

Información Pública

PROYECTO DE NORMA UNE

PNE 19601

Sistemas de gestión de compliance penal. Requisitos con orientación para su uso.

Management system for criminal compliance. Requirements with guidance for use.

CORRESPONDENCIA:

MODIFICA O REVIS A:

FECHA LÍMITE DE
RECEPCIÓN DE COMENTARIOS: 2017-03-20

UNE no se hace responsable de la utilización de este documento, ya que está sujeto a posibles modificaciones hasta su aprobación definitiva. Las observaciones deben dirigirse a:

normalizacion@une.org

Prólogo

Esta Norma UNE 19601 ha sido elaborada por el Subcomité Técnico CTN 307 SC1 *Sistemas de gestión del cumplimiento y sistemas de gestión anticorrupción*.

En esta norma se utilizan las siguientes formas verbales:

- "debe" indica un requisito;
- "debería" indica una recomendación;
- "puede" indica permiso, una posibilidad o una capacidad.

La información indicada como "NOTA" se presenta a modo de orientación para la comprensión o clarificación del requisito correspondiente.

Documento de Trabajo

0 Introducción

En el contexto en el que se desarrollan las actividades de las organizaciones (3.20) mínimamente complejas, pueden cometerse delitos en su beneficio, especialmente aquellos vinculados con la actividad económica. Las organizaciones (3.20) respetuosas de la legalidad pueden, mediante el establecimiento de una adecuada cultura (3.8) organizativa del cumplimiento, influir significativamente para evitar o, al menos, reducir el riesgo (3.28) de comisión de dichas conductas. El establecimiento de esta cultura (3.8) de cumplimiento se ha venido asociando cada vez en mayor medida a la responsabilidad social corporativa, permitiendo distinguir a los "buenos ciudadanos corporativos" de las organizaciones de aquellos (3.20) que no respetan en idéntica medida la legalidad.

La comisión de comportamientos delictivos en el desarrollo de las actividades propias de las organizaciones (3.20) no sólo genera ventajas anticompetitivas en relación con aquellos operadores respetuosos con el cumplimiento de la legalidad, sino que erosiona los fundamentos del buen gobierno corporativo y pone en riesgo (3.28) bienes jurídicos especialmente protegidos. Por todo ello, se ha considerado que consentir, posibilitar o incentivar el desarrollo de conductas punibles en el seno de las citadas organizaciones (3.20) constituye un delito propio de las organizaciones (3.20) que afecta a la actividad económica y perjudican al conjunto de la Sociedad.

Conscientes de esta realidad, y al igual que ha sucedido en otros ordenamientos, el legislador introdujo en España un régimen de sanciones penales para organizaciones (3.20), que desarrolló con más detalle para el caso de las personas jurídicas. Así, la Ley Orgánica 5/2010 por la que se modificó la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal no sólo estableció los delitos aplicables a las personas jurídicas y sus requisitos, sino que hizo referencia al establecimiento de medidas de vigilancia y control para su prevención y detección como fundamento expreso de una atenuación de su responsabilidad penal. A pesar de su novedad, dicho régimen fue reformado por la Ley Orgánica 1/2015, de 30 de marzo, que modificó nuevamente la citada Ley Orgánica 10/1995 del Código Penal. Este cambio legislativo vino a concretar en mayor medida el régimen de responsabilidad penal de las personas jurídicas en España, detallando los requisitos para disponer de sistemas de gestión y control que permitan a la persona jurídica acreditar su diligencia en el ámbito de la prevención y detección penal y, consiguientemente, ser exoneradas de responsabilidad criminal.

Aunque el contenido de la nueva regulación ha consolidado la necesidad de disponer de sistemas de gestión y control aplicados al ámbito de la prevención y detección penal, esta regulación constituye un marco de interpretación susceptible de ser desarrollado para disponer de sistemas eficaces y alineados con las buenas prácticas que vienen acordándose a nivel internacional. En este sentido, esta norma UNE viene a establecer un marco de referencia completo que no sólo permite disponer de sistemas de gestión de *compliance* penal (3.31) alineados con las exigencias del Código Penal español, sino completarlos con los estándares internacionales en materia de *compliance* que contribuyen a cincelar sus contenidos e incrementar su eficacia. Bajo tal premisa, esta norma UNE facilita diseñar o evaluar sistemas de gestión de *compliance* penal (3.31), que permitan generar o mejorar una adecuada cultura (3.8) organizativa sensible a la prevención y detección penal y opuesta a las malas praxis que toleran o amparan conductas ilícitas en el seno de las personas jurídicas.

Dado que en los estándares internacionales en materia de *compliance* se hace referencia al concepto de organización, a lo largo de esta norma UNE se hará referencia al concepto de organización y no de persona jurídica permitiendo así la aplicación de la misma tanto a personas jurídicas como entidades carentes de personalidad jurídica. Ello no sólo es relevante a los efectos del artículo 129 del Código Penal español, sino a los efectos de poder incluir bajo el sistema de gestión de *compliance* penal (3.31) de una organización a varias personas jurídicas pertenecientes a un mismo grupo de empresas.

A los efectos anteriores, una organización (3.20) sensibilizada con tales propósitos deberá disponer de un sistema de gestión que le permita alcanzar sus objetivos y su compromiso de integridad. La política, los objetivos, los procesos (3.26) y los procedimientos (3.25) conforman el núcleo de un sistema de gestión para la prevención, detección y gestión de riesgos penales (3.29) proyectado en el ámbito de la organización (3.20), evitando así posibles daños económicos, reputacionales o de otra índole.

Esta norma UNE facilita la implementación de sistemas de gestión de *compliance* penal (3.31), no sólo respetuosos con las exigencias legales españolas, sino también dirigidos a cumplir las expectativas que normalmente se depositan en las organizaciones (3.20) que operan en los mercados internacionales. En este sentido, su contenido recoge las exigencias de nuestro Código Penal bajo la estructura de alto nivel desarrollada por ISO para mejorar el alineamiento entre sus normas internacionales para sistemas de gestión e incorpora buenas prácticas ya reguladas en la Norma UNE-ISO 19600 *Sistemas de gestión de compliance. Directrices* y en la reciente Norma UNE-ISO 37001 *Sistemas de gestión antisoborno. Requisitos con orientación para su uso*. Puede utilizarse de manera conjunta con esas normas, así como con la Norma UNE-ISO 31000 *Gestión del riesgo. Principios y directrices* y otras *normas internacionales sobre modelos de gestión*.

La presente norma UNE puede aplicarse a organizaciones (3.20) de todos los tamaños y actividades, tanto del sector privado como público, con o sin ánimo de lucro. La exposición a los riesgos penales (3.29) variará según diferentes circunstancias, como su tamaño, el sector de actividad o las ubicaciones donde operen, así como por la diversidad y complejidad de sus transacciones. Sobre esta base, esta norma UNE define una serie de requisitos a desarrollar de manera proporcional a tales circunstancias para diseñar y evaluar sistemas para la prevención, detección y gestión de riesgos penales, adaptados y razonables a la realidad de cada organización (3.20).

A los efectos de facilitar su aplicación, también se incorporan notas, ejemplos, así como un conjunto de anexos que proporcionan directrices adicionales para interpretar y aplicar correctamente sus contenidos.

Esta norma UNE queda abierta, además a su posible aplicación y utilización en otros países donde la legislación contemple la responsabilidad penal o administrativo-sancionadora de las personas jurídicas, o de otro tipo de organizaciones (3.20).

Que una organización (3.20) cumpla con los requisitos de esta norma UNE no asegura completamente que no se hayan producido en su seno delitos, ni que no vayan a producirse en el futuro. Por consiguiente, esta norma UNE no brinda una garantía absoluta de eliminación del riesgo (3.28) de comisión de delitos que afronta una organización (3.20).

En el caso de la legislación española, el cumplimiento de esta norma UNE no asegura la exoneración o atenuación automática de la responsabilidad penal de la persona jurídica. No obstante, esta norma ayuda a las organizaciones (3.20) a desarrollar sistemas de gestión de *compliance* penal (3.31) con contenidos razonables para prevenir, detectar y gestionar conductas ilícitas generando así la cultura (3.8) organizativa del cumplimiento de la legalidad que pueda fundamentar, en última instancia, la exoneración de su responsabilidad. De igual modo, su contenido también podría aspirar a servir de referencia para los tribunales de justicia y demás operadores jurídicos a la hora de facilitarles el establecimiento de criterios para valorar el cumplimiento por parte de las personas jurídicas u otras organizaciones (3.20) de las exigencias previstas en la legislación penal.

El control de riesgos (3.28) y la supervisión de su gestión son elementos fundamentales del gobierno corporativo. El sistema de gestión propuesto en esta norma UNE se centra en la prevención y gestión del riesgo penal (3.29). Así, siguiendo el planteamiento de la legislación societaria española vigente en el momento de publicación de la norma, se considera que la fijación de la política de *compliance* penal (3.24) es una competencia indelegable del órgano de gobierno (3.22), en relación con las facultades indelegables del Consejo de Administración - así como, en general, la supervisión del sistema de gestión. Por otro lado, la supervisión de la eficacia del sistema de gestión es competencia del órgano de cumplimiento penal u homólogo legalmente equivalente - de nuevo de conformidad con la legislación ya mencionada, en relación con las funciones asignadas a la Comisión de Auditoría.

En el anexo A se establece la correlación de los requisitos establecidos en el artículo 31 bis del Código Penal vigente en el momento de la publicación de la norma respecto de las especificaciones contenidas en la misma.

Ha de advertirse, sin embargo, que, según el ordenamiento penal español, la implementación de un sistema de gestión acorde con esta norma UNE no agota las posibilidades de defensa y consiguiente exoneración de la persona jurídica en cuyo seno se haya producido la comisión del correspondiente delito.

Lo verdaderamente trascendente a efectos de esa responsabilidad será el que la persona jurídica de referencia pueda acreditar debidamente un comportamiento, en esta materia de prevención delictiva, que evidencie su cultura (3.8) organizativa de respeto a la norma que le atribuye obligaciones de colaboración con las Autoridades en la evitación de la comisión, en su seno, de delitos por parte de las personas físicas que la integran, objetivo que, obviamente, es también el que, con carácter esencial, se persigue en el contenido de la presente norma UNE.

Las declaraciones de conformidad (3.7) con esta norma UNE no son aceptables a menos que todos los requisitos estén incorporados en el sistema de gestión de *compliance* penal (3.31) de la organización (3.20) y se cumplan sin exclusiones.

1 Objeto y campo de aplicación

Esta norma UNE establece los requisitos y facilita las directrices para adoptar, implementar, mantener y mejorar continuamente (3.15) políticas de *compliance* penal (3.24) y el resto de los elementos de un sistema de gestión de *compliance* penal (3.31) en las organizaciones (3.20).

NOTA Una política de *compliance* penal (3.24) puede establecerse de manera independiente, o integrada en una política de *compliance* de mayor alcance, esto es, no limitada a la prevención penal. Análogamente, un sistema de gestión de *compliance* penal (3.31) puede establecerse de manera independiente, o integrado en un modelo de *compliance* de mayor alcance, esto es, no limitado a la prevención penal.

La norma es particularmente aplicable en el contexto de sistemas de gestión y control sobre riesgos penales (3.29), estableciendo requisitos (3.27) y directrices para disponer de modelos alineados con lo que exige la legislación penal española a los sistemas de control y gestión para la prevención y detección de delitos, tanto en su forma como en su fondo.

Sin perjuicio de lo anterior, esta norma UNE puede también ser de utilidad para establecer sistemas de control y gestión para la prevención y detección de delitos cometidos en el contexto de las actividades empresariales, aunque no comporten la responsabilidad penal de la persona jurídica en España ni concurren en organizaciones españolas (3.20).

Esta norma UNE es aplicable a:

- a) Cualquier tipo de organización (3.20), con independencia de su tipo, tamaño, naturaleza o actividad. Se proyecta sobre riesgos penales (3.29) en los siguientes contextos: sector privado, sector público, con o sin ánimo de lucro.
- b) Actividades desarrolladas, tanto por los miembros de la organización (3.17), como por socios de negocio (3.32) que actúen, tanto unos como otros, siguiendo instrucciones de la organización (3.20), representándola o en su beneficio.
- c) Conductas desarrolladas de manera directa como indirecta.

Esta norma UNE no se proyecta específicamente sobre otros riesgos (3.28) que hallándose relacionados con la esfera penal o suponiendo incumplimientos de la normativa, no guardan relación directa con ilícitos penales cometidos con el objetivo de beneficiar a la persona jurídica, como pueda ser el riesgo (3.28) de fraude en el seno de la organización (3.20). No obstante, la organización (3.20) puede decidir extender el alcance, tanto de la política de *compliance* penal (3.24), como del sistema de gestión de *compliance* penal (3.31) a estas esferas, en caso de que le resulte de utilidad.

Estos requisitos (3.27) deben aplicarse de manera proporcional a cada supuesto según las circunstancias que se especifican en los apartados 4.1, 4.2 y 6.2 de esta norma UNE.

Si la totalidad o parte de los requisitos (3.27) establecidos en esta norma UNE entrase en conflicto o estuviese prohibida por alguna disposición legal o criterio jurisprudencial, la organización (3.20) no estará obligada con el mismo o su parte afectada.

2 Normas para consulta

No se identifican normas para consulta.

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones (en orden alfabético) siguientes:

3.1 acción correctiva:

Acción para eliminar la causa de una no conformidad (3.18) y prevenir que se reproduzca.

