DEL CUMPLIMIENTO NORMATIVO A LA GESTIÓN INTEGRAL DE RIESGOS DE *COMPLIANCE*

JORGE ALEXANDRE GONZÁLEZ
Compliance Product Manager de EQA

Cumplimiento en sentido amplio, interacción normativa o transversalidad de obligaciones son conceptos que progresivamente dejarán de sonarnos extraños. Y este número dedicado a la evolución en la protección de datos en nuestro entorno resulta un lugar idóneo para hablar de ellos. Con este objetivo, durante las siguientes líneas trataremos de abordar brevemente algunas cuestiones legales, pero también de carácter organizativo, que exceden propiamente el ámbito de la protección de datos y nos introducen directamente en el ámbito de la gestión de riesgos de *compliance*, esto es, la gestión sobre la incertidumbre que produce la posibilidad de que se materialicen incumplimientos de determinadas obligaciones normativas —por ejemplo, aquellas relacionadas con la protección de datos— o bien de compromisos voluntarios o contractuales adquiridos, y que éstos a su vez conlleven un perjuicio para las organizaciones. No obstante, como veremos a continuación, el camino nos conducirá irremediablemente, también, al ámbito de la protección de datos.

CULTURA DE *COMPLIANCE* VS CUMPLIMIENTO DE NORMAS

Parece recomendable, como decimos, comenzar la exposición desde una perspectiva más amplia y general e ir progresivamente descendiendo sobre ámbitos concretos de obligaciones como puede ser el del cumplimiento en materia de protección de datos.

Compliance es un concepto que se viene asociando desde hace algunos años a la forma y método que deben seguir las empresas y otras organizaciones (ONGs, administraciones públicas, clubes de deportivos, partidos políticos, etc.) para conocer y cumplir con sus obligaciones —y, por tanto, mitigar sus riesgos de incumplimiento— tanto de aquellas obligaciones de carácter fundamentalmente imperativo, generalmente derivadas de imposiciones legales en muy diversas materias como puedan ser la protección de datos, la prevención del blanqueo de capitales, la lucha contra el fraude y prevención de la corrupción y otras muchas normativas sectoriales; como también aquellas obligaciones que las organizaciones asumen de forma semi-voluntaria, entre las que se pueden encontrar la asunción de determinados estándares de actuación y gestión para acceder a determinados mercados o marcar la diferencia con los competidores en la contratación pública y privada; y, finalmente, también a otros compromisos voluntariamente asumidos, generalmente asociados a la ética, la responsabilidad social y las buenas prácticas empresariales.

En el ámbito del *compliance,* a las normas ineludibles se las tiende a conocer como *requirements* y al resto como *commitments*. Lo cierto es que tal distinción es más sencilla en la teoría que en la realidad empresarial, en la que numerosos *commitments* se han convertido en auténticos requisitos para acceder a determinados mercados, de ahí que parezca más razonable proponer a su vez una división bipartita en la que encontremos compromisos semi-voluntarios, es decir, aquellos que la organización asume 'empujada' por la práctica empresarial y con el fin de poder competir en el mercado, y aquellos compromisos plenamente voluntarios, que asume a pesar de no tener un impacto tan relevante en su actividad ordinaria.

Un buen ejemplo de los *commitments* de naturaleza semi-voluntaria en el ámbito de la protección de datos serían las reiteradas referencias que realiza el ya vigente Reglamento Europeo de Protección de Datos al valor de las certificaciones en el ámbito de la protección de datos. Así, en su artículo 42.1 ya establece que *"los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos"*. Se desprende perfectamente de la redacción del texto legal que tales certificaciones no resultarán normativamente obligatorias, pero no asumirlas podría conllevar quedar fuera de determinados mercados, o ser incapaz, llegado el caso, de probar la existencia de mecanismos de prevención y control frente a los incumplimientos.

