

NOVEDADES DE LA PROYECTADA NORMA UNE 19601 PARA EL SISTEMA ESPAÑOL DE COMPLIANCE PENAL

Novedades de la proyectada Norma UNE 19601 para el sistema español de compliance penal

Este foro de actualidad tiene la finalidad de analizar las novedades introducidas por la proyectada Norma UNE 19601 sobre sistemas de gestión de riesgos penales, en su versión sometida a información pública en el BOE de 8 de febrero de 2017. Para ello, (i) se contextualizará la UNE 19601 en el panorama actual de compliance penal, (ii) se examinarán las especificidades de la Norma UNE 19601 y los requisitos de su articulado que no provienen estrictamente del artículo 31 bis del Código Penal español, y (iii) se concluirá con un breve detalle del proceso de auditoría que dará lugar, en su caso, a la emisión de una certificación de conformidad con la Norma UNE 19601.

Latest technical developments on Spain's criminal compliance system ex UNE 19601 standardized regulation

The objective of this article is to analyze the technical novelties brought by the project of standardized regulation UNE 19601 on criminal risks management systems (version published on 8 February 2017 for public consultation). This paper will (i) contextualize the UNE 19601 in the Spanish current criminal compliance scene; (ii) examine the regulation's specificities and explain the requisites that are not directly issued from article 31 bis of the Spanish criminal Code, and (iii) briefly explain the audit procedure that may conclude with a conformity certification, if successful.

PALABRAS CLAVE

Compliance, Cumplimiento, Penal, Normalización, UNE

KEY WORDS

Compliance, Criminal, Law, Standardization, ISO

Fecha de recepción: 31-5-2017

Fecha de aceptación: 3-6-2017

COMPLIANCE, BUEN GOBIERNO CORPORATIVO Y DERECHO PENAL

La *compliance* penal hizo una tímida pero trascendental aparición en 2010, y las vicisitudes posteriores demuestran que había llegado para quedarse.

Antes de entrar en materia, parece prudente comenzar por clarificar el concepto, pues la amplitud de lo que engloba el término *compliance* en su sentido literal tiende a difuminar su contenido, que necesita ser tangible para ser útil. La *compliance* o cumplimiento normativo es y debe ser un *desideratum* predicable de todos los que conforman la sociedad, individuos o agentes como las personas jurídicas y los organismos que, sin personalidad, funcionan de tal manera que su impacto trasciende la individualidad de quienes los componen. Sin embargo, aunque el cumplimiento normativo es exigible a personas físicas y jurídicas por igual, el término *compliance* en su acepción técnico-jurídica no se refiere al comportamiento de los seres humanos —o no de forma directa—, sino al de las personas jurídicas y entes sin personalidad. A modo de ejemplo, el concepto de *compliance* fue definido en 2015 por la OCDE como «las funciones, recursos y procedimientos implementados por una compañía para cumplir con las leyes y regulaciones que le son aplicables» (traducción libre de la definición contenida en la p. 9 del informe llamado *Corporate Governance and Business Integrity. A Stocktaking of Corporate Practices*).

La importancia de las empresas en la configuración de nuestra realidad y la evidencia de su huella en la economía contemporánea puso sobre la mesa la necesidad de convertirlas en sujetos normativos de primer orden, bajo el mismo título que las personas físicas. Los fallos puestos de manifiesto por casos como Enron / Worldcom hicieron tambalear los fundamentos de la economía liberal, construida sobre premisas que fueron reconsideradas a la luz de las nefastas distorsiones del mercado creadas por determinados comportamientos anticompetitivos y fraudulentos. Con ello se inició un proceso de atribución de responsabilidades jurídicas que debía superar las obligaciones formales a que las empresas estaban sometidas y que hasta entonces pretendían gobernar los grandes hitos de su existencia: creación e inscripción, obligaciones genéricas de actuación en el tráfico jurídico, insolvencia, liquidación y muerte. Se trata de una tendencia que ha pervivido hasta ahora, como puede extraerse fácilmente de las tres primeras frases del *Yates Memo*, de 9 de septiembre de 2015: «*Fighting corporate fraud and other misconduct is a top priority of the Department of Justice. Our nation's economy depends on effective enforcement of the civil and criminal laws that protect our financial system and, by extension, all our citizens*».

El primer paso en la normalización de la actividad corporativa recayó en las entidades financieras, pero la intensidad de esta tendencia creció de for-

ma exponencial con el diseño de las obligaciones anticorrupción derivadas de la *Foreign Corrupt Practices Act* («FCPA») estadounidense desde finales de los años 70. El impacto de esta ley en la homogeneización normativa internacional ha sido evidente, no solo como consecuencia de la extraterritorialidad de sus disposiciones, sino también del consenso global que ya entonces la arropaba, y que resulta manifiesto a través del florecimiento de normas de *soft law* tales como las Reglas de conducta de la Cámara de Comercio Internacional para combatir la extorsión y la corrupción (cuya génesis se remonta a 1977) o la posterior Convención de la OCDE para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales (1997). Con ello, las personas jurídicas no solo ocuparon el foco regulatorio (contable y financiero), sino que se fueron evidenciando como sujetos directos idóneos de las disposiciones de carácter jurídico-penal, en un ámbito material que se ha ido dilatando con el paso del tiempo.

La idea subyacente a esta nueva regulación no fue que las empresas respondieran de forma objetiva por los efectos dañosos derivados de su actividad, como ocurre en materia de productos defectuosos, sino impulsar su autorregulación y su organización responsable. Decía al inicio de este artículo que la *compliance* no se refiere directamente al comportamiento humano, pues sus obligaciones tienen por destinatario a la persona jurídica, pero es evidente que son los individuos que la componen los que deberán ejecutarlas. Y, para permitir la correcta organización interna de la persona jurídica y su fiscalización por terceros, deberán documentar su diligencia en programas de cumplimiento o *compliance programs*. Con ellos ha cristalizado el concepto de *compliance* (penal) y los sistemas de gestión de riesgos penales a los que está dedicado este artículo.

La *compliance* penal no se agota con el cumplimiento de las disposiciones de carácter penal, pero estas, sin duda, aglutinan los conceptos esenciales de los que se nutren los compromisos corporativos. No está pensada para escudar a la persona jurídica de responsabilidad penal —tampoco en España; ya lo adelantaba la Fiscalía General del Estado en su Circular 1/2016—, sino para fomentar una organización responsable e inspirar la ética de los negocios en cada uno de los actos que realicen las personas físicas que componen la compañía. En este sentido, la *compliance* y el buen gobierno corporativo son conceptos cuyos ámbitos se superponen parcial-

mente: el primero está centrado en el cumplimiento legal, el segundo tiende más genéricamente hacia la transparencia y la sostenibilidad de la actividad económica empresarial, pero ambos comparten un interés por el asentamiento de ética corporativa. Y esta, inevitablemente, llama a la doctrina penal como materia que reúne el mayor consenso sobre el bien y el mal, lo que está permitido y lo que no, lo que es ético y lo que no lo es.

