LOS MARCOS REGULATORIOS DEL *COMPLIANCE*: FUTUROS RETOS Y DESAFÍOS EN UN CONTEXTO GLOBAL CAMBIANTE

FRANCISCO BONATTI BONET

En las últimas cinco décadas, el modelo de gestión empresarial ha evolucionado desde un enfoque centrado en la calidad de productos y procesos hacia un modelo basado en la ética. En los años 70, influenciadas por estándares de calidad (como las primeras normas ISO 9000) y filosofías de mejora continua, muchas organizaciones priorizaban la excelencia técnica y la eficiencia productiva.

Sin embargo, el contexto histórico de aquel entonces –marcado por la descolonización y la apertura de nuevos mercados, la expansión de las multinacionales, el auge de la sociedad de consumo del bienestar tras la posguerra, los movimientos por los derechos civiles y la transparencia en la política– generó una conciencia social más crítica que empezó a demandar enfoques empresariales éticos y de buen gobierno.

DEL SIGLO XX AL SIGLO XXI, EL NUEVO PARADIGMA DE LA GESTIÓN ÉTICA

En 1974, la Conference on Business Ethics de Kansas, introdujo la ética empresarial como disciplina académica formal y señaló la necesidad de integrar valores éticos en la gestión corporativa. Durante los años 80, surgieron marcos conceptuales que ampliaron la responsabilidad social de la empresa más allá de los accionistas. Destaca la *teoría de los stakeholders* de R. Edward Freeman (1984), que definió a los grupos de interés como "cualquier grupo o individuo que puede afectar o ser afectado por los objetivos de la empresa". Esta visión retaba la postura clásica de Milton Friedman (1970), quien sostenía que la única responsabilidad social de la empresa era maximizar beneficios para los propietarios. A comienzos de los 90, Archie Carroll propuso la pirámide de la responsabilidad corporativa (1991)[1]. Paralelamente, cobró fuerza la idea de ciudadanía corporativa y la *ética de los stakeholders*, reconociendo que la empresa, como parte de la sociedad, debía contribuir al bien común más allá de lo estrictamente exigido por la ley. A finales de los 90, se popularizó también el concepto de desarrollo sostenible (impulsado por el *Informe Brundtland* de 1987), integrando las preocupaciones ambientales y de futuro en la agenda empresarial. En suma, a finales del siglo XX las empresas líderes comenzaban a complementar los tradicionales ejes

1 Con cuatro niveles: económico (ser rentable), legal (cumplir las leyes), ético (actuar con valores) y filantrópico (ser buen ciudadano corporativo)

de calidad, productividad y rentabilidad con un nuevo eje de gestión ética, incorporando políticas de responsabilidad social y códigos de conducta.

En la misma época, los escándalos financieros e institucionales evidenciaron deficiencias en la gobernanza de las organizaciones y llevaron a reformas orientadas al buen gobierno corporativo. Un referente inicial fue el Informe Cadbury (Reino Unido, 1992), que, ante problemas como la opacidad financiera y la ausencia de controles en los consejos de administración, recomendó prácticas de gobierno transparente bajo el principio de *"cumplir o explicar"*. A partir de Cadbury se instauraron códigos de buen gobierno en varios países, enfatizando la separación de funciones en el consejo, la existencia de comités de auditoría, controles sobre la remuneración de directivos y la rendición de cuentas a los accionistas. Organismos internacionales como la OCDE publicaron sus primeros Principios de Gobierno Corporativo en 1999 (actualizados en 2004), que sirvieron de guía global para fortalecer la diligencia y responsabilidad de los órganos de gobierno empresarial.

La relevancia de un buen gobierno efectivo quedó reforzada tras la crisis financiera global de 2007–2008. Investigaciones posteriores de la OCDE y la Unión Europea concluyeron que la toma de riesgos excesivos en muchas entidades se vio facilitada por una gobernanza deficiente: consejos que no supervisaron adecuadamente, culturas corporativas cortoplacistas y controles internos laxos en instituciones financieras. En España, esto motivó la creación de una *Comisión de Expertos en 2013*, cuyas recomendaciones derivaron en la Ley 31/2014, de 3 de diciembre, de mejora del gobierno corporativo. Esta reforma introdujo exigencias concretas para asegurar la integridad, transparencia y sostenibilidad en la gestión societaria. Asimismo, en años recientes han surgido normativas enfocadas en aspectos ESG que extienden el alcance del buen gobierno hacia la responsabilidad con el entorno y los distintos grupos de interés. (Volveremos sobre estas regulaciones ESG en apartados posteriores.)

Este recorrido histórico sentó las bases para el desarrollo del *Compliance*en las organizaciones. A medida que las empresas adoptaban compromisos éticos y prácticas de buen gobierno, se hizo patente la necesidad de sistemas internos que garantizaran el cumplimiento efectivo de esos principios y normas: se necesitaban estructuras operativas que permeasen esos compromisos a todos los niveles de la organización. Surgiendo el concepto de Compliance como una función especializada en la gestión de estos riesgos. Un hito fundacional en esta materia fue la aprobación en Estados Unidos de la Foreign Corrupt Practices Act (FCPA) en 1977, derivada de las investigaciones por sobornos internacionales (caso Lockheed, entre otros) que sacudieron la opinión pública y llevaron al legislador norteamericano a prohibir expresamente la corrupción de funcionarios extranjeros y a exigir controles contables internos en las empresas cotizadas. La FCPA, pionera mundial en combatir la corrupción corporativa, inauguró la era de los *programas de cumplimiento* dentro de las multinacionales, que buscaban evitar multas millonarias y sanciones penales implementando políticas internas antifraude. En décadas posteriores, esta tendencia se globalizó: organismos como la OCDE impulsaron en 1997 la Convención Anticohecho, y diversas jurisdicciones comenzaron a exigir o incentivar la existencia de modelos de prevención de delitos en las empresas.

En España, la llegada del Compliance estuvo marcada por la reforma penal de 2010 (Ley Orgánica 5/2010) que introdujo la responsabilidad penal de las personas jurídicas, reforzada posteriormente por la reforma de 2015 (LO 1/2015). A partir de 2010, las empresas españolas pueden ser penalmente responsables de ciertos delitos cometidos en su seno, pero el legislador ofreció una vía eximente: implantar modelos de organización y gestión eficaces para prevenir delitos (es decir, programas de Compliance Penal). Esto convirtió al Compliance en una necesidad jurídica tangible: dejar de ser simplemente "una buena práctica" para volverse esencial en la gestión empresarial si se quería evitar sanciones penales y daños reputacionales. Desde entonces, multitud de empresas han implementado sistemas preventivos acorde a las exigencias legales.

El eje de la gestión ética en las organizaciones

Podemos entender hoy la gestión ética corporativa como un eje integrado por tres componentes interrelacionados (ver figura 1):

- Ética corporativa (la organización): son los valores y principios declarados que rigen la cultura de la empresa, usualmente plasmados en un Código Ético o de Conducta. Orientan el *qué se espera* en términos de integridad y responsabilidad social.
- Buen Gobierno (el órgano de gobierno): son las estructuras y políticas mediante las cuales el Órgano de Gobierno y la alta dirección dirigen la compañía con transparencia y responsabilidad. Incluye códigos de buen gobierno, políticas de gobierno corporativo y mecanismos de control (comités de auditoría y de cumplimiento). Define *quién* supervisa que esos valores se integren en la estrategia y *cómo* se toman las decisiones clave.
- Compliance (los integrantes de la organización): es la función operativa que *aterriza* tanto los compromisos éticos como las obligaciones legales en normas y procedimientos internos concretos. Un Programa de Compliance traduce el "qué" y el "cómo" en controles, procedimientos y actividades de formación, para guiar la conducta diaria de directivos y empleados alineándolas con la voluntad del órgano de Gobierno y con el Código ético de la Compañía.