Por su parte, y aunque orientado al sector bancario, resulta de perfecta aplicación a otros ámbitos como la protección de datos la expresión *"compliance risk"* (riesgos de *compliance*) que se definió en el Acuerdo de Basilea II como el riesgo al que se expone una entidad por el incum-

plimiento de leyes, reglamentos y normas, y de aquellos acuerdos de autorregulación en políticas de organización y códigos de conducta aplicables a sus actividades y que pueden suponer sanciones legales o regulatorias, pérdidas financieras o de reputación.

Se puede decir, por tanto, que establecer una cultura de *compliance* va mucho más allá de cumplir con las normas o con las obligaciones. Establecer una cultura de *compliance* en las organizaciones se relaciona con el visible compromiso de la organización, desde el propio órgano de gobierno, con la implementación de metodologías para minimizar el riesgo de incumplimiento, dotando a una o varias personas de autonomía, responsabilidad y control para el mantenimiento de una estructura de *compliance* que sea adecuada para conseguir sus objetivos.

Entre otros referentes en la materia, a esta diferencia entre generar una cultura de *compliance* o limitarse a cumplir con las obligaciones, se refería recientemente Hui Chen (ex-primera asesora en *compliance* del Departamento de Justicia de Estados Unidos) en lo que ella denominaba las siete señales de un sistema de *compliance* ineficaz, las cuales me permito traducir libremente como:

- Falta de disciplina en relación con el control de los flujos financieros.
- Exceso de enfoque legal en las cuestiones de *compliance.*
- Diseñar un sistema basado en mínimos legales.
- Confundir la eficacia basada en métricas con el número de píldoras formativas o el grado de asistencia a las formaciones.
- Centrarse más en las medidas de control concretas que en la gestión del sistema en su conjunto.
- Basar el sistema en el cumplimiento de una normativa en lugar de basarlo en generar una cultura.
- Pensar que todo el cumplimiento se reduce a contar con una política de regalos.

Si bien no es preciso ahondar en este momento sobre el significado de estas siete señales, sí parece sencillo reconocer que generar una cultura de *compliance* va mucho más allá de limitarse a cumplir con las leyes. En el ámbito de la protección de datos, y recuperando como ejemplo el Reglamento General de Protección de Datos, encontramos una referencia clara a la necesidad de ir más allá del mero cumplimiento legal en su considerando 78, cuando señala que *"la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto."*

En resumen, no sólo hay que cumplir la ley, sino que hay también que comprometerse visiblemente con cumplirla, y establecer mecanismos para ello.

ÁREAS DE OBLIGACIONES DE *COMPLIANCE* Y RIESGOS DE INCUMPLIMIENTO

Cómo resulta obvio, en el momento en que las organizaciones inciden en las relaciones humanas, las mismas se ven sometidas a derecho positivo. De esta manera, en el momento en que las organizaciones nacen, todo un abanico de obligaciones jurídicas regula sus actividades y, consecuencia de dichas obligaciones, aparecen inevitablemente una serie de riesgos de incumplimiento que, como señalábamos, pueden acarrear sanciones de diversa índole si se materializan, además del correspondiente daño reputacional.

