EL COMPLIANCE EN LA ERA DE LA IA

La gestión de los riesgos jurídicos tras la irrupción de la IA en las empresas

XAVIER RIBAS

DIRECTOR

VÍCTOR MANUEL ANTUNES RIVERA
AGUSTINA BARISONE
ANA CANET ARANDA
CARLA CASAS
JULEN DOUSSINAGUE OYARZABAL
ELISABET ESCAYOLA
RAMÓN FAUS SANTASUSANA
QUERALT GARCÍAS
ALEJANDRO GIMÉNEZ GUTIÉRREZ
CARMEN LÓPEZ RUIZ
CARLOS MADRONA
AMEDEO MARCHELLI
ALBA MORENO
INÉS NÁJERA-ALESÓN RODRÍGUEZ-LOSADA
XAVIER RIBAS
MARC RIUS
ALEJANDRA SALAT FRAGA
CARLOS SOUCASE FURIÓ
JUAN PABLO TORNOS
REBECA VELASCO
JOAN XIFRA

Si quieres adquirir esta obra haz click aquí

ARANZADI

© **Xavier Ribas (Dir.) y otros** 2026
© **ARANZADI LA LEY, S.A.U.**

ARANZADI LA LEY, S.A.U.
C/ Serrano Galvache 26
28033 Madrid
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/publicaciones

Primera edición: 2026

Depósito Legal: M-27130-2026
ISBN versión impresa: 979-13-7061-022-7
ISBN versión electrónica: 979-13-7061-023-4

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

© **ARANZADI LA LEY, S.A.U.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, ARANZADI LA LEY, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.
Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, **www.cedro.org**) si necesita fotocopiar o escanear algún fragmento de esta obra.
El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.
El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.
ARANZADI LA LEY no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, o cualesquiera otras herramientas de participación. Igualmente, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.
ARANZADI LA LEY queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.
ARANZADI LA LEY se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.
Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **ARANZADI LA LEY, S.A.U.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Si quieres adquirir esta obra haz click aquí

Índice General

Página

1

MODELOS DE CUMPLIMIENTO 2026

CAPÍTULO 1.1.

ARGUMENTOS PARA MANTENER UN MODELO DE CUMPLIMIENTO EN LAS EMPRESAS ESPAÑOLAS EN 2026

CARLOS MADRONA 71

1. INTRODUCCIÓN 71

2. EVOLUCIÓN DE LA RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA EN ESPAÑA 71

3. EL ARTÍCULO 31 BIS DEL CÓDIGO PENAL: FUNDAMENTO Y ALCANCE 74

4. MODELOS DE ORGANIZACIÓN Y GESTIÓN: EL CORAZÓN DEL COMPLIANCE 74

5. ROL DE LOS ÓRGANOS DE GOBIERNO EN EL MODELO DE CUMPLIMIENTO 76

6. DECÁLOGO DE ARGUMENTOS A FAVOR DE MANTENER Y REFORZAR EL MODELO EN 2026 77

7. DESAFÍOS ACTUALES Y FUTUROS DEL COMPLIANCE EN ESPAÑA (2026 Y MÁS ALLÁ) 79

8. CONCLUSIONES 82

Si quieres adquirir esta obra haz click aquí

Página

9. REFERENCIAS LEGALES Y NORMATIVAS QUE JUSTIFICAN LOS MODELOS DE CUMPLIMIENTO (2026)..... 83

CAPÍTULO 1.2.

FATIGA NORMATIVA

XAVIER RIBAS..... 87

1. RÉCORD DE HIPERREGULACIÓN..... 87

2. FACTORES QUE FAVORECEN ESTA HIPERREGULACIÓN..... 88

3. EL INFORME DRAGHI..... 88

4. INICIATIVAS DE SIMPLIFICACIÓN NORMATIVA..... 89

5. INICIATIVA DIGITAL ÓMNIBUS..... 90

6. INICIATIVA ÓMNIBUS DE SOSTENIBILIDAD Y REPORTING CORPORATIVO..... 90

7. CONCEPTO DE FATIGA NORMATIVA..... 92

8. CONCLUSIÓN..... 95

CAPÍTULO 1.3.

HIPERREGULACIÓN, FATIGA NORMATIVA Y CUMPLIMIENTO

JUAN PABLO TORNOS..... 97

1. CUANDO CUMPLIR AL 100% ES IMPOSIBLE..... 97

2. LA GRADUACIÓN DE LAS SANCIONES..... 97

3. EL PRINCIPIO DE PROPORCIONALIDAD: LA HIPERREGULACIÓN EN LA PROPORCIONALIDAD DE LA SANCIÓN..... 98

4. EL PRINCIPIO DE CULPABILIDAD: LA HIPERREGULACIÓN COMO FACTOR ATENUANTE DE LA CULPABILIDAD..... 98

5. POR QUÉ EL CUMPLIMIENTO PARCIAL PUEDE ATENUAR..... 99

6. PRIORIZAR Y DOCUMENTAR..... 99

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 1.4.

EL CÓDIGO ÉTICO

REBECA VELASCO 101

1. INTRODUCCIÓN 101

2. FINALIDAD Y CONTENIDO DEL CÓDIGO ÉTICO 102

3. EL CÓDIGO ÉTICO EN LOS ESTÁNDARES ISO 37301, ISO 37001, ISO 37002 Y LA UNE-19601 103

4. LA ÉTICA COMO FUNDAMENTO DE LA SOSTENIBILIDAD CORPORATIVA 104

5. INDICADORES DE CUMPLIMIENTO 106

6. CONCLUSIONES 106

CAPÍTULO 1.5.

FUNCIONES DEL CONSEJO DE ADMINISTRACIÓN EN MATERIA DE CUMPLIMIENTO

AMEDEO MARCHELLI 109

1. INTRODUCCIÓN 109

2. BASE LEGAL EN ESPAÑA 110

2.1. Código Penal 110

2.2. Ley de Sociedades de Capital 110

2.3. Facultades Indelegables 111

2.4. Criterios de la Fiscalía General del Estado 111

2.5. Aplicación práctica en PYMEs 112

3. ESTÁNDARES INTERNACIONALES 112

3.1. ISO 37301: Sistema de Gestión de Compliance 112

3.2. Principios de la Función de Compliance 113

3.3. Otros Estándares Relevantes 114

4. DIRECTRICES DE ORGANISMOS REGULADORES NO ESPAÑOLES 114

4.1. Principios de la OCDE 114

4.2. Criterios del Departamento de Justicia de EE.UU. 114

4.3. Guía del UK Bribery Act 115

4.4. Principios del Comité de Basilea 115

Si quieres adquirir esta obra haz click aquí

Página

5. EL MODELO DE LAS TRES LÍNEAS 116
5.1. Responsabilidades del Consejo 116
5.2. Las Tres Líneas 116
5.3. Información al Consejo 116
5.4. Escalado del modelo de tres líneas en PYMEs 117
6. CÓDIGO DE BUEN GOBIERNO 117
7. NORMATIVA EUROPEA 117
7.1. Directiva de Protección del Informante 117
8. LEGISLACIÓN COMPARADA 118
9. FUNCIONES ESPECÍFICAS DEL CONSEJO 119
9.1. Aprobar 119
9.2. Supervisar 119
9.3. Garantizar 119
9.4. Decidir 120
10. INDICADORES DE COMPROMISO 120
11. RIESGOS DE UN CONSEJO PASIVO 121
12. CONCLUSIONES 121

CAPÍTULO 1.6.

