa responda penalmente de cometerse un delito y no haber sido correctamente supervisado el comportamiento de los empleados.

¿Quiénes son los proveedores de aseguramiento?

Si se decide hacerla, la a verificación de la efectividad del sistema de compliance puede ser realizada tanto por agentes externos como por personas internas de la organización. En el caso de la revisión interna, será el *compliance officer* el que realizará la verificación de este, aunque esto supone que revise su propio trabajo, de ahí que sea recomendable la verificación de un tercero.

Son las verificaciones externas las que otorgan mayor seguridad y proveen de una certificación al mismo debido a su independencia con respecto a la organización. En este caso, será un proveedor de aseguramiento quién realice el proceso de verificación y otorgue la certificación correspondiente. Las empresas de auditoría y consultoría son los principales proveedores de aseguramiento. En la mayor parte de los casos, estos proveedores son los mismos profesionales que aseguran el contenido de los informes de sostenibilidad o *reporting integrado* de las grandes firmas. A gran escala, un ejemplo serían las grandes firmas de auditoría.

¿Qué estándares de aseguramiento se siguen para verificar el sistema de compliance?

Los estándares de aseguramiento son aquellas normas en las que se debe basar el proceso aseguramiento para elaborar el informe en el que se verifique el sistema en cuestión. En el caso de los sistemas de compliance penal este aseguramiento es algo más complicado, ya que, al ser relativamente nuevo, el número de estándares existentes es limitado. Los más destacados son:

ISO 19600 y UNE 19601

Las normas ISO 19600, de Sistema de Gestión del Compliance, y UNE 19601, de Gestión del Compliance Penal en España, son los primeros estándares normativos en los que se puede basar el aseguramiento de los sistemas de compliance penal. En el caso de la primera, la ISO 19600, de carácter internacional, no es una norma certificable, sino que su finalidad es crear un marco de pautas para la implementación del sistema.

Por otro lado, la norma UNE 19601, de ámbito nacional, sí que tiene carácter certificable. Esta norma establece un marco de referencia completo que permite disponer de sistemas de gestión de compliance penal alineados con las exigencias del Código Penal y los estándares internacionales en materia de cumplimiento. Es una norma que facilita el diseño y evaluación de los sistemas de gestión de compliance penal, generando una cultura organizativa sensible a la prevención y detección penal y contraria a las malas praxis que toleran y/o amparan conductas ilícitas en el seno de las organizaciones.

Libro Blanco sobre la función de Compliance

La Asociación Española de Compliance (ASCOM) publicó el Libro Blanco sobre la función de Compliance con el objeto de facilitar a las empresas la identificación de los aspectos esenciales que definen la función de Compliance y perfilar las atribuciones de sus responsables, señalando las materias clave contempladas en los estándares internacionales. Este estándar no sólo se centra en la implementación de los sistemas de compliance, sino que también pretende ayudar a los profesionales de cumplimiento en el desempeño de sus funciones.

Los estándares enumerados anteriormente, son normas generales que proveen información sobre la implementación completa del sistema de compliance. Sin embargo, existen otros estándares de certificación sobre aspectos concretos, como son:

UNE-ISO 37001

La ISO 37001, de sistemas de gestión antisoborno, es parecida a la UNE 19601, aunque de carácter internacional y tiene como objetivo proporcionar una guía para establecer, implementar, mantener, revisar y mejorar un sistema de gestión antisoborno. El soborno es uno de los delitos en los que cualquier empresa puede responder penalmente . El sistema desarrollado bajo este estándar puede integrarse en un sistema de compliance.

UNE-ISO 19602

La UNE 19602, de compliance tributario, define una serie de requisitos y pautas que las organizaciones deben seguirse para implementar un sistema de gestión de compliance tributario. El objetivo de esta norma es evitar que se cometan delitos tributarios dentro de la organización.

05

Páginas web de interés donde encontrar más información

A continuación, dejamos una relación de páginas web que puede consultar si busca información específica sobre algún aspecto relacionado con el compliance:

Asociaciones de compliance

Asociación Española de Compliance, ASCOM

Asociación de profesionales de Compliance, CUMPLEN

Asociación Europea de Abogados y Economistas en Compliance, AEAEC

World Compliance Association

Webs especializadas

Compylaw

Confilegal

LegalToday

Estándares de aseguramiento

Normalización española, UNE

Agencia Española de Normalización, AENOR

Bureau Veritas

Delitos específicos para las personas jurídicas

LaLeyDigital