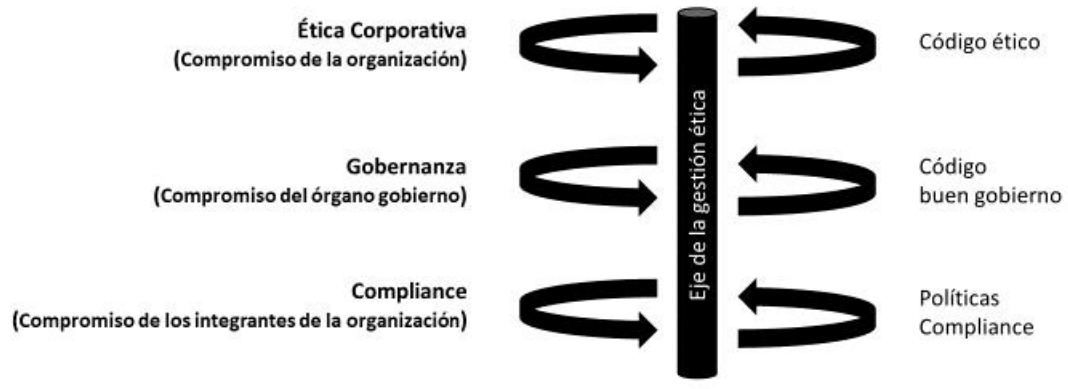
En otras palabras, la ética fija los principios, el buen gobierno establece la dirección y control desde arriba, y el compliance alinea los objetivos en la práctica cotidiana mediante reglas y herramientas específicas.

Este nuevo paradigma no sustituye a las metas de rentabilidad o excelencia técnica, sino que las supedita a un marco de responsabilidad y sostenibilidad: *no se concibe un negocio exitoso a largo plazo que no sea, a la vez, ético y cumplidor*. Y el instrumento que asegura esa alineación día a día es el Compliance[2].

MARCOS NORMATIVOS EN *COMPLIANCE*: DEL CONSENSO GLOBAL A LOS COMPONENTES ESENCIALES

En el ámbito de la gestión empresarial, un marco de referencia es un conjunto estructurado de directrices, estándares o buenas prácticas que sirve de modelo para diseñar e implementar sistemas o programas en una materia dada. En calidad, por ejemplo,

FIGURA 1
EJE DE LA GESTIÓN ÉTICA



Fuente: Elaboración propia

2 Como ha señalado la Fiscalía española, la meta última del Compliance es fomentar una "cultura ética empresarial" que prevenga comportamientos ilícitos, evitando así sanciones y reforzando la reputación y confianza en la empresa.

la ISO 9001 ha sido por décadas el marco de referencia internacional para sistemas de gestión de calidad. De manera análoga, en Compliance los marcos de referencia proporcionan las pautas y requisitos que delinean cómo debe ser un programa de cumplimiento "ideal" o efectivo. Sus características suelen incluir: una metodología clara (p. ej. etapas de planificar, implementar, verificar, mejorar), una enumeración de elementos o componentes esenciales que debe incluir el sistema, y a veces criterios de certificación o evaluación para medir si una organización cumple con el estándar.

El concepto de marco de Compliance se empezó a forjar con aportaciones variadas. Un antecedente importante fue la propia FCPA de 1977 en EE.UU.: si bien es una ley y no un estándar voluntario, la FCPA introdujo por primera vez requisitos específicos de controles internos anticorrupción, presionando a las empresas a crear manuales de conducta, registros contables transparentes y sistemas de verificación –en la práctica, los primeros pilares de un programa corporativo de cumplimiento–. Años después, en 1991, las Federal Sentencing Guidelines estadounidenses establecieron criterios atenuantes de pena para empresas con "programas efectivos de compliance y ética", enumerando elementos como capacitación, monitoreo y apoyo de la alta dirección.

En el mundo anglosajón no tardaron en surgir guías y estándares sobre cómo estructurar estos programas. Australia, por ejemplo, publicó uno de los primeros estándares nacionales: la AS 3806 *(Australian Standard on Compliance Programs)*, cuya versión de 2006 definió principios para implementar programas de cumplimiento normativo en cualquier tipo de organización[3]. En Alemania, el Instituto de Auditores (IDW) emitió en 2011 la norma IDW PS 980, un estándar para verificar la adecuación de los sistemas de Compliance, que define también siete componentes fundamentales de dichos sistemas y proporcionó un marco metodológico para su auditoría externa. Por su parte, la organización internacional de normalización ISO incorporó la gestión del cumplimiento a su catálogo ya entrado el siglo XXI, como veremos más adelante.

En suma, un marco de referencia de Compliance es una guía estructurada y reconocida para crear, evaluar o certificar un programa de cumplimiento. Puede provenir de entidades públicas (leyes, guías regulatorias) o de organismos privados de normalización; puede tener carácter voluntario o vinculante. Pero en todos los casos brinda un lenguaje común y un esquema armonizado para entender qué debe hacer una organización para gestionar adecuadamente sus riesgos de incumplimiento.

Evolución histórica: de EEUU al consenso global

Los primeros pasos para definir *qué es un buen programa de compliance* tuvieron lugar en Estados Unidos y se centraron en la lucha contra la corrupción y el fraude corporativo. Tras la FCPA, la proliferación de *deferred prosecution agreements* (acuerdos con fiscalía) en los 80 y 90 en casos corporativos impulsó la noción de *compliance program* en entornos empresariales. El concepto se extendió al mundo anglosajón: el Reino Unido, por ejemplo, en la UK Bribery Act de 2010 incluyó la "adecuate procedures defense"[4].

A nivel internacional, la OCDE en 2010 emitió su *Guía de buenas prácticas en controles internos, ética y cumplimiento* para combatir la corrupción transnacional, que animaba a empresas de todos sus países miembros a instaurar programas con elementos muy similares a los que reconocemos hoy[5]. En paralelo, organizaciones sin ánimo de lucro y asociaciones profesionales aportaron marcos voluntarios: la Open Compliance and Ethics Group (OCEG) publicó desde 2007 su modelo de Capacidades de GRC (Gobierno, Riesgo y Cumpli-

3 Entre ellos, el compromiso de la dirección, la identificación de obligaciones, evaluaciones periódicas, etc.

4 Es decir, la posibilidad de exonerar a una empresa de responsabilidad por soborno si podía demostrar que tenía "procedimientos adecuados" para prevenirlo, lo que motivó la publicación de guías oficiales de buenas prácticas por parte del Ministerio de Justicia británico en 2011

5 Compromiso de la dirección, análisis de riesgo, debida diligencia a terceros, canales de denuncia, sanciones disciplinarias, etc.

miento), que integraba estos tres ámbitos en un marco unificado; el comité de organizaciones patrocinadoras de la Treadway Commission lanzó el conocido modelo COSO de control interno (1992, actualizado 2013) y posteriormente su marco de gestión de riesgos (ERM, 2004), utilizados como referencia para controles financieros y no financieros.

Hacia la década de 2010, esta multitud de iniciativas convergía en principios comunes. La ISO tomó nota de la demanda global y, tras varios años de trabajos, emitió en 2014 la norma ISO 19600 (directrices sobre sistemas de gestión de compliance) primer estándar internacional, aunque inicialmente orientativo y no certificable. Finalmente, en 2021 publicó la ISO 37301, que reemplaza a la anterior convirtiéndose en un estándar certificable de sistemas de gestión de compliance. Con ello, el ámbito del cumplimiento normativo pasó a contar con una "norma ISO" al igual que calidad, medio ambiente o seguridad de la información, marcando su plena madurez como disciplina de gestión.

Todo este recorrido nos ha llevado en pocas décadas a un amplio consenso mundial sobre los componentes esenciales de los sistemas de Compliance.

Los siete pilares de un sistema de *compliance* eficaz

A pesar de sus diferentes orígenes, la mayoría de los marcos de referencia coinciden en una serie de elementos fundamentales que todo programa de Compliance debería incorporar. Este consenso se ha ido forjando con el aporte de autoridades y organizaciones de prestigio. Por ejemplo, la norma alemana IDW PS 980 (2011) identificó siete componentes de un sistema de Compliance; la ISO 37301 enumera requisitos muy similares; la Fiscalía General del Estado en España, en su Circular 1/2016, detalló también los criterios para considerar eficaz un modelo de prevención de delitos; y el Departamento de Justicia de EE.UU. evalúa los programas de cumplimiento de acuerdo con pautas análogas. A continuación, resumimos estos componentes esenciales:

1. Compromiso y ejemplo desde la alta dirección ("*tone at the top*"): Este es un pilar unánimemente reconocido. Implica que el consejo de administración y la alta dirección apoyen de forma visible el cumplimiento, asignen recursos suficientes y den ejemplo con su comportamiento[6]. El *tone at the top* crea la cultura en la cual el resto del sistema operará.