No debemos perder de vista que, en la realidad globalizada en la que nos desenvolvemos, la *compliance* y el buen gobierno corporativo son tanto más deseables cuanto más internacionalmente aceptados e implementados. Y, si aún es tarea pendiente encontrar un concepto de «ética fundamental» cuyo contenido sea admisible por todo ser humano, con más razón lo es hallar un consenso respecto de lo que constituyen prácticas empresariales deseables a nivel global. No sorprende, así, que las normas con vocación internacional extraigan sus criterios *de minimis* de la regulación jurídico-penal, abriendo la puerta a que esta disciplina sea la que rijan la organización e implementación de los sistemas de cumplimiento de las personas jurídicas. Esta interdependencia entre *compliance*, buen gobierno corporativo y Derecho penal queda perfectamente ilustrada en la conclusión alcanzada por D. Ángel Gurría, entonces Secretario General de la OCDE, el 2 de diciembre de 2014: «*The prevention of business crime should be at the centre of corporate governance*».

Sin duda, la Norma UNE 19601 sobre Sistemas de Gestión de *Compliance* Penal se inscribe en esta tendencia a la homogeneización de estándares y buenas prácticas. Para ello, desarrolla las particularidades de la *compliance* penal en España partiendo de los criterios y estructura sentados en 2015 por la Organización Internacional para la Normalización («ISO») en su genérica norma 19600 sobre Sistemas de Gestión de *Compliance* y replicados desde entonces, por ejemplo, en la ISO UNE 37001.

Cabe subrayar la solidez progresiva que ha adquirido el consenso internacional sobre la necesidad de mundializar estándares, y que queda perfectamente ilustrada con un rápido vistazo a los miembros de ISO: 162 entidades nacionales de normalización, correspondientes a 162 países. Con sus normas, ni vinculantes ni de carácter legal, ISO y UNE ponen al alcance de las empresas el poder alinearse con estándares globalmente aceptados de todo tipo, sin necesidad de esperar al dictado de detallada regulación legal sectorial.

LA NORMA UNE 19601 (versión sometida a información pública en el BOE de 8 de febrero de 2017)

Consideraciones generales sobre la Norma

La UNE 19601 viene a colmar una laguna característica de la *compliance* penal española, que nació huérfana de directrices que canalizaran las incertidumbres de las corporaciones en cuanto a la implementación de las disposiciones del Código Penal. No ha sido esta la tendencia en otros países en los que se han impuesto obligaciones de autocontrol a las empresas: la FCPA viene acompañada de la *resource guide* emitida conjuntamente por la División Criminal del Departamento de Justicia y la División de Ejecución de la Comisión de Bolsa y Valores de Estados Unidos; el Decreto Legislativo 231/2001 italiano del que bebe directamente nuestro artículo 31 bis CP vino de la mano de las *linee guida* emitidas poco después por Confindustria, y la UK *Bribery Act* dispone de una *guidance ad hoc*. Sin embargo, el Código penal español fue modificado en 2010 y de nuevo en 2015 sin apoyo adicional, ya fuera legal, regulatorio o en forma de buenas prácticas que permitieran a las empresas traducir a nivel operativo las expectativas importadas e impuestas por el artículo 31 bis del Código Penal.

Puesto que la Circular 1/2016 contenía una negativa expresa a llenar ese vacío, la Norma UNE 19601 será la primera guía española sobre gestión corporativa de riesgos penales. Es fruto del debate y del consenso alcanzado en el seno del subcomité técnico número 307 de la Agencia Española de Normalización y Certificación (AENOR), que se dedica a la normalización en materia de gestión de riesgos vía el establecimiento de directrices de diseño e implantación de sistemas corporativos para ello. En el seno del Subcomité 1 han participado, además del personal de AENOR, diversos grupos de interés como empresas nacionales y juristas, cuyo proyecto ha sido posteriormente sometido a información pública por un plazo de 40 días naturales, finalizado el 20 de marzo de 2017. La posibilidad de participación de grupos de interés públicos y privados en la redacción inicial de la norma y en su enmienda pretende asegurar que la redacción definitiva responderá a todas las inquietudes esenciales de quienes deban interactuar con los modelos de prevención de riesgos, ya sea en su creación, monitorización o fiscalización. Tras la revisión de los comentarios recibidos y, en su caso, de la modificación del texto de la proyectada norma, la UNE

19601 estará disponible con el objetivo de guiar a las empresas en el diseño, implementación y ajuste de sus sistemas de prevención de riesgos penales a la regulación internacional y a la legislación española. Nótese que el presente foro de actualidad ha sido redactado sobre el articulado sometido a información pública y, por tanto, no definitivo.

Como veremos, la Norma UNE 19601 no solo tiene sus raíces en los artículos que el Código Penal español dedica a la responsabilidad penal de la persona jurídica —31 bis y siguientes, que han demostrado ser excesivamente parcos—, sino que ha incluido en sus recomendaciones diversas prácticas de Derecho comparado, sugerencias provenientes de organizaciones internacionales y parte de las propuestas conceptuales que la Fiscalía General del Estado plasmó en su Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

Pese a tener un ámbito de aplicación material y geográficamente restringido, la UNE 19601 ha sido construida siguiendo una estructura globalmente aceptada en relación con los sistemas de gestión de riesgos de todo tipo. La estructura de la norma española proviene de la ISO 19600, dedicada a la gestión de riesgos genéricos, lo que permitirá a las empresas que ya hayan incorporado sus disposiciones en otros ámbitos (p. ej., riesgos laborales) ampliar su estructura a los riesgos penales sin dificultades añadidas.

Pese al título de la Norma UNE 19601, en el que se hace mención a la existencia de «requisitos» en su contenido, cabe resaltar que no se trata en su gran mayoría de elementos cuya necesidad provenga de la ley o cuya ausencia conduzca *per se* la ineficacia de un modelo de organización y gestión, pues las normas ISO o UNE no establecen requisitos legales —ni pueden hacerlo—. A salvo de las prescripciones incorporadas directamente del artículo 31 bis CP, los requisitos a los que se alude solo pueden referirse al carácter certificable de la norma y tendrán como efecto el otorgamiento o rechazo de la certificación del modelo conforme al articulado de la UNE 19601, en caso de ser solicitada.

Precisamente porque la Norma UNE 19601 contiene recomendaciones de seguimiento voluntario y parámetros de guía general, su lectura debe ser flexible y su implementación debe seguir lo que podríamos conceptualizar como un principio laxo de «cumplir o explicar», cuyo anclaje internacional es ya pacífico y ha sido incorporado en España, por

ejemplo, en el Código de Buen Gobierno de las Sociedades Cotizadas emitido por la Comisión Nacional del Mercado de Valores. El carácter genérico de su contenido deriva directamente de su voluntad de ser un «marco de referencia completo» para todo tipo de organizaciones, en cualquier sector de actividad. Sus previsiones, que son una orientación para la implementación de sistemas de gestión de riesgos penales, no deberían ser trasladadas sin más. La premisa de eficacia, nuclear en el concepto mismo de *compliance* y reflejada de forma expresa en el artículo 31 bis CP, requiere que la Norma UNE 19601 sea ajustada a las particularidades de cada sociedad o grupo de forma que su sistema de gestión de riesgos penales acabe estando hecho a medida.