3.2 alta dirección:

Persona o grupo de personas que dirigen y controlan una organización (3.20) al más alto nivel.

NOTA 1 La alta dirección (3.2) tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización (3.20).

NOTA 2 Si el alcance del sistema de gestión (3.31) comprende sólo una parte de una organización (3.20), entonces alta dirección (3.2) se refiere a quienes dirigen y controlan esa parte de la organización (3.20).

NOTA 3 Las organizaciones (3.20) están estructuradas bajo diferentes formas jurídicas, dependiendo del marco legal al que estén sujetas. Adicionalmente, las organizaciones (3.20) pueden estar estructuradas de diferentes maneras a causa de su tamaño, sector de actividad, etc. Algunas organizaciones (3.20) pueden disponer tanto de un órgano de gobierno (3.22), como de un órgano ejecutivo con atribuciones delegadas, o incluso pueden no tener las responsabilidades divididas sistemáticamente en diferentes órganos. Estas variaciones, tanto con relación a la organización (3.20) y las responsabilidades, se deberían contemplar cuando se apliquen los requerimientos del apartado 5 de esta norma UNE.

3.3 auditoría:

Proceso (3.26) sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1 Una auditoría interna la realiza la propia organización (3.20) o una parte externa en su nombre.

NOTA 2 Una auditoría puede ser combinada (combinando dos o más disciplinas).

NOTA 3 La independencia se puede demostrar por la ausencia de responsabilidad con relación a la actividad que se audita, o ausencia de sesgo y conflicto de intereses (3.6).

NOTA 4 La evidencia de auditoría consiste en registros, declaraciones de hechos, y demás información pertinente a los criterios de auditoría, que son verificables; los "criterios de auditoría" son el conjunto de políticas, procedimientos (3.25) o requisitos (3.27) usados como referencia, frente a los cuales se compara la evidencia de auditoría.

3.4 competencia:

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

3.5 *compliance* penal:

Cumplimiento de los requisitos (3.27).

3.6 conflicto de intereses:

Situación en la que intereses de negocios externos, financieros, familiares, políticos o personales podrían interferir en el juicio de los miembros de la organización (3.17) cuando llevan a cabo sus tareas en la organización (3.20).

3.7 conformidad:

Cumplimiento de un requisito (3.27).

3.8 cultura:

Valores, ética y creencias que existen en una organización (3.20) y que interactúan con las estructuras y sistemas de control de la organización (3.20) para producir normas de comportamiento que conducen a obtener los objetivos (3.19) derivados de la aplicación de esta norma UNE.

NOTA Los elementos fundamentales de la cultura (3.8) de *compliance* se encuentran referidos en el apartado 7.1.

3.9 desempeño:

Resultado medible.

NOTA 1 El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

NOTA 2 El desempeño se puede relacionar con la gestión de actividades, procesos (3.26), productos (incluidos servicios), sistemas u organizaciones (3.20).

3.10 diligencia debida:

Proceso (3.26) operativo que pretende obtener y evaluar la información para contribuir a la evaluación del riesgo penal (3.29).

3.11 eficacia:

Medida en la que se realizan las actividades planeadas y se obtienen los resultados previstos.

3.12 externalización:

Acuerdo mediante el cual una organización (3.20) externa realiza una función o proceso (3.26) de la organización (3.20).

NOTA Una organización (3.20) externa está fuera del alcance del sistema de gestión (3.31) aunque la función o proceso externalizado forme parte del alcance.

3.13 funcionario público:

Cualquier persona que tenga un cargo legislativo, administrativo o judicial, ya sea designado por sucesión o electo, o cualquier persona que ejerza una función pública, incluso para un organismo público o para una empresa pública, o cualquier funcionario o agente de una organización (3.20) nacional o internacional pública o cualquier candidato a funcionario público.

3.14 información documentada:

Información que una organización (3.20) tiene que mantener y controlar, y el medio en el que está contenida.

NOTA 1 La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2 La información documentada puede hacer referencia a:

- el sistema de gestión de *compliance* penal (3.31), incluidos los procesos (3.26) relacionados,
- la información generada para que la organización (3.20) opere (documentación),
- la evidencia de los resultados alcanzados (registros).

3.15 medición:

Proceso (3.26) para determinar un valor.

3.16 mejora continua:

Actividad o proceso (3.26) recurrente para mejorar el desempeño (3.9).

3.17 miembros de la organización:

Los integrantes del órgano de gobierno (3.22), directivos, empleados, trabajadores o empleados temporales o bajo convenio de colaboración, y voluntarios de una organización (3.20) y el resto de personas bajo subordinación jerárquica de cualquiera de los anteriores.

NOTA Los riesgos penales (3.29) pueden afectar a personas que, sin mantener una relación jurídico laboral con la organización (3.20), desarrollan de sus actividades de manera estable en su seno.

3.18 no conformidad:

Incumplimiento de un requisito (3.27).

3.19 objetivo de *compliance* penal:

Resultado a lograr.

NOTA 1 Los objetivos de *compliance* penal hacen referencia a la tolerancia cero de la organización (3.20) respecto de los riesgos penales (3.29), así como al establecimiento de medidas tendentes a su prevención, detección y gestión tempranas.

NOTA 2 Un objetivo puede ser estratégico, táctico u operativo.

NOTA 3 Los objetivos pueden referirse a diferentes disciplinas (tales como financieras, de salud y seguridad ambientales) y se pueden aplicar en diferentes niveles (tales como estratégicos, para toda la organización (3.20), para proyectos, productos y procesos (3.26).

NOTA 4 Un objetivo se puede expresar de diversas maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de *compliance*, o mediante el uso de términos con un significado similar (por ejemplo, finalidad o meta).

NOTA 5 En el contexto de sistemas de políticas de *compliance* penal (3.24) y sistemas de gestión de *compliance* penal (3.31) la organización (3.20) establece sus objetivos con la finalidad de lograr resultados específicos de manera eficaz (3.11).

3.20 organización:

Persona o grupo de personas que tienen sus propias funciones, con responsabilidades, autoridades y relaciones para el logro de sus objetivos.

NOTA 1 El concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización de caridad o institución, o una parte o combinación de éstas, ya estén constituidas o no, tanto públicas como privadas, con ánimo de lucro o sin él.

NOTA 2 Para organizaciones que tengan más de una unidad operativa, una sola unidad puede ser definida como una organización.

3.21 órgano de *compliance* penal:

Órgano de la organización (3.20) dotado de poderes autónomos de iniciativa y control al que se confía la responsabilidad de supervisar el funcionamiento y observancia del sistema de gestión de *compliance* penal.

NOTA El órgano de *compliance* penal, de naturaleza colegiada o unipersonal, puede ser:

- 1) Órgano de la organización (3.20) que tenga legalmente encomendada la función de supervisar la eficacia (3.11) de los controles internos de misma. En el caso de sociedades cotizadas, sociedades emisoras de valores y sociedades de interés público, es requisito (3.27) legal la creación de una Comisión de Auditoría con la función de supervisar los controles internos.
- 2) Órgano o unidad de la organización (3.20) *ad hoc* al que el órgano de administración le otorga poderes de iniciativa y control.
- 3) En el caso de las personas jurídicas de reducidas dimensiones el órgano de *compliance* penal puede ser el propio órgano de gobierno (3.22).

3.22 órgano de gobierno:

Grupo u organismo que tiene la responsabilidad y autoridad fundamental de las actividades, la gobernabilidad y las políticas una organización (3.20) y al que la alta dirección (3.2) informa y le rinde cuentas.

NOTA 1 No todas las organizaciones (3.20), especialmente las pequeñas, tendrán un órgano de gobierno independiente de la alta dirección (3.2).

NOTA 2 Un órgano de gobierno puede incluir pero no está limitado a una Junta directiva, comités de la junta, consejo de vigilancia, administradores y supervisores.

3.23 parte interesada:

Persona u organización (3.20) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

NOTA 1 Se aplica el concepto de parte interesada como equivalente en español a los términos *stakeholder* o *interested party*, de uso frecuente en textos internacionales.

NOTA 2 Las partes interesadas pueden ser externas o internas en una organización (3.20).

3.24 política de *compliance* penal:

Voluntad de una organización (3.20), según las expresa formalmente su alta dirección (3.2) o su órgano de gobierno (3.22), en relación con sus objetivos de *compliance* penal (3.19).

3.25 procedimiento:

Forma específica de llevar a cabo una actividad o proceso (3.26)

3.26 proceso:

Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

3.27 requisito:

Exigencia prevista y obligatoria.

NOTA 1 A los efectos de esta norma UNE, estas exigencias hacen referencia a lo contenido en las leyes penales y normativa complementaria que afectan a la organización (3.20).

NOTA 2 También quedan incluidas las exigencias derivadas de la política de *compliance* penal (3.24) y del sistema que le da soporte.

NOTA 3 Un requisito especificado es el que está declarado, por ejemplo, en el Código Penal, en las normas relacionadas con él o en la información documentada (3.14).

3.28 riesgo:

Efecto de la incertidumbre en los objetivos.

NOTA 1 Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

NOTA 2 Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, la probabilidad de que acontezca o sus consecuencias.

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a eventos potenciales y a consecuencias potenciales o a una combinación de éstos.

NOTA 4 Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la "probabilidad" asociada de que ocurra.

3.29 riesgo penal:

Riesgo (3.28) relacionado con el desarrollo de conductas que pudieran ser constitutivas de delito según el régimen de responsabilidad penal de las personas jurídicas establecido en el Código Penal español o, en caso de entidades carentes de personalidad jurídica, con el régimen de consecuencias accesorias establecido en el mismo texto legal.

NOTA 1 Para aquellas organizaciones (3.20) que así lo hayan decidido, el riesgo (3.28) también podrá incluir otras conductas que no supongan la responsabilidad penal de las personas jurídicas, ni la imposición de consecuencias accesorias.

NOTA 2 En el supuesto de aplicación de esta norma UNE a organizaciones (3.20) extranjeras o españolas con actividad en el extranjero, el riesgo (3.28) se refiere al desarrollo de conductas que sean constitutivas de delito, según el régimen de responsabilidad penal de las personas jurídicas establecida en la legislación local en la que opera.

3.30 seguimiento:

Determinación del estado de un sistema, un proceso (3.26), procedimiento (3.25) o una actividad.

NOTA 1 Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

NOTA 2 El seguimiento (3.30) no es una actividad que se realice una sola vez, sino un proceso (3.26) en el que se observa una situación de forma regular o continua.

3.31 sistema de gestión de *compliance* penal:

Conjunto de elementos de una organización (3.20) interrelacionados o que interactúan para concretar y medir (3.15) el nivel de consecución de objetivos (3.19) en materia de *compliance* penal, así como las políticas (3.24), procesos (3.26) y procedimientos (3.25) para lograr dichos objetivos (3.19).

NOTA 1 Los objetivos (3.19) en materia de *compliance* penal se relacionan con la tolerancia cero a los riesgos penales (3.29), desarrollando, para ello, actividades tendentes a su prevención, detección y gestión tempranas.

NOTA 2 Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 3 Los elementos del sistema de gestión incluyen la estructura de la organización (3.20), los roles y las responsabilidades, la planificación, la operación, etc.

NOTA 4 El alcance de un sistema de gestión puede incluir la totalidad de la organización (3.20), funciones o secciones específicas e identificadas de la organización (3.20) o de un grupo de organizaciones.

3.32 socio de negocio:

Cualquier parte, salvo los miembros de la organización (3.17), con quien la organización (3.20) tiene, o prevé establecer, algún tipo de relación de negocios.

NOTA 1 Los socios de negocio incluyen, pero no están limitados a, clientes, *joint ventures*, socios de *joint ventures*, socios de consorcios, contratistas, comisionistas, consultores, subcontratistas, proveedores, vendedores, asesores, agentes, distribuidores, representantes, intermediarios e inversores. Esta definición es deliberadamente amplia y debería interpretarse considerando el perfil de riesgo (3.28) de la organización (3.20).

NOTA 2 Distintos tipos de socios de negocio plantean diferentes tipos y grados de riesgo penal (3.29), y una organización (3.20) tendrá distintos grados de capacidad para influir en ellos. Por ello, los socios de negocio pueden ser tratados de forma distinta en función de la evaluación de riesgos (3.28) de la organización (3.20) y de sus procedimientos (3.25).

NOTA 3 El término "negocio" en esta norma UNE debe interpretarse en sentido amplio, refiriéndose a aquellas actividades que son fundamentales o beneficiosas para el propósito de la existencia de la organización (3.20).

3.33 tercero:

Persona física o jurídica u órgano que es independiente de la organización (3.20).

4 Contexto de la organización**4.1 Entendimiento de la organización y su contexto**

La organización (3.20) debe determinar los factores externos e internos que son relevantes a sus propósitos y para alcanzar sus objetivos de *compliance* penal (3.19), especificados en la política de *compliance* penal (3.24) y desarrollados en los elementos que conforman el resto del sistema de gestión de *compliance* penal (3.31). Esos factores incluyen, a título enunciativo no limitativo:

- a) el tamaño y la estructura de la organización (3.20);
- b) las ubicaciones y sectores en los que opera la organización (3.20) o prevé operar;
- c) la naturaleza, escala y complejidad de las actividades de la organización (3.20) y sus operaciones;
- d) las entidades sobre las cuales ejerce control;
- e) los miembros de la organización (3.17) y los socios de negocio (3.32);
- f) la naturaleza y extensión de las relaciones con funcionarios públicos (3.13); y
- g) las obligaciones y compromisos legales, contractuales o profesionales.

