CÓMO ELABORAR UN PLAN DE COMPLIANCE PARA SU EMPRESA

CONFEDERACIÓN CANARIA DE EMPRESARIOS
CEOE CEPYME

Gobierno de Canarias
Consejería de Economía, Conocimiento y Empleo

CONFEDERACIÓN CANARIA DE EMPRESARIOS

CEOE CEPYME

Gobierno de Canarias

Consejería de Economía, Conocimiento y Empleo

Este manual ha sido actualizado por la Confederación Canaria de Empresarios en el año 2019, en el marco de las diferentes actuaciones de Participación Institucional que desempeña esta Institución, y está financiada por la Consejería de Economía, Conocimiento y Empleo del Gobierno de Canarias.

Índice

¿Qué es un plan de compliance?

¿Qué es un plan de compliance?

El artículo 31 bis del Código Penal, en su nueva redacción, posibilita que las empresas sean halladas responsables por una serie de delitos. El compliance, respuesta a esta posibilidad, se define como el hecho de que una organización cumpla con toda la normativa que le es aplicable y, especialmente, con el artículo anteriormente mencionado. En definitiva, el compliance es una forma de autorregulación de las empresas con el fin de asegurarse de que su actividad se ajusta a la legalidad vigente.

El plan de compliance es el mecanismo a utilizar por las empresas para evitar ser halladas responsables penalmente de los delitos cometidos en su seno, o por personas físicas directamente relacionadas con ella. Un plan de compliance es, por tanto, un conjunto de normas internas y procesos, políticas y medidas, controles y evaluaciones, instaurados en y por la empresa con la finalidad de implementar un modelo de organización y gestión idóneo para evitar las penas por incumplimientos legales o, al menos, mitigar este riesgo en la medida de lo posible.

El objetivo principal es la creación de una especie de cortafuegos que impida la derivación de la responsabilidad de los delitos cometidos por directivos, empleados, y otras personas bajo la dirección de la organización. De forma secundaria, y resultado de la integración del compliance en el modelo de la empresa, se pretende instaurar una verdadera cultura del cumplimiento normativo en todos los aspectos de la organización, tanto internos como externos, evitando así la comisión de ilícitos penales. Por último, la implantación de un plan de compliance aporta valor a la empresa, ya no solo por evitar ser sujeto de procesos judiciales, sino por ofrecer una transparencia añadida y ahondamiento en el campo ético.

Fases de elaboración de un plan de compliance .

Creación de un equipo de compliance.

Análisis y gestión de los riesgos penales de la organización.

Definición de protocolos y procedimientos para la toma de decisiones en la organización.

Establecimiento de un Código Ético.

Establecimiento de un canal de denuncias interno y régimen disciplinario.

Diseño de un modelo de respuesta ante el riesgo de comisión de un delito.

Desarrollo e impartición de programas de formación y sensibilización.

Establecimiento de un registro de evidencias.

Establecimiento de un programa de auditoría y verificación periódica del plan.

Creación del equipo de compliance.

El equipo de compliance será el órgano, descrito en el artículo 31 bis del Código Penal (CP), de la persona jurídica que hará funcionar el programa o plan de compliance desarrollado. Sus funciones, atendiendo a dicho artículo, serán 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."

De forma más concreta, las funciones del equipo de compliance comprenden:

- Estudio de la organización y diseño del modelo de prevención penal.
- Gestión y supervisión del modelo de prevención.
- Revisión y actualización del modelo de prevención.
- Detección de los comportamientos delictivos.
- Formación a empleados y administradores.

El artículo 31 bis CP no hace referencia a la naturaleza de este órgano, dejando a elección de la persona jurídica el número de personas que lo conformarán siempre que tengan la suficiente formación y autoridad. Esta decisión va a depender, normalmente, de la dimensión de la empresa: una empresa con varios departamentos o una estructura clara podrá conformar un órgano colegiado en el que tenga presencia las unidades operativas de ésta, garantizando la participación de los departamentos en el plan y su integración en la actividad de la empresa. Será importante también de dotar al órgano con la autoridad y el respaldo suficiente para que pueda realizar su actividad de forma correcta.

En cuanto a formación, el equipo de compliace deberá contar con un perfil profesional formado como mínimo en conocimientos jurídicos, cumplimiento normativo y gestión del riesgo corporativo, así como conocimiento del funcionamiento de la organización, cultura corporativa y la normativa pública y privada que le es de aplicación en cada momento.

En el caso de las PYMES, siempre que puedan presentar cuenta de pérdidas y ganancias abreviadas, los administradores de la sociedad podrán desempeñar estas funciones de control del cumplimiento normativo. Por otro lado, y en el caso de grupos empresariales, se podrá crear un órgano único para todo el grupo, dependiendo del grado de la autonomía de las empresas del grupo respecto a la matriz: si existe grado de vinculación de las empresas con la central, se podrá crear un equipo de compliance para todo el grupo y equipos más reducidos o responsables para cada una de las empresas, mientras que si la autonomía es mayor, se deberán crear equipos de compliance para cada empresa que forme el grupo.

Cabe también la externalización de las diferentes funciones del equipo de compliance, por ejemplo, el diseño o la formación. No se deberá, por otro lado, dejar en manos de un equipo

externo el funcionamiento del plan de compliance pues se deberá estar al día de lo que ocurre en la empresa para poder prevenir y actuar ante ilícitos penales.

Análisis y gestión de riesgos penales.

El riesgo penal se corresponde con la probabilidad de que se cometa un ilícito penal en la empresa y las consecuencias de este incumplimiento respecto a las obligaciones de compliance de la persona jurídica, es decir, el impacto. El riesgo es, en resumidas cuentas, la incertidumbre en la consecución de los resultados de compliance, es decir, la evitación de ser hallada responsable de un delito.