2. Políticas y procedimientos claros: Un programa de compliance se articula mediante un conjunto normativo interno que traduce las obligaciones externas y los valores en conductas específicas esperadas[7]. El marco de compliance debe asegurar que todos en la empresa sepan qué se puede y no se puede hacer, ofreciendo guías escritas accesibles y actualizadas.

3. Identificación y evaluación de riesgos: La piedra angular para diseñar un sistema eficiente es realizar un risk assessment o análisis de riesgos[8]. Igualmente, se subraya que esta evaluación se revise periódicamente y ante cambios (nueva regulación, lanzamiento de un nuevo negocio, adquisición de otra empresa, etc.).

4. Controles internos y procedimientos de mitigación: Identificados los riesgos, el programa de compliance debe desplegar controles eficaces para prevenir o mitigar cada riesgo relevante[9].

6 Sin un liderazgo ético claro, cualquier política se convierte en letra muerta. Por ello, los marcos exigen evidencias como la aprobación de una política de compliance por el consejo, mensajes periódicos del CEO subrayando la importancia del código ético, y el establecimiento de una función de compliance con autoridad.

7 Esto comienza con un Código de Conducta o Código Ético que establece las pautas generales de comportamiento y los valores corporativos. Se complementa con políticas más específicas en áreas de riesgo (anticorrupción competencia, privacidad, etc.), y con procedimientos operativos que incorporan controles.

8 Consiste en identificar en qué actividades de la organización existe riesgo de incumplir normas o comprometer los valores éticos, evaluar la probabilidad e impacto de esos riesgos, y priorizarlos. Todos los marcos insisten en este enfoque proactivo: conocer los riesgos propios es necesario porque *no existe un sistema "único" válido para todos, debe ser proporcional*.

9 Estos controles pueden ser de diversa naturaleza: organizativos (p. ej., segregación de funciones en procesos sensibles, doble firma en pagos importantes), tecnológicos (filtros en sistemas informáticos, herramientas de monitoreo de transacciones), contrac-

5. Formación y comunicación: La capacitación continua del personal en materias de compliance es otro elemento universal[10].

6. Canales de denuncia y gestión de incidentes: Otro elemento crítico es contar con mecanismos para detectar y reaccionar cuando algo falla. El principal es un canal interno de denuncias (o *whistleblowing*)[11]. Tan importante como el canal en sí es el procedimiento de investigación interna[12]. Si de una investigación resulta confirmada una irregularidad, el sistema ha de prever la respuesta disciplinaria y correctiva adecuada. Un compliance efectivo requiere demostrar capacidad de *reacción* ante incidentes.

7. Supervisión, auditoría y mejora continua: Finalmente, todo sistema de gestión sigue el ciclo de mejora continua (*PDCA: Plan-Do-Check-Act*)[13].

Estos elementos constituyen, en esencia, los siete pilares del Compliance ampliamente reconocidos. Difícilmente un marco de referencia será considerado relevante si omite alguno de estos aspectos fundamentales. De hecho, cuando un regulador o juez evalúa un programa tras un incidente, suele verificar si estaban presentes y operativos todos estos componentes.

El papel de ISO y la normalización global

La llegada de la normalización internacional ha terminado de consolidar estos consensos. La ISO 37301:2021 establece de manera detallada requisitos para implantar, mantener y mejorar un Sistema de Gestión de Compliance. Sigue la estructura de alto nivel común a las normas de sistemas de gestión (HLS), facilitando la integración con ISO 9001 (calidad), ISO 14001 (medio ambiente), ISO 45001 (seguridad laboral), etc. De hecho, muchas organizaciones están aprovechando esta compatibilidad para construir *sistemas integrados de gestión ética*, donde las políticas de compliance, las de calidad y las de RSC conviven bajo una misma estrategia.

Además de ISO 37301, la normalización ha proliferado en sub-áreas: la ISO 37001:2016 sobre antisoborno brinda un marco certificable contra la corrupción (compatible con las recomendaciones de la OCDE y la FCPA); la ISO 37002:2021 da directrices sobre sistemas de gestión de denuncias (*whistleblowing*); la ISO 37008:2023 ofrece orientación para investigaciones internas; e incluso se han desarrollado normas sobre buen gobierno, como ISO 37000:2021.

En España, la entidad UNE ha publicado también normas que adaptan y concretan el Compliance a exigencias locales: la mencionada UNE 19601:2017 en el ámbito penal (alineada tanto con ISO 37301 como con los requerimientos del Código Penal español); la UNE 19602:2019 para programas de Compliance Tributario; más recientemente, en 2023, vieron la luz la UNE 19603 (compliance en libre competencia) y la UNE 19604 (compliance sociolaboral). Asimismo, en el campo de la Responsabilidad Social Corporativa (RSC) y la sostenibilidad, contamos con estándares como la ISO 26000:2010 (guía de responsabilidad social) y, a nivel nacional, la especificación UNE WG CSR Guidance:2017.

Todos estos marcos dan respuesta a las exigencias y requisitos del Eje de la Gestión Ética que mencionábamos: desde gobernanza y ética (ISO 26000 e ISO 37000) has-

tuales (cláusulas de cumplimiento en contratos con terceros), humanos (aprobaciones jerárquicas, revisiones por pares) o de supervisión (auditorías, revisiones periódicas de muestras de operaciones).

10 Los programas incorporan planes que incluyen formación *onboarding* al ingresar en la empresa y capacitación específica según el rol o el área de riesgo. Además, las empresas suelen establecer comunicaciones internas frecuentes –boletines, recordatorios, campañas de concienciación– para mantener vivo el mensaje de cumplimiento.

11 La reciente Directiva (UE) 2019/1937 de protección al informante, transpuesta en España por la Ley 2/2023, obliga ya a la mayoría de empresas medianas y grandes a tener estos canales.

12 El programa de compliance debe definir cómo se investigarán las alertas recibidas, quién lo hará, cómo se documentará y en qué plazos

13 Los programas de compliance deben incorporar procesos para monitorear su funcionamiento y evolucionar con el tiempo. Esto incluye la definición de indicadores clave de cumplimiento (KPIs), la realización de auditorías internas periódicas sobre aspectos del programa, la emisión de informes de cumplimiento al órgano de gobierno y la revisión periódica del propio sistema por parte del Compliance Officer y la dirección para introducir mejoras.

ta cumplimiento específico (UNE 19601, ISO 37001), la normalización técnica está proporcionando herramientas para estandarizar las mejores prácticas mundialmente.

TAXONOMÍA DE LOS MARCOS NORMATIVOS EN COMPLIANCE

Podemos clasificar la multitud de normas, guías y estándares de Compliance de varias formas complementarias:

Por su alcance

Algunos marcos son transversales o *generales*, aplicables a cualquier organización independientemente del sector o del riesgo específico. Ejemplos: ISO 37301 o las guías de la OCDE sobre Buen Gobierno (que aunque enfocadas en corrupción abarcan todo el sistema de controles) o las. Otros marcos son específicos por materia y se centran en un riesgo concreto. Ejemplos: ISO 37001 (anticorrupción), UNE 19602 (compliance tributario), estándares específicos para *compliance penal* como UNE 19601 en España, o lineamientos de Ministerios de Justicia como en Italia con el D.Lgs. 231/2001 y un largo etcétera según cada campo normativo.

Por último, están los marcos sectoriales, diseñados para industrias particulares con riesgos idiosincráticos. Por ejemplo, el sector financiero cuenta con los principios de Basilea y con guías de los supervisores bancarios que obligan a estructurar funciones de cumplimiento normativo en entidades de crédito; el sector farmacéutico tiene códigos de autorregulación para la promoción de medicamentos y estrictas normas de cumplimiento de Buenas Prácticas Clínicas en ensayos. Cada industria tiende a desarrollar, ya sea por regulación o autorregulación, sus propios referentes.

Por su origen o autoría

Aquí distinguimos entre marcos emanados de autoridades públicas (leyes, reglamentos, guías oficiales de reguladores) y marcos desarrollados por organismos independientes o comunidades profesionales (estándares ISO, normas UNE, códigos deontológicos, etc.).

Los marcos públicos tienen fuerza vinculante en muchos casos –por ejemplo, una Circular de la CNMV sobre la función de cumplimiento para servicios de inversión– mientras que los privados suelen ser voluntarios pero adoptados ampliamente por su credibilidad técnica. También entran aquí los llamados soft-law: documentos no obligatorios legalmente, pero emitidos por entes de prestigio que ejercen influencia. Un ejemplo de soft-law relevante son los Principios Rectores de la ONU sobre Empresas y Derechos Humanos (2011), que aunque no son ley, han servido de base para que las empresas adopten marcos de debida diligencia social (y para futuras leyes de debida diligencia, como veremos). En resumen, la comunidad de Compliance se nutre tanto de hard-law como de soft-law.