La eficacia del sistema y la inexistencia e inexigibilidad del riesgo cero

Ni que decir tiene que la implementación de las directrices establecidas en la UNE 19601 dará visibilidad a los esfuerzos de las empresas en cuanto a *compliance*, pero no será siempre una condición suficiente para la eficacia del sistema. Aunque esta no debería medirse exclusivamente en relación con la aplicación de la exención de responsabilidad penal de la persona jurídica, pues la señal más clara de eficacia del sistema sería la inexistencia de comportamiento que diera entrada a la jurisdicción penal, la relación entre eficacia y exención convierte a esta última en un parámetro muy útil de medición de la robustez del sistema. En efecto, en el indeseable caso de que se cometiera un delito que generara la responsabilidad penal de la persona jurídica ex artículo 31 bis CP, un modelo eficaz debería conducir a la aplicación de la exención de responsabilidad penal corporativa en los estadios preprocesal (por el Ministerio Fiscal) o procesal (en el seno del proceso penal). Así, podremos tener un sistema teóricamente eficaz si, *ex ante*, un análisis de su estructura y contenido permite concluir que sus disposiciones conllevarían la aplicación de la exención para la persona jurídica. Pero, como decíamos, no bastará con que el sistema cumpla con lo establecido en la norma UNE 19601 para ser eficaz. Según puede leerse en su propia introducción, «esta norma UNE no brinda una garantía absoluta de eliminación del riesgo de comisión de delitos que afronta una organización» y, por supuesto, «no asegura la exoneración o atenuación automática de la responsabilidad penal de la persona jurídica». Lo que sí asegura el cumplimiento de los principios y reco-

mendaciones de la UNE 19601 es la obtención de una certificación de conformidad con ella, que podrá ser exhibida en un procedimiento judicial a los efectos de acreditar los más altos estándares de diligencia organizativa de la compañía. Y el elevado grado de exigibilidad de dichos estándares es, en el estado actual de la técnica (reflejado en una norma UNE), lo más próximo a un sistema de cumplimiento eficaz.

Pese al consenso internacional sobre la imposibilidad de exigir la reducción del riesgo penal a cero, esta obviedad todavía no había sido plasmada de forma expresa en nuestro sistema jurídico, posiblemente a causa del escepticismo que parece tener la Fiscalía respecto a la capacidad de las empresas de organizarse en clave ética. Precisamente por ello, resulta refrescante la nota que la Norma contiene en su epígrafe 4.4, según la cual «[n]o es posible eliminar completamente el riesgo penal, y no puede pedirse a ningún sistema de gestión de compliance penal que sea capaz de prevenir, detectar y gestionar todos los riesgos penales».

¿Qué valor tendrá la certificación de conformidad con la UNE 19601? ¿Qué debo tener en cuenta para certificar mi sistema de prevención de riesgos penales?

La certificación, expedida tras el correspondiente proceso de auditoría, constituirá un elemento indiciario que ilustrará al Ministerio Fiscal, Juez o Tribunal sobre (i) las medidas adoptadas por la empresa para organizarse de forma ética y transparente, y (ii) el nivel de diligencia de sus dirigentes respecto a la prevención de criminalidad corporativa. Como tal elemento indiciario, deberá ser valorado en conjunto con el resto de indicios obrantes en las actuaciones judiciales siguiendo el criterio de la sana crítica racional. Esta conclusión ya fue adelantada por la Fiscalía General del Estado en su Circular 1/2016, con las siguientes palabras: «[l]as certificaciones sobre la idoneidad del modelo expedidas por empresas, corporaciones o asociaciones evaluadoras y certificadoras de cumplimiento de obligaciones, mediante las que se manifiesta que un modelo cumple las condiciones y requisitos legales, podrán apreciarse como un elemento adicional más de su observancia pero en modo alguno acreditan la eficacia del programa, ni sustituyen la valoración que de manera exclusiva compete al órgano judicial» (p. 52 *in fine*).

En todo caso, es premisa para que la certificación tenga valor de conformidad con la UNE que sea

otorgada por un ente independiente de la empresa o grupo de empresas sobre la(s) que recae la certificación, lo que inhabilita al asesor que haya participado en el diseño e implementación del sistema de gestión de riesgos penales para emitirla. Esta cuestión podría parecer no tener más relevancia que la meramente logística, pero lleva implícita la necesidad de documentar las razones que respaldan todas y cada una de las decisiones tomadas en relación con el sistema de prevención de riesgos penales, lo que facilitará la auditoría posterior. En la práctica, resulta habitual que el órgano de administración o el órgano de supervisión adopten decisiones tras recibir el *input* de los asesores externos, sin que ello venga siempre respaldado por un documento que exteriorice las razones jurídicas y operativas que sustentan la decisión final.

Por ello, las empresas que empleen la Norma UNE 19601 como guía previa a la certificación deberán disponer de la justificación documentada de las particularidades de su sistema de gestión de riesgos, que resultan inevitables a la vista de que el concepto de eficacia requiere la tenencia de un sistema a medida. Así, los auditores deben ser capaces de comprender la *ratio essendi* de los riesgos incluidos y excluidos del mapa de riesgos, de aprehender las decisiones que gobernaron la definición del ámbito de aplicación del sistema (p. ej., exclusión de una de las ramas de actividad de la cobertura del sistema) o la atribución de determinadas obligaciones de reporte a la alta dirección y no al órgano de supervisión. En otras palabras, para que el proceso de auditoría y certificación sea fluido resultará fundamental que la organización pueda proporcionar información documentada que acredite por qué su sistema de prevención de riesgos penales está perfectamente adaptado a sus circunstancias operativas y organizativas.

A mi juicio, el epígrafe introductorio de la Norma UNE 19601 ha incluido un último guiño a la Circular 1/2016 al remarcar que las posibilidades de defensa de la persona jurídica y de exoneración de su responsabilidad penal no se circunscriben a la tenencia de un sistema certificado conforme a la UNE 19601: «[h]a 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» (p. 5). Con ello, la Norma parece hacer una velada referencia a la única causa que conllevará en todo caso, según la Fiscalía General del Estado, la

solicitud de aplicación de la exención: la autodenuncia de la persona jurídica (p. 54 de la Circular 1/2016). Y es que el foco jurídico penal parece estar retornando a su sujeto inicial, la persona física, como claramente indica el *U.S. Attorney's Manual* tras la inclusión de las directrices impulsadas por Sally Q. Yates en su memorándum de 9 de septiembre de 2015 sobre la responsabilidad individual por la delincuencia corporativa: «[o]ne of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing».