A través del proceso de análisis se concretarán los riesgos a los que la empresa se enfrenta y su nivel de exposición a los distintos tipos de delitos que se puedan producir en su seno. Esta investigación no debe hacerse como algo aislado del resto de áreas de cumplimiento legal de la empresa, sino evaluar todas las operaciones y procedimientos de la empresa donde pueden existir riesgos penales: gestión de la seguridad de la información y protección de datos, recursos humanos, prevención y blanqueo de capitales, marketing, propiedad intelectual, etc.

A la hora de identificar los riesgos, se podrá utilizar un método que permita diferenciar entre delitos relevantes o no relevantes, de acuerdo con la probabilidad de que sean cometidos por empleados y otros vinculados a la empresa, así como la exposición de ésta a los mismos:

- Delitos relevantes serán todos aquellos respecto de los cuales la actividad de la empresa presente un cierto nivel de exposición al riesgo de ser cometidos, dando lugar a conducta de riesgo penal y potencial responsabilidad penal de la empresa.
- Delitos no relevantes son aquellos que, por motivo de la razón social de la empresa, actividad o características de ésta, difícilmente serán cometidos en el seno de la empresa dándole a ésta un beneficio. La probabilidad de incurrir en ellos es, por tanto, inapreciable y haciendo que su incorporación al plan de compliance sea innecesario.

El mapeo de riesgos penales es la herramienta más común a la hora de averiguar y calcular los riesgos a los que la persona jurídica se enfrenta, pues facilita la prevención de los riesgos a los que está expuesta la empresa mediante su identificación. Éste deberá realizarse siempre considerando la actividad de la empresa, los diferentes departamentos de ésta y la existencia de actores externos cuya actividad pueda afectar a la empresa. Del mismo modo, el mapa podrá centrarse en un tipo de riesgo o departamento de la empresa, o podrá ser transversal, cubriendo riesgos financieros, reputacionales o penales, por ejemplo. Podrán incluirse también riesgos que, aunque no conllevan un reproche penal, tienen consecuencias económicas negativas (sanciones administrativas, por ejemplo) o reputacionales para la empresa.

A la hora de valorar los riesgos, se deben tener en cuenta extremos como los siguientes:

- Acciones cometidas por cualquier persona con capacidad de representar a la empresa, y obtener un beneficio directo o indirecto. La empresa deberá tener especial cuidado y seguimiento sobre las personas que puedan actuar en nombre de la sociedad sin necesidad de notificar a los administradores, pues pueden actuar en beneficio propio al margen de la persona jurídica.

- Acciones cometidas por personas que están sometidas a la autoridad del empresario. Éste quedará exento de responsabilidad penal si prueba que, previamente a la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión adecuado para la prevención de delitos.

La evaluación de los riesgos dependerá también del tamaño y sector de la empresa, así como el detalle del mapeo. Por ejemplo, una empresa de gestión de residuos está más expuesta a delitos de tipo medioambiental que una empresa dedicada a la producción audiovisual. No obstante, determinados riesgos son comunes a toda actividad económica: delitos económicos, discriminación, falta de licencias, etc.

La UK Bribery Act 2010 recoge las siguientes tres fases a la hora de realizar una evaluación del riesgo:

1. Revisión de los riesgos inherentes a la actividad de la empresa. Por ejemplo, uso de agentes, países en los que opera, etc.
2. Identificación de todos los controles y políticas con los que la compañía cuenta para mitigar el riesgo.
3. Evaluación de los fallos o vacíos en estas políticas.
4. Elaboración de un plan de cumplimiento contra la posible corrupción basado en el riesgo presente, los controles y las medidas adicionales necesarias para proporcionar un nivel de seguridad razonable.

En cuanto a la plasmación de la valoración del riesgo y la probabilidad, se deberán crear varios niveles en concordancia con la potencial amenaza para la persona jurídica. Por ejemplo, al tratar la probabilidad se podría crear una escala con tres valoraciones diferentes: improbable, el grado más bajo con riesgos que difícilmente aparecerán en el seno de la empresa; probable, un grado intermedio con riesgos que, aunque no están presentes en el día a día de la empresa existen de forma habitual; y muy probable, con riesgos que se encuentran en el día a día de la empresa y, por tanto, tienen una alta probabilidad de comisión. En el caso del impacto que la realización de un riesgo tendría en la empresa, se podría utilizar la siguiente escala: bajo, para riesgos que provocarían penas de índole económica únicamente; alto, para los casos en los que la comisión del delito puede conllevar consecuencias que desbordan el ámbito penal; y grave, para las conductas que, de ser cometidas en la empresa, podrían llevar incluso a provocar la disolución de ésta. Podrían utilizarse, también, valores numéricos.

Como parte de este programa, las empresas llevarán a cabo normalmente entrevistas a sus empleados y agentes, análisis financieros y exámenes de sus operaciones. La medida de las operaciones dependerá de muchos factores, entre ellos el sector y ámbito geográfico de la empresa.

Un ejemplo del análisis de los riesgos para una empresa dedicada a la compraventa de inmuebles puede ser:

RIESGO	DELITO	PROBABILIDAD	IMPACTO
REVELAR DATOS PERSONALES	Descubrimiento y revelación de secretos y allanamiento informático (197 CP)	Probable	Alto
ACEPTAR PAGO CON FONDOS DE PROCEDENCIA ILÍCITA	Descubrimiento y revelación de secretos y allanamiento informático (197 CP)	Probable	Grave

El análisis de riesgos podrá incluir también el departamento en el que se localiza el riesgo y las medidas presentes para evitarlo. Por ejemplo:

RIESGO	DELITO	ÁREA	PROBABILIDAD	IMPACTO	MEDIDAS
REVELAR DATOS PERSONALES	Descubrimiento y revelación de secretos y allanamiento informático (197 CP)	Ventas	Probable	Alto	Formación de los comerciales en protección de datos y código ético de la empresa
ACEPTAR PAGO CON FONDOS DE PROCEDENCIA ILÍCITA	Descubrimiento y revelación de secretos y allanamiento informático (197 CP)	Contabilidad	Probable	Grave	Proceso de comprobación del background del comprador y procedencia de los fondos

Definición de protocolos y procedimientos para la toma de decisiones en la organización.