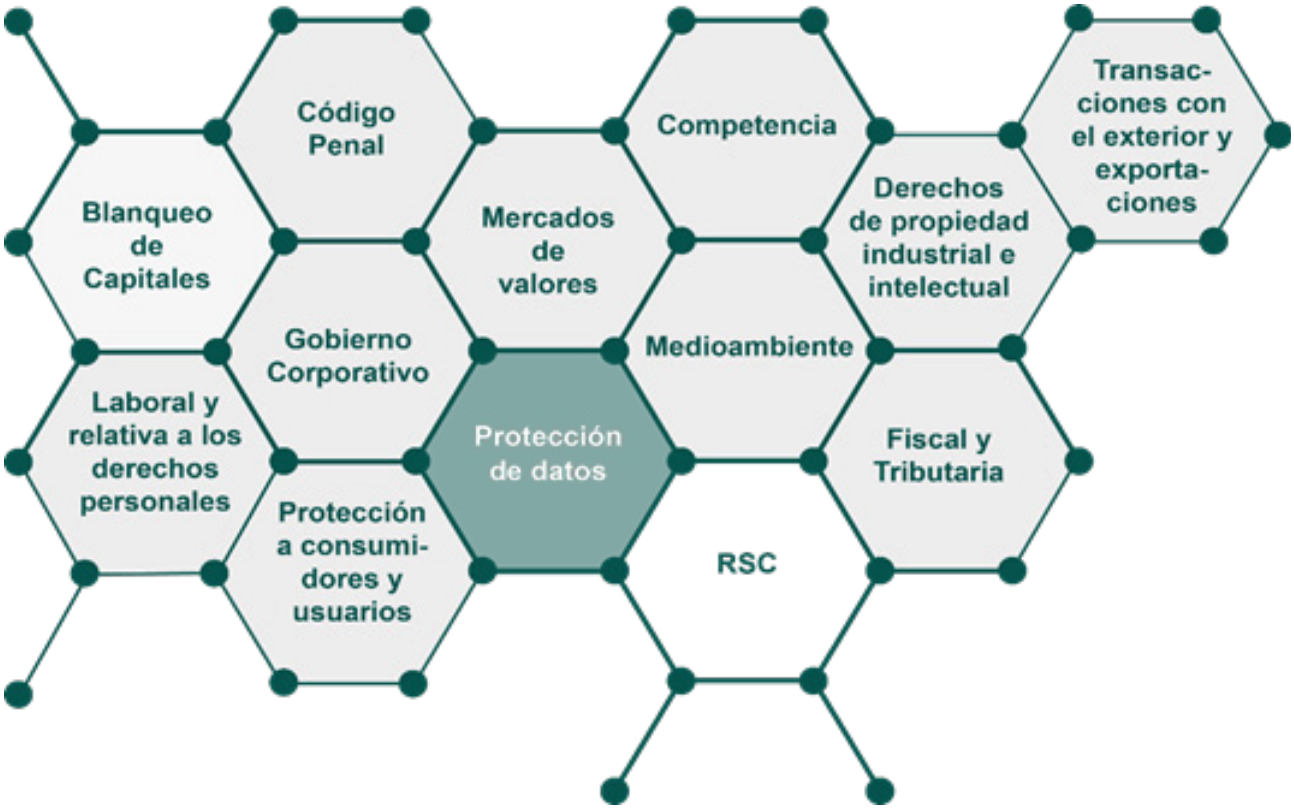
Ante esta situación, cobra relevancia el contexto en el que opera la organización y la naturaleza de sus actividades y relaciones con terceros. Conocer exactamente esta información es el primer paso para conocer las obligaciones a las que se encuentra sometida y, por tanto, los riesgos de incumplimiento ante los que se encuentra expuesta. En efecto, existen múltiples obligaciones que las organizaciones deben conocer, saber afrontar y para las que resulta necesario establecer estructuras de *compliance.* Aunque la siguiente división

puede ser ampliamente matizada, divida o ampliada, podríamos dividir dichas obligaciones (y compromisos) en cuatro grandes bloques por su relevancia actual:

- Obligaciones y compromisos en materia societaria, tributaria y de competencia.
- Obligaciones y compromisos en el ámbito laboral, incluida la seguridad y la salud en el trabajo.
- Obligaciones y compromisos en el ámbito de la seguridad de la información y la protección de datos de carácter personal.
- Obligaciones y compromisos en el ámbito de la prevención penal, especialmente en materia de lucha contra el fraude y la corrupción.

En definitiva, las organizaciones deben conocer los riesgos a los que se encuentran expuestas en función de su contexto y la naturaleza de sus actividades y relaciones con terceros.