Por su ámbito geográfico

Algunos marcos son internacionales (aplicables globalmente). Las normas ISO son el ejemplo claro, al igual que las guías de la OCDE o las directrices de organizaciones sectoriales mundiales. Otros son supranacionales/regionales, como directivas de la UE que afectan a un conjunto de países (v.gr. Directiva UE 2019/1937 de *whistleblowing*). Otros son estrictamente nacionales, adaptados a la legislación y cultura de un país concreto: p.ej., la Norma Mexicana NMX-R-019-SCFI-2015 de sistemas de gestión antisoborno, o el Programa de Integridad exigido por la ley argentina 27.401/2017.

Sin embargo, cabe notar que la tendencia es hacia la convergencia: muchos estándares nacionales acaban alineados con internacionales (v.g., la UNE 19601 española se basó en gran medida en estándares como el IDW PS 980 alemán y la ISO 19600, buscando equivalencia internacional).

Complementariedad de los marcos de referencia

Esta diversidad puede parecer abrumadora, pero en la práctica muchos marcos de referencia son complementarios. Las empresas multinacionales suelen adherirse

a estándares globales (ISO, lineamientos OCDE) y a la vez cumplir con los requisitos específicos de cada jurisdicción donde operan.

Una compañía española puede certificar ISO 37301 su sistema global de compliance, y a la vez tener sistemas específicos para cumplir con la Ley Sapin II francesa (anticorrupción) al operar en Francia, con la SOX estadounidense si cotiza en NYSE, con la Ley 2/2023 española de *whistleblowing*, etc.

La armonización internacional hace que todos estos marcos hablen un idioma parecido, facilitando la integración. Hoy día, implementar un programa de compliance según ISO 37301 prácticamente asegura cubrir lo esencial que piden tanto la fiscalía española en su Circular 1/2016 como el Departamento de Justicia de EE.UU. en sus evaluaciones de compliance –lo cual demuestra el grado de consenso lograd–o.

IMPACTO DE FENÓMENOS RECIENTES EN EL MODELO DE GESTIÓN ÉTICA

En los últimos años, el entorno de Compliance se ha transformado radicalmente debido a fenómenos emergentes que obligan a evolucionar el modelo de gestión ética corporativa. Destacaremos tres ámbitos clave:

1. Retos de buen gobierno, sostenibilidad ambiental y derechos humanos desde la UE.
2. El "tsunami legislativo" y actual la tendencia a la simplificación normativa.
3. La revolución tecnológica (digitalización e IA) y su impacto operativo-regulatorio.

Estos factores configuran una "segunda oleada del Compliance": más amplia, transversal y compleja. La función de cumplimiento debe reinventarse para seguir siendo el eje vertebrador de la ética empresarial, integrando nuevas materias especializadas y marcos de referencia acordes a las nuevas exigencias. A continuación, analizamos cada reto, cómo impacta en el Compliance y qué estándares recientes sirven de guía.

Nuevas exigencias de gobernanza sostenible y derechos humanos (UE)

Europa lidera una agenda ambiciosa de sostenibilidad y deber de diligencia que extiende la responsabilidad corporativa a ámbitos antes considerados externos. Las empresas, especialmente las grandes, encaran normativas comunitarias que elevan el listón en gobierno corporativo responsable, protección de derechos humanos y medio ambiente. En particular, la Directiva (UE) 2022/2464 (CSRD) exige reportes ESG detallados sobre desempeño ambiental, social y de gobernanza. Esto obliga a recopilar datos rigurosos de sostenibilidad. Un programa de Compliance maduro apoya dicha tarea: sus métricas sobre formación ética, controles internos, sanciones o denuncias nutren los informes ESG de forma estructurada.

Aún más disruptiva es la nueva Directiva de Diligencia Debida en Sostenibilidad (aprobada en 2024), también conocida como *Corporate Sustainability Due Diligence* (CSDD). Esta norma exige a las grandes empresas europeas implantar procesos de diligencia debida obligatoria para identificar, prevenir y subsanar impactos negativos en derechos humanos y medio ambiente a lo largo de toda la cadena de suministro. En la práctica, la compañía debe mapear riesgos como trabajo infantil, explotación laboral, deforestación o contaminación incluso en sus filiales, proveedores y contratistas globales, e implementar medidas contractuales o de apoyo para evitarlos.

Además, la UE está integrando criterios ESG en la gobernanza corporativa. Por ejemplo, se incorporan objetivos de sostenibilidad en la remuneración de directivos, cuotas de diversidad en Consejos (Directiva 2022/2381) e incluso la expectativa de que los Consejos supervisen estrategias climáticas y dialoguen con stakeholders. Se espera mayor responsabilidad del Consejo de Administración en materia de sostenibilidad, reforzando la obligación de "buen gobierno sostenible".

Impacto en *Compliance*

El Compliance amplía su alcance "más allá de las puertas" de la empresa. Ya no basta

con cumplir internamente; ahora *debe velar por el comportamiento íntegro de terceros vinculados*. Este salto representa un enorme reto operativo, pero a la vez una evolución natural: un sistema de compliance robusto simplemente incorporará los nuevos riesgos ESG a su mapa de riesgos, extendiendo controles a proveedores, algo que muchas firmas ya hacían voluntariamente como parte de su RSC. En cambio, para empresas sin gestión ética, este mandato será un choque mayor.

En España, todo ello implica que la función de Compliance deberá coordinarse muy estrechamente con las áreas de sostenibilidad y gobierno corporativo. Ya no son compartimentos separados: la transparencia ESG, la debida diligencia en derechos humanos y la ética en el Consejo se entrelazan con Compliance. La "columna vertebral" de políticas y controles de cumplimiento tendrá que ensancharse para abarcar dimensiones de derechos humanos, medio ambiente y gobierno responsable.

Ante estos desafíos, los estándares que ayudan a guiar la respuesta empresarial se enriquecen, por ejemplo, a través de las EMAS[14].

En resumen, los nuevos desafíos ESG europeos ensanchan el terreno de juego del Compliance. Lejos de restarle importancia, lo robustecen y le dan mayor protagonismo: la función de Compliance debe ser garante de la ética empresarial de extremo a extremo, incorporando controles sobre terceros y asegurando la veracidad de la información no financiera divulgada. Las empresas con sistemas de cumplimiento maduros partirán con ventaja en esta transición.

"Tsunami legislativo" y actual tendencia a la simplificación

Paralelamente, las organizaciones llevan años navegando un mar de regulación creciente, especialmente intenso en Europa. Se ha hablado de un "tsunami normativo" que satura a empresas y reguladores con nuevas obligaciones en serie. Sus rasgos principales son:

- Proliferación acelerada de normas especializadas: En pocos años la UE ha desplegado grandes regulaciones: el RGPD en privacidad (2016), la Directiva de *whistleblowers* (2019), los Reglamentos de Servicios Digitales y Mercados Digitales (DSA/DMA, 2022), la citada CSRD (2022) de sostenibilidad, la Directiva de Diligencia Debida (2024), nuevos Reglamentos anti-blanqueo con autoridad europea (AMLA), la Directiva NIS2 de ciberseguridad (2022), entre otras.
- Además, el umbral de exigencia en muchas de estas regulaciones baja sensiblemente, afectando en su nivel inferior a empresas con plantillas superiores a 50 trabajadores. *Nunca tantas empresas europeas habían enfrentado tantos requisitos nuevos simultáneamente*.
- A nivel nacional, se trasponen estas normas (ej. Ley 2/2023 de protección al informante en España) y se crean otras locales (leyes de igualdad retributiva, consumidor financiero, etc.).
- Gran complejidad y detalle: Cada regulación viene con *mandatos muy específicos*: no solo qué cumplir sino cómo implementarlo[15]. Esto ha forzado a muchas empresas a crear departamentos o puestos dedicados exclusivamente a ciertos cumplimientos[16]. El riesgo es fragmentar el cumplimiento en silos altamente técnicos.
- Mayor supervisión y sanciones: Este torrente normativo viene acompañado de organismos de control más robustos y de sanciones severas. La probabilidad de ser fiscalizado y castigado por infracciones ha aumentado, incrementando

14 (EMAS-Eco-Management and Audit Scheme), esquema europeo voluntario de gestión ambiental, que complementa ISO 14001. Su adopción demuestra un compromiso proactivo con excelencia ambiental y facilita el cumplimiento de las nuevas exigencias verdes.