Los protocolos de actuación son las herramientas que establecen instrucciones a seguir en la toma de decisiones o cuando ocurren determinadas circunstancias. Establecen el modo de comportarse, qué información trasladar y a quién, modos de proceder, etc., evitando dejar al arbitrio la forma de afrontar ciertas situaciones dentro del seno de la empresa que pudieran resultar en daños a la empresa o terceros e, incluso, su responsabilidad penal.

Los protocolos suelen plasmarse documentalmente en manuales o guías, que pueden seguir la estructura básica siguiente:

- Objetivo y finalidad.
- Ámbito de aplicación.
- Principios de actuación.
- Procedimiento y actuaciones.
- Régimen sancionador.
- Control, revisión y formación.
- Comunicación y denuncia.

No será necesario elaborar un protocolo para todos los procesos o situaciones que puedan acontecer en la empresa, pero si para aquellos casos que tengan implicaciones relevantes desde la perspectiva del cumplimiento normativo. Para evitar elaborar protocolos que no son del todo necesarios, se podrá llevar a cabo con anterioridad un proceso para discernir que procedimientos y situaciones serán relevantes.

Los protocolos podrán oscilar entre una gran sencillez a una gran complejidad, involucrando a diferentes agentes y áreas de la organización, o incorporando modelos, etc.

Establecimiento de un Código Ético.

El código ético es el instrumento normativo de mayor nivel del sistema de compliance, contiene los principios éticos que la empresa desea aplicar en todos sus ámbitos de actividad y representa el compromiso de la empresa con el cumplimiento de leyes y valores éticos. Es, en definitiva, un conjunto de normas internas de conducta en el ámbito de la empresa que regula sus responsabilidades respecto a sus interlocutores y/o la conducta de sus empleados.

Tiene como finalidad principal la de prevenir riesgos legales derivados de incumplimientos normativos en la actividad diaria de la empresa ofreciendo, tanto a empleados como órganos de dirección, una guía con los objetivos, principios, normas y valores de la organización, así como procedimientos de actuación. Aunque a nivel interno el código ético genere obligaciones y pautas de comportamientos, no tiene la consideración de norma dentro del ordenamiento jurídico al ser un documento emanado de una decisión unilateral del empresario, que será quien determinará su forma, alcance y contenido.

Un código ético tiene como ventaja que ayuda a la plantilla a conocer cómo debe actuar, fomenta la igualdad de trato y la imparcialidad ante diferentes situaciones, a dar respuesta eficaz y ágil en caso de conflictos y propicia la creación de una sólida cultura organizacional. Entre los beneficios externos de un código ético tenemos, por otro lado, el minimizar las situaciones de crisis, un aumento de la confianza de inversores y accionistas mejora la reputación e imagen corporativa y fomenta la fidelidad de los consumidores y proveedores.

El código ético debe ser un documento escrito, con una estructura clara y disponible para todos los empleados, directivos e interesados en la empresa, del que emanan obligaciones y pautas de comportamiento. En cuanto a su naturaleza, podemos distinguir entre códigos laborales o no laborales; empresariales, de suscripción o modelo, dependiendo de quien lo elabore; externos o internos; y códigos éticos de la empresa y en la empresa, dependiendo de a quién estén dirigidos.

La estructura del código ético puede seguir un modelo como el siguiente:

1. Introducción y valores corporativos.
2. Ámbito de aplicación y sujetos afectados.
3. Contenidos y medidas del código.
4. Proceso sancionador y vigencia del código ético.

De forma general, deberá incluir, como mínimo, los siguientes puntos:

- Objeto y ámbito de aplicación del código, es decir, a qué empleados, departamentos, incluso empresas dentro de un conglomerado va a afectar el código ético y cuál es el objetivo que persigue.
- Principios y valores de la empresa. Son las características que la empresa considera deben afectar su actividad y resultados. Por ejemplo: el trabajo en equipo, transparencia, etc.

- Regulación de las relaciones entre empleados, indicando qué se espera de ellos en el desarrollo de su relación laboral y cómo tratar los activos de la empresa.
- Regulación de las relaciones de la empresa con terceros, tanto con sus empleados, como de los principios que debe marcar la actividad de la empresa: honestidad, equidad, responsabilidad, etc.
- Responsabilidad social o corporativa, o las actuaciones a llevar a cabo por la empresa encaminadas a la mejora de la sociedad en la que opera. Por ejemplo: política medioambiental, transparencia o su actuación en la sociedad.
- Supervisión de la implementación y cumplimiento del código. Se debería animar a la discusión del mismo con los empleados, informar de los canales de denuncia, sanciones por incumplimiento, etc.