NOTA Una organización (3.20) ejerce el control sobre otra cuando directa o indirectamente controla su gestión, lo que incluye disponer de la participación mayoritaria en ella o de sus derechos de voto.

4.2 Entendimiento de las necesidades y expectativas de los grupos de interés

La organización (3.20) debe determinar:

- Las partes interesadas (3.23) que son relevantes a los efectos tanto de la política de *compliance* penal (3.24) como del resto del sistema de gestión de *compliance* penal (3.31).
- Los requisitos (3.27) a considerar en relación con esas partes interesadas (3.23).

NOTA En el proceso (3.26) de identificación de los requisitos (3.27) de las partes interesadas (3.23), una organización (3.20) puede distinguir entre los que son de carácter obligado y aquellos que no lo son y constituyen compromisos asumidos voluntariamente frente a ellos o incluso meras expectativas de los mismos.

4.3 Determinación del alcance del sistema de gestión de *compliance* penal

La organización (3.20) debe determinar el alcance objetivo y subjetivo del sistema de gestión de *compliance* penal (3.31).

A efectos de determinar ese alcance, la organización (3.20) debe considerar:

- Los factores externos e internos referidos en el apartado 4.1 de esta norma UNE.
- Los requisitos (3.27) referidos en el apartado 4.2 de esta norma UNE.
- Los resultados de la evaluación de riesgos penales (3.29) referida en el capítulo 6 de esta norma UNE.

El alcance del sistema de gestión de *compliance* penal (3.31) debe hallarse a disposición como información documentada (3.14).

4.4 Sistemas de gestión de *compliance* penal

La organización (3.20) debe adoptar, implementar, mantener y mejorar continuamente un sistema de gestión de *compliance* penal (3.31), que incluya las políticas, procesos (3.26) y procedimientos (3.25) necesarios así como sus interacciones, de acuerdo con los requisitos (3.27) establecidos por esta norma UNE.

El sistema de gestión de *compliance* penal (3.31) debe incluir medidas diseñadas para evaluar el riesgo penal (3.29), prevenirlo, detectarlo y gestionarlo de manera temprana.

NOTA No es posible eliminar completamente el riesgo penal (3.29), y no puede exigirse a ningún sistema de gestión de *compliance* penal (3.31) que sea capaz de prevenir, detectar y gestionar todos los riesgos penales (3.29).

El sistema de gestión de *compliance* penal (3.31) en todos sus componentes, debe ser razonable y proporcionado, considerando los factores a que se refiere el apartado 4.3 de esta norma UNE.

5 Liderazgo

5.1 Liderazgo y compromiso

El liderazgo dentro de la organización (3.20) debe desempeñar un papel fundamental en la formación e implementación con éxito del sistema de gestión de *compliance* penal (3.31).

5.1.1 Órgano de gobierno

El órgano de gobierno (3.22) debe demostrar su liderazgo y compromiso en relación con el sistema de gestión de *compliance* penal (3.31). A tal fin, el órgano de gobierno (3.22) debe:

- a) establecer y defender como uno de los valores fundamentales de la organización (3.20) que las actuaciones de los miembros de la organización (3.17), sean siempre conformes al ordenamiento jurídico, en general, y al de naturaleza penal, en particular, promoviendo una cultura (3.8) de *compliance* adecuada en el seno de la organización (3.20);
- b) adoptar, implementar, mantener y mejorar continuamente un sistema de gestión de *compliance* penal (3.31) idóneo para prevenir y detectar delitos o para reducir de forma significativa el riesgo (3.28) de su comisión;
- c) dotar al sistema de gestión de *compliance* penal (3.31) y en concreto al órgano de *compliance* penal (3.21) de los recursos financieros, materiales y humanos adecuados y suficientes para su funcionamiento eficaz (3.11);

NOTA Ocurre en ocasiones que la política de *compliance* penal (3.24), al ser un documento de alto nivel aprobado por el Consejo, no recoge expresamente las actividades y delitos asociados y sea en otro documento de menor nivel (emitido por el órgano de *compliance* penal (3.21)) el que recoja con detalle actividades y riesgos (3.28).

- d) aprobar la política de *compliance* penal (3.24) de la organización (3.20);
- e) evaluar periódicamente la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31), modificándolo, si es preciso, cuando se detecten incumplimientos graves o se produzcan cambios en la organización (3.20), en la estructura de control o en la actividad desarrollada;
- f) establecer un órgano de *compliance* penal (3.21) al que se encomienda la supervisión del funcionamiento y la ejecución del sistema de gestión de *compliance* penal (3.31), otorgándole poderes autónomos de iniciativa y control a fin de que pueda desarrollar eficazmente su labor;
- g) asegurar que se establecen los procedimientos (3.25) que concreten el proceso (3.26) de formación de la voluntad de la organización (3.20), de toma de decisiones y de ejecución de las mismas promoviendo una cultura (3.8) de *compliance* que garantice altos estándares éticos de comportamiento.

5.1.2 Órgano de *compliance* penal

- a) El órgano de *compliance* penal (3.21), trabajando conjuntamente con la dirección, debe ser responsable de:
 - 1) impulsar y supervisar la implementación del sistema de gestión de *compliance* penal (3.31) en los distintos ámbitos de la organización (3.20);
 - 2) asegurarse de que se proporcione apoyo formativo continuo a los miembros de la organización (3.17) para garantizar que todos los miembros relevantes son formados con regularidad;
 - 3) promover la inclusión de las responsabilidades de *compliance* penal (3.5) en las descripciones de puestos de trabajo y en los procesos (3.26) de gestión del desempeño (3.9) de los miembros de la organización (3.17);
 - 4) poner en marcha un sistema de información y documentación de *compliance* penal;
 - 5) adoptar e implementar procesos (3.26) para gestionar la información, tales como las reclamaciones y/o comentarios recibidos de líneas directas, un canal de denuncias u otros mecanismos;
 - 6) establecer indicadores de desempeño (3.9) de *compliance* penal (3.5) y medir el desempeño (3.9) de *compliance* penal (3.5) en la organización (3.20);
 - 7) analizar el desempeño (3.9) para identificar la necesidad de acciones correctivas (3.1);
 - 8) identificar y gestionar los riesgos penales (3.29) incluyendo los relacionados con los socios de negocio (3.32);
 - 9) asegurar que el sistema de gestión de *compliance* penal (3.31) se revisa a intervalos planificados;

- 10) asegurar que se proporcione a los empleados acceso a los recursos de *compliance*;
- 11) informar al órgano de gobierno (3.22) sobre los resultados derivados de la aplicación del sistema de gestión de *compliance* penal (3.31).
- b) Cuando se asignen las responsabilidades, se debe considerar la forma de asegurar que el órgano de *compliance* penal (3.21) no tiene conflictos de intereses y que ha demostrado:
- integridad y compromiso con *compliance* penal (3.5);
 - habilidades de comunicación eficaz y de capacidad de influencia;
 - capacidad y prestigio para que sus consejos y directrices tengan aceptación;
 - competencia (3.4) necesaria.
- c) El órgano de *compliance* penal (3.21) debe personificar la posición de máximo garante de la supervisión, vigilancia y control de las obligaciones de *compliance* penal en la organización (3.20), tanto hacia dentro como hacia fuera de la misma, por lo que debe disponer de suficientes recursos y contar con personal que tenga las competencias (3.4), estatus, autoridad e independencia adecuadas.
- d) El órgano de *compliance* penal (3.21) debe tener acceso directo e inmediato al órgano de gobierno (3.22) en caso de que sea preciso elevar hechos o conductas sospechosas o asuntos relacionados con los objetivos de *compliance* penal (3.19) y, por lo tanto, con la política de *compliance* penal (3.24) y el sistema de gestión de *compliance* penal (3.31).
- e) El órgano de *compliance* penal (3.21) debe ocupar una posición en la organización (3.20) que le acredite para solicitar y recibir la colaboración plena de los demás órganos de la misma.

NOTA El órgano de *compliance* debería, además:

- contribuir a la identificación de las obligaciones de *compliance* penal (3.5), con el apoyo de los recursos necesarios, y colaborar para que esas obligaciones se traduzcan en políticas, procedimientos (3.25) y procesos (3.26) viables,
- colaborar para que las obligaciones de *compliance* penal (3.5) se integren en las políticas, procedimientos (3.25) y procesos (3.26) existentes,
- asegurar que hay acceso a un asesoramiento profesional adecuado para la adopción, implementación, mantenimiento y mejora continua del sistema de gestión de *compliance*,
- proporcionar asesoramiento objetivo a la organización en materias relacionadas con *compliance*.

5.1.3 Alta dirección

La alta dirección (3.2) debe demostrar liderazgo y compromiso con respecto al sistema de gestión de *compliance* penal (3.31) de la organización (3.20). Para ello, en el ejercicio de sus funciones ejecutivas la alta dirección (3.2) debe:

- a) garantizar que el sistema de gestión de *compliance* penal (3.31) se implemente de forma adecuada para conseguir los objetivos de *compliance* penal (3.19) establecidos en la política de *compliance* penal (3.24) y afrontar de manera eficaz (3.11) los riesgos penales (3.29) de la organización (3.20);

- b) garantizar que las exigencias derivadas del sistema de gestión de *compliance* penal (3.31) se incorporan a los procesos (3.26) y procedimientos (3.25) operativos de la organización (3.20);
- c) garantizar la disponibilidad de recursos adecuados y suficientes para la ejecución eficaz (3.11) del sistema de gestión de *compliance* penal (3.31);
- d) cumplir y hacer cumplir, tanto interna como externamente, la política de *compliance* penal (3.24);
- e) comunicar internamente la importancia de una gestión eficaz (3.11) de *compliance* penal (3.5), coherente con los objetivos (3.19) y requisitos (3.27) de la política de *compliance* penal (3.24), así como del sistema de gestión de *compliance* penal (3.31);
- f) dirigir y apoyar al personal a fin de lograr la observancia de los requisitos (3.27) y la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31) de acuerdo con su rol en la organización (3.20);
- g) promover la mejora continua (3.16) y apoyar los diversos roles de gestión para demostrar liderazgo en la prevención de delitos y en la detección de riesgos penales (3.29) en lo concerniente a sus áreas de responsabilidad;
- h) fomentar el uso de procedimientos (3.25) para la puesta en conocimiento de conductas potencialmente delictivas que puedan afectar a la organización (3.20) y sus actividades;
- i) garantizar que ningún miembro de la organización (3.17) es objeto de represalia, discriminación o sanción disciplinaria por comunicar de buena fe violaciones, o sospechas fundadas de violaciones, de la política de *compliance* penal (3.24), o por rehusar participar en actuaciones delictivas, incluso si ello conduce a una pérdida de negocio de la organización (3.20).

5.2 Política de *compliance* penal

El órgano de gobierno (3.22) debe impulsar y aprobar una política de *compliance* penal (3.24) que:

- a) exija el cumplimiento de la legislación penal aplicable a la organización (3.20);
- b) sea congruente con los fines de la organización (3.20);
- c) identifique las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos;
- d) prohíba la comisión de hechos delictivos;
- e) minimice la exposición de la organización (3.20) a los riesgos penales (3.29);
- f) proporcione un marco adecuado para la definición, revisión y consecución de los objetivos de *compliance* penal (3.19);
- g) incluya un compromiso para cumplir con los requisitos (3.27) de la política de *compliance* penal (3.24) y del sistema de gestión de *compliance* penal (3.31);
- h) imponga la obligación de informar sobre hechos o conductas sospechosas relativas a riesgos penales (3.29), garantizando que el informante no sufrirá represalias;

- i) incluya un compromiso con la mejora continua (3.16) del sistema de gestión de *compliance* penal (3.31);
- j) explicita la autoridad e independencia del órgano de *compliance* penal (3.21), si éste no coincide con el órgano de gobierno (3.22);
- k) exponga las consecuencias de no cumplir los propios requisitos (3.27) de la política de *compliance* penal (3.24), así como de los derivados del sistema de gestión de *compliance* penal (3.31).

La política de *compliance* penal (3.24) debe:

- 1) estar disponible como información documentada (3.14);
- 2) comunicarse con un lenguaje e idioma adecuados al personal de la organización (3.20), así como a las partes asociadas que puedan representar riesgos penales (3.29);
- 3) estar disponible para las partes interesadas (3.23), según proceda.

5.3 Roles, responsabilidades y autoridades en la organización

5.3.1 Roles y responsabilidades

La alta dirección (3.2) debe asegurarse que la responsabilidad y autoridad en las funciones relevantes se asignen y comunican en todos los niveles de la organización (3.20).

Los responsables de cada nivel deben asegurarse de que los miembros de la organización (3.17) adscritos a sus departamentos, funciones o proyectos cumplan, observen y hagan cumplir y observar los requisitos (3.27) del sistema de gestión de *compliance* penal (3.31).

Los miembros de la organización (3.17) son responsables de comprender, observar y aplicar dichos requisitos (3.27) en lo concerniente a su rol en la organización (3.20).

5.3.2 Delegación de facultades

En los casos en que el órgano de gobierno (3.22), el órgano de *compliance* penal (3.21) o la alta dirección (3.2) delegue la responsabilidad o autoridad para la toma de decisiones en ámbitos en los que exista riesgo penal (3.29) la organización (3.20) debe establecer y aplicar un procedimiento (3.25) y un sistema de controles que garanticen que el proceso (3.26) de decisión y el nivel de autoridad de los decisores sean adecuados y estén libres de conflictos de interés reales o potenciales.

En la delegación de responsabilidad y autoridad, la alta dirección (3.2) debe identificar y actuar para gestionar conflictos de interés (3.6) reales o potenciales.