EL PAPEL DEL SECRETARIO DEL CONSEJO EN LA LEY DE SOCIEDADES DE CAPITAL

VÍCTOR MANUEL ANTUNES RIVERA 123

1. INTRODUCCIÓN. REGULACIÓN EN LA LEY DE SOCIEDADES DE CAPITAL 123
2. ¿PUEDE EL COMPLIANCE OFFICER SER NOMBRADO SECRETARIO DEL CONSEJO DE ADMINISTRACIÓN? 124
3. DEFINICIÓN Y DELIMITACIÓN DE LAS FUNCIONES DEL SECRETARIO DEL CONSEJO. EJEMPLO DE CLÁUSULA DELIMITADORA DE FUNCIONES 125
4. CÓMO EJERCER LA FUNCIÓN DE SECRETARIO: ACCIONES PARA EL BUEN DESARROLLO DE LA FUNCIÓN 127

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 1.7.

COMPLIANCE OFFICER Y COMITÉ DE COMPLIANCE

VÍCTOR MANUEL ANTUNES RIVERA 131

1. EL COMPLIANCE OFFICER Y EL COMITÉ DE COMPLIANCE. CONCEPTO Y FUNCIONES 131

2. COMITÉ DE COMPLIANCE. COMPOSICIÓN. FUNCIONAMIENTO 133

3. CARACTERÍSTICAS PARA DESEMPEÑAR EL ROL DE COMPLIANCE OFFICER 137

CAPÍTULO 1.8.

LA INTELIGENCIA ARTIFICIAL COMO NUEVO EJE DEL COMPLIANCE CORPORATIVO: GOBERNANZA, RIESGOS, RESPONSABILIDADES Y USO

ANA CANET ARANDA 139

1. INTRODUCCIÓN 141

1.1. La inteligencia artificial como una cuestión de Compliance 141

1.2. De la digitalización a la toma de decisiones automatizada 141

1.3. El nuevo rol del Compliance Officer 141

1.4. Objetivos y alcance de este capítulo 142

1.5. Enfoque práctico: de la teoría a la implantación real 142

2. CONCEPTOS FUNDAMENTALES DE INTELIGENCIA ARTIFICIAL (PARA COMPLIANCE) 142

2.1. Qué es (y qué no es) la inteligencia artificial desde la óptica del Compliance 142

2.2. Tipologías de inteligencia artificial relevantes para Compliance ... 143

2.3. El ciclo de vida de un sistema de inteligencia artificial 143

2.4. Los datos como principal fuente de riesgo 144

2.5. Modelos, entrenamiento y validación: una visión no técnica 144

2.6. Autonomía, supervisión humana y control 144

2.7. Implicaciones prácticas para el Compliance Officer 145

3. INTELIGENCIA ARTIFICIAL Y FUNCIÓN DE COMPLIANCE 145

3.1. La inteligencia artificial como nuevo objeto de Compliance 145

Si quieres adquirir esta obra haz click aquí

Página

3.2. La inteligencia artificial como herramienta de Compliance 145
3.3. El encaje de la inteligencia artificial en el modelo de tres líneas de defensa 146
3.4. Nuevas responsabilidades del Compliance Officer 146
3.5. Relación con otras funciones clave de la organización 146
3.6. Accountability algorítmica y rendición de cuentas 147
3.7. Implicaciones prácticas para la función de Compliance 147
4. MARCO NORMATIVO Y DOCTRINAL APLICABLE A LA INTELIGENCIA ARTIFICIAL 147
4.1. La inteligencia artificial como objeto regulatorio emergente 147
4.2. Panorama regulatorio internacional 147
4.2.1. Enfoque estadounidense dentro del marco internacional 148
4.3. El enfoque europeo: regulación de la inteligencia artificial 148
4.4. Relación con otras áreas normativas clave 149
4.5. Soft law, estándares y guías de referencia 149
4.6. Implicaciones para los programas de Compliance existentes 150
4.7. Enfoque práctico para el Compliance Officer 150
5. TAXONOMÍA DE RIESGOS DE LA INTELIGENCIA ARTIFICIAL 150
5.1. La necesidad de una taxonomía específica de riesgos de IA 150
5.2. Riesgos legales y regulatorios 150
5.3. Riesgos éticos 151
5.4. Riesgos operativos *151*
5.5. Riesgos reputacionales *151*
5.6. Riesgos relacionados con derechos fundamentales *151*
5.7. Riesgos derivados de terceros y de la cadena de suministro *151*
5.8. Riesgos emergentes y no evidentes *152*
5.9. Implicaciones prácticas para el mapa de riesgos de Compliance ... 152
6. EVALUACIÓN DE RIESGOS DE LA INTELIGENCIA ARTIFICIAL DESDE LA ÓPTICA DE COMPLIANCE 152
6.1. La evaluación de riesgos como eje estructural del Compliance en materia de IA 152

Si quieres adquirir esta obra haz click aquí

Página

6.2. Integración del riesgo de IA en el mapa global de riesgos corporativos 153
6.3. Identificación e inventario de sistemas de inteligencia artificial ... 153
6.4. Clasificación de los sistemas en función de su nivel de riesgo 153
6.5. Evaluación ex ante como mecanismo de prevención 153
6.6. Evaluación continua y revisión periódica 154
6.7. Documentación, trazabilidad y valor probatorio 154
6.8. El papel del Compliance Officer en la priorización y elevación de riesgos 154
6.9. Implicaciones para programas de Compliance avanzados 155
6.10. Principio de proporcionalidad y defendibilidad en la evaluación del riesgo algorítmico («good enough & defendible») 155
6.11. Gestión de la inteligencia artificial en PYMES 155

7. GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL 157
7.1. La gobernanza de la inteligencia artificial como pilar del Compliance moderno 157
7.2. Principios estructurales de la gobernanza de la IA 157
7.3. Modelos organizativos de gobernanza de la inteligencia artificial . 157
7.4. Roles y responsabilidades en la gobernanza de la IA 158
7.5. Comités de inteligencia artificial y su encaje con Compliance 158
7.6. Políticas internas de inteligencia artificial 158
7.7. Integración de la gobernanza de la IA en el sistema de Compliance 159
7.8. Escalado, toma de decisiones y gestión de conflictos 159
7.9. Implicaciones prácticas para el Compliance Officer 159

8. CONTROLES INTERNOS APLICABLES A SISTEMAS DE INTELIGENCIA ARTIFICIAL 160
8.1. Controles internos como concreción operativa de la gobernanza de la IA 160
8.2. Tipología de controles aplicables a la inteligencia artificial 160
8.3. Controles preventivos 160
8.4. Controles detectivos 160
8.5. Controles correctivos y gestión de incidentes 161

Si quieres adquirir esta obra haz click aquí

Página

8.6. Controles técnicos y organizativos 161
8.7. Evidencias y auditoría interna 161
8.8. Proporcionalidad y enfoque basado en riesgos 161
8.9. Implicaciones prácticas para el diseño del sistema de controles 161

9. GESTIÓN DE TERCEROS Y PROVEEDORES DE INTELIGENCIA ARTIFICIAL 162
9.1. La externalización de la IA como foco de riesgo 162
9.2. Principio de no delegación de la responsabilidad 162
9.3. Identificación y clasificación de proveedores 162
9.4. Due diligence específica en materia de IA 162
9.5. Cláusulas contractuales clave 162
9.6. Transparencia y límites razonables 163
9.7. Supervisión continua del proveedor 163
9.8. Responsabilidad compartida y zonas grises 163
9.9. Implicaciones prácticas para el Compliance Officer 163