ANÁLISIS DEL ARTICULADO DE LA NORMA UNE 19601

Ámbito de aplicación del sistema de gestión de riesgos penales (Bloque n.º 4)

El primer epígrafe con contenido normativo de la UNE 19601 (Contexto de la organización) tiene el objetivo de guiar a las empresas en la definición del ámbito de aplicación de su sistema de gestión de riesgos penales. Para ello, la organización deberá decidir, justificar y documentar qué entes están sometidos al sistema, lo que resulta relevante en esquemas societarios complejos o en organizaciones dedicadas a una variedad de actividades operativas divididas en ramas.

La flexibilidad en la implementación de la Norma, a la que hemos aludido anteriormente, encuentra sus únicas fronteras en la razonabilidad y la eficacia de las decisiones adoptadas, cuya ausencia se erigirá como barrera al otorgamiento de la certificación de conformidad. *A priori*, y salvo que existieran motivos en un caso concreto para sostener lo contrario, parecería razonable disponer de un solo sistema de gestión para un mismo grupo de sociedades en España o incluir todas las ramas de actividad bajo la cobertura del modelo, pero no cabe descartar *ex ante* la existencia de una justificación satisfactoria a la implementación de otro sistema.

Aun así, a mi entender existen situaciones cuya justificación aparece como prácticamente imposible —por contravenir frontalmente la intención del legislador penal y el consenso internacional sobre la vocación de la *compliance* para crear un entorno de confianza y transparencia— como, por ejemplo, la exclusión de una de las sociedades o rama de actividad de cualquier sistema de gestión de riesgos penales, o la no vinculación de los terceros contratados por la persona jurídica a sus pre-

visiones éticas más básicas (generalmente, el código de conducta). Y ello porque la voluntad del legislador es fomentar un cambio de paradigma en el que carecer de un sistema de prevención de riesgos penales constituya una rareza. Si esto fuera así, la empresa que careciera de modelo se vería presionada por sus socios de negocio a adoptarlo y, en caso contrario, podría llegar a ser expulsada de su sector de actividad por no alcanzar los estándares mínimos establecidos por el mercado. En este panorama, resulta difícilmente justificable no solo carecer de un *compliance program*, sino también excluir una parte del grupo o un grupo de interés, lo que parece constituir una deliberada vía de escape. Así, cuando un grupo de sociedades haya implementado más de un sistema de prevención de riesgos penales para cubrir a sus sociedades miembros, deberá disponer de un documento que desgane perfectamente las razones por las que ello lo dota de mayor eficacia que un sistema unificado.

En buena lógica, el ejercicio de determinación del alcance del sistema de gestión de riesgos penales deberá realizarse en paralelo a la confección del mapa de riesgos y de forma consistente con su resultado, de manera que el sistema cubra todos los riesgos aparejados a la actividad corporativa. De lo contrario, podría ocurrir que la decisión sobre el ámbito de aplicación del sistema de gestión de riesgos deba ser revisada a la vista del resultado del análisis de riesgos penales. Lo que sucederá cuando, a raíz de dicho análisis, se detecte un riesgo que no había sido previsto y que aconseje incluir una determinada sociedad inicialmente excluida o una categoría concreta de terceros.

Política de compliance penal (Bloque n.º 5)

El epígrafe 5.2 de la Norma impone la necesidad de que el sistema de gestión de riesgos penales esté anclado en una «*política de compliance penal*» impulsada y aprobada por el órgano de gobierno de la sociedad. Dentro del contenido requerido por la UNE 19601 se encuentran compromisos genéricos y transversales (p. ej. el compromiso de todos los miembros de la organización con el cumplimiento normativo), directrices para salvaguardar la eficacia del sistema (p. ej. que la política sea congruente con los fines de la organización) y el detalle parcial de las reglas de *compliance* (p. ej., se deja constancia de la autonomía del órgano de supervisión y de la posibilidad de imponer sanciones disciplinarias

como consecuencia del incumplimiento del sistema de gestión de riesgos penales).

Si bien los elementos de esta política resultan consistentes con lo que se espera del órgano de administración en relación con la *compliance* penal, de la que debe ser impulsor por mandato del legislador penal (art. 31 bis.2.1ª CP), el formato que plantea la UNE 19601 resulta heterogéneo respecto a la práctica habitual. En efecto, el epígrafe hace referencia a la adopción por el órgano de administración de un solo documento que, además, tiene el rango de política —palabra cuyo sentido técnico no se le ha escapado al comité normalizador—.

Esta terminología parece hacer eco de la empleada por ISO en la norma 37001 sobre sistemas de gestión de los riesgos de cohecho y de corrupción en el sector privado, publicada en 2016. En efecto, la ISO 37001 expone en su introducción: «[a] *well-managed organization is expected to have a compliance policy supported by appropriate management systems to assist it in complying with its legal obligations and commitment to integrity. An anti-bribery policy is a component of an overall compliance policy*». La UNE 19601 define la «política de *compliance* penal» como la «*voluntad de una organización, según la expresa formalmente su alta dirección o su órgano de gobierno en relación con sus objetivos de compliance penal*». En ambos casos, el término «política» parece referirse a una intención corporativa más que a un documento en particular. Sin embargo, la redacción del epígrafe 5.2, en el que se detalla en contenido y formalidades de la política de *compliance* penal, puede inducir a confusión a este respecto en tanto en cuanto alude a ella exclusivamente en singular, sin prever la atomización de su contenido en varios documentos de distinto rango jerárquico. A continuación se listan los requisitos de esta política y se hace mención a la problemática que podrían presentar.

Según la Norma UNE 19601, la política de *compliance* penal debe:

- (i) Identificar las actividades corporativas que tienen aparejados riesgos penales [5.2 c)], lo cual es más propio del mapa y del análisis de riesgos, documentos específicos que no suelen tener rango de política.
- (ii) Minimizar la exposición de la organización a los riesgos penales [5.2 e)]. Requisito genérico que podría predicarse de cada uno de los elementos que componen el sistema, pero que parece más razonable exigir del sistema en su conjunto.

(iii) Exigir el cumplimiento de la legislación penal aplicable a la organización [5.2 a)], prohibir la comisión de hechos delictivos [5.2 d)], incluir el compromiso de cumplir con la política de *compliance* penal y con el sistema de gestión de riesgos penales [5.2 g)], imponer la obligación de informar sobre hechos que puedan constituir un incumplimiento del sistema de *compliance* y garantizar la ausencia de represalias al informante [5.2 h)] y exponer las consecuencias de los incumplimientos [5.2 k)]. Elementos todos ellos propios de un código ético o de conducta y no tanto de una política específica.

(iv) Incluir un compromiso con la mejora continua del sistema de gestión de *compliance* penal [5.2 i)] y explicitar la «*autoridad e independencia del órgano de compliance penal, si éste no coincide con el órgano de gobierno*» [5.2 j)].