A propuesta del órgano de *compliance* penal (3.21) o la alta dirección (3.2), el órgano de gobierno (3.22) debe revisar periódicamente dicho procedimiento (3.25).

NOTA La delegación de la toma de decisiones no exonera a la alta dirección (3.2), al órgano de *compliance* penal (3.21), ni al órgano de gobierno (3.22) de sus propios deberes y responsabilidades en cuanto a la prevención de los riesgos penales (3.29). Tampoco transfiere a las personas delegadas las posibles responsabilidades legales en materia de supervisión o adopción de decisiones que les corresponda.

6 Planificación

6.1 Acciones para abordar riesgos y oportunidades

La organización (3.20) debe identificar las actividades en cuyo ámbito puedan materializarse los riesgos penales (3.29). Al planificar su sistema de gestión de *compliance* penal (3.31), la organización (3.20) debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos (3.27) referidos en el apartado 4.2 de esta norma UNE, determinando los riesgos penales (3.29) y oportunidades que es necesario abordar con el fin de:

- asegurar que el sistema de gestión de *compliance* penal (3.31) pueda lograr los objetivos de *compliance* penal (3.19), constituyéndose en modelo de organización (3.20) y gestión que incluya las medidas de vigilancia y control idóneas para prevenir delitos o para reducir de forma significativa el riesgo (3.28) de su comisión;
- prevenir o reducir efectos no deseados;
- lograr la mejora continua (3.16).

La organización (3.20) debe determinar la manera de:

- integrar e implementar dentro de sus propios procesos (3.26) de negocio los procesos (3.26), procedimientos (3.25) y demás acciones propias del sistema de gestión de *compliance* penal (3.31);
- evaluar la eficacia (3.11) de estas acciones;
- generar evidencias de cumplimiento en el momento de realizar los controles o revisiones y su gestión propia o por terceros (3.33) de forma inalterable e íntegra para su posible presentación en futuros procedimientos judiciales que afecten a la organización (3.20).

6.2 Identificación, análisis y valoración de los riesgos penales

6.2.1 Generalidades

La organización (3.20) debe desarrollar un proceso (3.26) de identificación, análisis y valoración del riesgo penal (3.29) para:

- a) identificar los riesgos penales (3.29) que la organización (3.20) pueda razonablemente anticipar, considerando los factores relacionados en el apartado 4.1 de esta norma UNE;
- b) analizar y valorar los riesgos penales (3.29) identificados;
- c) evaluar la adecuación del diseño y eficacia (3.11) de los controles existentes en la organización que permitan detectar los riesgos penales (3.29) que se han valorado y contribuyan a mitigarlos.

6.2.2 Análisis de los riesgos penales

La organización (3.20) debe analizar los riesgos penales (3.29) considerando las causas y las fuentes de incumplimientos de *compliance* penal (3.5) y la gravedad de sus consecuencias, así como la probabilidad de que ocurran incumplimientos de *compliance* penal (3.5) y las consecuencias asociadas.

NOTA Las consecuencias pueden incluir, por ejemplo, daño personal y ambiental, pérdidas económicas, daño reputacional y responsabilidades administrativas.

6.2.3 Evaluación de los riesgos penales

La organización (3.20) debe establecer criterios para evaluar su nivel de riesgo penal (3.29), considerando sus objetivos de *compliance* penal (3.19) y, por lo tanto, los compromisos asumidos a través de su política de *compliance* penal (3.24) y demás políticas o instrucciones internas relacionadas con ella.

NOTA 1 La evaluación de los riesgos (3.28) debería incluir la consideración del umbral de riesgo que la organización (3.20) está dispuesta a aceptar, de manera que si el riesgo resultante del análisis realizado es superior a dicho umbral, la organización (3.20) debería implementar controles adicionales para reducir dicho riesgo.

NOTA 2 Respecto de la gestión del riesgo (3.28) se puede consultar la UNE-ISO 31000 *Gestión del riesgo. Principios y directrices*.

6.2.4 Revisión de la evaluación de riesgos penales

La evaluación del riesgo penal (3.29) deber revisarse:

- a) de manera regular, de modo que los cambios y la nueva información puedan ser adecuadamente considerados según la frecuencia definida por la organización (3.20);
- b) en caso de cambios significativos en la estructura o actividades de la organización (3.20);
- c) en caso de incumplimientos de *compliance* penal (3.5);
- d) en caso de que aparezca jurisprudencia o se produzcan cambios legislativos relevantes.

6.2.5 Información documentada sobre riesgos penales

La organización (3.20) debe mantener información documentada (3.14) de la identificación, análisis y evaluación de riesgos penales (3.29) y de la metodología y criterios utilizados.

6.3 Objetivos de prevención de delitos y planificación para lograrlos

La organización (3.20) debe establecer objetivos de *compliance* penal (3.19) para las funciones y niveles pertinentes.

Los objetivos de *compliance* penal (3.19) deben:

- a) ser coherentes con lo establecido en la política de *compliance* de penal (3.24) y con los resultados de la identificación y evaluación de riesgos penales (3.29);
- b) ser medibles (si es posible);

- c) tener en cuenta los requisitos (3.27) aplicables;
- d) ser objeto de seguimiento (3.30);
- e) comunicarse;
- f) actualizarse, según corresponda.

La organización (3.20) debe conservar información documentada (3.14) sobre los objetivos de *compliance* penal (3.19).

Al planificar cómo lograr sus objetivos de *compliance* penal (3.19), la organización (3.20) debe determinar:

- 1) qué se va a hacer y quién será responsable;
- 2) qué recursos se requerirán, debiendo disponer de modelos de gestión de los recursos financieros adecuados para impedir la materialización de los riesgos penales (3.29);
- 3) cuándo se finalizará;
- 4) cómo se evaluarán los resultados.

7 Elementos de apoyo

7.1 Cultura de *compliance*

El *compliance* penal (3.5) es el resultado de que una organización (3.20) cumpla con sus objetivos de *compliance* penal (3.19), a través del cumplimiento de los requisitos (3.27) que se derivan de su política de *compliance* penal (3.24) y del resto del sistema de gestión de *compliance* penal (3.31), y se hace sostenible introduciéndola en la cultura (3.8) de la organización (3.20) y en el comportamiento y en la actitud de las personas que se vinculan con ella.

El desarrollo de una cultura (3.8) de *compliance* exige que el órgano de gobierno (3.22) y la alta dirección (3.2) tengan un compromiso visible, consistente y sostenido en el tiempo con un estándar común y publicado de comportamiento que se requiera en todas y cada una de las áreas de la organización (3.20), así como a sus socios de negocio (3.32).

NOTA Normalmente el estándar común de comportamiento exigido, tanto a los miembros de la organización (3.17), como a los socios de negocio (3.32) constará en la política de *compliance* penal (3.24), aunque también pueden encontrarse referencias al respecto en un código de conducta, código ético, código de valores o documento análogo en la organización (3.20).

Son elementos de una cultura (3.8) de *compliance*:

- a) una política de *compliance* penal (3.24);
- b) que se constate el respeto y la implementación activa por parte de la dirección de la política de *compliance* penal (3.24);

- c) consistencia en el tratamiento de acciones similares, con independencia de la posición;
- d) guiar, entrenar y predicar con el ejemplo;
- e) realizar evaluaciones adecuadas a los potenciales empleados antes de su contratación;
- f) un programa de iniciación u orientación adecuado que enfatice el *compliance* penal (3.5) y los valores de la organización (3.20);
- g) formación continua de *compliance* penal (3.5), incluyendo actualizaciones de la formación;
- h) comunicación continua, abierta y adecuada sobre *compliance* penal;
- i) sistemas de remuneración que valoren el logro de objetivos de *compliance* penal (3.19) y parámetros clave de sistema de gestión de *compliance* penal (3.31);
- j) reconocimiento visible de los logros en la gestión de *compliance* y en sus resultados;
- k) medidas disciplinarias rápidas y proporcionadas en caso de conductas penales o no conformidades (3.18) respecto de la política de *compliance* penal (3.24) o el resto del sistema de gestión de *compliance* penal (3.31).

La existencia de una cultura (3.8) de *compliance* se mide por el grado en que se cumplan los requisitos (3.27) señalados arriba:

- 1) las partes interesadas, (3.23) y especialmente los miembros de la organización (3.17), creen que se han implementado dichos requisitos;
- 2) los miembros de la organización (3.17) comprenden la relevancia de las obligaciones de *compliance* penal (3.5) relativas a sus propias actividades y, en su caso, a las de sus unidades de negocio;
- 3) se logran remediar los riesgos penales (3.29), y las no conformidades (3.18) se asumen y se gestionan en todos los niveles de la organización (3.20) cuando sea necesario;
- 4) se valora el papel del *compliance* penal (3.5) y sus objetivos (3.19);
- 5) se permite y se anima al personal a que comunique sus preocupaciones de *compliance* penal (3.5) adecuadamente;
- 6) se conoce, respeta y colabora con el rol del órgano de *compliance* penal (3.21).

7.2 Recursos

La organización (3.20) debe determinar y proporcionar los recursos necesarios para la adopción, implementación, mantenimiento y mejora continua del sistema de gestión de *compliance* penal (3.31) de acuerdo con los parámetros que se indican en el apartado 4.1 de esta norma UNE. Los recursos incluyen, como mínimo, los financieros, tecnológicos y humanos, así como el acceso, en su caso, a asesoramiento externo.

7.3 Competencia

7.3.1 Requisitos en relación con la competencia del personal de *compliance*

La organización (3.20) debe:

- a) determinar la competencia (3.4) necesaria de las personas que realizan tareas relacionadas con el *compliance* penal (3.5), bajo el control de la organización (3.20);
- b) asegurarse de que estas personas sean competentes, basándose en una educación, formación o experiencia adecuadas;
- c) cuando sea aplicable, tomar acciones para que esas personas adquirieran la competencia (3.4) necesaria, y evaluar la eficacia (3.11) de las acciones tomadas;
- d) conservar la información documentada (3.14) apropiada, como evidencia de la competencia (3.4) existente o adquirida.

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

7.3.2 Diligencia debida con los miembros de la organización

7.3.2.1 Diligencia debida común a todos los miembros de la organización

En relación con los miembros de la organización (3.17), se deben establecer, implementar y mantener actualizados procedimientos (3.25) tendientes a que:

- a) se entregue a los miembros de la organización (3.17), en el proceso de incorporación, una copia de la política de *compliance* (3.24) o se le facilite el acceso a la misma;
- b) se facilite el acceso a la política de *compliance* vigente a todos los miembros de la organización (3.17);
- c) se requiera que todos los miembros de la organización (3.17) cumplan con la política de *compliance* penal (3.24) y el resto del sistema de gestión de *compliance* penal (3.31);
- d) se adopten acciones disciplinarias proporcionales contra aquellos miembros de la organización (3.17) que incumplan los requisitos (3.27) derivados de la política de *compliance* penal (3.24) o del resto del sistema de gestión de *compliance* penal (3.31);
- e) no se adopte ningún tipo de represalia contra los miembros de la organización (3.17):

- 1) por negarse a participar o rechazar cualquier actividad en la que puede considerarse razonablemente que existe riesgo penal (3.29), siempre que lo haya comunicado por la vía oportuna,
- 2) por reportar de buena fe a través de los canales establecidos al efecto por la organización (3.20).

NOTA 1: Minusvaloraciones, acciones disciplinarias, traslados, despidos y acosos laborales constituyen ejemplos de las represalias que no deben adoptarse.

NOTA 2: Canales de denuncias, líneas de ayuda, buzones de opinión son ejemplos de posibles canales de reporte.

7.3.2.2 Diligencia debida relativa a personas que ocupan posiciones especialmente expuestas

En relación con personas que ocupan posiciones especialmente expuestas a riesgos penales (3.29) mayores que bajo, de conformidad (3.7) con el apartado 6.2 de esta norma UNE, la organización (3.20) debe cumplir, además de con los requisitos (3.27) establecidos en 7.3.2.1, con los siguientes requisitos (3.27):

- a) Se realiza un procedimiento de diligencia debida (3.10) (véase anexo B) en relación con candidatos a empleados antes de que éstos suscriban el contrato de trabajo, sean trasladados o promocionados por la organización (3.20), con el objetivo de verificar, de un modo razonable, que su empleo o nueva posición de empleo es apropiado/a y que resulta lógico creer que comprenderán en toda su extensión y cumplirán con la política de *compliance* penal (3.24) y el resto del sistema de gestión de *compliance* penal (3.31) en todo aquello que les afecte.
- b) Se revisan periódicamente los objetivos de rendimiento, las primas por rendimiento y otros elementos de remuneración para asegurarse de que existen salvaguardas razonables para evitar que incentiven la asunción de riesgos penales (3.29) o promuevan conductas inapropiadas en relación con el *compliance* penal (3.5).
- c) Dicho personal formaliza una declaración, a intervalos planificados en proporción al riesgo (3.28) identificado, confirmando su cumplimiento de la política de *compliance* penal (3.24).

7.4 Formación y concienciación en *compliance*

La organización (3.20) debe fomentar que los miembros de la organización (3.17) se conciencien y se formen adecuada, eficaz y proporcionalmente respecto de los riesgos penales (3.29), con la finalidad de evitarlos, detectarlos o saberlos gestionar conforme al sistema de gestión de *compliance* penal (3.31).