15 Por ejemplo, RGPD obliga a nombrar Delegados de Protección de Datos (DPO) en ciertos supuestos con funciones definidas; la Directiva de canales de denuncia especifica plazos y procedimientos para la gestión de reportes; la propuesta de Reglamento de IA clasifica y regula tecnologías de forma minuciosa.

16 DPO para datos, CISO para ciberseguridad, responsables ESG, compliance Officer tributario, etc.

la presión por un cumplimiento "real" y no solo formal.

Impacto en *Compliance* del "Tsunami legislativo"

Las más pequeñas organizaciones se han visto alcanzadas por este tsunami sin disponer de una función de Compliance, y en muchas otras que contaban con ella, se ha visto sobrepasada en alcance y complejidad. Un Compliance Officer en 2025 o bien debe entender de anticorrupción, privacidad, control exportaciones, competencia, ciberseguridad, ESG, blanqueo, protección de consumidores financieros o debe optar por sumar especialistas o delegar en otras áreas, corriendo el peligro de perder visión de conjunto. En algunas empresas ha florecido la burocracia (matrices y checklists interminables) en detrimento de la eficacia real, fenómeno llamado *paper compliance*.

A nivel macro se alzan voces para frenar la sobre-regulación europea y equilibrarla con competitividad e innovación. Un hito fue el Informe Draghi (septiembre 2024), encargado por la Comisión Europea, que advirtió que el exceso normativo podría lastrar a la UE frente a EE.UU. y China. Como consecuencia, Bruselas anunció una "pausa regulatoria": algunas iniciativas se están retrasando o replanteando, y se buscan formas de simplificar trámites (por ejemplo, consolidar múltiples reportes en uno solo). En el terreno de la IA, la UE ha moderado su postura inicialmente muy restrictiva, consciente de no ahogar el desarrollo tecnológico europeo. No se trata de desregular drásticamente, sino de legislar con más mesura y feedback de la industria[17].

En cualquier caso, el Compliance Officer debe apostar por la simplificación interna esté o no respaldada por reguladores. Algunas buenas prácticas en esta línea:

- Priorizar el enfoque a riesgos y seleccionar objetivos mediante criterios de proporcionalidad.
- Eliminar controles redundantes o "heredados" que ya no aportan valor.
- "Empaquetar" obligaciones dispersas en políticas integrales (por ej., crear un *Manual de Cumplimiento* único que abarque varias normativas sectoriales en vez de múltiples documentos).
- Aprovechar un mismo recurso para varios fines: por ejemplo, utilizar una auditoría de ISO 37301 para cubrir requisitos de auditoría de prevención penal al mismo tiempo.
- Formar al personal con una visión global de integridad, en lugar de saturar con cursos aislados por normativa.
- Apostar por la automatización y el RegTech.

Finalmente, evitar el *over-compliance* (un celo excesivo que paraliza la agilidad de negocio) es crucial. Como bien se apunta, el objetivo es la eficacia real: un sistema de cumplimiento sencillo pero vivo es preferible a uno barroco en el papel. En suma, tras el tsunami normativo, viene la marea baja: quienes logren estabilizar su programa de compliance con enfoque basado en riesgo, automatización e integración serán más resilientes ante los cambios pendulares en la regulación.

Revolución tecnológica e inteligencia artificial: impacto en *compliance*

La cuarta revolución industrial –digitalización masiva, big data, redes sociales, inteligencia artificial (IA), blockchain, etc.– está redefiniendo los modelos de negocio y planteando nuevos dilemas ético-legales inéditos una década atrás. Para Compliance, la tecnología es un arma de doble filo:

Oportunidades para *Compliance*

Las mismas innovaciones pueden potenciar la eficacia del compliance (lo que a ve-

17 Tendencia clave: *Stop the Clock*. A finales de 2024, la Comisión propuso flexibilizar la entrada en vigor de ciertos requerimientos (apodado "*stop the clock*") atendiendo a la dificultad de cumplimiento para muchas empresas. Un ejemplo es la CSRD: se planteó escalonar más los plazos y simplificar reportes para pymes cotizadas, reconociendo que no estaban preparadas. Esta reacción muestra una sensibilidad creciente a la capacidad real de cumplimiento del tejido empresarial, especialmente tras la pandemia y con nuevas tensiones geopolíticas.

ces se denomina *Compliance 4.0* o *Compliance digital*). Por ejemplo:

- Automatización de controles: Las herramientas de *RegTech*, la IA aplicada al compliance o la analítica de datos permiten diseñar a un Compliance más preventivo, proactivo y basado en datos, en lugar de reactivo.
- Comunicación y formación innovadoras: La cultura de cumplimiento en la era digital requiere nuevos canales[18].
- Eficiencia documental: Tecnologías como blockchain pueden garantizar la trazabilidad y autenticidad de registros de compliance, reforzando evidencias ante inspecciones. Los portales web y sistemas en la nube centralizan la gestión documental, permitiendo a la función compliance manejar matrices de riesgo, mapas de controles y procedimientos actualizados en tiempo real, accesibles a auditoría y dirección.

Nuevos riesgos y áreas de regulación

Por otro lado, la tecnología genera riesgos emergentes que pasan a integrar el ámbito del Compliance:

- **Ciberseguridad**: Las operaciones dependen de sistemas IT. Los ciberataques pueden causar violaciones legales[19] . La Directiva NIS2 (UE 2022) impone a empresas de sectores críticos reforzar medidas de seguridad y notificar incidentes graves en 24 horas. Esto ha llevado a muchas a nombrar un *Chief Information Security Officer (CISO)*. Si bien el CISO gestiona lo técnico, Compliance colabora estrechamente: un incidente mayor activa protocolos regulatorios (notificar a autoridades de datos, posibles responsabilidades si no se tomaron cautelas). El compliance contribuye a asegurar que existen políticas de seguridad de la información, plan de respuesta a incidentes y que el CISO reporta los eventos relevantes para evaluación legal.
- **Inteligencia Artificial (IA)**: La IA ya se utiliza en tareas como la selección de personal, concesión de créditos, diagnósticos médicos, publicidad, generando preocupaciones de ética y derechos (sesgos discriminatorios, falta de transparencia, toma de decisiones automatizadas). Europa busca regularla: el Reglamento de IA prohíbe usos inaceptables (p.ej. "score social" tipo China) y exige requisitos de compliance para IAs de "alto riesgo" (ej. algoritmos de recursos humanos, salud, transporte)[20]. Aunque la regulación final puede suavizarse, es claro que las empresas que desarrollen o usen IA deberán atender principios éticos: no discriminación, explicabilidad, seguridad, supervisión humana. Compliance jugará un rol incorporando la revisión de sistemas de IA en su radar: asegurando auditorías algorítmicas, verificando que proveedores de IA cumplan estándares y formando comités de ética digital. De hecho, el *Libro Blanco de la Función de Compliance 2024* en España menciona explícitamente el "uso responsable de la IA" como una posible área que un programa de compliance debe abarcar.
- **Privacidad y datos personales**: Tras el RGPD, la privacidad se volvió un ámbito especializado con su propio responsable (el DPD o DPO). Aquí se ve un modelo de nueva función de cumplimiento que coexiste con Compliance. Muchas veces el DPO no reporta al Compliance Officer sino directamente a alta dirección o consejo, para garantizar independencia. No obstante, Compliance debe coordinarse: las infracciones de datos implican riesgo legal y reputacional, por lo que integran el mapa de riesgos global. El Compliance apoya al DPO fomentando formación en privacidad, monitorizando implementación de políticas de protección de datos, e incluyendo al

18 Muchas empresas crean apps móviles internas para que empleados reporten inquietudes éticas fácilmente o consulten políticas al instante. Otras usan micro-vídeos, podcasts y gamificación e-learning para formar en Compliance, adaptándose a las generaciones jóvenes habituadas a contenido interactivo. Así, el mensaje de integridad cala mejor.

19 Brechas de datos personales, interrupciones que incumplen obligaciones con clientes, robo de secretos comerciales

20 Estos requisitos incluirán evaluaciones de conformidad, documentación técnica, controles de precisión y ausencia de sesgos, etc. España se adelantó con la creación de la Agencia Española de Supervisión de IA (AESIA).