Los pasos a seguir para su elaboración se pueden resumir como sigue:

1. Decisión de la alta dirección, que fijará la postura de la organización hacia el compromiso ético y llamará al área responsable y otras áreas afines o partes interesadas a desarrollar el documento.
2. Identificación de los interesados, definiendo el alcance del código ético dependiendo del impacto que un posible incumplimiento normativo pueda tener sobre la empresa. Deberá incluir, en todo caso, a todos los niveles de la organización.
3. Creación de un equipo que dinamice el proceso de elaboración del documento, ya sea con personas de la organización o de fuera de ésta. Este equipo tendrá la responsabilidad de definir los temas, plazos, recursos, etc., así como las acciones a realizar y el cronograma.
4. Acciones de sensibilización y participación en la elaboración del código ético, con el objetivo de favorecer el intercambio y discusión sobre casos que se dan en el día a día de la empresa, y cuáles son las acciones que se deberían adoptar. Se deberá integrar a diferentes niveles de la empresa.
5. Redacción del documento, de acuerdo con las características y necesidades de la empresa y sus grupos de interés.
6. Consultas, tanto a los diferentes equipos de la empresa como a expertos, y posterior modificación y corrección del documento.

En cuanto a su implantación, se podrá seguir un proceso como el siguiente:

1. Aprobación y presentación del documento a través de un mensaje de la dirección, cuando sea posible, para demostrar el compromiso de la empresa con el mismo y motivar a seguir sus preceptos.
2. Difusión del código ético, por ejemplo, a través de ejemplos de la actividad de la empresa. Se podrán utilizar diferentes vías (presencial, comunicados, correos electrónicos), pero se deberá cerciorar de la adhesión de todos los empleados, agentes y directivos al mismo a través de prueba documental.
3. Comunicación externa, a través de la web corporativa (permitiendo la consulta del código por cualquier persona) o enviando una copia a los integrantes de su cadena de valor, por ejemplo.
4. Establecimiento de mecanismos para fomentar y controlar el cumplimiento del código, como herramientas para la resolución de conflictos surgidos de éste, buzón de preguntas y sugerencias, nombramiento de un encargado para la resolución de dudas y conflictos, etc.

5. Establecimiento de mecanismos de revisión y actualización para el rediseño del documento según los cambios en la empresa, con su posterior comunicación a todos los interesados.

Establecimiento de un canal de denuncia interna y régimen disciplinario.

Los canales de denuncia interna (whistleblowing) son una obligación introducida por el artículo 48 de la Ley 3/2007, de 22 de marzo, para la Igualdad Efectiva de Mujeres y Hombres, y reafirmada por la reforma del artículo 31 bis CP, en el que se instaura la "obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia del modelo de prevención". En el ámbito internacional, las Noma ISO 19600 y la Norma norteamericana SA 8000 regulan también los canales internos de queja o denuncia por incumplimientos legales.

Los canales de denuncia interna se configuran como sistemas corporativos internos a través de los cuales se canalizan las denuncias o quejas de empleados sobre comportamientos, acciones o hechos cometidos por otros empleados, directivos o agentes de la compañía que pueden constituir infracciones de las leyes, de la normativa interna de la empresa o de los códigos éticos. Su finalidad es, así, la de prevenir incumplimientos normativos y corregir los detectados.

Se recomienda que estos canales contengan cinco elementos esenciales:

- Negociación con los representantes de los trabajadores, que en virtud del art. 64.5 del Estatuto de los Trabajadores y del art. 48 de la Ley de Igualdad tienen derecho a ser informados y consulados y participar en la negociación de las medidas que la empresa tome para prevenir incumplimientos laborales.
- Información y formación previa a los empleados sobre la existencia y finalidad del canal de denuncias internas. Se deberá informar también sobre su funcionamiento (forma de presentar la denuncia, órganos, plazos), de la garantía de confidencialidad y de información al denunciado.
- Objetividad y transparencia en la resolución de las denuncias para garantizar la confiabilidad del sistema.
- Garantía de indemnidad y protección al denunciante, configurando como una obligación de los empleados la de informar acerca de riesgos e incumplimientos al encargado de vigilar el funcionamiento del modelo de prevención. En este sentido es esencial que la empresa implemente una regulación protectora del denunciante, garantizando su confidencialidad mediante sistemas adecuados de comunicación y que no sufrirá represalias con motivo de la presentación de la denuncia.
- Régimen disciplinario ante incumplimientos, no solo para las infracciones detectadas por el propio canal interno, sino también para el incumplimiento de la obligación de informar.

A estos cinco elementos se le deberá unir la evaluación periódica del funcionamiento del sistema, para detectar posibles deficiencias relacionadas con la percepción de los propios empleados del canal de denuncias, la no correlación de los resultados o informes resultantes de la investigación con las necesidades de la compañía o fugas de información.

La Agencia Española de Protección de Datos (AEPD) especificaba en su Informe Jurídico 128/2007 que estos procedimientos, aunque deberán garantizar la confidencialidad de las denuncias, no podrán ser anónimos para garantizar así la exactitud e integridad de la información contenida en dichos sistemas: la confidencialidad se garantiza, según la Agencia, a través del hecho de que la persona denunciada no pudiera acceder a los datos identificativos de la persona denunciante. Sin embargo, la L.O. 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, concretamente, en su artículo 24 determina que se podrán hacer anónimamente las denuncias sobre la comisión de actos o conductas que pudiesen resultar contrarios a la normativa general o sectorial que fuese aplicable. El tratamiento de los datos personales derivado de la existencia del sistema de denuncia estará sujeto a la legislación de protección de datos de carácter personal vigente (Ley Orgánica de Protección de Datos (LOPD) y al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Para garantizar la efectividad del canal de denuncias, será necesario instaurar también un régimen disciplinario para el caso en que se cometan ilícitos penales, o violaciones de las normas internas de la empresa, o se omita su denuncia. El plan de compliance descansa en las penas que su incumplimiento puede acarrear, es decir, su autorregulación; y demuestra el compromiso de la organización con el mismo, llegando, incluso, a ser un requisito indispensable para probar que la empresa ha cumplido con los requisitos del art. 31 bis CP.