En primer lugar, el normalizador amalgama aquí los conceptos de «autonomía» (exigido por el Código Penal del órgano de supervisión) y de «independencia», lo que resulta en un precepto de difícil implementación en la práctica. En efecto, pues el órgano de gobierno tiene como función indelegable la supervisión de los riesgos corporativos —*ex arts. 225, 249 bis y 529 ter 1b*) de la Ley de Sociedades de Capital, tras la introducción de la reforma que incluyó directrices de buen gobierno corporativo—, lo que implicará en todo caso el control de la actividad del aquí llamado órgano de *compliance* (que será, con ello, autónomo pero no independiente).

En segundo lugar, ambos requisitos parecen pertenecer más al ámbito del reglamento del órgano de supervisión de riesgos penales que al de una política.

Con todo, parece claro que la terminología empleada en este punto por el normalizador puede inducir a error, e incluso generar fallas de eficacia en el sistema, si no es correctamente interpretada e implementada. Por ello, tal vez hubiera sido oportuno disipar la posible confusión del lector añadiendo una nota aclaratoria al final del epígrafe 5.2.

En todo caso, el principio de flexibilidad en la implementación de la UNE 19601 arroja dos posibilidades: (i) la creación de una política que contenga los elementos establecidos en las letras a) a k) del epígrafe 5.2, ya sea de forma íntegra o por remisión. Esta opción no sería la más recomendable, ya que en ambos casos resultará en un documento

poco legible que, precisamente por ello, perderá eficacia y utilidad. O (ii), la incorporación de los elementos establecidos en las letras a) a k) del epígrafe 5.2 de forma atomizada en la estructura ética corporativa y, preferentemente, en las normas reseñadas *supra*.

Liderazgo, roles y responsabilidades respecto al sistema de gestión de riesgos penales (Bloque n.º 5)

El bloque 5 de la Norma UNE 19601 desgrana las responsabilidades que deberían tener los órganos de gobierno de la sociedad en relación con el sistema de gestión de riesgos penales. Además de los sujetos a los que el propio Código Penal hace referencia —órgano de administración y órgano de supervisión, que no tienen por qué ser entes o individuos distintos—, la UNE otorga una relevancia especial a la alta dirección.

La relevancia del «*tone from the top*» (motivar desde la cúspide) ya fue anunciada en la Circular 1/2016 como parámetro para medir si la *compliance* penal era efectivamente traducida de la teoría a la práctica, de una biblioteca de papel a un sistema de gestión de riesgos penales, de normas escritas a un sistema comprensible, coherente y con aplicación real. Con ello, la UNE 19601 se hace eco del consenso internacional respecto a la necesidad de involucrar activa y efectivamente a los directivos en la cultura ética corporativa, de forma que descienda de los más altos niveles jerárquicos e impacte de forma transversal en la operativa diaria.

Los requisitos establecidos respecto de la alta dirección en el epígrafe 5.1.3 constituyen manifestaciones diversas de un mismo concepto: lo que se espera de la alta dirección es que actúe como correa de transmisión entre los empleados y terceros, de un lado, y los órganos de administración y supervisión, de otro, al velar por el cumplimiento del sistema de *compliance* penal. En efecto, en un esquema societario teórico clásico:

(i) el órgano de administración define los objetivos operativos, la estrategia para alcanzarlos y controla que su ejecución se lleva a cabo de acuerdo con las pautas establecidas por él (tiempos, nivel de riesgo, etc.);

(ii) el órgano de *compliance* supervisa la correcta ejecución del sistema de gestión de riesgos, monitoriza cualquier necesidad de ajuste y lo propone formalmente, y

(iii) la alta dirección traslada los objetivos, la estrategia y las previsiones del sistema de cumplimiento a la operativa diaria.

La alta dirección es, en este esquema, el personal de mayor rango jerárquico en contacto diario con los procedimientos normalizados de trabajo, las medidas de control y con su ejecución por los empleados y colaboradores externos de la sociedad. Esa labor de relé resulta esencial en todo sistema corporativo de cumplimiento normativo, pues una gestión discordante con el contenido del código ético o con los parámetros de tolerancia al riesgo marcados por la cúspide de la compañía pueden dejar en jaque la integridad del sistema. Piénsese, por ejemplo, en la facilidad con la que podrían verse socavadas las normas que prohíben la corrupción entre particulares con un muy deficiente control de la alta dirección sobre el cumplimiento del *third party due diligence process*. La exposición de la Fiscalía General del Estado, en su Circular 1/2016, merece ser extractada por su contundencia y claridad: «[c]ualquier programa eficaz depende del inequívoco compromiso y apoyo de la alta dirección de la compañía. El comportamiento y la implicación del Consejo de Administración y de los principales ejecutivos son claves para trasladar una cultura de cumplimiento al resto de la compañía. Por el contrario, su hostilidad hacia estos programas, la ambigüedad, los mensajes equívocos o la indiferencia ante su implementación traslada a la compañía la idea de que el incumplimiento es solo un riesgo que puede valer la pena para conseguir un mayor beneficio económico. Si los principales responsables de la entidad incumplen el modelo de organización y de prevención o están recompensando o incentivando directa o indirectamente a los empleados que lo incumplen, difícilmente puede admitirse que exista un programa eficaz, que refleje una verdadera cultura de respeto a la ley en la empresa».

Es pacífico, pues, que la alta dirección resulta idónea para transmitir la importancia de respetar el sistema de prevención de riesgos penales, evaluar su cumplimiento por los empleados en su trabajo diario, detectar anomalías, fomentar el uso del buzón ético o identificar necesidades de mejora en los controles corporativos, funciones que le son encomendadas, entre otras, por este bloque de la Norma UNE 19601.

Sin embargo, las empresas no están obligadas a implementar el esquema tal y como se ha descrito. Pese a que resulta recomendable que el órgano de supervisión (o sus miembros, si es pluripersonal) carezca de funciones operativas u ostente la doble

condición de supervisor ético y de alto directivo, resulta frecuente que la supervisión de riesgos penales se haya atribuido a la dirección legal, a la dirección de auditoría o a la dirección financiera. En este caso, varias de las funciones encomendadas por la UNE 19601 a la alta dirección ya vendrán encomendadas por el sistema al órgano de supervisión.

La flexibilidad en la implementación de la Norma, en este caso, requerirá de un análisis de eficiencia que permita a la empresa asegurarse de que las responsabilidades asignadas en relación con la supervisión del modelo no entorpecen el trabajo de los individuos a quienes vienen encomendadas. Dicho lo anterior, parece que siempre que exista un contacto constante entre el órgano de supervisión y la alta dirección que asegure que esta realiza su labor de transmisión de información, las competencias establecidas por la UNE 19601 en su epígrafe 5.1.3 podrán estar encomendadas al órgano de supervisión sin que ello implique una merma en la eficacia del modelo. Antes al contrario, la elevación del empeño de funciones vitales para el control y actualización del modelo a un órgano tan próximo al Consejo de Administración como lo es el órgano de supervisión parecería potenciar la eficacia del modelo. Con una salvedad evidente: cuando el órgano de administración es también el órgano de *compliance* penal, disponer de visibilidad sobre la ejecución de la operativa corporativa diaria a través de la alta dirección parece ser no solo apropiado, sino necesario.