DPO en comités de cumplimiento. Este patrón se repite con otras funciones emergentes, la clave es no trabajar en silos.

- **Entorno laboral digital**: La tecnología cambió la forma de trabajar (teletrabajo, comunicaciones virtuales permanentes). Surgen cuestiones antes inexistentes[21], que se materializan en políticas de empresa (política de teletrabajo, de uso de email y herramientas corporativas, de clasificación de información). Compliance colabora con RR.HH. para desarrollar y difundir estas normas de conducta en lo digital, asegurando que respeten las leyes laborales y de privacidad al tiempo que protegen a la empresa[22].

En resumen, la innovación tecnológica expande el tablero de Compliance en dos direcciones. Primero, proporciona nuevas armas para hacer cumplir las normas con más eficacia (automatización, análisis masivo, e-learning creativo). Segundo, plantea nuevos frentes que el compliance debe cubrir (ciber, IA, privacidad, etc.), a menudo en colaboración con especialistas. Las organizaciones inteligentes integran ambos lados: usan la tecnología para gestionar los riesgos de la propia tecnología. Por ejemplo, usar IA para detectar filtraciones de datos internas a la par que se implementan controles éticos en las IA de negocio. Las empresas que logren incorporar la gestión de riesgos digitales en su sistema de compliance global tendrán una ventaja en resiliencia. Como reflexiona el Libro Blanco 2024, el Compliance Officer del futuro deberá ser también un *agente de cambio cultural* en materia digital, promoviendo no solo el cumplimiento formal sino el uso ético por convicción de estas herramientas disruptivas.

Ante estos desafíos, los estándares que ayudan a guiar la respuesta empresarial se enriquecen, por ejemplo, a través de las ya aplicadas normas ISO 27001 / ISO 27701: estándares de seguridad de la información y privacidad, respectivamente[23].

En este ámbito, el crecimiento de marcos normativos es equivalente al ritmo de crecimiento de la tecnología, de modo que no podemos dejar de citar la importancia que adquieren progresivamente la norma ISO/IEC 42001 (en desarrollo): futuro estándar de gestión de IA confiable[24], las Guías éticas publicadas por organismos como IEEE o la UE (Directrices Éticas para una IA fiable, 2019)[25] o la NIST AI Risk Management Framework (EE.UU., 2023)[26].

En conclusión, la revolución tecnológica exige que Compliance evolucione a un enfoque 360° que abarque los riesgos digitales. La misión esencial –asegurar integridad y cumplimiento– permanece, pero el tablero se hace más complejo con piezas como algoritmos y ciberamenazas. Las compañías que integren en su ADN de cumplimiento la dimensión tecnológica navegarán mejor el futuro. En palabras de un informe del Real Instituto Elcano, *"la creciente geopolítica económica exige a las empresas un compliance robusto en sanciones y control de exportaciones, so pena de graves consecuencias"*, a lo que podemos añadir: la creciente digitalización exige un compliance robusto en ciberseguridad y ética de la IA.

EVOLUCIÓN DE LA FUNCIÓN DE COMPLIANCE ANTE ESTOS DESAFÍOS

Los tres ámbitos descritos trazan una clara premisa: lejos de volverse obsoleto, el Com-

21 Derecho a la desconexión digital, control del uso de dispositivos corporativos, protección de secretos comerciales en entornos remotos, monitoreo de productividad vs. privacidad de empleados, etc.

22 Un ejemplo es establecer directrices claras sobre no enviar correos fuera de horario salvo urgencia (para cumplir la desconexión) o sobre qué información puede subirse a nubes públicas.

23 Aunque a cargo de TI, su adopción conlleva requisitos de gobierno, evaluación de riesgo y controles que encajan en las mejores prácticas de compliance. Certificar ISO 27001 demuestra a reguladores y socios un compromiso serio con ciberseguridad, ayudando a cumplir NIS2.

24 La normalización internacional de IA está en marcha, y contar con frameworks técnicos voluntarios puede mitigar riesgos legales. Por ejemplo, si una IA certificada bajo un esquema reconocido falla, la empresa podría demostrar diligencia debida.

25 Incluir esos principios (justicia, transparencia, rendición de cuentas) en las políticas internas o en la evaluación de proveedores de IA anticipa el cumplimiento de la venidera regulación e inspira confianza en stakeholders.

26 marco voluntario de EE.UU. para la gestión de riesgos de IA. Dado que la regulación americana es más laxa, muchas empresas globales adoptarán esquemas como el de NIST para mostrar autorregulación.

pliance se expande y gana centralidad en la gobernanza corporativa. Sin embargo, para responder efectivamente, la propia función de Compliance debe transformarse en su enfoque y estructura.

Integración y gobernanza de la función

Con tantos riesgos nuevos y especialistas involucrados, aumenta la importancia de que exista un "director de orquesta". Con independencia del modelo de gobernanza del Compliance que hayan optado, muchas organizaciones están optando por modelos de gestión en que la Función de Compliance Corporativa actúa como función *paraguas* que coordina o supervisa funcionalmente a los responsables de cumplimiento especializados (penal, protección de datos, seguridad de la información, fiscal, ESG, etc.), aunque orgánicamente dependan de otras áreas. Así se mantiene un eje vertebrador único y se previene la visión fragmentada. Este enfoque coincide con la idea de crear una "superestructura de Compliance" mencionada en el Libro Blanco de ASCOM 2024: un programa de cumplimiento transversal que agrupa los diversos programas específicos, garantizando coherencia y cobertura integral.

En la práctica, esto requiere que la Función de Compliance:

- Establezca mecanismos de reporte unificado para intercambiar hallazgos y avances, consolidando esa información en un informe único al Consejo o Comité de Auditoría.
- Desarrolle metodologías comunes: Alineando matrices de riesgos, criterios de evaluación y procedimientos disciplinarios en todos los ámbitos. Así, si surge un caso, se aplica un protocolo uniforme (investigación, comité sancionador) sea por un fraude contable o un acoso sexual, adaptando las peculiaridades, pero manteniendo principios consistentes.
- Impulse sin acaparar: El Libro Blanco recalca diferenciar las tareas propias de Compliance de las que esta función debe fomentar en otras áreas[27]. Esta coordinación y supervisión diferenciada refuerza al Compliance Officer como especialista corporativo en riesgos con visión independiente.

Mejora de recursos y capacidades

La dirección espera más del Compliance Officer: no solo evitar multas, sino ayudar a navegar un entorno complejo de expectativas sociales y regulatorias. Para lograrlo, la función necesitará:

- Recursos adecuados: presupuestos y equipos dimensionados a su ampliada misión. Invertir en tecnología de compliance (como vimos) es esencial; también puede requerir consultoría externa en áreas emergentes (p.ej., contratar un *ethics by design* especialista para IA).
- Formación permanente: El Compliance Officer del futuro debe dominar nociones de *data analytics*, entender bases de inteligencia artificial, conocer estándares ESG... además de refinar sus habilidades blandas: liderazgo ético, comunicación efectiva, persuasión a la alta dirección. Como indica el Libro Blanco, las cuestiones culturales y de valores serán cada vez más centrales en su rol.
- Colaboración interdepartamental: Compliance deberá estrechar lazos con Recursos Humanos (cultura ética, clima, sanciones), Auditoría Interna (planes de auditoría de cumplimiento), Asesoría Jurídica (interpretación normativa), Riesgos (alinear metodologías) y Sostenibilidad (objetivos ESG voluntarios). Incluso se ve la figura integrada de Director de Cumplimiento y Sostenibilidad en algunas empresas, reconociendo la sinergia entre ambas áreas.

En definitiva, la función de Compliance evoluciona hacia ser la "columna vertebral" especializada en riesgos éticos y legales que da coherencia y liderazgo interno. En lugar de diluirse entre tantas funciones

27 Ejemplo: la formación en ciberseguridad la ejecutará TI, pero Compliance debe asegurarse de que se realice y cubra los riesgos relevantes, actuando como catalizador. Igual con sostenibilidad: el departamento ESG elaborará el plan ambiental, pero Compliance vela porque se integren los requisitos legales (p.ej. límites emisiones) y se reporte con veracidad.

nuevas, el Compliance debe ser el eje que aporta sentido y unidad a la gestión ética de la organización en el siglo XXI.