10. INTELIGENCIA ARTIFICIAL Y CULTURA DE COMPLIANCE 163
10.1. La cultura de Compliance como factor crítico 163
10.2. El factor humano en entornos de IA 163
10.3. Concienciación sobre el uso responsable de la IA 164
10.4. Formación adaptada por colectivos 164
10.5. IA generativa y riesgos culturales 164
10.6. Shadow AI y control cultural 164
10.7. Canales de alerta y denuncia 164
10.8. El tono desde la alta dirección 165
10.9. Implicaciones prácticas para un Compliance sostenible 165

11. CASOS DE USO DE INTELIGENCIA ARTIFICIAL APLICADOS AL COMPLIANCE 165
11.1. La inteligencia artificial como palanca operativa del Compliance moderno 165
11.2. Monitorización continua del cumplimiento normativo 165
11.3. Prevención del blanqueo de capitales y KYC 165

Si quieres adquirir esta obra haz click aquí

Página

11.4. Revisión contractual y gestión de riesgos legales 166
11.5. Monitorización de comunicaciones corporativas 166
11.6. Detección de fraude y riesgos internos 166
11.7. Inteligencia artificial generativa en Compliance 166
11.8. Integración de IA en plataformas GRC 166
11.9. Límites, riesgos y criterios de uso responsable 167
12. INTELIGENCIA ARTIFICIAL GENERATIVA Y COMPLIANCE 167
13. DOCUMENTACIÓN, REPORTING Y EVIDENCIAS EN SISTEMAS DE INTELIGENCIA ARTIFICIAL 167
14. RESPONSABILIDAD Y TOMA DE DECISIONES EN SISTEMAS DE INTELIGENCIA ARTIFICIAL 169
15. OPORTUNIDADES ESTRATÉGICAS DE LA INTELIGENCIA ARTIFICIAL PARA LA FUNCIÓN DE COMPLIANCE ... 170
16. HOJA DE RUTA PRÁCTICA PARA IMPLANTAR LA GESTIÓN DE LA INTELIGENCIA ARTIFICIAL DESDE COMPLIANCE 170
17. ERRORES FRECUENTES EN LA GESTIÓN DE LA INTELIGENCIA ARTIFICIAL DESDE COMPLIANCE 171
18. CONCLUSIONES 172
ANEXO I. CHECKLIST DE ARRANQUE PARA LA GESTIÓN DE LA INTELIGENCIA ARTIFICIAL DESDE COMPLIANCE (30-90 DÍAS) 173

CAPÍTULO 1.9.

RESPONSABILIDAD DE LOS DIRECTIVOS Y DE LA FUNCIÓN DE COMPLIANCE: OMISIÓN DEL DEBER DE CONTROL
VÍCTOR MANUEL ANTUNES RIVERA 177
1. DEFINICIÓN DEL CONCEPTO DE DIRECTIVO. MARCO DE RESPONSABILIDAD 177
2. RESPONSABILIDAD CIVIL-MERCANTIL DE LOS DIRECTIVOS 178
3. RESPONSABILIDAD PENAL DE LOS DIRECTIVOS: OMISIÓN DE CONTROL Y PAPEL DEL PROGRAMA DE COMPLIANCE 179

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 1.10.

PROTOCOLO DE TOMA DE DECISIONES

VÍCTOR MANUEL ANTUNES RIVERA 181

1. LA TOMA DE DECISIONES EN EL ÁMBITO DEL COMPLIANCE 181

2. MATRIZ RACI Y PROTOCOLO DE TOMA DE DECISIONES PARA APLICARLO EN UNA ORGANIZACIÓN 182

CAPÍTULO 1.11.

PRUEBA DE LA FECHA DE IMPLANTACIÓN, LA ANTIGÜEDAD Y EL HISTORIAL DE VERSIONES DEL CONTROL

MARC RIUS 185

1. INTRODUCCIÓN 185

2. LA EXIGENCIA DE ACREDITAR LA EXISTENCIA DEL CONTROL 186

2.1. La fecha de implantación 187

2.2. La antigüedad del control como indicador de madurez 188

2.3. El historial de versiones y el control de cambios 189

3. MECANISMOS PROBATORIOS 189

3.1. Documentación interna: políticas, actas, comunicaciones y aprobaciones 189

3.2. Evidencias operativas derivadas de la ejecución del control 190

3.3. Evidencias derivadas de auditorías, revisiones y simulacros 190

3.4. Evidencias tecnológicas: logs, registros automáticos y sistemas GRC 191

4. SELLADO DE TIEMPO Y CERTIFICACIÓN ELECTRÓNICA DE EVIDENCIAS 191

4.1. El certificado electrónico de documento como acreditación del contenido 192

4.2. El sellado de tiempo como garantía de anterioridad 192

5. HERRAMIENTAS TECNOLÓGICAS PARA LA GESTIÓN DEL REPOSITORIO DE EVIDENCIAS 193

5.1. Sistemas de gestión documental 193

Si quieres adquirir esta obra haz click aquí

Página

5.2. Plataformas GRC y automatización de evidencias 193

5.3. Repositorios de versiones y almacenamiento inmutable 194

6. PROTOCOLIZACIÓN NOTARIAL 194

6.1. Acta notarial de exhibición de documentos 194

6.2. Escrow documental 195

7. ANÁLISIS DE RIESGOS ESPECÍFICOS 195

7.1. Riesgo de impugnación por manipulación documental 195

7.2. Riesgo de falta de continuidad en el control 196

7.3. Riesgo de obsolescencia no documentada 196

8. CASO PRÁCTICO 197

8.1. Descripción del supuesto 197

8.2. Evidencias disponibles y su evaluación probatoria 197

8.3. Evaluación final del caso 198

CAPÍTULO 1.12.

CANALES DE DENUNCIA

VÍCTOR MANUEL ANTUNES RIVERA 199

1. ¿QUÉ ES UN CANAL DE DENUNCIAS? BREVE RESUMEN DE SU REGULACIÓN EUROPEA Y ESPAÑOLA 199

2. GESTIÓN DEL CANAL DE DENUNCIAS: OBLIGACIONES A REFLEJAR EN LA POLÍTICA DEL CANAL DE DENUNCIAS 202

2.1. Implementación obligatoria o voluntaria 202

2.2. Gestión interna o externa del canal de denuncias 202

2.3. Prioridad del canal interno 204

2.4. Requisitos de la denuncia, acuse de recibo, medio de recepción e información sobre la decisión de investigación 204

2.5. Procedimiento de investigación dentro del canal de denuncias: ¿a qué se refiere? 205

Si quieres adquirir esta obra haz click aquí

Página

2.6. Protección del denunciante 206

2.7. Registro de denuncias 208

2.8. Revisión y remediación de las deficiencias detectadas como consecuencia de las investigaciones 209

CAPÍTULO 1.13.