Asimismo, la organización (3.20) debe proporcionar formación a su personal en las siguientes materias:

- a) la política de *compliance* penal (3.24) y el resto del sistema de gestión de *compliance* penal (3.31) y los procedimientos (3.25) asociados con él, y de su obligación de cumplir con los requisitos (3.27) asociados con todo ello;
- b) el riesgo penal (3.29) y el perjuicio, tanto para el personal como para la organización (3.20), en el supuesto de su materialización;
- c) las circunstancias en las cuales, en el desempeño (3.9) de su trabajo, se puede materializar un riesgo penal (3.29), y cómo reconocer dichas circunstancias;
- d) cómo pueden ayudar a prevenir y detectar riesgos penales (3.29), evitando su materialización y reconociendo los factores de riesgo (3.28) principales;
- e) su contribución a la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31), incluyendo los beneficios derivados de una mejora del *compliance* penal (3.5) y de reportar posibles delitos o no conformidades (3.18);

- f) las implicaciones y consecuencias potenciales de no conformidades (3.14) relativas a los requisitos (3.27) establecidos, tanto por la política de *compliance* penal (3.24), como por el resto del sistema de gestión de *compliance* penal (3.31);
- g) cómo y a quién deben reportar sus dudas y preocupaciones en esta materia, según lo establecido en el apartado 8.8 de esta norma UNE.

La organización (3.20) debe proporcionar información documentada (3.14) acerca de la formación y otros recursos disponibles para mejorar su conocimiento en el ámbito del *compliance* penal (3.5).

NOTA La concienciación y formación de los miembros de la organización (3.17) debería tener en consideración los resultados de la evaluación del riesgo penal (3.29) referida en el apartado 6.2 de esta norma UNE y, en caso de ser relevantes, los resultados del proceso de diligencia debida (3.10) referido en el apartado 8.2 de esta norma UNE.

La organización (3.20) debería fomentar de manera continua (a intervalos planificados) entre los miembros de la organización (3.17) la concienciación respecto del *compliance* penal (3.5) a través de campañas de sensibilización y ciclos formativos. Dicha labor debería realizarse considerando sus roles, los riesgos penales (3.29) a los que están expuestos, y otras circunstancias coyunturales. La concienciación y los programas de formación deberían ser actualizados periódicamente sobre la base de la nueva información disponible.

Sobre la base de los riesgos (3.28) identificados en las actividades de la organización (3.20) según se establece en el apartado 6.2 de esta norma UNE, la organización (3.20) debería también establecer, implementar y mantener actualizados procedimientos (3.25) que trasladen la necesidad de concienciación y formación sobre el *compliance* penal (3.5) de los socios de negocio (3.32) que pudieran representar un riesgo penal (3.29) mayor que bajo para la organización (3.20). Estos procedimientos (3.25) deberían identificar los socios de negocio (3.32) para las cuales dicha concienciación y formación son necesarias, el contenido mínimo de la formación, y los medios a través de los cuales se debe proporcionar y actualizar dicha formación.

7.5 Comunicación

7.5.1 Requisitos para las comunicaciones

La organización (3.20) debe determinar la necesidad de realizar comunicaciones internas y externas relevantes para la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31), que incluyan:

- el contenido de la comunicación;
- cuándo comunicar;
- a quién comunicar;
- cómo comunicar;
- quién debe realizar la comunicación;
- los idiomas y el lenguaje en el que deberá realizarse la comunicación.

7.5.2 Comunicación de la política

La política de *compliance* penal (3.24) debe hacerse accesible a todos los miembros de la organización (3.17) así como a los socios de negocio (3.32) que supongan riesgo penal (3.29) mayor que bajo, y debe publicarse adecuadamente a través de los canales de comunicación internos y externos de la organización (3.20).

7.6 Información documentada

7.6.1 Generalidades

El sistema de gestión de *compliance* penal (3.31) de la organización (3.20) debe incluir:

- la información documentada (3.14) requerida por esta norma UNE;
- la información documentada (3.14) que la organización (3.20) ha determinado como necesaria para la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31).

7.6.2 Creación y actualización

Al crear y actualizar información documentada (3.14), la organización (3.20) debe asegurarse de que lo siguiente sea apropiado:

- la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
- el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);
- la revisión y aprobación con respecto a la idoneidad y adecuación.

7.6.3 Control de la información documentada

La información documentada (3.14) requerida por el sistema de gestión de *compliance* penal (3.31) se debe controlar para asegurarse de que:

- esté disponible y sea idónea para su uso, donde y cuándo se necesite;
- esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada (3.14), la organización (3.20) debe tratar las siguientes actividades, según corresponda:

- distribución, acceso, recuperación y uso;
- almacenamiento y preservación, incluida la preservación de la legibilidad;
- control de cambios (por ejemplo, control de versión);
- conservación y disposición final.

NOTA El acceso puede implicar una decisión en relación al permiso solamente para consultar la información documentada (3.14), o al permiso y a la autoridad para consultar y modificar la información documentada (3.14).

La información documentada (3.14) de origen externo que la organización (3.20) determina como necesaria para la planificación y operación del sistema de gestión de *compliance* penal (3.31) se debe identificar, según sea adecuado, y controlar.

El anexo C relaciona la información documentada (3.14) mínima necesaria en un sistema de gestión de *compliance* penal.

NOTA La información documentada (3.14) se puede preparar con el propósito de obtener asesoramiento legal y, por tanto, puede estar sometida a secreto profesional.

8 Operación

8.1 Planificación y control operacional

La organización (3.20) debe planificar, implementar y controlar los procesos (3.26) necesarios para cumplir los requisitos (3.27) derivados del sistema de gestión de *compliance* penal (3.31) y para implementar las acciones determinadas en el apartado 6.1 de esta norma UNE, mediante:

- el establecimiento de los procesos (3.26) y procedimientos (3.25);
- la implementación del control de los procesos (3.26) y procedimientos (3.25) anteriores;
- el almacenamiento de información documentada (3.14) en la medida necesaria para disponer de evidencias que soporten que los procesos (3.26), procedimientos (3.25) y controles se han llevado a cabo según lo planificado.

Estos procesos (3.26) y procedimientos (3.25) deben estar sujetos a los controles específicos que se detallan en los apartados 8.2 a 8.9 de esta norma UNE.

La organización (3.20) debe supervisar las eventuales modificaciones de sus procesos (3.26), procedimientos (3.25) y sus controles asociados, así como analizar las consecuencias de dichas modificaciones o cambios, tanto planificados como no previstos, tomando medidas para mitigar cualquier consecuencia adversa, cuando resulte necesario.

Además, la organización (3.20) debe contemplar los procesos externalizados (3.12) en su sistema de gestión de *compliance* penal (3.31), evaluando los riesgos penales (3.29) en dichas actividades e implantando controles razonables para evitarlos, detectarlos y gestionarlos de manera temprana.

8.2 Diligencia debida

La organización (3.20) debe realizar un análisis con el fin de identificar aquellas actividades en cuyo ámbito puedan materializarse riesgos penales (3.29) que deban ser prevenidos, y hacerlo de acuerdo con el apartado 6.2 de esta norma UNE.

Donde el análisis de riesgo (3.28) realizado por la organización (3.20) arroje un riesgo penal (3.29) superior a bajo en relación con:

- transacciones, proyectos o actividades específicas;
- relaciones de negocio actuales o planificadas con determinados socios de negocio (3.32);
- categorías de personal en posiciones específicas;

la organización (3.20) debe valorar la naturaleza y el alcance de dicho riesgo, contemplando, si lo considera necesario, la realización de procedimientos de diligencia debida (3.10), los cuales deben ser actualizados convenientemente.

NOTA Para más información, véase el anexo B.

8.3 Controles financieros

La organización (3.20) debe disponer de modelos de gestión de sus recursos financieros que contribuyan a prevenir, detectar o gestionar riesgos penales (3.29) de manera temprana.

NOTA La organización (3.20) debería implementar aquellos controles financieros que resulten adecuados para impedir la comisión de delitos en el seno de su actividad. Dependiendo del tamaño de la organización (3.20), estos controles pueden incluir:

- existencia de una adecuada política de segregación de funciones,
- circuitos de aprobación necesarios para la gestión de los recursos financieros,
- implementación de sistemas de control y gestión de riesgos (3.28) en el proceso (3.26) de emisión de información financiera,
- realización de auditorías (3.3) financieras.

8.4 Controles no financieros

La organización (3.20) debe contar con controles sobre las compras, las operaciones, la comercialización y otros procesos (3.26) no financieros que resulten adecuados para evitar, detectar o gestionar riesgos penales (3.29) de manera temprana y que aseguren que dichos procesos están siendo gestionados adecuadamente.

La organización (3.20) debe implementar aquellos controles no financieros que resulten adecuados para impedir la comisión de delitos en el seno de su actividad.

NOTA 1 Los controles variarán en gran medida dependiendo de la naturaleza de la actividad desarrollada por la organización (3.20) y de los riesgos (3.28) a los que se encuentre expuesta, así como del tamaño de la misma.

NOTA 2 Cualquier actividad, transacción o relación de negocio puede estar sujeta a controles financieros y no financieros.

8.5 Implementación de controles en las filiales y en socios de negocio

8.5.1 Entidades bajo control

En aquellas entidades bajo su control, la organización (3.20) debe implantar procedimientos (3.25) que garanticen que dichas entidades:

- adopten el sistema de gestión de *compliance* penal (3.31) de la entidad matriz; o
- adopten sus propios sistemas de gestión de *compliance* penal (3.31), adaptados a su actividad y entorno.

En cualquier caso, dichos procedimientos (3.25) deben adoptarse siempre y cuando resulte razonable y proporcionado en relación con el riesgo penal (3.29) al que la entidad controlada se encuentre expuesta, de acuerdo con la evaluación del riesgo (3.28) indicada en el apartado 6.2 de esta norma UNE.

8.5.2 Entidades no controladas por la organización

En relación con las entidades sobre las que la organización (3.20) no tiene control pero tiene algún tipo de vinculación y para las que se haya identificado algún riesgo penal (3.29) mayor que bajo, la organización (3.20) debe considerar:

- evaluar si los controles implantados por aquellas son suficientes para evitar, detectar o gestionar adecuadamente la exposición al riesgo penal (3.29);
- si no existen controles previamente implantados por aquellas, la organización (3.20) debe:
 - requerir la implementación de controles que mitiguen sus riesgos penales (3.29),
 - en caso de no resultar posible la implementación de controles en aquellas, considerar este hecho en la evaluación del riesgo (3.28) que conlleva desarrollar operaciones con ellas, analizando las distintas opciones para evitarlo o gestionarlo.

NOTA 1 Se entenderá por vinculación mantener algún tipo de presencia en los órganos de gobierno de la entidad sin que signifique control.

NOTA 2 Una organización (3.20) tiene control sobre otra si directa o indirectamente controla su gestión.

NOTA 3 Para más información, véase el anexo D.

8.6 Condiciones contractuales

La organización (3.20) debe requerir cláusulas específicamente orientadas a reducir el riesgo penal en sus relaciones contractuales con socios de negocio (3.32) que supongan un riesgo penal (3.29) mayor que bajo para la misma.

NOTA 1 Puede resultar conveniente en determinados casos incluir cláusulas que contemplen el derecho a realizar auditorías (3.3) por parte de la organización (3.20). En caso de no resultar posible la inclusión de dicha cláusula, este hecho debería considerarse en la evaluación del riesgo (3.28).

NOTA 2 Para más información, véase el anexo E.

8.7 Gestión de deficiencias de los controles

Ante deficiencias identificadas en el sistema de control, la organización (3.20) debe tomar medidas para remediarlas, por ejemplo, implantando planes de acción que mitiguen los riesgos (3.28) asociados a los controles deficientes, conforme al apartado 6.2 de esta norma UNE.

Si se identifican deficiencias del sistema en transacciones, procesos (3.26), actividades o cualquier relación de negocio con socios de negocio (3.32), donde la organización no pueda o no esté dispuesta a implantar controles adicionales, la organización (3.20) debe tomar las medidas necesarias para la mitigación del riesgo penal (3.29).

NOTA Se entiende por medidas de mitigación las encaminadas a terminar, discontinuar, suspender o rechazar dicha transacción, proceso (3.26), actividad o relación de negocio lo antes posible.

8.8 Comunicación de incumplimientos e irregularidades

La organización (3.20) debe implantar procedimientos (3.25) adecuados para:

- facilitar canales de comunicación para que tanto los miembros de la organización (3.17) como terceros (3.33) comuniquen de buena fe y, sobre la base de indicios razonables, aquellas circunstancias que puedan suponer la materialización de un riesgo penal (3.29) para la organización (3.20), así como incumplimientos o debilidades del sistema de gestión de *compliance* penal (3.31);
- garantizar la confidencialidad o el anonimato de la identidad de las personas que hagan uso de dichos canales de comunicación;
- permitir la realización de comunicaciones de manera anónima o confidencial;
- prohibir cualquier tipo de represalia, tomando las medidas necesarias para proteger a aquellos miembros de la organización (3.17) o terceros (3.33) que realicen comunicaciones de buena fe y, sobre la base de indicios razonables, a través de dichos canales de comunicación;
- facilitar asesoramiento a aquellas personas que planteen dudas o inquietudes relacionadas a través de los canales de comunicación establecidos por la organización (3.20);
- garantizar que los miembros de la organización (3.17) conocen los canales de comunicación existentes y los procedimientos (3.25) que regulan su funcionamiento;
- fomentar el uso de los canales de comunicación entre los miembros de la organización (3.17).

NOTA 1 El procedimiento (3.25) de comunicación de incumplimientos e irregularidades relacionados con el sistema de gestión de *compliance* penal (3.31) puede formar parte de otros procedimientos (3.25) de la organización (3.20) sobre comunicación de incumplimientos e irregularidades relacionadas con otras materias (por ejemplo, seguridad, irregularidades financieras, etc.).