Las empresas que comprendan esto fortalecerán dicha función dotándola de autoridad suficiente, sabiendo que de su buen hacer depende en gran medida la resiliencia y reputación corporativa en un contexto cambiante. O como resume el Libro Blanco 2024: "una sólida cultura de cumplimiento es la mejor brújula para navegar un entorno global incierto".

Marcos normativos para la segunda oleada del *compliance*

Acompañando esta evolución interna, han surgido estándares recientes que ayudan a formalizar y profesionalizar la función de compliance adaptada a estos retos (ver figura 2).

FIGURA 2
PRINCIPALES ESTÁNDARES Y GUÍAS EMERGENTES DE COMPLIANCE

Marco de referencia	Ámbito / Propósito	Contribución al nuevo Compliance
ISO 37301:2021 (Compliance)	Sistema de gestión de cumplimiento certificable (sustituye ISO 19600).	Estructura integral PDCA para integrar nuevos riesgos ESG, IA, etc. Facilita auditoría y mejora continua de todo el programa6.
ISO 37000:2021 (Gobernanza)	Principios de buen gobierno corporativo.	Refuerza tono ético desde el Consejo, alineando la gobernanza con objetivos sostenibles y apoyo a Compliance.
ISO 37002:2021 (Denuncias)	Directrices para canales de denuncia y protección del informante.	Asegura sistemas confidenciales y efectivos para destapar irregularidades, clave para identificar riesgos ocultos.
ISO 37003:2025 (Antifraude)	Guía para implementar un sistema de control de fraudes.	Provee metodología global contra el fraude corporativo, fortaleciendo la respuesta a un riesgo atemporal con enfoque moderno.
ISO 37008:2023 (Investigaciones)	Orientación sobre cómo conducir investigaciones internas éticas y efectivas.	Garantiza que al investigar un incidente (fraude, acoso, ciberataque) se sigan procesos justos, rigurosos y bien documentados.
EMAS (revisado) (Ambiental)	Esquema UE de gestión y auditoría ambiental (Reglamento 1221/2009).	Demuestra compromiso ambiental más allá de mínimos legales. Ayuda a cumplir con confianza futuras exigencias climáticas y de economía circular.
Libro Blanco Compliance 2024 (ASCOM)	Guía nacional sobre gobernanza, autonomía, tareas y perfil del Compliance Officer.	Define la "superestructura" de Compliance y la diferenciación de funciones. Profesionaliza el rol alineándolo con mejores prácticas y expectativas judiciales.
NIST AI Framework 2023 (USA)	Marco voluntario de gestión de riesgos en sistemas de IA.	Sugiere controles y evaluaciones para IA fiables (transparencia, sesgos, seguridad). Sirve de base para anticipar cumplimiento de normativas IA.
Principios OCDE 2023 (Gob. Corp.)	Actualización de principios de gobierno corporativo de la OCDE.	Incorpora factores ESG y diligencia debida en gobierno. Orienta a Consejos a supervisar cultura compliance y riesgos emergentes.
Guías Ética Digital UE (2019)	Pautas para lograr una IA fiable (Trustworthy AI).	Recomiendan integrar ética en diseño de IA. Su seguimiento voluntario posiciona a la empresa como responsable y reduce riesgo de futuros conflictos legales o reputacionales.

Fuente: OEPM

ISO 37301:2021 – Sistemas de gestión de *compliance*

Norma internacional certificable que sustituye a ISO 19600. Establece de forma holística los requisitos para implantar, mantener y mejorar un programa de compliance efectivo. Su adopción facilita integrar compliance con otros sistemas (calidad, ambiental) gracias a su estructura común de alto nivel. Para muchas empresas, certificarse en ISO 37301 se ha vuelto el *gold standard* para demostrar a partes interesadas (inversores, reguladores) que su modelo de cumplimiento sigue las mejores prácticas globales.

ISO 37000:2021 – Gobernanza de las organizaciones

Guía internacional de buen gobierno corporativo. Aunque dirigida al Consejo y alta dirección, guarda relación con Compliance pues promueve principios de transparencia, integridad, sostenibilidad en la toma de decisiones. Un Consejo que siga ISO 37000 creará el tono adecuado ("tone at the top") y soportes a la función de compliance. Así, ISO 37000 + 37301 forman una dupla potente de gobernanza ética.

ISO 37002:2021 – Sistemas de gestión de denuncias (whistleblowing)

Brinda directrices para establecer canales internos de denuncia y gestionar las investigaciones con confidencialidad, imparcialidad y protección del informante. Permite crear sistemas transversales que apliquen a todas las jurisdicciones y empresas de una organización al mismo tiempo que permiten cumplir los requisitos concretos de un país o regulación específica.

ISO 37003:2025 – *Fraud Risk Management Systems*

Es un nuevo estándar (publicado en mayo 2025) que ofrece guía completa para gestionar el riesgo de fraude en las organizaciones. Cubre desde la evaluación de vulnerabilidades de fraude hasta las respuestas correctivas. Dada la sofisticación creciente del fraude global, ISO 37003 llena un vacío, proporcionando un marco estructurado para controles antifraude.

Libro Blanco de la Función de *Compliance* (ASCOM 2024)

Este documento de la Asociación Española de Compliance (segunda edición revisada) fija un marco de referencia profesional para el Compliance Officer y para el desarrollo de la Función de Compliance en todo tipo de organizaciones. Define la gobernanza ideal de la función (dependencia jerárquica, autonomía, independencia), los cometidos esenciales (prevención, detección, gestión de riesgos de compliance operando uno o varios programas), y las competencias requeridas. Incorpora nuevas tendencias como la gestión de *compliance transversal* y actualiza las responsabilidades a la luz de los últimos cambios normativos. Es una guía no vinculante, pero muy influyente en todo el mundo: orienta a empresas, auditores y tribunales sobre qué esperar de un programa y un responsable de compliance bien estructurados. Por ejemplo, subraya la necesidad de dotar a Compliance de recursos proporcionados, de formalizar su interacción con el Consejo (informes periódicos, canales de comunicación directa) y de establecer esa diferenciación de tareas propias vs. delegadas que mencionamos. Seguir las recomendaciones del Libro Blanco ayuda a cumplir con la *"exigencia de organización adecuada"* que pide el Código Penal español para eximir responsabilidad a la persona jurídica. Asimismo, profesionaliza la función: promueve la certificación de los compliance officers (CESCOM®) y reconoce la complejidad técnica de su labor. En definitiva, adoptar internamente las directrices del Libro Blanco eleva la madurez de la función de compliance y la prepara para enfrentar los retos actuales con rigor.

En suma, estos marcos aumentan la capacidad del Compliance para adaptarse y responder a los nuevos desafíos: dotan de método, estandarización y credibilidad a la función en su versión ampliada. Un programa guiado por ISO 37301 integrará sin problemas los riesgos ESG y digitales en su ciclo PDCA; un Compliance Officer apoyado por el Libro Blanco sabrá cómo estructurar su relación con el Consejo en temas emer-

gentes; un sistema ISO 37002 asegurará que la voz de los denunciantes (claves para detectar abusos de IA, por ejemplo) sea escuchada y protegida. Las organizaciones harían bien en apoyarse en estas referencias para fortalecer su compliance "2.0".

REFLEXIÓN FINAL: EL FUTURO DEL COMPLIANCE ANTE TENDENCIAS GLOBALES

Al proyectar hacia los próximos años, el universo del Compliance seguirá condicionado por dinámicas globales complejas que plantean tanto desafíos como oportunidades para reafirmar su valor en las organizaciones. Entre esas dinámicas destacan: una posible desglobalización o fragmentación de mercados, las asimetrías normativas entre EE.UU. y Europa, los intentos de simplificación regulatoria en la UE para recuperar competitividad, y los realineamientos geopolíticos (conflictos, cambios de poder) que afectan al comercio y a las reglas del juego internacionales. Tratamos de responder a continuación qué significan estos fenómenos para la gestión ética y el Compliance.

Regulación en un mundo multipolar

Tras décadas de globalización económica que favorecieron cierta armonización emergen tendencias de fragmentación por bloques. Tensiones comerciales, nacionalismos y búsqueda de autosuficiencia hacen pensar en una divergencia mayor de marcos regulatorios entre regiones. Ya hoy EE.UU. y la UE tienen enfoques regulatorios distintos en varios campos.

Para las multinacionales, esto supone operar en un entorno con estándares divergentes. Un mismo acto puede ser legal en un país, pero sancionable en otro. La empresa global debe cumplir todas las que le apliquen, lo cual es complejo.