Las sanciones que se recojan en el régimen disciplinario deberán cumplir los requisitos de proporcionalidad y graduación, es decir, no se podrán imponer las sanciones más gravosas a cualquier incumplimiento. Del mismo modo, y como piedra angular para la validez de las sanciones, se deberá haber informado a los trabajadores y otros interesados de las obligaciones que se le imponen en el plan de compliance, de modo que la transgresión de estas suponga desobediencia o indisciplina.

Uno de los problemas a los que la empresa se enfrenta a la hora de establecer un régimen disciplinario es su posible colisión con la normativa laboral, debiendo esta última prevalecer debido a su rango y obligatoriedad frente al compliance, que es voluntario e inferior a la ley. Por lo tanto, las sanciones deberán ser acordes a los principios y normas del derecho laboral (Estatuto de los Trabajadores, convenios aplicables, etc.), respetando lo estipulado para la terminación de los contratos, por ejemplo.

Para la exoneración de la empresa de responsabilidad penal, no será suficiente con contar con un plan de compliance, canal de denuncias y régimen sancionador, sino que, en el caso de que la violación sea constitutiva de delito, la empresa tiene la obligación de ponerla en conocimiento de las autoridades bajo consideración ser considerada encubridora del ilícito penal y cumpliendo su compromiso con el compliance.

En el caso de que la violación haya proscrito de acuerdo con la normativa laboral y de compliance de la empresa, deberemos estar atentos a si se trata de la comisión de un delito o un incumplimiento general que no constituye delito. En el primer caso, y cuando en el ámbito penal haya también prescrito, no habrá necesidad de hacer nada pues si la responsabilidad penal para

el autor material ha prescrito, también lo ha hecho para la empresa. En el caso de que el plazo para actuar siguiendo el procedimiento disciplinario ha prescrito, pero no el plazo para tomar acciones en sede judicial, la empresa deberá denunciar el delito.

Diseño de un modelo de respuesta ante el riesgo de comisión de un delito.

Se deberá establecer un modelo de respuesta ante el riesgo de comisión de un delito, o ante la aparición de indicios de que se ha cometido un delito en el seno de la empresa. Las actividades de respuesta buscan corregir situaciones que son o podrían convertirse en incumplimientos de la legislación vigente o el plan de compliance de la empresa. Entre las diferentes medidas de respuesta tenemos la investigación interna, la investigación o fiscalización externa, la corrección del modelo de compliance, etc.

El modelo de respuesta ante una violación de la legislación o el plan de compliance, recogido en un protocolo en el que también se regularán plazos, métodos, y vías, podrá tener las siguientes fases:

1. Recepción. Con frecuencia, las denuncias se recibirán a través del canal de denuncias internas implantado como parte del plan de compliance y resultado de la obligación que tienen trabajadores y directivos de informar de cualquier acto delictivo dentro de la empresa. Cualquiera que sea el medio de recepción, así como si la denuncia se realiza de forma anónima, se deberá tratar la denuncia con la misma importancia, dando inicio al proceso de respuesta.
2. Determinación de la importancia y tipo de denuncia. Se deberá decidir los procedimientos y normas de actuación a seguir según la denuncia que se reciba: ilícito penal o cualquier otro tipo de violación de la normativa. Del mismo modo, se deberá dar traslado de la denuncia y los hechos al órgano encargado de revisar su contenido y decidir si se van a tomar acciones.
3. Instrucción del expediente, que incluye:
   - Un análisis preventivo, en el que se valorará desde las pérdidas ocasionadas por el ilícito (y la posibilidad de recuperación), las pruebas necesarias, la pertinencia de comunicar a las autoridades o si es necesario recabar colaboración de expertos, por ejemplo.
   - Un estudio de la información aportada, valorando su fiabilidad y exactitud, valorando también la noticia y al denunciante, a través de la discriminación de la información (separación entre datos objetivos y subjetivos), valoración del denunciante y de la noticia, análisis de la información, generación de una hipótesis (explicación y resultados), y la información del denunciado.
4. Emisión de un informe. Con la información obtenida y el análisis realizado, se deberá confeccionar un informe con elementos como los siguientes:
   - Información descriptiva de la denuncia: fecha de recepción, identificación, etc.
   - Datos aportados en la denuncia, con discriminación de datos objetivos y subjetivos.
   - Valoración del contenido de la denuncia y fiabilidad del denunciante.
   - Análisis de la información e hipótesis más probables y de mayor riesgo.
   - Medidas propuestas o puestas en marcha resultado del análisis preventivo.
   - Proposición de solución a la debilidad detectada y que da lugar a los hechos objeto de denuncia.
   - Propuesta de actuación, ya sea de resolución de la denuncia o de investigación, dependiendo de si es necesario profundizar en la información.

5. Elaboración de un proyecto de investigación. Entre otros extremos, deberá plantear:
   - Objetivos de la investigación.
   - Equipo de investigación, que deberá garantizar la independencia de la investigación y ser conformado acorde con los conocimientos necesarios y la persona sujeto de la investigación.
   - Calendario.
   - Presupuesto.
   - Coordinación con otros equipos que deban ser involucrados en la investigación.
6. Investigación, que se llevará a cabo de acuerdo con las hipótesis y prioridades planteadas en el informe. No existe un patrón fijo para el desarrollo de una investigación, sino que deberá adaptarse a las circunstancias de la empresa, los hechos a investigar, etc. Se deberá tener en cuenta, por otro lado, circunstancias que puedan ocasionar perjuicios a la empresa:
   - Riesgo de destrucción de pruebas.
   - Riesgo de litigios con otras empresas.
   - Riesgo de incumplimientos normativos.
7. Resolución, fruto del primer informe y de los resultados de la fase de investigación. Se deberán elaborar también recomendaciones encaminadas a mejorar los controles internos identificados como insuficientes o defectuosos a lo largo del proceso. Por último, se deberá dar noticia de la resolución al denunciado, acompañando a la resolución de las sanciones que sean aplicables.