NOTA 2 La organización (3.20) podrá externalizar (3.12) la tramitación de las comunicaciones mediante la contratación de una firma externa e independiente.

Las obligaciones de informar deben establecerse de forma clara en la política de *compliance* penal (3.24) y procedimientos (3.25) derivados del sistema de gestión de *compliance* penal (3.31) de la organización (3.20) y reforzarse por otros medios, tales como refuerzos informales de la dirección durante su trabajo de día a día con el personal.

8.9 Investigación de incumplimientos e irregularidades

La organización (3.20) debe implementar procedimientos (3.25) que:

- aseguren la investigación de todas las comunicaciones recibidas;
- requieran la adopción de medidas adecuadas y proporcionadas en caso de verificación de dichas comunicaciones;

- garanticen que se dispone de recursos con capacidad, autonomía e independencia para realizar las investigaciones pertinentes, y que todas áreas o funciones de la organización (3.20), si son requeridas, colaboran con ellos;
- garanticen que el órgano de *compliance* penal (3.21) está oportunamente informado del estado y resultados de cada investigación;
- garanticen los derechos del denunciante y del denunciado.

NOTA Las medidas a adoptar en caso de no conformidad (3.18) o irregularidad variarán en función de la severidad del caso, pudiendo incluir la adopción de medidas disciplinarias (desde la amonestación hasta el despido disciplinario); proporcionar retroalimentación al personal involucrado; comunicación a las autoridades; así como mejorar y actualizar los controles del modelo para prevenir que se produzcan situaciones similares.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

9.1.1 Generalidades

La organización (3.20) debe determinar:

- a) a qué es necesario hacer seguimiento (3.30) y qué es necesario medir para conocer la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31);
- b) quién es el responsable de realizar el seguimiento (3.30);
- c) los métodos de seguimiento (3.30), medición (3.15), análisis y evaluación, según sea aplicable, para asegurar resultados válidos;
- d) cuándo se deben llevar a cabo el seguimiento (3.30) y la medición (3.15);
- e) cuándo se deben analizar y evaluar los resultados del seguimiento (3.30) y la medición (3.15);
- f) a quién se debe facilitar la información del seguimiento (3.30) y la medición (3.15).

La organización (3.20) debe conservar la evidencia de los resultados del seguimiento (3.30) y medición (3.15), así como los informes de prevención como información documentada (3.14).

La organización (3.20) debe evaluar el desempeño (3.9) del *compliance* penal (3.5) y la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31).

9.1.2 Seguimiento

Se debe hacer seguimiento (3.30) del sistema de gestión de *compliance* penal (3.31) a fin de asegurar que se alcanzan los objetivos de *compliance* penal (3.19)). Para ello, la organización debe establecer un plan de seguimiento (3.30) continuo, definiendo los procesos (3.26), programas y recursos del seguimiento (3.30) y la información que se debe recoger.

NOTA 1 El seguimiento (3.30) del *compliance* penal (3.5) es el proceso (3.26) consistente en recoger información con el objetivo de evaluar la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31) y, por lo tanto, el desempeño (3.9) del *compliance* penal (3.5) de la organización (3.20).

NOTA 2 El seguimiento (3.30) del sistema de gestión de *compliance* penal (3.31) típicamente incluye:

- eficacia (3.11) de la formación,
- eficacia (3.11) de los controles, por ejemplo, a través de los resultados de análisis sobre una muestra significativa en función del análisis de riesgo (3.28) realizado,
- asignación eficaz (3.11) de responsabilidades para cumplir con las obligaciones de *compliance* penal (3.5),
- actualización de las obligaciones de *compliance* penal (3.5),
- eficacia (3.11) en la gestión de fallos de *compliance* penal (3.5) previamente identificados,
- casos en los que no se llevan a cabo, según lo previsto, inspecciones internas derivadas del sistema de gestión de *compliance* penal (3.31).

NOTA 3 El seguimiento (3.30) del desempeño (3.9) de *compliance* penal (3.5) típicamente incluye:

- no conformidades (3.18) y conatos (es decir, incidentes sin efectos adversos),
- casos en los que no se cumplen los requisitos (3.27) derivados de la política de *compliance* penal (3.24) y del resto del sistema de gestión de *compliance* penal (3.31),
- casos en los que no se alcanzan los objetivos de *compliance* penal (3.19),
- estado de la cultura (3.8) de *compliance*,
- indicadores predictivos y reactivos establecidos en apartado 9.1.6 de esta norma UNE.

9.1.3 Fuentes de opinión sobre el desempeño de prevención penal

La organización (3.20) debe establecer, implementar y mantener actualizados procedimientos (3.25) para solicitar y recabar opiniones del desempeño (3.9) de su sistema de gestión de *compliance* penal (3.31) recurriendo a distintas fuentes.

Las opiniones deben servir como una fuente clave de mejora continua (3.16), tanto de la política de *compliance* penal (3.24), como del resto del sistema de gestión de *compliance* penal (3.31).

NOTA La información puede provenir de:

- el personal,
- los clientes,
- los proveedores,
- los reguladores,
- los registros de control de procesos (3.26) y los registros de actividad (incluyendo tanto electrónicos como en papel).

9.1.4 Métodos de recogida de información

Cada organización (3.20) debe seleccionar el método de recogida de información considerado relevante, según las circunstancias, teniendo en cuenta los factores que se relacionan en los apartados 4.1 y 6.2 de esta norma UNE.

NOTA Ejemplos de recogida de información incluyen:

- informes ad hoc de no conformidades (3.18) cuando aparecen o sean identificados;
- información obtenida en líneas directas, reclamaciones y otras fuentes, incluyendo el canal de denuncias;
- discusiones informales, talleres de trabajo y grupos temáticos;
- pruebas integrales y por muestreo;
- resultados de encuestas de percepción;
- observaciones directas, entrevistas formales, visitas a las instalaciones e inspecciones;
- auditorías (3.3) y revisiones;
- consultas a las partes interesadas (3.23), peticiones de formación y opiniones recogidas durante la formación, especialmente las del personal.

9.1.5 Análisis de la información

La información recogida debe analizarse y evaluarse de forma crítica para identificar el origen y las acciones adecuadas que se necesitan tomar. El análisis debe considerar, entre otros, los problemas sistémicos y recurrentes para proceder a su corrección o mejora.

9.1.6 Desarrollo de indicadores

Las organizaciones (3.20) deben desarrollar un conjunto de indicadores medibles (3.15) que ayuden a cada organización (3.20) a medir el logro de sus objetivos de *compliance* penal (3.19) y a cuantificar el desempeño (3.9) de su sistema de gestión de *compliance* penal (3.31).

Este proceso (3.26) debe tener en cuenta los resultados de la evaluación de los riesgos penales (3.29) para asegurar que los indicadores están relacionados con los riesgos penales (3.29) que afronta la organización (3.20).

NOTA 1 La determinación de qué se debería medir y cómo para conocer el desempeño (3.9) del sistema de gestión de *compliance* penal (3.31) puede ser un asunto complejo en ocasiones, pero, sin embargo, es un factor clave para demostrar la eficacia (3.11) de dicho sistema. Además, los indicadores necesarios variarán a medida que la organización (3.20) y el sistema de gestión de *compliance* penal (3.31) evolucionen.

NOTA 2 Ejemplos de indicadores de actividad incluyen:

- porcentaje de personal al que se haya impartido formación de forma eficaz (3.11),
- nivel de utilización de mecanismos para obtener opiniones (incluyendo comentarios sobre el valor de dichos mecanismos por parte de sus usuarios),
- número y tipo de acciones correctivas (3.1) que se tomaron frente a cada no conformidad (3.18).

NOTA 3 Ejemplos de indicadores predictivos del riesgo incluyen:

- riesgos (3.28) de no conformidades (3.18), a través de la medición de la pérdida potencial de los objetivos (salud y seguridad, reputación, etc.) a lo largo del tiempo,
- tendencias de no conformidades (3.18) basadas en datos históricos, comparativos y sectoriales;

NOTA 4 Ejemplos de indicadores sobre la efectividad:

- problemas y no conformidades (3.18) identificados y comunicados, por tipo, área y frecuencia;
- consecuencias que se han derivado de las no conformidades (3.18), que pueden incluir valoración del impacto que resulte de compensaciones monetarias, multas y otras sanciones, coste de remediar sus efectos, pérdida de reputación o coste del tiempo del personal;
- la cantidad de tiempo utilizado para informar y adoptar acciones correctivas (3.1).

9.1.7 Informes de *compliance* penal

El órgano de gobierno (3.22), la alta dirección (3.2) y el órgano de *compliance* penal (3.21) deben asegurarse de estar correcta y puntualmente informados sobre el desempeño (3.9) del sistema de gestión de *compliance* penal (3.31) y de su mejora continua (3.16), incluyendo todas las no conformidades (3.18) relevantes, promoviendo activamente una cultura (3.8) de información completa y transparente.

Las disposiciones relativas a la información interna deben asegurar que:

- a) se establecen criterios adecuados y obligaciones de información;
- b) se establecen programas de informes periódicos;

NOTA Sería recomendable la realización de informes excepcionales que faciliten información *ad hoc* sobre las no conformidades (3.18) especialmente graves o de evolución rápida.

- c) se facilita una información exacta y completa a las funciones o áreas de la organización (3.20) apropiadas, para permitir que se adopten acciones preventivas, correctivas (3.1) y remediadoras;
- d) se decide el formato, el contenido y la periodicidad de los informes internos de *compliance* penal (3.5) para que sean adecuados a las circunstancias de la organización (3.20) y a los factores que se relacionan en el apartado 4.1 de esta norma UNE.

NOTA Los informes de *compliance* penal (3.5) pueden incorporarse en otros informes de la organización (3.20).

- e) todas las no conformidades (3.18) relevantes se informan adecuadamente.

NOTA Mientras que los informes de problemas sistémicos y recurrentes son particularmente importantes, un incumplimiento puntual puede ser igualmente preocupante si es grave o deliberado. Incluso un fallo pequeño puede indicar una gran debilidad en los procesos (3.26) existentes y en el sistema de gestión de *compliance* penal (3.31). Si no se informa sobre el puntualmente, puede deducirse que el fallo no es relevante para la organización, aun pudiendo darse el caso de que dicho fallo se convierta en un problema sistémico.

9.1.8 Contenido de los informes de *compliance* penal

Los informes de *compliance* penal (3.5) deben incluir:

- a) cualquier materia relacionada con riesgos penales (3.29) sobre la que la organización (3.20) haya sido requerida por cualquier regulador o autoridad, incluida la judicial;
- b) cambios en las obligaciones de *compliance* penal (3.5), en su impacto en la organización (3.20) y las propuestas para cumplir con las nuevas obligaciones;
- c) mediciones (3.15) del desempeño (3.9) de *compliance* penal (3.5), incluyendo las no conformidades (3.18) y la mejora continua (3.16);
- d) número y detalle de posible(s) no conformidad(es) (3.18) y su análisis subsiguiente;
- e) acciones correctivas (3.1) adoptadas;
- f) información sobre la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31), sus logros y tendencias;
- g) contactos y desarrollo de las relaciones con los reguladores;
- h) resultados de las auditorías (3.3), así como de las actividades de seguimiento (3.30).

La política de *compliance* penal (3.24) debe fomentar el informe inmediato de cuestiones materialmente significativas que surjan fuera de los periodos previstos para el informe periódico.

9.2 Auditoría interna

La organización (3.20) debe llevar a cabo auditorías (3.3) a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de *compliance* penal (3.31):

- es conforme con los requisitos (3.27) de *compliance* penal (3.5) establecidos por la organización (3.20) a través de su política de *compliance* penal (3.24) y el propio sistema de gestión de *compliance* penal (3.31) y con los requisitos (3.27) de esta norma UNE;
- se implementa y mantiene eficazmente.

NOTA 1 Se pueden realizar auditorías (3.3) adicionales en caso de que sea necesario.

NOTA 2 Se pueden obtener directrices sobre los sistemas de gestión de auditorías (3.3) en ISO 19011.

NOTA 3 El ámbito y escala de las actividades de auditoría (3.3) interna de la organización (3.20) pueden variar dependiendo de una variedad de factores, incluyendo el tamaño, la estructura, la madurez y la localización de la organización (3.20).

La organización (3.20) debe:

- a) planificar, establecer, implementar y mantener uno o varios programas de auditoría (3.3) que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos (3.27) de planificación y la elaboración de informes, teniendo en consideración la importancia de los procesos (3.26) involucrados y los resultados de auditorías (3.3) previas;
- b) definir los criterios de la auditoría (3.3) y el alcance para cada auditoría (3.3);

- c) seleccionar los auditores y llevar a cabo auditorías (3.3) para asegurarse de la objetividad y la imparcialidad del proceso (3.26) de auditoría (3.3);
- d) asegurarse de que los resultados de las auditorías (3.3) se ponen en conocimiento del órgano de gobierno (3.22) y de la alta dirección (3.2), así como de otras áreas o funciones cuando proceda a efectos de mejorar la prevención penal; y
- e) conservar información documentada (3.14) como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías (3.3).