INVESTIGACIONES INTERNAS

JUAN PABLO TORNOS 211

1. INTRODUCCIÓN 212

2. CONCEPTO Y EVOLUCIÓN DE LAS INVESTIGACIONES INTERNAS 212

2.1. Concepto de investigación interna 212

2.2. Evolución y expansión de las investigaciones internas 213

2.3. Legislación actual relacionada con investigaciones internas 215

3. OBJETIVOS DE LAS INVESTIGACIONES INTERNAS 216

4. APLICACIÓN DE GARANTÍAS EN LAS INVESTIGACIONES INTERNAS 217

4.1. Garantías relacionadas con la propia investigación 217

4.1.1. Confidencialidad 217

4.1.2. Objetividad y conflictos de intereses 217

4.1.3. Respuesta diligente y motivada 217

4.1.4. Ausencia de represalias 218

4.2. Garantías específicas para los denunciantes 218

4.2.1. Anonimato 218

4.2.2. Ausencia de represalias a denunciantes de buena fe 218

4.2.3. Deber de información 219

4.3. Garantías específicas para los denunciados 219

4.3.1. Presunción de inocencia y derecho al honor 219

4.3.2. Declarar y presentar pruebas 219

4.3.3. Asistencia y asesoramiento 220

4.3.4. Procedimiento justo 220

Si quieres adquirir esta obra haz click aquí

Página

4.3.5. Ser informado 220
4.3.6. Derecho de acceso al expediente de investigación 220
5. PERSONAL INVESTIGADOR 221
5.1. Personal interno y/o externo 221
5.2. Declaraciones de confidencialidad y conflictos de intereses 222
5.2.1. Acuerdo de confidencialidad 222
5.2.2. Declaración de ausencia de conflicto de intereses 222
5.3. Características personales de un investigador 223
5.4. Sesgos y criterio de variabilidad 223
5.4.1. Concepto de sesgo y variabilidad 223
5.4.2. Impacto en las investigaciones 223
5.4.3. Cómo evitar los sesgos y variabilidad 224
6. MEDIOS Y RECURSOS QUE DESTINAR A LA INVESTIGACIÓN 224
6.1. Recursos técnicos 224
6.2. Recursos humanos 224
6.3. Recursos económicos 225
7. ADOPCIÓN DE MEDIDAS PROVISIONALES O CAUTELARES 225
8. PLAN DE INVESTIGACIÓN 226
9. PRÁCTICA DE PRUEBA 226
9.1. Obtención de pruebas materiales 226
9.1.1. Intervención de dispositivos electrónicos - Caso Barbulescu 227
9.1.2. Investigadores privados 228
9.2. Declaración del denunciante y testigos 228
9.3. Declaración del denunciado 229
9.4. Grabaciones de entrevistas 229
9.5. Falta de colaboración en entrevistas 230

Si quieres adquirir esta obra haz click aquí

Página

9.6. Cuestiones prácticas para las entrevistas 230
9.6.1. Dónde realizar la entrevista 230
9.6.2. Actitud positiva, lenguaje sencillo y cercano 230
9.6.3. Analizar el estado emocional de los entrevistados 231
9.6.4. Anonimizar la información 231
10. INFORME DE INVESTIGACIÓN 231
11. CÓMO ABORDAR LAS DENUNCIAS FALSAS 232
11.1. Concepto de denuncia falsa 232
11.2. Contenido del informe de investigación de una denuncia falsa ... 232
11.3. Consecuencias legales de una denuncia falsa 233

CAPÍTULO 1.14.
FORMACIÓN Y SENSIBILIZACIÓN – UNE 19601
JOAN XIFRA 235
1. INTRODUCCIÓN 235
2. MARCO NORMATIVO Y CONCEPTUAL 237
2.1. Relación con el artículo 31 bis del Código Penal 237
2.2. UNE 19601:2025 y su enfoque sobre formación y conciencia 238
2.3. Estándares internacionales y convergencia 238
2.4. Responsabilidad individual y organización 239
3. FORMACIÓN EN EL SGCP: REQUISITOS Y DISEÑO AVANZADO 239
3.1. Requisitos materiales de la formación; lo que se debe incluir 239
3.2. Enfoque basado en riesgos 241
3.3. Segmentación de colectivos y niveles de profundidad 242
3.4. Metodologías formativas avanzadas 242
3.5. Evaluación: no solo test, también comportamiento 243
4. TOMA DE CONCIENCIA Y SENSIBILIZACIÓN: CULTURA Y HERRAMIENTAS 243
4.1. Función de la sensibilización en la cultura de cumplimiento 243
4.2. Herramientas típicas de sensibilización 244

Si quieres adquirir esta obra haz click aquí

Página

4.3. Contenido mínimo de la toma de conciencia 245
4.4. Medición indirecta de la sensibilización 245
5. PLAN ANUAL DE FORMACIÓN PENAL 246
5.1. Estructura típica del Plan 246
5.2. Proceso de elaboración 248
5.3. Conexión con RRHH y otros sistemas 249
6. EVIDENCIAS Y DOCUMENTACIÓN: DEJAR RASTRO PROBATORIO 249
6.1. Qué debe documentarse 249
6.2. Criterios de conservación y accesibilidad 250
6.3. Uso en un procedimiento penal 250
7. PERSPECTIVA DE LA FISCALÍA Y JURISPRUDENCIA 251
7.1. Enfoque de la Fiscalía 252
7.2. Tendencias jurisprudenciales 252
7.3. Conclusión jurisprudencial 253
8. ERRORES FRECUENTES Y BUENAS PRÁCTICAS 254
8.1. Errores frecuentes 254
8.2. Buenas prácticas 254

CAPÍTULO 1.15.

INDICADORES Y REPORTING – UNE-19601 (PLANES DE ACCIÓN)

JOAN XIFRA 257

1. INTRODUCCIÓN 258
2. MARCO NORMATIVO: UNE 19601, ISO 37301, FISCALÍA Y PLANES DE ACCIÓN 259
3. TIPOLOGÍA DE INDICADORES EN COMPLIANCE PENAL 261
3.1. Indicadores de desempeño (KPIs): medición de la actividad del sistema 261
3.2. Indicadores de eficacia (KEIs): medición de la capacidad preventiva del modelo 262

Si quieres adquirir esta obra haz click aquí

Página

3.3. Indicadores de riesgo (KRIs): señales tempranas y predicción de exposición penal 263
3.4. Indicadores de cultura de cumplimiento: medición del elemento más intangible del SGCP 263
3.5. Indicadores reactivos y proactivos: dos lentes complementarias 264
3.6. El cuadro de mando penal: integración operativa de los indicadores . 264
4. DISEÑO AVANZADO DE INDICADORES DEL SGCP 264
4.1. Principios rectores del diseño de indicadores 265
4.2. Cómo diseñar indicadores basados en riesgos penales 266
4.3. ¿Qué debe medir un buen indicador penal? 267
4.4. Qué NO debe medir un indicador penal 267
4.5. Relación entre indicadores y el mapa de riesgos 268
4.6. Indicadores como herramienta de defensa penal 268
5. REPORTING DEL SGCP 269
5.1. Finalidad del reporting dentro del SGCP 269
5.2. Reporting operativo y reporting estratégico: dos niveles complementarios 270
5.3. Contenido mínimo del reporting estratégico 271
5.4. Requisitos formales del reporting: claridad, rigor y consistencia ... 271
5.5. El reporting como evidencia de supervisión ante Fiscalía y tribunales .. 271
5.6. Conexión del reporting con la mejora continua 272
6. PLANES DE ACCIÓN Y MEJORA CONTINUA SEGÚN UNE 19601 272
6.1. Naturaleza y finalidad de los planes de acción 273
6.2. Cuándo se activa un plan de acción 273
6.3. Estructura recomendada del plan de acción 274
6.4. El análisis de causa raíz: elemento diferenciador de madurez 275
6.5. Ejecución y seguimiento del plan de acción 275
6.6. Priorización de acciones: cómo decidir qué corregir primero 276
6.7. Documentación del plan de acción: valor probatorio ante Fiscalía 276
6.8. Los planes de acción como motor de la mejora continua 276
6.9. Madurez del SGCP: niveles evolutivos del uso de planes de acción 277

Si quieres adquirir esta obra haz click aquí

Página

7. ERRORES FRECUENTES Y BUENAS PRÁCTICAS 277

7.1. Errores frecuentes en la definición y uso de indicadores 277

7.2. Errores frecuentes en la construcción del reporting 278

7.3. Errores frecuentes en los planes de acción 278

7.4. Buenas prácticas en el uso de indicadores 279

7.5. Buenas prácticas en el reporting 279

7.6. Buenas prácticas en los planes de acción 280

8. CONCLUSIÓN 280

CAPÍTULO 1.16.