Desarrollo e impartición de programas de formación y sensibilización.

Al igual que se instruye a los empleados en materias de prevención de riesgos laborales o blanqueo de capitales como medidas para demostrar el compromiso de la empresa en la prevención en estos dos campos, la empresa deberá ofrecer también la formación adecuada a sus empleados, directivos y agentes en materia de compliance. La formación y sensibilización en materias de compliance juega un papel primordial en la buena marcha del plan de prevención de riesgos penales: es necesario que los empleados, directivos y otros agentes de la empresa no solo conozcan el plan de compliance y la normativa detrás del mismo, sino también cómo evitar los incumplimientos legales y reaccionar ante uno.

Uno de los principales objetivos de la empresa a la hora de formar a sus empleados y directivos en el conocimiento y contenido de los programas de compliance consiste en evitar que se cometan actos delictivos en el seno de ésta, pero también, en el caso de producirse, reducir la gravedad de la pena y evitar que la sociedad sea hallada responsable penal por un juez. El programa de formación, así como su oportuna ejecución, es responsabilidad del equipo de compliance bajo los términos del artículo 31 bis CP.

La Circular 1/2006 de la Fiscalía General del Estado y el Tribunal Supremo han recogido de forma expresa la necesidad de que la formación sea parte esencial de los planes de compliance y su éxito como medida de prevención de riesgos penales. Es a través de la formación como normalmente se comunican las normas y procedimientos de los programas de compliance a los empleados y directivos, además de proporcionando copias de dicho plan y documentos relacionados que sean necesarios.

Entre los requisitos que estos programas de formación deben cumplir están:

- Formación adaptada a cada área o departamento de la empresa, con la finalidad de que el trabajador conozca las obligaciones y riesgos de su puesto de trabajo.
- Formación inicial con la creación de la relación laboral y continuada con la evolución del plan de compliance, los riesgos o los conflictos.
- Evaluación de la formación, midiendo su eficacia o los conocimientos adquiridos por los empleados.
- Registro de la formación, tanto de la educación proporcionada como que los empleados han recibido la misma, y la evaluación de ésta.

Junto con la formación, se deberá garantizar la comunicación a los empleados de los distintos elementos del plan de compliance, proporcionando copias de los documentos según sea apropiado. Esta comunicación, así como la formación, podrá realizarse en cualquier momento, aunque sería recomendable que proporcionara la documentación en el momento de la incorporación del trabajador, como parte del *welcome pack*, y de forma periódica a lo largo de la relación laboral.

Se deberá registrar la participación de los empleados en los cursos de formación en materias de compliance, así como que han recibido la documentación pertinente a este respecto. Para ello, se podrá utilizar un modelo como el siguiente:

ACUSE DE RECIBO

El abajo firmante, ……, con DNI .....

DECLARO

- Que he recibido una copia del Manual de Riesgos así como del Código de Conducta de la empresa, que lo he leído y entendido.
- Que he recibido formación pertinente en prevención de riesgos penales.
- Que me comprometo a respetar y a cumplir todas sus disposiciones.
- Que me comprometo a comunicar cualquier acción contraria al Código de la que tenga conocimiento a través del canal de denuncias.
- Conozco las medidas disciplinarias derivadas del incumplir el Código.

La participación en los planes de formación acerca del plan y otras materias de compliance podrá registrarse a través de hojas de firmas o manteniendo un registro de los certificados de finalización de la acción formativa si se opta por externalizar esta función.

Establecimiento de un registro de evidencias.

La posible exoneración de la empresa, de acuerdo con el artículo 31 bis CP, pasa por la adopción y ejecución eficaz de un modelo de prevención de riesgos penales, así como la supervisión del funcionamiento del mismo mediante la asignación de estas tareas a un órgano especializado. Ahondando en los requisitos necesarios para que la empresa sea absuelta de un ilícito penal, será necesario contar con la acreditación necesaria de la existencia del plan de compliance, siendo responsabilidad de la persona jurídica aportar evidencias de su existencia, implantación y difusión. Se deberá, por tanto, asegurarse que existen evidencias documentales suficientes y adecuadas de:

- La existencia del modelo.
- La atribución de su supervisión a un órgano con poderes autónomos (órgano de compliance).
- Su difusión y promoción entre empleados, directivos y agentes de la empresa.

La acreditación de la existencia del modelo solo será satisfecha con la existencia, efectividad y continuidad en el tiempo del conjunto de medidas de prevención de riesgos penales. Es decir, será necesario que la documentación cubra la integridad del plan de compliance, demostrando que se ha realizado la evaluación de los riesgos, establecido el canal de denuncias, formación y difusión, evaluación y modificación del modelo, etc., para demostrar la solvencia del modelo.

Para el correcto desarrollo del registro de evidencias del plan de compliance, se podrá seguir el procedimiento establecido en la norma ISO 19600:

- Documentar y controlar toda la información necesaria para la eficacia del programa, haciéndola disponible y protegiéndola adecuadamente.
- Mantener los registros exactos, actualizados y protegidos de las actividades del programa de compliance.
- Utilizar herramientas de captura, recogida y custodia de evidencias, contenido y fecha de los controles, para probar la existencia y eficacia de los controles establecidos en el plan de prevención de riesgos penales y acreditar su contenido y fecha de implantación.
- Conservar el repositorio con todas las evidencias, debidamente ordenadas.