Con respecto a los órganos de administración y de supervisión, la Norma UNE 19601 desgrana funciones clásicas que no ofrecen una problemática particular y que, por ello, no serán analizadas en este foro de actualidad.

Por último, es preciso hacer una mención a otro actor fundamental en la *compliance*. Sin perjuicio de los roles y responsabilidades que la UNE 19601 asigna de forma nominativa al órgano de administración, al órgano de supervisión y a la alta dirección, su concepción del sistema de gestión de riesgos penales descansa en el respeto y cumplimiento por todos y cada uno de los miembros que componen la compañía (e incluso de determinados terceros). Resulta innegable la importancia de que los trabajadores y terceros estén comprometidos con el cumplimiento normativo, pues de lo contrario incluso el más férreo compromiso de los órganos de gobierno resultará baldío. Precisamente por ello, la Norma UNE 19601 hace expresa mención a la asig-

nación de responsabilidades de cumplimiento normativo en las descripciones de puestos de trabajo (*job descriptions*) [5.1.2.a)3)], yendo hasta exigir la existencia de «*sistemas de remuneración que valoren el logro de objetivos de compliance penal*» [7.1.i)]. Con ello, la norma mutualiza la obligación de cumplir con las normas del sistema de gestión de riesgos penales, responsabilizando a todos los miembros de la sociedad de forma que el comportamiento corporativo deviene el resultado de la suma de todas esas actividades individuales.

Identificación, análisis y valoración de riesgos penales (Bloque n.º 6)

La UNE 19601 no recoge ni introduce novedades sustanciales respecto a los mapas y análisis de riesgos, salvo en lo atinente al nivel de riesgo aceptable por la empresa, también denominado «*risk appetite*» en la comunidad internacional (*vid.* ISO 37001:2016(E), Appendix A.4, p.25). Pese a que la Circular 1/2016 de la Fiscalía General del Estado hacía referencia al «*nivel de riesgo global aprobado por la alta dirección de las entidades, y con los niveles de riesgo específico establecidos*» (p. 43 *in fine*), suele

ser una función atribuida al órgano de administración de la compañía, en tanto que responsable último de la gestión de riesgos y de la emisión de directrices para el cumplimiento de los objetivos sociales a corto, medio y largo plazo. Con una visión tal vez más pragmática que la FGE, la UNE 19601 parece aconsejar únicamente determinar el nivel aceptable para cada uno de los riesgos contenidos en el mapa, «*de manera que si el riesgo resultante del análisis realizado es superior a dicho umbral, la organización deberá implementar controles adicionales para reducir dicho riesgo*».

Así pues, resultará necesario que la compañía disponga de un mapa que identifique los riesgos penales inherentes a su actividad corporativa, analizados en abstracto y en concreto (es decir, atribuyéndoles un valor de riesgo calculado antes y después de tomar en consideración las medidas de mitigación adoptadas). Como hemos visto, la nota 1 del epígrafe 6.2.3 de la Norma UNE 19601 recomienda incluir una mención al nivel de riesgo aceptable por la empresa en cada caso. A modo de ejemplo, a los efectos de incluir toda esta información, el mapa de riesgos podría adoptar el formato de una tabla con las siguientes columnas:

Riesgo	Nivel de riesgo en abstracto	Medidas adoptadas	Nivel de riesgo en concreto	Nivel de riesgo aceptable	Necesidad de medidas adicionales
--------	------------------------------	-------------------	-----------------------------	---------------------------	----------------------------------

Tratándose de un documento que precisa estar en constante evolución, el objetivo de la persona jurídica no debería centrarse tanto en reducir al mínimo todos sus riesgos desde el primer momento como en conseguir, con el tiempo, que todos los riesgos identificados en la tabla resulten reducidos, mediante las medidas adoptadas, al nivel de riesgo previamente aceptado y de forma tal que la respuesta a la casilla de la última columna acabe siendo negativa.

Como tal elemento vivo del sistema de gestión de riesgos penales, el mapa de riesgos deberá ser revisado con carácter periódico, y cada vez que ocurra una circunstancia que lo aconseje. Pues bien, entre los sucesos enumerados por la UNE 19601 no solo se encuentran los referidos por el Código penal (p. ej., cambio significativo en la estructura societaria), sino también una mención a la existencia de cambios jurisprudenciales relevantes [6.2.4.d)] que puede ser muy difícil y costosa de implementar por las personas jurídicas de cualquier tamaño y que, por ello, puede resultar excesiva.

Además, la necesidad de disponer de información documentada sobre la «*identificación, análisis y evaluación de riesgos penales y de la metodología y criterios utilizados*» (epígrafe 6.2.5) implicará, en relación con su mapa de riesgos, que las empresas deberán proceder a especificar por escrito cuáles han sido los criterios tenidos en cuenta para:

- (i) determinar los riesgos incluidos y excluidos del mapa de riesgos;
- (ii) asignar el nivel de riesgo en abstracto y en concreto;
- (iii) priorizar y clasificar los riesgos;
- (iv) fijar el nivel de riesgo aceptable por el órgano de administración;
- (v) realizar el seguimiento de los objetivos de *compliance* establecidos (qué, quién, cuándo, cómo y con qué recursos), y
- (vi) medir su cumplimiento.

Se tratará de una justificación especialmente importante para aquellas empresas que quieran obtener la certificación de conformidad con la UNE 19601, pues será un elemento esencial para el análisis y evaluación del mapa de riesgos por los auditores externos.

Elementos de apoyo del sistema de gestión de compliance penal (Bloque n.º 7)

El Bloque 7 de la Norma UNE 19601 identifica los elementos que refuerzan la eficacia de las medidas establecidas documentalmente para gestionar los riesgos penales de la empresa. Se trata de:

(i) La cultura ética corporativa. En relación con ella, la UNE 19601 hace un notable esfuerzo por proporcionar ejemplos que permitan hacer de un elemento tan etéreo algo tangible. A la vista de la importancia que la Fiscalía General del Estado atribuía a la cultura ética en su Circular 1/2016 —aunque seriamente matizada por el Tribunal Supremo en su Sentencia 154/2016 de 29 de febrero—, la utilidad de la lista contenida en el epígrafe 7.1 no es menor.

(ii) Los recursos dedicados al cumplimiento normativo penal, que deben ser suficientes para satisfacer los objetivos de *compliance* fijados por el órgano de supervisión o de administración.