FORMACIÓN OBLIGATORIA EN MATERIA DE IA

XAVIER RIBAS 283

1. EL PUNTO DE PARTIDA DEL CUMPLIMIENTO EN IA 283

2. EL MARCO NORMATIVO: ARTÍCULOS 4 Y 3.56 Y CONSIDERANDO 20 283

3. QUIÉN ESTÁ OBLIGADO Y QUÉ SE SANCIONA 284

4. LOS DOS REQUISITOS DE ADAPTACIÓN QUE EXIGE EL ARTÍCULO 4 285

5. ESTRUCTURA MODULAR 286

6. ADAPTACIÓN AL PERFIL DEL DESTINATARIO DE LA FORMACIÓN 286

7. OBJETIVOS Y CONTENIDOS EXIGIBLES 287

8. TRAZABILIDAD, EVIDENCIA Y VERIFICACIÓN 287

9. LA FORMACIÓN DE LA FUNCIÓN DE SUPERVISIÓN HUMANA 288

10. CARÁCTER DINÁMICO DEL PLAN 290

11. CONCLUSIONES 290

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 1.17.

CONTROL DE TERCEROS, PROVEEDORES Y CADENA DE SUMINISTRO

AMEDEO MARCHELLI 291

1. INTRODUCCIÓN 291

2. ESTRUCTURA DE LA CADENA DE VALOR 292

2.1. Canales de Suministro y Distribución 292

3. POR QUÉ CONTROLAR A LOS TERCEROS 292

3.1. Riesgos Legales 292

3.2. Riesgos Reputacionales 293

3.3. Riesgos Financieros 293

4. MARCO LEGAL 293

4.1. Normativa Española 293

4.2. Normativa Europea 293

5. ENFOQUE BASADO EN RIESGOS 294

5.1. Principios Generales 294

5.2. Factores de Riesgo 294

5.3. Niveles de Diligencia Debida 295

6. LAS TRES FASES DE LA DILIGENCIA DEBIDA 295

6.1. Fase de Selección y Evaluación 295

6.2. Fase de Formalización 295

6.3. Fase de Seguimiento y Reevaluación 296

7. CONTROLES ESPECÍFICOS POR TIPO DE TERCERO 297

7.1. Agentes Comerciales e Intermediarios 297

7.2. Proveedores de Bienes y Servicios 298

7.3. Socios en Joint Ventures y Alianzas 298

7.4. Contratistas y Subcontratistas 298

8. DOCUMENTACIÓN 298

9. ORGANIZACIÓN Y RESPONSABILIDADES 299

9.1. Responsabilidades por Función 299

9.2. Flujo de Aprobación 299

Si quieres adquirir esta obra haz click aquí

Página

10. SEÑALES DE ALERTA 300
11. CONCLUSIONES 300

CAPÍTULO 1.18.
CERTIFICACIONES DE COMPLIANCE ISO-UNE
JUAN PABLO TORNOS 301
1. INTRODUCCIÓN 301
2. CONCEPTO DE CERTIFICACIÓN DE COMPLIANCE 302
3. OBJETIVO Y UTILIDAD DE LAS CERTIFICACIONES 302
4. ALCANCE Y DURACIÓN DE LAS CERTIFICACIONES 303
5. PRINCIPALES NORMAS DE COMPLIANCE ISO-UNE CERTIFICABLES 304
5.1. ISO 37001 – Sistema de gestión antisoborno 305
5.2. UNE 19601 – Sistema de gestión de compliance penal 305
5.3. ISO 37001 – Sistema de gestión de compliance 305
6. ESTRUCTURA DE UNA CERTIFICACIÓN ISO-UNE 305
6.1. Contexto de la organización 306
6.1.1. Alcance, contexto y partes interesadas 306
6.1.2. Obligaciones de compliance 306
6.1.3. Evaluación de riesgos 307
6.2. Liderazgo 307
6.3. Planificación 308
6.4. Apoyo 309
6.5. Operación 309
6.6. Evaluación del desempeño 309
6.7. Mejora 309
7. SINERGIAS E INTEGRACIÓN ENTRE NORMAS 309
8. INTERPRETACIONES, SESGOS Y ZONAS GRISES DE LAS NORMAS CERTIFICABLES 310
9. PREPARACIÓN PARA LA OBTENCIÓN DE UNA CERTIFICACIÓN ISO-UNE 310
9.1. Planificación y revisión inicial 311

Si quieres adquirir esta obra haz click aquí

Página

9.2. Auditoría previa de la organización 311
9.3. Evaluación previa de la entidad certificadora 311
9.4. Auditoría de la entidad certificadora 312

CAPÍTULO 1.19.

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE TRADE COMPLIANCE: UNA GUÍA PRÁCTICA PARA COMPLIANCE OFFICERS

ANA CANET ARANDA 313

1. INTRODUCCIÓN 314
1.1. Consideraciones iniciales y tesis interpretativas sobre el Trade Compliance 314
1.2. El Trade Compliance en un entorno de enforcement creciente 314
2. CONCEPTO Y ALCANCE DEL TRADE COMPLIANCE 315
3. EL TRADE COMPLIANCE COMO SUB-PROGRAMA DEL COMPLIANCE MANAGEMENT SYSTEM 316
4. AUTORIDADES COMPETENTES Y MARCO INSTITUCIONAL DEL TRADE COMPLIANCE 317
4.1. Autoridades Aduaneras 317
4.2. Autoridades de control a la exportación 317
4.3. Autoridades responsables de sanciones y embargos internacionales 318
4.4. Autoridades con competencias indirectas 318
5. ESTÁNDARES INTERNACIONALES, GUÍAS Y SOFT LAW DE REFERENCIA 318
6. PRINCIPALES ÁMBITOS DE RIESGO EN TRADE COMPLIANCE 319
7. LA PRIMERA Y LA SEGUNDA LÍNEA DE DEFENSA EN TRADE COMPLIANCE 320
8. SINERGIAS CON OTROS PROGRAMAS DE COMPLIANCE. 321
9. DISEÑO DE UN MODELO PROPORCIONAL DE TRADE COMPLIANCE 321
9.1. Particularidades del Trade Compliance en PYMES 322

Si quieres adquirir esta obra haz click aquí

Página

10. SUPERVISIÓN, INDICADORES Y MEJORA CONTINUA EN TRADE COMPLIANCE 323

11. ENFORCEMENT Y RÉGIMEN SANCIONADOR EN TRADE COMPLIANCE 324

12. EL VALOR DEL COMPLIANCE EN LA PREVENCIÓN Y MITIGACIÓN DE SANCIONES EN TRADE COMPLIANCE. 325

13. TECNOLOGÍA, AUTOMATIZACIÓN Y USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL EN TRADE COMPLIANCE 327

14. IMPLEMENTACIÓN DESDE CERO DE UN PROGRAMA DE TRADE COMPLIANCE 328

14.1. Alcance y encaje organizativo 328

14.2. Evaluación de riesgos 329

14.3. Elaboración de estándares internos 329

14.4. Implementación de controles 329

14.5. Formación y comunicación 329

14.6. Supervisión, mejora continua y reporting 330

15. CONCLUSIONES 330

ANEXO I. CHECKLIST DE ARRANQUE Y ROADMAP DE 90 DÍAS PARA LA IMPLANTACIÓN DE UN PROGRAMA DE TRADE COMPLIANCE 331

ANEXO II. ERRORES FRECUENTES EN LA IMPLANTACIÓN DEL TRADE COMPLIANCE 332

ANEXO III. INDICADORES BÁSICOS RECOMENDADOS (KPIS Y KRIS) EN TRADE COMPLIANCE 334

CAPÍTULO 1.20.