Los sistemas de compliance deberán ser muy flexibles y sofisticados, capaces de adaptar políticas a diferentes marcos legales. Se hará más común la estrategia de la *"lex más estricta"* como estándar interno –es decir, la empresa adopta globalmente el criterio más exigente de los países donde opera, para no incurrir en incumplimiento en ningún lugar–. De hecho, muchas ya lo hacen (por ej., aplican políticas GDPR en todas sus filiales mundiales, porque es más simple y segura una única norma alta que múltiples niveles). Sin embargo, cuando las reglas son directamente incompatibles aparecerán verdaderos dilemas estratégicos. El Compliance Officer deberá asesorar en decisiones difíciles de cumplimiento transfronterizo, ponderando riesgos jurídicos vs. comerciales. Apoyarse en redes internacionales de asesoría (bufetes globales, asociaciones profesionales) será vital para interpretar nuevas leyes de jurisdicciones lejanas.

Desglobalización y cadenas regionales

Si las cadenas de suministro se reconfiguran hacia entornos más locales o por bloques, algunos riesgos bajan, pero otros suben. Menos proveedores lejanos con estándares laborales dispares pueden reducir riesgos de abuso de DD.HH., pero surgen nuevas regulaciones proteccionistas: controles de exportación más estrictos, exigencias de contenido local, aranceles comerciales, etc. Por ejemplo, EE.UU. y UE impulsan leyes para proteger tecnologías sensibles (chips, IA) de adversarios: esto comporta cumplir estrictas normativas de seguridad nacional y export control. Las empresas también deben robustecer su compliance en comercio internacional y sanciones, área clásica que cobra vigor renovado. Todo ello añade carga al compliance global: habrá que desarrollar expertise local o delegar en equipos regionales de compliance que aseguren alineación con normativas del bloque.

Simplificación vs. Intervención

Si la UE concreta su voluntad de simplificación normativa, podría aliviar duplicidades burocráticas: por ejemplo, se discute unificar distintos informes (igualdad, no financiero, gobierno corporativo) en uno solo

integral, o eximir totalmente a pymes de ciertas cargas. Pero no esperemos "barra libre": en temas críticos no habrá marcha atrás. Al contrario, en ciertos ámbitos podríamos ver nuevas regulaciones globales impulsadas por foros internacionales[28].

Asimismo, la historia muestra ciclos: periodos de desregulación seguidos de reacciones reguladoras tras crisis (v.gr. 2008-2010 con finanzas). Por tanto, Compliance debe cultivar una vigilancia estratégica, escaneando el horizonte normativo y político para anticipar giros. El uso de herramientas de inteligencia (monitorización de propuestas legislativas, análisis de noticias) será parte del trabajo preventivo. Aquellas funciones de compliance con *foresight* podrán preparar a su empresa (p.ej., viendo venir la regulación de IA, comenzar ya un comité ético interno para ganar experiencia).

Geopolítica y *Compliance*

Factores políticos pueden redefinir prioridades de cumplimiento casi de la noche a la mañana. El gobierno Trump ha comportado un auténtico cambio de paradigma respecto a los objetivos ESG en EEUU o la relajación de normas financieras, pero intensificar las sanciones comerciales y controles migratorios. Se constata una menor cooperación internacional en estándares comunes y más énfasis en leyes nacionales diferenciales. Para empresas globales, mantener políticas uniformes será más complicado: quizá tengan que segmentar sus operaciones por bloques regulatorios (un juego de reglas para UE, otro para EE.UU., otro para China/Rusia).

Además, crisis geopolíticas –conflictos bélicos, guerras comerciales– generan oleadas de sanciones y normativas de emergencia. Lo hemos comprobado con Ucrania: en semanas se prohibieron transacciones con decenas de entidades rusas y se vetó exportar tecnología dual; muchas empresas tuvieron que cesar actividades o reestructurar cadenas inmediatamente. Un buen sistema de compliance se diseña también para reaccionar rápido: tener identificados terceros críticos, incluir cláusulas contractuales de fuerza mayor por sanciones, monitorear diariamente listas de personas bloqueadas, etc. Esta agilidad será cada vez más apreciada: la "incertidumbre permanente" es parte del entorno.

Rol futuro del *Compliance Officer*

En este contexto volátil, el profesional de compliance debe reforzar su perfil *estratégico*. Tendrá que saber comunicar a la alta dirección no solo qué norma cumplir, sino por qué conviene hacerlo más allá de la multa, y cómo encaja con la estrategia corporativa y reputacional. Será un diplomático interno: ayudando a conciliar las demandas a veces opuestas de distintos stakeholders (inversores piden rentabilidad, reguladores cumplimiento estricto, consumidores comportamientos éticos, empleados equilibrio trabajo-vida). En situaciones no contempladas por la ley, será la brújula ética de la empresa: si la norma no llega donde la tecnología avanza, la cultura corporativa sostendrá las decisiones correctas, y ahí el Compliance Officer es guardián de esos valores.

La tecnología, paradójicamente, puede ser aliada para gestionar lo impredecible: las IAs generativas podrían en unos años ayudar al compliance a *predecir áreas de riesgo emergente* analizando big data (noticias, redes, discursos políticos) y proponiendo medidas preventivas. Pero la esencia del compliance –la responsabilidad humana de "hacer lo correcto"– seguirá sin substituto. Como recalca el Libro Blanco, la cultura de cumplimiento, el respeto a los valores y a la legalidad, traducido en conductas efectivas, es el ancla más segura en tiempos inciertos.

En síntesis, el futuro del *Compliance* requerirá equilibrio en múltiples ejes:

- Global vs. local: adoptar estándares internacionales altos, pero adaptarse con flexibilidad a requisitos locales. Proba-

28 Ejemplo: acuerdos OCDE/G20 para tributación global (impuesto mínimo a multinacionales) que forzarán compliance fiscal más complejo. O en big tech, tras el DSA europeo, otros países podrían replicar normas de contenidos o competencia.

blemente, la empresa responsable optará por exceder voluntariamente las exigencias donde estas sean laxas (ej. aplicar políticas anticorrupción estrictas globalmente aunque algunos países no las exijan), creando un mínimo común elevado.

- Regulación vs. innovación: proteger sin ahogar. El Compliance deberá aprender a decir "sí, pero..." en lugar de solo "no". ¿Se puede lanzar tal innovador producto digital? Sí, pero incorporando desde diseño protecciones de privacidad y algoritmos auditables (*compliance by design*). Este rol de facilitador –no mero policía– será crucial para que la empresa no vea cumplimiento como freno sino como garantía de *sustainable business*.
- Exigencias de distintos grupos de interés: inversores piden gobierno corporativo sólido, ONGs piden responsabilidad social, reguladores cumplimiento de la ley, clientes calidad y ética. El Compliance Officer actuará como generador de equilibrio, ayudando a la dirección a encontrar la senda donde la empresa puede ser competitiva sin sacrificar integridad.

En las organizaciones basadas en un modelo de gestión ética, Compliance ha dejado de ser un centro de coste inevitable, para convertirse en un habilitador de negocio sostenible a largo plazo. Las organizaciones pioneras lo integrarán en su planificación estratégica (p.ej. evaluando riesgos geopolíticos antes de entrar a cierto mercado, decisión donde Compliance aporta inteligencia).

En definitiva, la premisa clave permanece: cumplir con la ley y con la ética es la única forma de construir confianza y éxito a largo plazo. En tiempos convulsos, esa confianza deviene el activo más valioso de la empresa.

Cerramos con la idea de que, en el siglo XXI, el Compliance no es un freno, sino un eje dinamizador: es el cimiento de confianza sobre el cual se pueden construir innovaciones y crecer en nuevos mercados con seguridad. Lejos de ser una moda pasajera, se ha vuelto una función tan indispensable como finanzas o TI. Por tanto, el futuro no es *menos* compliance, sino mejor compliance: más integrado en la estrategia, más inteligente en su ejecución y más valorado por todos.

Los marcos normativos del Compliance apuntan en esa dirección, los retos globales que afrontemos encontrarán en la empresa ética un aliado para superarlos, porque una sólida cultura de cumplimiento es –y seguirá siendo– la mejor brújula para navegar un contexto global cambiante.

SOBRE EL AUTOR

Francisco Bonatti Bonet es consultor y auditor de Compliance, así como secretario de la Junta Directiva de la Asociación Española de Compliance.