Estas auditorías (3.3) deben ser razonables, proporcionadas y realizadas con un enfoque basado en el riesgo (3.28), siguiendo procesos (3.26) de auditoría (3.3) interna u otros procesos (3.26) de revisión de procedimientos (3.25), controles y sistemas destinados a detectar indicios de:

- 1) materialización de riesgos penales (3.29);
- 2) no conformidades (3.18) relacionadas con la política de *compliance* penal (3.24) y el resto del sistema de gestión de *compliance* penal (3.31);
- 3) fallos en el cumplimiento de los requisitos (3.27) de *compliance* penal (3.5) susceptibles de constituir riesgos penales (3.29) para la organización (3.20) por las conductas desarrolladas tanto por el personal como por las partes asociadas; y
- 4) debilidades o posibilidades de mejora en la política de *compliance* penal (3.24) o el resto del sistema de gestión de *compliance* penal (3.31).

Para asegurar la objetividad y la imparcialidad de estos programas de auditoría (3.3), la organización (3.20) se debe asegurar de que estas auditorías (3.3) se llevan a cabo por:

- una función independiente o una persona en la organización (3.20) específicamente designada para realizar este proceso (3.26);
- el órgano de *compliance* penal (3.21), excepto si el alcance de la auditoría (3.3) incluye procedimientos (3.25) o controles de cuya ejecución directa se ocupe el propio órgano de *compliance* penal (3.21);
- una persona apropiada de un departamento o función distinta del que está siendo auditado;
- una tercera parte apropiada; o
- un grupo que comprenda cualquiera de los definidos en los cuatro puntos anteriores.

El proceso (3.26) debe asegurar que ningún auditor está auditando su propia área de trabajo o el trabajo desarrollado por él previamente.

9.3 Revisión por el órgano de *compliance* penal

Como resultado de las actividades de supervisión, el órgano de *compliance* penal (3.21) debe evaluar de forma periódica si el sistema de gestión de *compliance* penal (3.31):

- a) es adecuado para gestionar eficazmente los riesgos penales (3.29) de la organización (3.20); y
- b) está siendo eficazmente implementado.

El órgano de *compliance* penal (3.21) debe informar al órgano de gobierno (3.22) y a la alta dirección (3.2), o a una comisión o comité delegado de éstos, a intervalos planificados o siempre que sea necesario, sobre la adecuación e implementación del sistema de gestión de *compliance* penal (3.31), incluyendo los resultados de las investigaciones y las auditorías (3.3).

La organización (3.20) debe conservar información documentada (3.14) como evidencia de los resultados de las revisiones realizadas por el órgano de *compliance* penal.

NOTA 1 La frecuencia de los informes dependerá de los requisitos (3.27) de la organización (3.20), pero se recomienda que sea, al menos, anual.

NOTA 2 Una organización (3.20) puede servirse de otra organización (3.20) para asistir en la revisión, siempre que sus observaciones sean comunicadas de forma apropiada al órgano de *compliance* penal (3.21).

9.4 Revisión por la alta dirección

Con base en información remitida por el órgano de *compliance* penal (3.21) sobre la adecuación e implementación del sistema de gestión de *compliance* penal (3.31), incluyendo los resultados de las investigaciones y las auditorías (3.3), la alta dirección (3.2) debe realizar, a intervalos planificados, una revisión del sistema de gestión de *compliance* penal (3.31) de la organización (3.20).

Esta revisión debe considerar:

- a) el estado de las acciones de las revisiones por la dirección previas;
- b) los cambios en las cuestiones externas e internas que afecten al sistema de gestión de *compliance* penal (3.31);
- c) la información sobre el desempeño (3.9) del *compliance* penal (3.5), incluidas las tendencias relativas a:
- no conformidades (3.18) y acciones correctivas (3.1),
 - seguimiento (3.30) y resultados de las mediciones (3.15),
 - resultados de la auditoría (3.3),
 - investigaciones,
 - denuncias,
 - análisis informes de *compliance* penal,
 - comunicaciones relacionadas con las partes interesadas (3.23), incluyendo las reclamaciones,
 - la naturaleza y la extensión del riesgo penal de la organización,

- d) las oportunidades de mejora continua (3.16), tanto de la política de *compliance* penal (3.24) como del resto del sistema de gestión de *compliance* penal;
- e) la adecuación de los protocolos o procedimientos (3.25) de *compliance* penal (3.5);
- f) el grado en el que se han cumplido los objetivos de *compliance* penal (3.19);
- g) la adecuación de los recursos asignados al *compliance* penal (3.5);
- h) la eficacia (3.11) de las acciones adoptadas para gestionar los riesgos penales (3.29) y las oportunidades.

El resultado de la revisión realizada por la dirección debe incluir las decisiones relacionadas con las oportunidades de mejora continua (3.16) y cualquier necesidad de cambio, tanto en la política de *compliance* penal (3.24) como en el resto del sistema de gestión de *compliance* penal (3.31).

Debe incluir también decisiones acerca de:

- 1) la necesidad de cambios en las políticas, procedimientos (3.25) o controles asociados al sistema de gestión de *compliance* penal (3.31);
- 2) cambios de los procesos (3.26) y procedimientos (3.25) relacionados con el *compliance* penal (3.5) para asegurar su integración eficaz con las prácticas operacionales y sistemas de la organización (3.20);
- 3) áreas sobre las que hacer seguimiento (3.30) de no conformidades (3.18) futuras potenciales;
- 4) acciones correctivas (3.1) respecto a las no conformidades (3.18) detectadas;
- 5) lagunas o carencias en la política de *compliance* penal (3.24), en el resto del sistema de gestión de *compliance* penal (3.31) e iniciativas de mejora continua (3.16), tanto a corto como a medio y largo plazo;
- 6) reconocimiento de comportamientos ejemplares relacionados con la política de *compliance* penal (3.24) y el resto del sistema de gestión de *compliance* penal (3.31) de la organización (3.20).

La organización (3.20) debe conservar información documentada (3.14) como evidencia de los resultados de las revisiones realizadas por la dirección, debiéndose facilitar una copia al órgano de gobierno (3.22).

NOTA La revisión del sistema de *compliance* penal (3.31) realizado por la alta dirección (3.2) ha de entenderse como el proceso (3.26) por el cual, con base en el resultado de la revisión del sistema de *compliance* penal (3.31) realizado por el órgano de *compliance* penal (3.21), la alta dirección (3.2) analiza la información disponible y adopta las decisiones oportunas para la efectiva implantación y ejecución de los controles y medidas necesarios para el adecuado funcionamiento del sistema de *compliance* penal (3.31) en la organización (3.20).

9.5 Revisión por el órgano de gobierno

El órgano de gobierno (3.22) se debe encargar de examinar periódicamente el sistema de gestión de *compliance* penal (3.31) con base en la información proporcionada por el órgano de *compliance* penal (3.21), la alta dirección (3.2) y cualquier otra información que el órgano de gobierno (3.22) pueda solicitar u obtener.

La organización (3.20) debe conservar el resumen de la información documentada (3.14) como evidencia de los resultados de las revisiones del órgano de gobierno (3.22).

10 Mejora

10.1 No conformidades y acciones correctivas

Cuando se detecte una no conformidad (3.18), la organización (3.20) debe:

- a) Reaccionar de manera rápida y transparente. Asimismo, en la medida que sea aplicable:
 - adoptar las acciones oportunas para tomar el control de la situación y corregirla, y
 - gestionar las consecuencias, tratando de reducir sus efectos adversos.
- b) Valorar la necesidad de acciones de mejora para eliminar las causas que han ocasionado la no conformidad (3.18), de modo que no se reproduzca. Para ello debe:
 - analizar la no conformidad (3.18),
 - determinar sus causas,
 - averiguar si pueden estar produciéndose otras no conformidades (3.18) similares o si podrían llegar a producirse.
- c) Implementar las acciones que sean precisas.
- d) Realizar el seguimiento (3.30) de las acciones adoptadas, de forma que se conozca su eficacia (3.11) o la necesidad de acciones adicionales.
- e) Realizar los cambios que sean precisos en la política de *compliance* penal (3.24) o el resto del sistema de gestión de *compliance* penal (3.31), en caso de que sea necesario.

Las acciones correctivas (3.1) deben ser apropiadas para evitar o mitigar las no conformidades (3.18) detectadas.

La organización (3.20) debe mantener información documentada (3.14) que acredite:

- 1) La naturaleza de las no conformidades (3.18) detectadas y las acciones que se hayan adoptado en relación con ellas.
- 2) Los resultados de las acciones correctivas (3.1) adoptadas.

10.2 Mejora continua

La organización (3.20) debe mejorar de forma continua (3.16) la sostenibilidad, adecuación y eficacia (3.11), tanto de su política de *compliance* penal (3.24), como del resto del sistema de gestión de *compliance* penal (3.31).

Anexo A (Informativo)

Relación de la Norma UNE 19601 con el Código Penal español

El siguiente cuadro señala los apartados de la Norma UNE 19601 que se encuentran directamente relacionados con los requisitos que establece el numeral 5 del artículo 31 bis del Código Penal español vigente en el momento de publicación de la norma

Artículo del Código Penal	Texto	Apartado de la norma UNE	Comentarios informativos
31 bis 5 numeral 1º	Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos	4.3. Determinación del alcance del sistema de gestión de <i>compliance</i> penal	Especialmente en lo referente a la consideración de los resultados de la evaluación de <i>riesgos penales</i> (3.29)
		5.2. Política de <i>compliance</i> penal Apartado c)	Relativo a la identificación de las actividades en cuyo ámbito puedan ser cometidos los delitos a prevenir
		6.2. Identificación, análisis y evaluación de riesgos penales	El apartado, en su conjunto y de manera general, guarda relación con identificar los riesgos penales que afectan a la organización
		8.2. Diligencia debida	Relativo al desarrollo de un análisis con el fin de identificar aquellas actividades en cuyo ámbito pueden materializarse riesgos penales (3.29), de acuerdo con el apartado 6.2
31 bis 5 numeral 2º	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.	5.1.1. Órgano de gobierno Apartado g)	Relativo al establecimiento de los procedimientos (3.25) que concreten el proceso (3.26) de formación de la voluntad de la organización (3.20), de toma de decisiones y ejecución de las mismas

Documento de Trabajo

Artículo del Código Penal	Texto	Apartado de la norma UNE	Comentarios Informativos
31 bis 5 numeral 3º	Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos	5.1.1. Órgano de gobierno Apartado c)	Relativo a la dotación al sistema de gestión de <i>compliance</i> penal (3.31) de los recursos financieros, materiales y humanos adecuados y suficientes
		5.1.3. Alta dirección Apartado c)	Relativo a la disponibilidad de los recursos adecuados y suficientes para la ejecución eficaz (3.11) del sistema de gestión de <i>compliance</i> penal (3.31)
		6.3. Objetivos de prevención de delitos y planificación para lograrlos Numeral 2)	Relativos a considerar qué recursos se precisarán, en el momento de planificar cómo lograr los objetivos de <i>compliance</i> penal (3.19). También en relación con la disposición de modelos de gestión de recursos financieros adecuados para impedir la materialización de los riesgos penales (3.29)
		8.3. Controles financieros	Relativo a la disposición de modelos de gestión de recursos financieros que contribuyan a prevenir, detectar o gestionar riesgos penales (3.29)
31 bis 5 numeral 4º	Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.	5.1.3. Alta dirección Apartado h)	Relativo a fomentar el uso de procedimientos (3.25) para la puesta en conocimiento de conductas potencialmente delictivas
		5.2. Política de <i>compliance</i> penal Apartado h)	Relativo a la obligación de informar sobre hechos o conductas sospechosas relativas a riesgos penales (3.29)
		8.8. Comunicación de incumplimientos e irregularidades	Relativo a canales de comunicación y procedimientos asociados con ellos
31 bis 5 numeral 5º	Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo	5.1.3. Alta dirección Apartado d)	Relativo a hacer cumplir, tanto interna como externamente, la política de <i>compliance</i> penal (3.24)
		5.2. Política de <i>compliance</i> penal Apartado k)	Relativo a exponer las consecuencias de no cumplir con los requisitos de la política de <i>compliance</i> penal (3.24) y del sistema de gestión de <i>compliance</i> penal (3.31)
		7.3.2.1. Diligencia debida común a todos los miembros de la organización Apartado d)	Relativo a la adopción de acciones disciplinarias proporcionales

Artículo del Código Penal	Texto	Apartado de la norma UNE	Comentarios informativos
31 bis 5 numeral 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	5.1.1. Órgano de gobierno (Apartado e)	Relativo a la evaluación periódica de la eficacia (3.11) del sistema de gestión de <i>compliance</i> penal (3.31)
		8.7. Gestión de deficiencias de los controles	Relativo a la adopción de medidas para remediar deficiencias de los controles, cuando se detectan
		9.2. Auditoría interna	Relativo al desarrollo de auditorías (3.3) sobre el sistema de gestión de <i>compliance</i> penal (3.34)
		9.3. Revisión por el órgano de <i>compliance</i> penal	Relativo al resultado de las actividades de supervisión del órgano de <i>compliance</i> penal (3.21) y la evaluación periódica del sistema de gestión de <i>compliance</i> penal (3.31)
		9.4. Revisión por la alta dirección	Relativo a la revisión del sistema de gestión de <i>compliance</i> penal (3.31) por parte de la alta dirección (3.2), sobre la base de la información remitida por el órgano de <i>compliance</i> penal (3.21) y el resultado de las auditorías (3.3) desarrolladas
		9.5. Revisión por el órgano de gobierno	Relativo al examen periódico del sistema de gestión de <i>compliance</i> penal (3.31) por parte del órgano de gobierno (3.22) con base en la información proporcionada por el órgano de <i>compliance</i> penal (3.21)
		10. Mejora	El apartado, en su conjunto y de manera general, guarda relación con las acciones de mejora ante no conformidades. En particular, su apartado e) se refiere a la introducción de cambios en la política de <i>compliance</i> penal (3.24) y el sistema de gestión de <i>compliance</i> penal (3.31) en estos escenarios

Documento de Trabajo

Anexo B (Informativo)

Diligencia debida

B.0 Generalidades

El objetivo de llevar a cabo procedimientos de diligencia debida (3.10) sobre los socios de negocio (3.32) o los miembros de la organización (3.17) es evaluar con mayor profundidad la naturaleza y el alcance de los riesgos penales (3.29) en aquellas actividades que presenten un riesgo penal (3.29) considerado mayor que bajo. Igualmente, estos procedimientos pueden actuar como controles preventivos y detectivos de posibles riesgos penales (3.29), aportando información útil a la organización (3.20) para la toma de decisiones.