LA ISO 37303 COMO ESTÁNDAR DE GOBERNANZA DEL FACTOR HUMANO EN EL COMPLIANCE MANAGEMENT SYSTEM

ANA CANET ARANDA 337

1. INTRODUCCIÓN 338

1.1. La evolución del Compliance: del control normativo a la capacidad humana 338

Si quieres adquirir esta obra haz click aquí

Página

1.2. Por qué la competencia se ha convertido en un riesgo crítico de Compliance 339

2. LA ISO 37303 EN EL ECOSISTEMA DE ESTÁNDARES DE COMPLIANCE 339

2.1. La ISO 37303 en el ecosistema de estándares de Compliance 339

2.2. Relación con la ISO 37301 Compliance Management Sistemas 340

2.2.1. Relación estructural 340

2.2.2. Relación funcional 340

2.3. Relación funcional con la ISO 37302 340

3. LA COMPETENCIA COMO EJE ESTRUCTURAL DEL COMPLIANCE MANAGEMENT SYSTEM 341

3.1. El error conceptual: confundir competencia con formación 341

3.2. La competencia como condición de eficacia del CMS 341

3.3. Alcance subjetivo de la ISO 37303: funciones, roles y órganos afectados 342

3.3.1. Órgano de Gobierno 342

3.3.2. Alta Dirección 342

3.3.3. Función de Compliance 342

3.3.4. Management y mandos intermedios 344

3.3.5. Personal expuesto a riesgos de cumplimiento 344

3.3.6. Personal que trabajan bajo el control de la organización 344

3.3.7. Terceros que actúan en nombre de la organización 344

3.3.8. Investigadores y responsables de investigaciones internas 344

3.3.9. Responsables de formación y desarrollo en Compliance 344

3.3.10. Funciones de apoyo relevantes 345

4. LA ISO 37303 COMO ESTÁNDAR DE GESTIÓN DEL RIESGO HUMANO 345

4.1. El riesgo humano en Compliance: definición y alcance 345

4.2. Las cuatro dimensiones de competencia como tipología de riesgo 345

4.2.1. Competencia personal 346

4.2.2. Competencia metodológica 346

Si quieres adquirir esta obra haz click aquí

Página

4.2.3. Competencia técnica 347
4.2.4. Competencia social 347

5. DE «*TONE FROM THE TOP*» A «*JUDGMENT FROM THE ORGANIZATION*» 347

5.1. Alcance y límites del liderazgo ético tradicional 347
5.2. El juicio organizativo como nueva métrica de madurez del CMS . 348
5.3. El papel de las competencias en la toma de decisiones reales 348

6. LA ISO 37303 COMO PUENTE ENTRE COMPLIANCE, RRHH Y GOBIERNO CORPORATIVO 349

6.1. La fragmentación tradicional de responsabilidades 349
6.2. El nuevo rol de la función de Compliance como arquitecta del criterio 349
6.3. RRHH como garante del desarrollo competencial crítico 350
6.4. El Órgano de Gobierno y la supervisión informada del capital humano 350
6.5. La ISO 37303 como lenguaje común interfuncional 350

7. IDENTIFICACIÓN DE NECESIDADES DE COMPETENCIA Y ANÁLISIS DE RIESGOS (APARTADO 4 DE LA ISO 37303) 351

7.1. Identificación de roles y funciones con impacto material en el CMS 351
7.1.1. Análisis del modelo de negocio y cadena de valor 351
7.1.2. Mapeo de procesos críticos y puntos de decisión 351
7.1.3. Análisis de riesgos de Compliance y vinculación con roles 351
7.1.4. Análisis de incidentes pasados y near misses 352
7.1.5. Evaluación de la gestión de terceros 352
7.1.6. Entrevistas estructuradas con funciones clave 352
7.1.7. Validación por el Órgano de Gobierno 352
7.2. La gestión de terceros relevantes desde la perspectiva de la ISO 37303 352
7.3. Matriz de responsabilidades y competencias por función 353
7.4. Proceso para identificar y gestionar la evolución de las necesidades de competencia en el Compliance Management System 355

Si quieres adquirir esta obra haz click aquí

Página

7.5. Evaluación de riesgos asociados a una determinación incorrecta de competencias 355
7.6. Identificación, evaluación y gestión de brechas competenciales 356
7.6.1. Definición de las competencias requeridas 356
7.6.2. Identificación de funciones y población evaluada 356
7.6.3. Evaluación de las competencias existentes 356
7.6.4. Comparación sistemática y detección de brechas 356
7.6.5. Priorización de brechas en función del riesgo 357
7.6.6. Definición de planes de acción y desarrollo competencial 357
7.6.7. Validación, seguimiento y mejora continua 357
8. DESARROLLO DE COMPETENCIAS (APARTADO 5 DE LA ISO 37303) 357
9. EVALUACIÓN, SEGUIMIENTO Y MEJORA DE COMPETENCIAS (APARTADO 6 DE LA ISO 37303) 358
10. EL ANEXO DE LA ISO 37303 COMO GUÍA OPERATIVA 359
10.1. Función y valor practico del Anexo 359
10.2. Identificación de competencias 359
10.3. Diseño de matrices competenciales 359
10.4. Desarrollo competencial orientado a la acción 359
10.5. Evaluación y seguimiento 360
10.6. Integración con el CMS y otros sistemas 360
11. APLICACIÓN DIFERENCIADA DE LA ISO 37303 SEGÚN EL CONTEXTO ORGANIZATIVO 360
11.1. Un estándar escalable y basado en riesgos 360
11.2. Pequeñas y medianas empresas 360
11.3. Empresas medianas en crecimiento 360
11.4. Grandes empresas y multinacionales 361
11.5. Aplicación según la madurez del CMS 361
11.6. Riesgos de una implementación inadecuada 361
12. LA ISO 37303 COMO RESPUESTA AL COMPLIANCE FATIGUE 361

Si quieres adquirir esta obra haz click aquí

Página

13. LA ISO 37303 COMO MARCO DE EXPLICABILIDAD Y DILIGENCIA RAZONABLE 362
13.1. De la prevención a la explicabilidad ex post 362
13.2. La competencia como eje de la diligencia razonable 362
13.3. Evidencia estructurada y trazabilidad decisional 362
13.4. Soporte del relato ante terceros 363
13.5. De respuestas reactivas a una lógica estructural de diligencia 363
14. CONCLUSIÓN 363
ANEXO I. PLANTILLA DE ENTREVISTAS POR ROL 364
ANEXO II. CHECKLIST DE IMPLEMENTACIÓN POR FUNCIÓN 365

CAPÍTULO 1.21.

