



Apuntes prácticos para elaborar una estrategia empresarial de compliance

En un mundo complejo, el riesgo cero no existe, pero la labor de los profesionales del cumplimiento normativo es imprescindible

Autor: **Ricardo Noreña**, miembro de la Junta Directiva de Cumplen y socio director de RN Consulting

Una implementación efectiva es clave en toda estrategia de compliance empresarial, la cual debe adaptarse a cada modelo de negocio y aunar el conjunto de acciones premeditadas que va a acometer la organización, con la finalidad de conseguir cumplir con la ley y con los compromisos éticos de la organización.

Eso sí, el cumplimiento no debe prevalecer sobre la propia actividad de la empresa, pues este enfoque asfixia la operativa de la compañía. Del lado opuesto, no se puede pretender blanquear las actividades ilícitas mediante una estrategia de cumplimiento. Por ello, es necesario conocer y evaluar cuáles son los riesgos de la organización: financieros, operativos, tecnológicos, legales, fiscales, sociales, medioambientales, reputacionales, etc.

Los riesgos no desaparecen completamente por el hecho de que se tomen medidas de mitigación y prevención ya que siempre queda un riesgo residual. Por ejemplo, en una empresa de transportes existe un riesgo de accidentes, que denominaremos riesgo inherente a la actividad de transportes. Se pueden tomar diferentes medidas y controles destinados a la prevención y mitigación como, por ejemplo, adoptar un proceso de capacitación y formación de conductores, diferentes controles internos destinados a controlar la actuación de los conductores y hacer seguimiento, contratar seguros, seguimiento de los vehículos por vía de GPS, etc. A pesar de todo ello, el accidente puede ocurrir igualmente. Este es el riesgo residual.

En las diferentes argumentaciones de profesionales de la justicia en tribunales penales se escuchan alegatos que consideran que, si se ha materializado un delito, hay necesariamente que concluir que los controles no funcionaron o no existían. Se ignora el riesgo residual, aspecto que, sin duda, debe ser tenido en cuenta al determinar la responsabilidad penal.

Otra de las claves pasa por formalizar, aprobar y difundir dentro y fuera de la empresa cuáles son los pilares básicos de su estrategia de compliance. No basta con tener un sistema de compliance, hay que formalizarlo y difundirlo. Y es que, un sistema de control interno diligente tiene como objetivo garantizar que las funciones de aseguramiento de una empresa cubren los posibles riesgos a los que está expuesta.

Asegurar el cumplimiento con las leyes y el código ético de la organización forma parte del sistema de control interno. El compliance tiene un componente legal y un componente de control interno, por ello los profesionales reúnen formación y experiencia en ambas materias. Hay que tener en cuenta que las herramientas informáticas son una ayuda para gestionar y sistematizar el modelo de compliance, pero no sustituyen a los compliance officer.

Es frecuente la afirmación de que evaluar y determinar si un sistema de compliance está bien diseñado y funciona de manera efectiva es una interpretación legal. Esta afirmación es incorrecta. Los profesionales del compliance son los encargados de llevar a cabo su evaluación. Es habitual en la práctica procesal ver informes periciales.

La comisión de un delito o un comportamiento no ético en el entorno de una organización no equivale directamente a un fallo en el diseño o el funcionamiento efectivo del modelo de compliance. Concluir en esta dirección sin hacer una rigurosa investigación forense puede llevar a cometer graves errores o injusticias. Pongamos dos ejemplos. La figura del management override, es decir, cuando la alta dirección de la empresa es la que se salta los controles. Esta situación no lleva a concluir que haya un problema de diseño o que no esté funcionando de manera efectiva el modelo de compliance. Según COSO, referente en materia de control interno, el sistema de control interno no puede ser más eficaz que las personas responsables de su funcionamiento". Estos casos ponen en riesgo la supervivencia de las organizaciones.

El avance de la tecnología hace que en numerosas ocasiones los sistemas de control no se encuentren adaptados a nuevas operativas fraudulentas. Según la Comisaría Provincial de Málaga, a una anciana se le han sustraído recientemente 240.000 euros de su cuenta corriente utilizando pequeños pagos de Bizum. La víctima no recuerda haber llevado a cabo ninguna actividad inusual. ¿Se trata de un caso de falta de actualización de los sistemas de control achacable a las compañías? ¿Es un problema de falta de formación y adaptación de los usuarios más veteranos a las nuevas herramientas? ¿Es justo buscar responsabilidades penales para las organizaciones privadas y no para el Estado?

Los sistemas de compliance están sujetos a una permanente actualización en un mundo complejo en el que riesgo cero no existe. En este contexto, la labor de los profesionales del compliance se ha vuelto imprescindible para las empresas y la Administración de Justicia.

Fuente: Cinco Días