La naturaleza, tipo y alcance de los procedimientos de diligencia debida (3.10) dependerán de factores tales como la capacidad para obtener la información necesaria por parte de la organización (3.20), el coste de obtención de dicha información y el nivel de riesgo penal (3.29) asociado.

Los procedimientos de diligencia debida (3.10) implantados por la organización (3.20) deberían ser consistentes para los mismos tipos o niveles de riesgo (3.28), requiriendo análisis más profundos y detallados para aquellos que supongan un mayor riesgo (3.28) para la organización (3.20).

B.1 Diligencia debida sobre socios de negocio:

Se requerirán diferentes tipos de análisis en función del tipo de socio de negocio (3.32), por ejemplo:

- Aquellos socios de negocio (3.32) con capacidad de actuar en nombre de la organización (3.20) suponen un mayor riesgo (3.28) para la misma que los proveedores de bienes o servicios desde la perspectiva de una potencial responsabilidad penal.
- El grado de influencia de la organización (3.20) sobre sus socios de negocio (3.32) también puede afectar al alcance de las averiguaciones. Por ejemplo, será más sencillo obtener información exhaustiva de los socios en una *joint venture* o de agentes comerciales de una organización (3.20) que de los clientes.

Los procedimientos de diligencia debida (3.10) sobre socios de negocio (3.32) pueden incluir, por ejemplo:

- envío de cuestionarios;
- búsqueda de información pública sobre el socio de negocio (3.32), sus accionistas y directivos;
- búsqueda del socio de negocio (3.32) en listas de entidades sancionadas;
- búsqueda en fuentes oficiales, judiciales, nacionales o internacionales;
- contratación de un tercero (3.33) especializado.

La organización (3.20) podría solicitar al socio de negocio (3.32) en cuestión información adicional en función de las respuestas proporcionadas.

Los procedimientos de diligencia debida (3.10) no son una herramienta perfecta. Un tercero (3.33) podría exponer a la organización (3.20) a una situación de riesgo (3.28) aun cuando no exista información negativa, del mismo modo que un tercero (3.33) para el que si exista información negativa podría no suponer riesgo (3.28) alguno para la organización (3.20). Sin embargo y en cualquier caso, los resultados obtenidos deberían ser analizados con atención y rigor, y la organización (3.20) debería valorarlos con base en la información y hechos objetivos de los que disponga. En definitiva, la intención es que la organización (3.20) realice consultas e indagaciones razonables y proporcionadas sobre sus socios de negocio (3.32), considerando las actividades que se van a llevar a cabo y el riesgo (3.28) inherente en las mismas, de modo que pueda contar con una valoración razonable del riesgo (3.28) al que se expone si entra en dicha relación de negocio.

B.2 Diligencia debida sobre el personal

Los procedimientos de diligencia debida (3.10) sobre candidatos a ser miembros de la organización (3.17), dependiendo de las funciones propuestas y el riesgo (3.28) asociado, podrían incluir:

- informar sobre la política de *compliance* (3.26) durante la entrevista, procurando obtener una opinión sobre si el candidato parece entender y aceptar la importancia de la misma;
- verificar la exactitud y veracidad de las cualificaciones del candidato;
- obtener referencias de los responsables del candidato en puestos de trabajo anteriores;
- tomar las medidas necesarias para asegurar razonablemente que la oferta de empleo no responde a la devolución de un favor injustificado proporcionado por el candidato en su empleo previo, o que la oferta de empleo al candidato no va destinada a garantizar un tratamiento favorable injustificado para la organización (3.20);
- identificar posibles conflictos de interés que presente el candidato, especialmente las relaciones del candidato con la administración o funcionarios públicos (3.13).

Anexo C (Normativo)

Información documentada mínima necesaria en un sistema de gestión de *compliance* penal

- a) El alcance del sistema de gestión de *compliance* penal (3.31) (4.3).
- b) La política de *compliance* penal (3.24) (5.2).
- c) La identificación, el análisis y la evaluación de riesgos penales (3.29), así como la metodología y criterios utilizados (6.2.5).
- d) Los objetivos de *compliance* penal (3.19) (6.3).
- e) La evidencia de la competencia (3.4) existente o adquirida en relación con el personal de *compliance* (7.3.1).
- f) La información acerca de la formación y otros recursos disponibles para mejorar su conocimiento en el ámbito del *compliance* penal (3.5) (7.4).
- g) La información que la organización (3.20) ha determinado como necesaria para la eficacia (3.11) del sistema de gestión de *compliance* penal (3.31) (7.6.1).
- h) La información documentada (3.14) de origen externo que la organización (3.20) ha considerado como necesaria para la planificación y operación del sistema de gestión de *compliance* penal (3.31) (7.6.3).
- i) La considerada necesaria para disponer de evidencias que soporten que los procesos (3.26), procedimientos (3.25) y controles se han llevado a cabo según lo planificado (8.1).
- j) La evidencia de los resultados del seguimiento (3.30) y medición (3.15), así como los informes de prevención (9.1.1).
- k) La evidencia de la implementación del programa de auditoría (3.3) y de los resultados de las auditorías (9.2).
- l) La evidencia de los resultados de las revisiones realizadas por el órgano de *compliance* penal (9.3).
- m) La evidencia de los resultados de las revisiones realizadas por la alta dirección (3.2) (3.21) (9.4).
- n) La evidencia de los resultados de las revisiones realizadas por el órgano de gobierno (3.22) (9.5).

Anexo D (Informativo)

Implementación del modelo de prevención penal en las filiales de la organización y en socios de negocio

La organización (3.20) debe considerar y evaluar la conveniencia de hacer extensiva la implementación del modelo de prevención penal en sus filiales sobre las que ejerza el control, así como en sus socios de negocio (3.32), ya que sus actividades podrían entrañar un riesgo (3.28) para la sociedad, resultando en una posible responsabilidad penal para la organización (3.20) en caso de comisión de delito por parte de la filial o del socio de negocio (3.32) en el contexto de su relación.

Puede considerarse que una organización (3.20) tiene el control sobre otra cuando directa o indirectamente controla su gestión y posee la mayoría de sus participaciones o sus derechos de voto. Del mismo modo, en relación a la participación en una *joint venture* o consorcio, se puede entender que una organización (3.20) ejerce el control si tiene la mayoría de los votos en el órgano de gobierno (3.22) o la mayoría de las acciones. En este sentido, el control no debe ser valorado, exclusivamente, en función del volumen de negocio que la organización (3.20) mantiene con sus socios. Es razonable esperar que la organización (3.20) que ejerce el control promueva la adopción de su modelo de prevención penal en sus sociedades controladas, o bien de un modelo propio y específico de las mismas, siempre considerando, en todo caso, la evaluación de la exposición al riesgo (3.28) fruto del análisis de riesgos llevado a cabo por la organización (3.20), conforme al punto 6.2.

En cuanto a las sociedades no controladas, si el análisis de riesgos (3.28) realizado por la matriz concluye que no existe riesgo (3.28), o el riesgo (3.28) asociado es mínimo, no sería necesario tomar medidas adicionales. Sin embargo, si se identifica un riesgo (3.28) mayor que bajo, se debería evaluar la conveniencia de implementar controles de prevención de delitos en dichas sociedades, que operen, al menos, en relación con las transacciones llevadas a cabo en el contexto de la relación con la misma. El objetivo de este requisito (3.27) es disminuir el riesgo (3.28) que puede entrañar para una organización (3.20) mantener relaciones de negocio con sus socios de negocio (3.32), promoviendo que sus contrapartes adopten medidas que disminuyan su exposición al riesgo (3.28).

Si no resulta viable para una organización (3.20) implantar controles que mitiguen el riesgo (3.28) de comisión de delitos en las sociedades o socios de negocio (3.32) no controlados, debería tener en cuenta este hecho como un factor negativo en su análisis de riesgo (3.28) o diligencia debida (3.10) de dicha relación de negocio. Este hecho no implica que la organización (3.20) no pueda llevar a cabo dicha relación o transacción, pero sí debería, sin duda, considerar que la sociedad o contraparte no controlada está expuesta a una probabilidad de comisión de algún delito que pudiera conllevar responsabilidad para la organización (3.20).

El hecho de que resulte viable o no la implementación de controles o modelos de prevención penal en las contrapartes no controladas depende de varias circunstancias, por ejemplo:

- generalmente será viable si la organización (3.20) tiene un grado de influencia significativo sobre la contraparte. Por ejemplo, si la organización (3.20) quiere contratar un agente para trabajar en su nombre para una transacción en particular, o a un subcontratista para un trabajo de alcance considerable, probablemente pueda requerir la implementación de controles de prevención de riesgos penales (3.29) como una condición para la contratación;

- podrá no resultar viable, sin embargo, cuando la organización (3.20) no cuente con la necesaria influencia sobre la contraparte, por ejemplo:
 - clientes,
 - subcontratistas o proveedores específicos propuestos por el cliente,
 - subcontratistas o proveedores que tengan un mayor poder de negociación que la organización (3.20) (un ejemplo sería cuando la organización compre material a un proveedor bajo las condiciones de compra del proveedor),
- podrá no resultar viable igualmente cuando la contraparte no cuente con los recursos o experiencia para implantar dichos controles.

El tipo de controles que la organización (3.20) debería requerir a sus contrapartes deberían ser razonables y proporcionales al riesgo (3.28), y dependerán de la naturaleza del socio así como del tipo de riesgo (3.28). Por ejemplo:

- en el caso de socios de negocio (3.32) con una valoración alta de riesgo (3.28) y un alcance del trabajo amplio y complejo, la organización (3.20) podrá requerir la implantación de controles equivalentes a los contemplados en esta norma UNE,
- en el caso de socios de negocio (3.32) de tamaño medio y con una valoración de riesgo (3.28) media, la organización (3.20) podrá requerir la implantación de unos controles mínimos en el contexto de su relación de negocio, como por ejemplo una política de prevención de delitos, formación a sus empleados, la existencia de un órgano de supervisión (órgano de *compliance* penal (3.21)), reporte, etc.;
- en el caso de socios de negocio (3.32) pequeños (por ejemplo, agentes o proveedores menores) la organización (3.20) puede requerir la realización de actividades de formación a personal en puestos relevantes, y la implantación de controles sobre transacciones claves y concretas, en el contexto de su relación de negocio.

Estos requerimientos deberían incluirse como condición para el establecimiento de la relación contractual, y podrían formar parte del propio contrato.

La organización (3.20) no está obligada a verificar el cumplimiento total de estos requisitos (3.27) de sus socios de negocio (3.32) no controlados. Sin embargo, debería adoptar las medidas necesarias y adecuadas para asegurarse de que el socio de negocio (3.32) cumple razonablemente (por ejemplo, requiriéndole para que le proporcione copias de sus políticas y procedimientos (3.25) más relevantes). En los casos de mayor riesgo (3.28) (por ejemplo, agentes) la organización (3.20) podría implantar medidas y procedimientos (3.25) de supervisión que pueden incluir flujos de reporte y auditorías (3.3).

La implementación de medidas de prevención penal requiere generalmente tiempo, por lo que la organización (3.20) debería conceder el tiempo necesario a sus socios de negocio (3.32) para implantarlas adecuadamente, pudiendo trabajar con ellos mientras tanto, aunque considerando la ausencia de dichas medidas durante ese periodo como un factor negativo en su análisis de riesgo (3.28) o diligencia debida (3.10).

Anexo E (Informativo)

Cláusulas contractuales

Determinadas cláusulas deberían ser requeridas en los contratos con socios de negocio (3.32) que supongan un riesgo (3.28) superior a bajo para la organización (3.20), cuando resulte viable, esto es, cuando la organización (3.20) tenga influencia suficiente sobre el socio de negocio (3.32) (por ejemplo, en la contratación de agentes o de proveedores para realizar un proyecto o trabajo de gran alcance). Estas cláusulas podrían incluir, entre otras, las siguientes provisiones:

- prohibir expresamente la comisión de delitos -tolerancia cero a los riesgos penales (3.29)-, tanto de manera directa como a través de terceros (3.33), en relación con la actividad contratada;
- exigir la existencia de un sistema de gestión de *compliance* penal (3.31) o equivalente a los efectos de dar eficacia (3.11) al punto anterior;
- contemplar el derecho de resolución de la relación contractual en caso de incumplimiento de lo indicado anteriormente o incumplimiento de lo establecido en el sistema de gestión de *compliance* penal (3.31).

En ocasiones, la organización (3.20) no tendrá suficiente influencia para incluir estas cláusulas en contratos con socios de negocio (3.32) con alto poder de negociación. Si finalmente se firma un contrato en ausencia de tales cláusulas, este hecho debería ser considerado como un factor en la evaluación del riesgo (3.28) que supone dicha contratación.