PROGRAMA DE COMPLIANCE EN DEFENSA DE LA COMPETENCIA

ANA CANET ARANDA 369

1. INTRODUCCIÓN 370
1.1. El entorno económico y su impacto en el Compliance de competencia 371
1.2. Objetivos del artículo y enfoque 371
1.3. El Compliance en competencia como indicador de madurez organizativa 371
1.4. Fuentes regulatorias y doctrinales clave para el Compliance en competencia 372
1.4.1. La Norma UNE en materia de defensa de la competencia. 373
1.5. Sobre la denominación del Compliance en materia de competencia: alcance y precisión conceptual 373
2. MARCO NORMATIVO Y REGULATORIO DE LA COMPETENCIA 374
2.1. Normativa europea 374
2.2. Régimen sancionador 374
2.2.1. Prohibición de contratar con Administraciones Públicas y su relación con el Compliance en materia de competencia 375
2.3. Guías y soft law relevantes en materia de Compliance en defensa de la competencia 375

Si quieres adquirir esta obra haz click aquí

Página

2.4. Referencias internacionales: la aportación de la FTC y otras autoridades 376

2.5. Guías europeas y nacionales de especial relevancia para Compliance 376

3. EL RIESGO DE COMPETENCIA DESDE LA PERSPECTIVA DEL COMPLIANCE 376

3.1. Tipologías de riesgo en defensa de la competencia 377

3.2. Riesgos emergentes 378

3.3. Otros riesgos 378

3.4. Conductas prohibidas vs. conductas de riesgo 379

3.5. Excepciones por eficiencias y su gestión práctica en el programa de Compliance 379

3.6. Casos relevantes 380

3.7. Competencia desleal y su encaje operativo en el programa de Compliance 380

4. EL PROGRAMA DE COMPLIANCE EN COMPETENCIA COMO PARTE DEL SISTEMA GLOBAL 380

4.1. Integración con otros sistemas clave 381

4.2. El papel del órgano de administración y la alta dirección 381

4.3. Qué espera una autoridad de competencia de un programa «eficaz» . 381

5. DISEÑO E IMPLEMENTACIÓN DEL PROGRAMA DE COMPLIANCE DE COMPETENCIA 382

5.1. Asegurar el mandato y el respaldo institucional 382

5.2. Entender el negocio antes que la norma 382

5.3. Identificación preliminar del riesgo de competencia 383

5.4. Definir el alcance y el modelo del programa 383

5.5. Establecer reglas claras para las situaciones de mayor riesgo 384

5.6. Formación inicial orientada a riesgos reales 384

5.7. Crear canales de consulta antes que de denuncia 384

5.8. Medidas reactivas internas inmediatas y contención del riesgo antitrust 384

5.9. Sistema de consecuencias internas y mecanismos de enforcement del programa 385

Si quieres adquirir esta obra haz click aquí

Página

5.10. Trazabilidad, evidencias y mejora continua del programa 385

5.11. Preparación ante dawn raids dentro del programa de Compliance en defensa de la competencia 386

6. IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO DE COMPETENCIA 387

6.1. Enfoque basado en riesgos aplicado a la competencia 387

6.1.1. Factores sectoriales 387

6.1.2. Factores organizativos y de modelo de negocio 387

6.1.3. Factores geográficos e internacionales 387

6.2. Identificación de áreas y funciones de mayor riesgo 387

6.2.1. Área comercial y ventas 388

6.2.2. Compras y aprovisionamiento 388

6.2.3. Alta dirección y dirección general 388

6.3. Metodología práctica de evaluación del riesgo 388

6.4. Actualización y revisión periódica 388

6.5. Checklist práctico: evaluación del riesgo de competencia 389

7. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES INTERNOS EN MATERIA DE COMPETENCIA 389

7.1. La política de defensa de la competencia: función y alcance 389

7.1.1. Contenido mínimo de una política eficaz 389

7.1.2. Errores habituales en la práctica 390

7.2. Procedimientos clave para la gestión del riesgo en defensa de la competencia 390

7.2.1. Procedimiento sobre contactos con competidores 390

7.2.2. Procedimiento de participación en asociaciones empresariales 390

7.2.3. Procedimiento de fijación de precios y condiciones comerciales 390

7.3. Controles internos: prevención, detección y corrección 390

7.3.1. Controles preventivos 391

7.3.2. Controles detectivos 391

Si quieres adquirir esta obra haz click aquí

Página

7.3.3. Controles correctivos 391

7.4. Proporcionalidad y adaptación al negocio 391

8. FORMACIÓN Y CONCIENCIACIÓN EN MATERIA DE COMPETENCIA 392

8.1. Limitaciones de la formación tradicional en competencia 392

8.2. Formación basada en riesgos y perfiles 392

8.2.1. Formación para el órgano de administración y la alta dirección 393

8.2.2. Formación para áreas comerciales y de ventas 393

8.2.3. Formación para compras, marketing y otras áreas sensibles 393

8.3. Metodologías formativas eficaces 393

8.3.1. Uso de casos reales y dilemas prácticos 393

8.3.2. Formación recurrente y refuerzos periódicos 393

8.4. Documentación y evidencias de la formación 394

9. GESTIÓN PRÁCTICA DEL DÍA A DÍA: CUANDO EL COMPLIANCE SE ENFRENTA A LAS ZONAS GRISES 394

9.1. Ferias, congresos y eventos sectoriales 394

9.2. Contactos bilaterales con competidores 394

9.3. Clientes comunes y solicitudes de información sensible 394

9.4. Colaboraciones, consorcios y proyectos conjuntos 395

9.5. El papel del Compliance Officer en la toma de decisiones 395

10. DETECCIÓN DE INCUMPLIMIENTOS, INVESTIGACIONES INTERNAS Y REACCIÓN 395

10.1. Detección temprana del riesgo en defensa de la competencia 396

10.2. Investigación interna en materia de competencia 396

10.3. Reacción y gestión de consecuencias 397

10.4. Documentación y aprendizaje organizativo 397

11. PROGRAMAS DE CLEMENCIA Y RELACIÓN CON LAS AUTORIDADES DE COMPETENCIA 397

11.1. Los programas de clemencia: concepto y finalidad 398

11.2. Marco europeo y nacional de la clemencia 398

Si quieres adquirir esta obra haz click aquí

Página

11.3. El rol del Compliance Officer en decisiones de clemencia 398
11.4. Gobernanza de la decisión de acogerse a la clemencia 398
11.5. Relación con las autoridades: cooperación y credibilidad 399
12. SUPERVISIÓN, REPORTING Y MEJORA CONTINUA DEL PROGRAMA DE COMPLIANCE EN COMPETENCIA..... 399
12.1. Supervisión del programa: roles y responsabilidades 399
12.2. Reporting en materia de competencia..... 400
12.3. Revisión periódica y mejora continua 400
12.4. Demostración de la eficacia del programa..... 401

CAPÍTULO 1.22.