En este aspecto, conociendo las diversas obligaciones de *compliance,* podemos comenzar a gestionar los riesgos de incumplir con dichas obligaciones y, llegado el caso, establecer medidas de control para mitigarlos. Se puede afirmar sin miedo que el riesgo de incumplimiento está presente en todo tipo de organizaciones y actividades destacando que, generalmente, no es posible establecer mecanismos para mitigarlo completamente por lo que es imprescindible gestionarlo de forma adecuada. Es por ello que las organizaciones, a fin de poder gestionar sus riesgos, deberán realizar evaluaciones de riesgo en relación con cada área de obligaciones, incluyendo la identificación, el análisis y la valoración de esos riesgos, todo ello como paso previo a establecer controles que mitiguen la consumación de dichos riesgos. Como es habitual referir, es importante señalar que el enfoque basado en el riesgo no significa que, para situaciones de riesgo bajo, una organización acepte incumplimientos, sino que sirve de ayuda a la organización para centrar la atención primaria y los recursos en los riesgos más elevados de forma prioritaria, si bien en última



instancia, lo lógico es tender a cubrir todos los riesgos que le afectan.

Las prácticas internacionalmente reconocidas indican en este sentido que las organizaciones deben desarrollar procesos de identificación, análisis y valoración del riesgo que permita, por un lado, identificar los riesgos atendiendo a sus actividades, así como a los miembros de la organización y sus partes interesadas por medio de un catálogo completo de los riesgos inherentes a los que la organización podría exponerse en virtud de la naturaleza y ubicación de sus actividades, así como a sus relaciones con terceros; por otro lado, analizar los riesgos identificados, de manera previa y de cara a su valoración, analizando las consecuencias para la organización en caso de que dichos riesgos se conviertan en realidad así como la probabilidad de que esto ocurriese; y, por último, determinar qué riesgos identificados son de mayor importancia para la organización como paso previo para priorizar la asignación de recursos y la implementación de controles.

Consecuencia de lo anterior, las organizaciones deberían establecer y definir su apetito al riesgo en cada uno de los ámbitos que presentan riesgos de incumplimiento (recordemos una vez más que la protección de datos no será sino un área más dentro un largo etc.). En este sentido, la organización podría determinar que es aceptable tener un nivel de control bajo sobre las actividades de riesgo bajo.

Se pueden encontrar diversas definiciones de apetito al riesgo en los principales marcos de buenas prácticas internacionales en materia de gestión y control interno. El estándar 'ISO-UNE GUÍA 73:2010 IN Gestión del riesgo. Vocabulario' define apetito al riesgo como la *"cantidad y tipo de riesgo que una organización está dispuesta a aceptar o retener"*. En términos similares se refiere el marco COSO al definirlo como *"los tipos y la cantidad de riesgos, en un nivel amplio, que una organización está dispuesta a aceptar en la búsqueda de generar valor".*

Como señala el estándar ISO 37001 para el ámbito del soborno, pero de perfecta aplicación a otros ámbitos como la protección de datos, la evaluación de riesgos de incumplimiento debería diseñarse como una herramienta para ayudar a la organización a priorizar sus esfuerzos y debería también ser revisado periódicamente en base a cambios en la organización o en las circunstancias, por ejemplo, cuando se accede a nuevos mercados

o productos, se producen cambios regulatorios y jurisprudenciales, etc.

Producto de la evaluación de riesgos y la definición de su apetito al riesgo, la organización se encontrará en disposición de implementar las medidas de control que considere adecuadas para mitigar los riesgos de incumplimiento a los que se encuentra expuesta.

UNA SUPERESTRUCTURA ORGANIZATIVA PARA GESTIONAR TODOS LOS RIESGOS DE *COMPLIANCE*

A pesar de que todos los riesgos de incumplimiento tienen un factor en común, que no es sino el riesgo a sufrir una sanción en la organización y las consecuencias económicas, operacionales, reputacionales, etc. que ello conlleva, en la actualidad resulta habitual que los riesgos de incumplimiento a los que se enfrenta una organización, a la vista de su contexto, existan y se gestionen de forma autónoma por diversos departamentos de la organización, llegando en casos no tan extraños a existir una total falta de comunicación entre responsables de diferentes áreas de obligaciones.