(iii) La idoneidad y competencia de los individuos que se dedican al *compliance* penal, previa o coetánea a la asignación de tales funciones, y el compromiso de todos los miembros de la organización con el cumplimiento del sistema de gestión de riesgos penales.

Para garantizar la idoneidad de los miembros clave de la compañía, la UNE 19601 requiere que sean seleccionados, trasladados o promocionados tras un procedimiento de diligencia debida tendente a asegurar su comprensión del sistema de gestión de riesgos penales y su compromiso con él. Con la finalidad de velar por la continuidad en el tiempo de esta idoneidad *prima facie*, además, la persona jurídica deberá impedir el otorgamiento o concesión de retribuciones económicas, fijas o variables, que no se adecúen al riesgo aceptable determinado por el órgano de administración o con el respeto del sistema de *compliance* penal en su conjunto.

(iv) La formación impartida y la información proporcionada sobre el sistema. En este aparta-

do, la Norma incide también sobre la oportunidad de alentar a los miembros de la organización a plantear sus dudas en relación con el sistema de gestión de riesgos penales, además de las denuncias de potenciales incumplimientos de los que sean conocedores. Se trata de una cuestión nuclear para el buen funcionamiento del modelo: la formulación de preguntas y la aportación de respuestas temporáneas por el órgano de supervisión (directa o indirectamente, a través de la alta dirección, en su caso) permitirá identificar redactados poco claros, necesidades de formación o fallos en el sistema, pudiendo dar lugar a su refuerzo antes incluso de que tenga lugar un incumplimiento. Sin duda alguna, se trata de sinergias altamente deseables que maximizarán la eficacia del sistema de gestión de riesgos penales.

(v) Un sistema de reportes claro y adecuado.

(vi) La integridad de la información. En este apartado se requiere la tenencia de medios técnicos que aseguren a la persona jurídica la trazabilidad de su información de *compliance* penal y protejan su integridad. Si bien no queda específicamente recogido en el texto de la Norma, esta parece tener en mente las medidas técnicas de sellado de tiempos o *time stamp*, a las que también hace referencia en el epígrafe 6.1 *in fine*, cuya popularidad va en aumento a nivel nacional.

Aunque no se hace mención específica al órgano de supervisión y al sistema de sanciones disciplinarias, ambos están acertadamente incluidos como subelementos de apoyo, como mecanismos claramente disuasorios de comportamientos contrarios al sistema de gestión de riesgos penales.

Supervisión del cumplimiento del sistema de gestión de riesgos penales (Bloque n.º 8)

Este bloque normativo está destinado a detallar las medidas que la persona jurídica debería implementar para asegurarse de que las disposiciones del sistema de gestión de riesgos penales están respaldadas por medidas de control eficaces que dificulten seriamente cualquier potencial incumplimiento. La empresa deberá establecer controles financieros y no financieros que recaigan sobre empleados, directivos, administradores, filiales y socios de negocio, para minimizar todos los riesgos identificados en el ámbito de aplicación del sistema.

Cuando sea conveniente, los controles deberán extenderse a terceros contratados para prestar un servicio a la compañía, siempre que su actuación pueda entrañar un riesgo penalmente relevante. Si bien se trata de sujetos no contemplados de forma específica por el artículo 31 bis CP, su inclusión como sujetos cuya actuación puede generar responsabilidad penal de la persona jurídica ya fue adelantada por la Circular 1/2016 de la Fiscalía General del Estado. Esta posibilidad es coherente con la dinámica adoptada por la normativa internacional en materia anticorrupción y, en particular, la FCPA y la UK Bribery Act, que resultan muy relevantes a efectos interpretativos. Según estas, la ajenidad al dominio social de la compañía no se considera como un obstáculo a la responsabilidad penal del contratante cuando el tercero contratado actúa en representación de este y, por tanto, siguiendo sus instrucciones. Y ello, más allá de la configuración legal que se pueda otorgar al vínculo existente entre ambos en el contrato de consultoría. A la postre, lo verdaderamente relevante para las normas de prevención del cohecho es que el tercero haya sido contratado para prestar un servicio a la sociedad (que redundará en su beneficio directo o indirecto), en tanto en cuanto ello limita su independencia frente a los estándares profesionales y éticos de la sociedad contratante, que debe velar por que la articulación mercantil de la relación no constituya un obstáculo al cumplimiento de las leyes ni una vía de escape respecto de sus propias previsiones éticas.

Como es evidente, la suficiencia de los controles establecidos por la persona jurídica sobre sus socios de negocio dependerá en cada caso de la posibilidad real de influencia que tenga sobre ellos. Sin embargo, la contratación con un tercero sobre el que se carece de control en un área de riesgo alto para la persona jurídica, existiendo otros terceros que podrían prestar el servicio en condiciones más alineadas con los estándares éticos y de cumplimiento normativo de la empresa, resultará difícilmente cohonestable con la existencia de un compromiso real con el cumplimiento normativo.

Como es evidente, la supervisión y la actualización del sistema de gestión de riesgos penales descansan fuertemente sobre la identificación de áreas de mejora y sobre el reporte de dudas e irregularidades reales o sospechadas. Precisamente por ello, la UNE 19601 detalla los requisitos del canal ético o de denuncias y del proceso posterior de investigación, aunque sin establecer novedades reseñables. Cabe esperar, en todo caso, que el epígrafe 8.8 sea

modificado en el sentido de eliminar las referencias al anonimato de la persona denunciante, por tratarse de una cuestión ya solventada —y no permitida— por la Agencia Española de Protección de Datos.

Seguimiento y actualización del sistema de compliance penal (Bloque n.º 9)

Puesto que el sistema de gestión de riesgos penales debe estar en constante evolución, la persona jurídica debe establecer los procesos que garanticen que está permanentemente actualizado y que los objetivos establecidos se cumplen en plazo. De nuevo, será necesario que la empresa especifique y documente, para permitir la auditoría de su modelo, los pormenores sobre los que descansan sus procedimientos de seguimiento, análisis y actualización. Entre otras cosas, ello deberá incluir: (i) los parámetros a tener en cuenta para medir la eficacia del sistema; (ii) los métodos de seguimiento de objetivos y los elementos de valoración de su cumplimiento; (iii) las personas responsables de llevar a cabo el seguimiento y actualización; (iv) el establecimiento de plazos; (v) la forma de los reportes, etc.

Una de las novedades de la UNE 19601 con respecto al Código Penal, a la Circular y a las sentencias del Tribunal Supremo sobre responsabilidad penal de la persona jurídica consiste en requerir que la empresa disponga de procedimientos para «solicitar y recabar opiniones del desempeño de su sistema de gestión de compliance penal» (epígrafe 9.1.3) «como fuente de mejora continua». La información podrá provenir de los empleados, directivos y administradores de la empresa, pero también de sus clientes, proveedores y del regulador de su sector de actividad. Así, el comité normalizador entiende que la percepción de los terceros constituye un criterio que puede guiar la mejora del sistema de prevención de riesgos penales, lo cual es una idea novedosa que no resulta *ex ante* descartable.