Por otro lado, habrá que conservar la documentación generada por otros procesos relacionados con el plan de compliance: formación, canal de denuncias, etc., para la acreditación ante sede judicial, o cualquier otro actor que lo requiera, de la eficacia y funcionamiento de las herramientas puestas en marcha. Del mismo modo, se deberá contar con la información obtenida de la propia ejecución del plan, principalmente para poder evaluar su funcionamiento.

Habrá que estar atento también a qué información se pone a disposición de los interesados. No cabe duda de que, tomando parte en una auditoría, es del interés de la empresa proporcionar toda la información y detalle que le sea posible. Lo mismo sucedería en caso de requerimiento judicial cuando la empresa desee probar que ha puesto en marcha los mecanismos y herramientas adecuados para prevenir la comisión de delitos en su seno.

Establecimiento de un programa de auditoría y verificación periódica del plan.

El artículo 31 bis CP recoge la necesidad de la verificación periódica del modelo de prevención de riesgos penales, práctica que deberá reflejarse en la documentación del mismo plan. La regulación legal deja un gran margen interpretativo y libertad a la hora de decidir el tipo de revisiones a llevar a cabo por la empresa, por lo que queda a criterio de ésta escoger las revisiones que más se adecuen a las necesidades de la organización y asegurar su consistencia a lo largo del tiempo.

Más allá de la necesaria revisión periódica del plan de compliance, una verificación de este puede ser resultado, sobre todo, del requisito legal de mantener su utilidad frente a la naturaleza cambiante de las empresas y el entorno en el que operan. Así, una revisión del plan de compliance puede ser necesaria por circunstancias internas, como la modificación del accionariado o el equipo de gestión de la empresa, o externas, como un cambio en el marco legal. Del mismo modo, las revisiones pueden ser programadas, cuando se realizan de forma periódica y sin que concurran circunstancias especiales que requiera de su ejecución, o sobrevenidas, cuando se producen como resultado de una situación especial. El Código Penal solo hace referencia a la obligatoriedad de este último tipo de revisiones, aunque, siguiendo las buenas prácticas recomendadas, no se recomienda reducir la actividad verificadora a estas ocasiones únicamente. Otros casos en los que la revisión del modelo será necesario son la inclusión de nuevas actividades de control, la modificación de los controles o evidencias de estos o el cambio de los responsables del control.

En cuanto al órgano encargado de estas verificaciones, nada se indica en la legislación vigente. Se podrá dejar la verificación del modelo a un órgano interno de la organización, tal y como permite la legislación española en temas de auditoría, por ejemplo; o se podrá confiar en un encargado externo, que, en casos por su tamaño o naturaleza, será la opción esperada para aquellas organizaciones que deseen mostrar su sensibilización en materia de compliance. En el caso de que se confíe la revisión del modelo de compliance al órgano de compliance de la empresa, posibilidad aceptable, se podría ver afectado por falta de independencia al estar evaluando su propio trabajo de diseño y ejecución de políticas, procedimientos y controles, por lo que se deberá contemplar esta posibilidad en la eficacia de la evaluación y el compromiso de la organización con el cumplimiento normativo.

Se deberá mantener un registro con la documentación relevante sobre estas verificaciones, tanto periódicas como las que resulten de una situación sobrevenida. Estos documentos tienen la finalidad de acreditar la ejecución de las verificaciones, y por tanto los preceptos del artículo 31 bis CP, y permitir a la organización evaluar su evolución en materia de prevención de riesgos penales.

En cuanto a los tipos de verificaciones mínimas a realizar, podemos considerar tres:

- Valoración de la adecuada implementación del modelo, contrastando que su diseño sea el adecuado para prevenir, detectar y mitigar los riesgos sobre los que se proyectan. En resumen, se trataría de comprobar que el modelo implementado no se limita a establecer un marco de actuación genérico, sino que se adecua a las necesidades de la organización y ha sido desarrollado conforme a los objetivos que se intentan alcanzar.
- Valoración del diseño general del modelo, que consistiría en analizarlo para contrastar si la documentación que lo representa recoge los elementos esenciales requeridos del plan de prevención de riesgos penales. En el caso español, podría basarse en los requisitos exigidos por el Código Penal, aunque la organización podría ir un paso más lejos y optar por contrastar su modelo de compliance con un marco de referencia completo (norma ISO 9600, por ejemplo) e incluso proceder a su certificación.
- Verificaciones de su eficacia a través de pruebas que permitan valorar su aplicación real y la consistencia del modelo, así como su adecuación a la organización. Estas pruebas de fondo se conocen como "testeos", y se realizan con la intención de verificar la aplicación práctica de lo que se ha plasmado en los documentos del plan de compliance. En cuanto a la metodología, se podrá seguir la utilizada para auditorías, pudiendo variar de la misma forma la extensión y finalidades de la verificación: procedimientos acordados para evaluar el funcionamiento de ciertos controles; aseguramiento limitado, que verifique los controles aplicables de un muestreo restringido; o aseguramiento razonable, con un muestreo más amplio.