Así, es frecuente encontrar un área fiscal (interna o externa) que gestiona los riesgos de cometer una infracción (o delito) de naturaleza tributaria; el área jurídica a menudo se encarga de gestionar riesgos en relación con las infracciones de competencia; un *compliance officer* que se encuentra enfocado exclusivamente en el ámbito del *compliance* penal y la prevención del delito en la organización; un delegado de protección de datos que se encuentra ubicado más cercano a los departamentos de informática que a las áreas anteriores; o un responsable de calidad y gestión ambiental con escasa relación con todos los anteriores, y que sin embargo es responsable de los sistemas de gestión y los procesos operacionales de la organización. Esta realidad actual de muchas organizaciones en nuestro entorno da la espalda a principios básicos de eficacia y eficiencia, genera duplicidades, e impide la posibilidad de generar sinergias en áreas orientadas al *compliance* y el cumplimiento normativo.

Por poner un ejemplo, como hemos señalado anteriormente, una organización, de forma previa a analizar las obligaciones y evaluar los riesgos a los que se encuentra sometida, debería determinar el contexto exacto en que opera, incluyendo en dicho contexto el sector o los sectores, la naturaleza de sus actividades, y las partes interesadas que participan en dichas actividades; y si bien este ejercicio es –o debería ser– habitual encontrarlo en cada área de obligaciones de *compliance*, resultaría sin duda más eficaz que se realizase en detalle, con la participación de las personas adecuadas, una sola vez. Evitaría duplicidad de trabajo y, mejor aún, evitaría que existieran definiciones de contexto diferentes en función del área de la organización que la ha desarrollado, pudiendo en el peor de los casos encontrar ausencias, incongruencias o contradicciones.

Si el objetivo es gestionar riesgos de forma integral, las organizaciones deberían comenzar a integrar –en la medida de lo posible– aquellas acciones que realizaba para gestionar una sola de sus áreas de obligaciones, en una superestructura de *compliance* de nivel superior.

En el ejemplo que planteábamos, relativo al contexto en el que opera la organización, el objetivo debería ser determinar el alcance de una eventual superestructura de *compliance.* Ese alcance no sería más que una declaración basada en hechos, representativa de todas las operaciones de la organización incluidas dentro de los límites de su sistema de *compliance,* que si bien no necesariamente tendría que abarcar la totalidad de las actividades que realiza la organización, éste debería ser el objetivo final de toda superestructura de *compliance.*