La mención a las auditorías internas está contenida en este bloque y no en el que le precede (Bloque n.º 8 sobre supervisión del modelo), probablemente por ser considerada una de las fuentes más importantes de información sobre las vicisitudes del sistema de prevención de riesgos penales. En este punto, la UNE 19601 establece requisitos tendentes a asegurar la periodicidad de las auditorías y la exhaustividad en su ejecución, así como su eficacia en cuanto a la identificación de errores o incon-

sistencias. La referida exhaustividad, que es ciertamente importante, se hace descansar sobre una variedad de elementos, como por ejemplo la competencia profesional de las personas encargadas de la auditoría, la inexistencia de conflictos de interés o la previa identificación de indicadores objetivos que deban ser controlados. Con todo, la Norma UNE no presenta en este aspecto novedades especialmente reseñables.

Por supuesto, el sistema de reportes constituye la clave de bóveda del seguimiento del modelo, pues asegura la existencia de un flujo continuo de información relevante para la eficacia de las labores de supervisión y control. En coherencia con la implicación en la *compliance* exigida de los órganos de administración, de supervisión y de la alta dirección, también ellos son los protagonistas de los informes que deben ser confeccionados con carácter periódico. Los reportes mínimos detallados por la UNE 19601 son (i) el reporte del órgano de supervisión al órgano de administración y (ii) el reporte de la alta dirección al órgano de supervisión. Respecto de los reportes a efectuar por esta última, la norma detalla pormenorizadamente el contenido mínimo que, entendemos, deberá permitir al órgano de supervisión tomar el pulso real del cumplimiento del sistema de gestión de riesgos por parte de empleados y terceros bajo el ámbito de control de cada alto directivo. Se trata de un contenido ilustrador que podrá y deberá ser trasladado, *mutatis mutandis*, cuando las competencias otorgadas en materia de *compliance* no se correspondan exactamente con el sistema triangular diseñado por la Norma UNE 19601.

Finalmente, aunque la UNE 19601 no requiere expresamente la emisión de un informe por el órgano de administración de la sociedad, sí le impone el deber de conservar la evidencia de haber tomado en consideración los reportes recibidos (esto es, como mínimo, el informe anual del órgano de supervisión). Sin embargo, su rol como máximo responsable del control de riesgos corporativos y de impulsor y rector de la *compliance* penal requerirán, en la práctica, la exteriorización de una diligencia que supere la mera revisión de reportes. En efecto, deberá posicionarse respecto a cualquier propuesta de mejora que le sea planteada y, por ejemplo, justificar su no adopción. De lo contrario, un sistema de gestión de riesgos penales perfectamente diseñado y adaptado —en y para un momento determinado en el tiempo— acabará por verse desfasado y perderá eficacia.

Mejora del sistema de compliance penal (Bloque n.º 10)

El último bloque de la Norma UNE 19601 está dedicado a establecer las obligaciones de mejora del sistema de gestión de riesgos penales y a detallar actuaciones que lo permitan, careciendo de novedades o particularidades que deban ser analizadas aquí.

PROCESO DE AUDITORÍA Y OTORGAMIENTO DE LA CERTIFICACIÓN DE CONFORMIDAD CON LA UNE 19601

Además de erigirse como una guía para el diseño e implementación de un sistema de gestión de riesgos penales, cuya utilidad es en sí misma innegable, la UNE 19601 es singular por ser certificable.

Habida cuenta de las numerosas particularidades enumeradas anteriormente, resulta muy recomendable que las empresas cuya intención sea certificar que su sistema es conforme a la UNE 19601 realicen un ejercicio previo de contraste y ajuste a su contenido.

En efecto, la mayoría de los elementos puestos de relieve aquí lo han sido por ser ajenos al sistema español, esto es, al Código penal y, en menor medida, a la Circular 1/2016 y a las sentencias del Tribunal Supremo sobre responsabilidad penal de la persona jurídica. El hecho de que hayan sido importados del derecho y de la práctica comparados, o que deriven de las exigencias del propio proceso de auditoría, implican una alta probabilidad de que los sistemas diseñados e implementados con anterioridad a la UNE 19601 no cumplan con todos ellos, o no en el modo específicamente requerido por la Norma. De nuevo, resulta importante tener en cuenta que se trata de un proceso de ajuste a la Norma UNE 19601, y no de un proceso de acomodación a la legislación penal sobre cumplimiento normativo. Por tanto, las divergencias con el articulado de la UNE 19601 no implican, en la mayoría de los casos, un incumplimiento del artículo 31 bis CP.

Sea como fuere, la realización de este análisis previo garantizará la mayor rapidez del proceso de auditoría, bien porque los auditores serán capaces de aprehender las razones que justifican las particularidades del sistema con base en los documentos preparados al efecto por la compañía, bien porque las dudas que les puedan surgir serán

fácilmente dilucidables en el contexto de una reunión, bien porque se cumplan milimétricamente todos los requisitos de la UNE 19601.

El proceso de auditoría podrá diferir en función de la empresa a la que se encomiende, pero debería responder al siguiente patrón general:

Fase 1 - Análisis documental. Los auditores analizarán las normas internas, procedimientos, medidas de control y todo documento relacionado con el sistema de gestión de riesgos penales, y contrastarán su contenido con las previsiones de la Norma UNE 19601.

Fase 2 - Análisis *in situ*. En esta fase, los auditores analizarán las medidas tecnológicas y recursos destinados por la empresa al sistema de gestión de riesgos penales, realizarán entrevistas y muestreos con la finalidad de aseverar el cumplimiento real de la estructura normativa de *compliance* penal.

Fase 3 - Informe. Tras las dos primeras fases, la auditora emitirá un informe sobre el trabajo realizado, en el que se detallarán las constataciones y conclusiones alcanzadas. Cuando el

informe establezca alguna no conformidad, otorgará a la empresa un plazo determinado para adoptar medidas correctoras al respecto. Una vez adoptadas dichas medidas, y siempre que sean consideradas suficientes por los auditores, se emitirá un informe de conformidad, sobre cuya base se otorgará la certificación.

Una vez otorgada, la certificación resulta válida por un plazo de 3 años bajo la condición de ser revisada anualmente, y ello so pena de que la certificación obtenida resulte públicamente suspendida.

A modo de brevísimas conclusiones sobre el articulado de la proyectada Norma UNE 19601, si bien queda por ver la opinión que merecerá en la práctica jurídica la certificación de los sistemas de gestión de riesgos penales conforme a ella, la existencia de una norma estandarizada que establezca los requisitos básicos de un sistema de gestión de riesgos penales tiene un valor intrínseco innegable, y será sin duda un elemento clave para fomentar un tejido empresarial ético y transparente.

MATILDE FOUREY GONZÁLEZ*

* Abogada del Área de Derecho Público, Procesal y Arbitraje de Uría Menéndez (Barcelona).