Por último, el Departamento de Justicia de los Estados Unidos de América (DoJ) ha publicado una guía a utilizar por sus fiscales a la hora de evaluar la idoneidad de los programas de compliance, y que las empresas pueden seguir en sus verificaciones ante la falta de mayor detalle en las normas de compliance españolas. Entre los elementos que analizan y que se tendrán en cuenta para la exoneración de la empresa encontramos:

- La conducta que merece reproche penal: sus causas, las indicaciones de su existencia y las medidas adoptadas para ponerle fin.
- La actuación de los directivos frente a la conducta penal: su implicación en la prevención de riesgos penales y su supervisión de este.
- Autonomía y recursos del equipo de compliance: el papel de los responsables de la prevención de delitos en la empresa, su importancia dentro de la organización, su formación y experiencia (y, en general, idoneidad para llevar a cabo su trabajo), su autonomía y comunicación con la administración de la empresa, su financiación y recursos para realizar su labor y la externalización de la función de compliance, si fuera aplicable.
- Políticas y procedimientos: diseño y comunicación plan de compliance y políticas de prevención de riesgos penales de la empresa, papel de actores clave dentro de la empresa, integración de las políticas en la empresa, controles establecidos y posible certificación del modelo.
- Evaluación del riesgo (mapeo de riesgos penales): metodología seguida para la evaluación, información compilada y análisis de los riesgos.
- Formación y comunicación: formación dada a los empleados y directivos; su contenido, forma y efectividad; materiales de guía puestos a disposición de los empleados y la comunicación interna de la empresa respecto a casos en los que se detecte la comisión de un ilícito penal.
- Investigación y sistemas de denuncias: efectividad del sistema de denuncias, realización de investigaciones adecuadas por personal cualificado, e implantación de modificaciones o mejoras tras los hallazgos de las investigaciones.

- Medidas disciplinarias e incentivos para el cumplimiento del plan de compliance: qué medidas disciplinarias se han tomado y desde qué niveles ante incumplimientos del plan, la participación de recursos humanos, la aplicación consistente del sistema disciplinario, y el sistema de incentivos para que los empleados y directivos respeten y cumplan el plan de compliance.
- Mejoras, testeos y revisión del modelo de compliance: realización de auditorías internas, aprovechamiento de sus resultados, revisión de los controles implantados, y puesta al día de los riesgos y diseño del plan ante los cambios o hallazgos realizados por investigaciones.
- Aplicación a su relación con terceros: integración de los riesgos provenientes de agentes externos en el plan de compliance, establecimiento de los controles oportunos, y actuación ante los riesgos identificados en sus relaciones con terceros.
- Fusiones y adquisiciones: realización de los procesos de diligencia debida, integración del plan de compliance en la fusión o adquisición, e investigación y solución de los problemas de compliance detectados durante el proceso de adquisición.

Certificación del plan de compliance.

Aunque no es un paso obligatorio, y debe ser realizado por una entidad externa a la organización, la certificación del plan de compliance se presenta como una opción para la empresa que quiere probar la eficacia e idoneidad de su plan de prevención de riesgos penales. Tal y como planteamos con la implementación del plan de compliance, la certificación es aplicable a todas las empresas sin importar tamaño, actividad o sector, variando únicamente los diferentes elementos y contenidos de la certificación en función de los riesgos y las circunstancias de la empresa: mercados en los que opera, sector, complejidad de las transacciones, etc.

La UNE 19601:2017, emitida por el organismo de normalización AENOR, es la norma técnica normalmente seguida a la hora de certificar el plan de compliance, dado que permite la implementación de sistemas de gestión de compliance penal en concordancia con los requisitos de las leyes españolas e internacionales. Esta norma tiene como eje central la gestión de riesgos de delitos penales y ofrece con mayor detalle los principios de un modelo de gestión sólido y cogerente con el funcionamiento de la empresa, además de incorporar las mejores prácticas internacionales en materia de cumplimiento normativo. Entre los requisitos desarrollados en la norma encontramos que las empresas deben:

- Identificar, analizar y evaluar los riesgos penales (mapa de riesgos penales).
- Disponer de recursos financieros, adecuados y suficientes para conseguir los objetivos.
- Usar procedimientos para la puesta en conocimiento de las conductas potencialmente delictivas (canal de denuncias).
- Adoptar acciones disciplinarias si se producen incumplimientos de los elementos del sistema de gestión.
- Supervisar el sistema por parte del órgano de compliance penal (evaluación).
- Crear una cultura en la que se integren la política y el sistema de gestión de compliance.

Por otro lado, si la empresa decide llevar a cabo la certificación, puede aprovecharse de una serie de beneficios:

- Demuestra el compromiso de la organización con el compliance.
- Proporciona una auditoría con resultados totalmente independientes, asegurando a la empresa el cumplimiento de los requisitos legales de su plan de compliance.
- Elemento valorado positivamente por los diferentes órganos regulatorios y judiciales ante los que se debería demostrar las medidas de prevención de riesgos penales adecuados para la exoneración de la empresa, evitando o minimizando las sanciones.
- Consolida la cultura ética y de cumplimiento en la organización, reforzando las posibilidades del éxito y sostenibilidad del plan.
- Protege la integridad de la empresa al contribuir a la difusión de un comportamiento socialmente responsable.
- Mejora la imagen y relaciones de la empresa frente a usuarios, proveedores, socios, administraciones públicas, etc., al garantizar la eficacia del plan de compliance.

Aunque la certificación comporta una serie de ventajas claves para la empresa en materia de compliance, no conlleva por si misma la exoneración automática de la empresa en caso de ser juzgada por un delito cometido en su seno. Por otro lado, la certificación si demostrará el compromiso de la empresa con el cumplimiento normativo y la puesta en marcha de las medidas adecuadas para evitar la comisión de delitos, favoreciendo dicha exoneración o la minimización de las penas para la organización.

La certificación se llevará a cabo a través de una auditoría de certificación, que es una auditoría externa, independiente y transparente realizada por el agente para evaluar el plan de compliance de la empresa, así como el grado de madurez y la adecuación del plan. Antes de la realización de esta auditoría, la empresa podrá también realizar preauditorías, con el objetivo de conocer su situación para afrontar un proceso de certificación.

Por último, y a la hora de elegir a la organización o empresa a la que confiar la certificación del plan de compliance, cabe recordar que la Entidad Nacional de Acreditación (ENAC) ha recomendado acudir a empresas que cuenten con su sello para garantizar la fiabilidad de su examen.