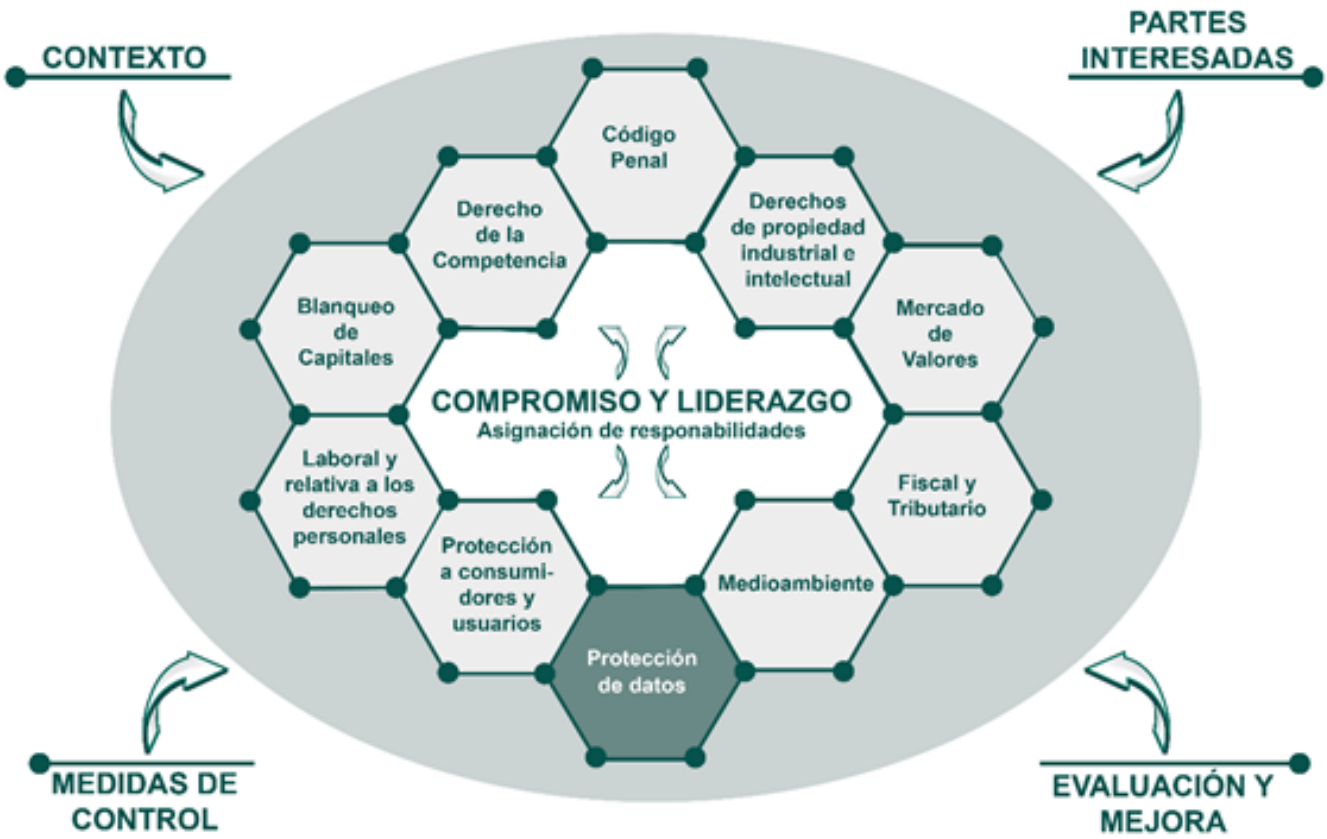
Ejemplo típico de la libertad para establecer el alcance de un sistema de *compliance* sería la organización que, por diversos motivos, por ejemplo, porque trata alguna de sus áreas de obligaciones de forma absolutamente independiente al resto, decide dejar fuera del alcance de su superestructura de *compliance* una determinada actividad. Si ese fuera el caso, los elementos propios del sistema de *compliance* tendrían escaso o nulo impacto sobre esta actividad y los sujetos que participan en ella. Dicha exclusión de la organización puede estar motivada por el escaso riesgo de incumplimiento que suponen estos sujetos y actividades, aunque también podría ser síntoma de un excesivo apetito al riesgo de la organización, siendo en todo caso

recomendable documentar cualquier limitación del alcance bajo el principio *comply or explain.* Lo idóneo sería no limitarse a excluir alcances del sistema sin más, sino precisamente explicar el motivo por el que se excluyen cuando aparentemente debería quedar sometidos al sistema.

En definitiva, el alcance del sistema de *compliance* está previsto para aclarar tanto los límites físicos a los que aplica el sistema, como los límites organizacionales, y cobra especial importancia cuando tratamos con organizaciones o actividades en las que existen relaciones complejas. Una organización tiene la libertad y la flexibilidad para definir sus límites y puede decidir implementar el sistema de *compliance* en toda la organización, o sólo en partes específicas de ella. Aun así, y como avanzábamos, resultaría un error y una *mala praxis* en este ámbito la exclusión de actividades, productos, servicios, instalaciones o grupos de personas sobre los que puedan recaer riesgos significativos de incumplimiento.

Una vez la organización conoce el contexto en el que opera, reconoce y agrupa de forma pertinente a sus partes interesadas, ha determinado el alcance para su sistema de *compliance* y ha identificado, analizado y valorado los riesgos de incumplimiento a los que se encuentra expuesta, es cuando realmente se encuentra en disposición de implementar lo que podemos denominar,

SUPERESTRUCTURA DE COMPLIANCE



en sentido estricto, su sistema de gestión de *compliance* razonablemente integrado.

Aunque el método para generar superestructuras de *compliance* es objeto de estudio hoy en día, la estructura por la que parecen inclinarse profesionales y organizaciones es la de establecer metodologías basadas en un ciclo PDCA de mejora continua. Máximo representante de este tipo de metodologías es la seguida por el estándar internacional ISO 19600:2014 sobre sistemas de gestión de *compliance.*

La reconocida norma ISO 19600 sobre sistemas de gestión de *compliance* basa su estructura en el ciclo de Deming *Plan-Do-Check-Act* (PDCA) y aunque su contenido detallado se circunscribe a recomendaciones, la estructura que desarrolla se configura como el marco general que deberían seguir las organizaciones de cara a establecer una superestructura de *compliance*. En dicha estructura se pueden observar perfectamente el encaje, tanto de los elementos ya tratados en las líneas anteriores, tales como el análisis del contexto, partes interesadas, alcance del sistema, evaluación de riesgos, etc., dando lugar a continuación a la necesidad de implementar medidas de control para mitigar los riesgos de incumplimiento, así como establecer mecanismos de evaluación del desempeño, auditoría interna, revisión a distintos niveles y mejorar continuamente el sistema.

Pero volviendo a la estructura propuesta, y una vez analizados los elementos externos e internos de la organización, resulta del todo necesario detenernos en la necesidad de establecer una suerte de compromiso y liderazgo unificado dentro de la organización, al menos al más alto nivel. El denominado *tone from the top* debe ser visible, incluyendo declaraciones explícitas tanto públicas como de índole interno de las personas relevantes de la organización, así como la asunción de determinadas responsabilidades a la hora de destinar recursos, realizar supervisiones del sistema de *compliance* o de alguna de sus áreas de obligaciones y asignar responsables, por ejemplo, la designación del órgano de *compliance* general que coordine todas las áreas de obligaciones y a sus responsables, las necesidades de formación, la supervisión de las medidas de control, etc. Aun así, será habitual que en las áreas concretas de obligaciones de *compliance,* y así queda patente por ejemplo en el ámbito de la protección de datos (arts. 24 a 39 del Reglamento sobre el responsable, el encargado y el delegado de protección de datos), existan determinados responsables a diferentes niveles con una serie de obligaciones claramente definidas dentro de cada área.

Asignadas las responsabilidades y fijado el marco fundamental de actuación en relación con sus obligaciones de *compliance* dentro de la propia organización, se debe planificar, implementar y controlar los procesos necesarios para afrontar riesgos y oportunidades derivados de sus actividades. En otras palabras, los procesos y procedimientos de la organización deben estar sujetos a los controles específicos que mitiguen los riesgos de incumplimiento. Integrar estructuras de *compliance* puede resultar en este ámbito especialmente eficaz, en la medida en que las mismas medidas de control puedan servir para mitigar riesgos de incumplimiento de diferente naturaleza.

Y en estrecha relación con lo anterior, y no menos importante, resultan relevantes las políticas de formación y concienciación de los empleados, trabajadores e incluso colaboradores y socios. Será idóneo coordinar y en la medida de lo posible integrar el fomento de la concienciación y formación de los miembros de la organización y otras partes interesadas de manera adecuada, eficaz y proporcionalmente respecto de los riesgos de incumplimiento que existen en la organización. Y todo lo anterior, siempre sometido a una revisión periódica para localizar insuficiencias y mejorar continuamente el sistema de *compliance*.

En definitiva, las organizaciones de nuestro entorno se encuentran en una complicada encrucijada. Deben afrontar los riesgos de incumplimiento que provoca la gran cantidad de obligaciones que les afectan —especialmente las de naturaleza legal y normativa— y deben hacerlo de una forma eficiente e integral, de tal manera que sean capaces de generar sinergias entre ámbitos *a priori* tan dispares como lo pueden ser la protección de datos personales, el de las infracciones de competencia o la prevención del blanqueo de capitales. Aquellas organizaciones capaces de generar superestructuras de *compliance* para dar una respuesta integrada a esta realidad, tendrán una clara ventaja sobre sus competidores en el corto y el medio plazo.