GOVERNANCE Y COMPLIANCE EN PRIVATE EQUITY Y ENTIDADES DE INVERSIÓN

CARLOS SOUCASE FURIÓ, INÉS NÁJERA-ALESÓN RODRÍGUEZ-LOSADA Y RAMÓN FAUS SANTASUSANA 405
1. INTRODUCCIÓN Y CONCEPTOS..... 406
1.1. Entidades de Capital Riesgo (ECR)..... 406
1.2. Entidades de Inversión Colectiva de tipo Cerrado (EICC) 407
1.3. Sociedades Gestoras de Capital Riesgo (SGEIC)..... 407
2. MARCO NORMATIVO DE APLICACIÓN..... 408
2.1. Marco normativo sectorial 408
2.2. Normativa transversal de cumplimiento..... 408
3. DISEÑO DE LA FUNCIÓN DE CUMPLIMIENTO EN EL CAPITAL RIESGO..... 409
3.1. Estructura organizativa: modelo de las tres líneas de defensa..... 409
3.2. Matriz de compatibilidades 410
3.3. Verificación del cumplimiento (cumplimiento normativo)..... 410
3.3.1. Medidas de control de la función de verificación del cumplimiento..... 411
3.3.2. Calendario mínimo de reportes a realizar..... 412
3.3.3. Ejemplos prácticos..... 412

Si quieres adquirir esta obra haz click aquí

Página

3.4. Gestión de riesgos 415
3.4.1. Medidas de control de la función de gestión de riesgos ... 415
3.4.2. Calendario mínimo de reportes a realizar 416
3.4.3. Ejemplos prácticos 416
3.5. Auditoría interna 416
3.5.1. Medidas de control de la función de auditoría interna 417
3.5.2. Calendario mínimo de reportes a realizar 417
3.5.3. Ejemplos prácticos 417
3.6. Excepcionalidad de las SGEIC Capítulo I 418
3.6.1. Simplificaciones aplicables 418
3.6.2. Obligaciones que sí subsisten para las SGEIC de Capítulo I 419

4. OBLIGACIONES DE CUMPLIMIENTO DERIVADAS DE OTRAS NORMATIVAS 419
4.1. Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBCFT) 419
4.1.1. Medidas de control interno de la función de PBCFT 420
4.1.2. Calendario mínimo de reportes a realizar 421
4.1.3. Ejemplos 421
4.2. Sistema Interno de Información (Ley 2/2023) 421
4.2.1. Elementos clave del SII 422
4.3. Protección de datos (RGPD / LOPDGDD) 422
4.3.1. Elementos clave 423

5. ÁMBITOS EMERGENTES EN EL CAPITAL RIESGO: ESG Y NUEVAS TECNOLOGÍAS 424
5.1. Sostenibilidad y divulgación (SFDR/taxonomía) 424
5.1.1. Marco y a quién aplica 424
5.1.2. Obligaciones «a nivel entidad» que se deben publicar en la web 424
5.1.3. Obligaciones «a nivel producto» (fondos/vehículos gestionados) - precontractual, web del producto y reporting 425
5.1.4. Coherencia publicitaria («anti-greenwashing» básico) 426
5.1.5. Taxonomía UE (UE 2020/852): qué añade a SFDR 426

Si quieres adquirir esta obra haz click aquí

Página

5.1.6. Ejemplo: Checklist ejecutivo de cumplimiento en materia de sostenibilidad 426
5.2. Resiliencia operativa digital y ciberseguridad (DORA / NIS2) 427
5.2.1. Obligaciones bajo DORA 427
5.2.1.1. Gobernanza: responsabilidad del órgano de administración 427
5.2.1.2. Marco de gestión del riesgo TIC (el «sistema») 428
5.2.1.3. Gestión y notificación de incidentes TIC 428
5.2.1.4. Pruebas de resiliencia operativa digital 428
5.2.1.5. Gestión del riesgo TIC derivado de terceros (outsourcing/IT providers) 428
5.2.1.6. Supervisión 428
5.2.2. Obligaciones NIS2 429
5.2.2.1. Gestión de riesgos (medidas mínimas NIS2) 429
5.2.2.2. Notificación de incidentes (plazos «24h/72h/1 mes») 429
5.2.2.3. Gobernanza y sanciones 429
5.2.2.4. Estado de transposición en España 429
5.2.3. Ejemplo: Checklist ejecutivo de cumplimiento en materia de resiliencia digital 429
6. COMPLIANCE PENAL EN EL SECTOR CAPITAL RIESGO 430
6.1. Catálogo orientativo de principales riesgos 430
7. INSTRUMENTOS DE TRANSFERENCIA DEL RIESGO 431
7.1. Mecanismos de mitigación 431
7.2. Resumen 432

CAPÍTULO 1.23.

EL REGISTRO DE CASOS DE USO DE LA IA

XAVIER RIBAS 433

1. SIN INVENTARIO NO HAY GOBERNANZA 433
2. POR QUÉ LA PREGUNTA ABIERTA PRODUCE UN REGISTRO INCOMPLETO 433
3. UNA CONSTANTE OBSERVADA DESDE 1987 434

Si quieres adquirir esta obra haz click aquí

Página

4. EL DISCOVERY TÉCNICO NO RESUELVE EL PROBLEMA 434
5. EL SHADOW AI Y EL USO NO DECLARADO 435
6. UNA METODOLOGÍA BASADA EN CATÁLOGOS..... 435
7. MARCO NORMATIVO 436
8. CONCLUSIONES 436

CAPÍTULO 1.24.

LA EVALUACIÓN DE IMPACTO EN SISTEMAS DE INTELIGENCIA ARTIFICIAL COMO INSTRUMENTO DE CUMPLIMIENTO NORMATIVO. *RIESGOS, GOBERNANZA Y EVIDENCIAS ANTE EL REGLAMENTO (UE) 2024/1689*

ALEJANDRO GIMÉNEZ GUTIÉRREZ 437

1. INTRODUCCIÓN 438
2. MARCO NORMATIVO Y CONTEXTO REGULATORIO 438
2.1. El enfoque basado en el riesgo del Reglamento Europeo de IA..... 438
2.2. Relación con la normativa de Protección de Datos 439
2.3. Tendencias de supervisión y control 439
3. CONCEPTO, FINALIDAD Y VALOR PRÁCTICO DE LA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL... 440
4. LA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL Y SU RELACIÓN CON OTRAS EVALUACIONES DE IMPACTO 441
5. RIESGOS ASOCIADOS AL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL DESDE UNA PERSPECTIVA JURÍDICO-PRÁCTICA 442
5.1. Riesgos para los Derechos Fundamentales y la Igualdad de Trato. 442
5.2. Riesgos derivados de la opacidad y la falta de explicabilidad..... 443
5.3. Riesgos de Seguridad, Integridad y Uso Indebido 443
5.4. Riesgos organizativos, reputacionales y de dependencia tecnológica 443
6. INTEGRACIÓN DE LA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL EN EL SISTEMA DE COMPLIANCE 443
6.1. Incorporación de la IA al mapa de riesgos corporativo 444

Si quieres adquirir esta obra haz click aquí

Página

6.2. Traducción de la evaluación de impacto en controles operativos ... 444

6.3. Indicadores, seguimiento y reporting 444

6.4. Integración de la AIA en el repositorio de evidencias del compliance .. 445

6.5. Coordinación entre áreas y cultura de cumplimiento tecnológico .. 445

7. GOBERNANZA, ROLES Y RESPONSABILIDADES EN LA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL 445

7.1. El papel del órgano de administración y la Alta Dirección 446

7.2. Función del área de Compliance 446

7.3. Responsabilidades de las áreas técnicas y de Seguridad de la Información 446

7.4. Papel del área jurídica y de protección de datos 446

7.5. Responsabilidad del área de negocio y usuarios del sistema 447

7.6. Comités y modelos de gobernanza colegiada 447

8. METODOLOGÍA PRÁCTICA PARA LA REALIZACIÓN DE UNA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL 447

8.1. Identificación y delimitación del sistema de Inteligencia Artificial .. 447

8.2. Análisis del marco normativo aplicable y clasificación del sistema . 448

8.3. Identificación de impactos y escenarios de riesgo 448

8.4. Valoración y priorización del riesgo 448

8.5. Definición de medidas de mitigación y control 448

8.6. Aceptación del riesgo residual y toma de decisiones 448

8.7. Monitorización continua y revisión periódica 449

8.8. Documentación, evidencias y archivo 449

9. LA EVALUACIÓN DE IMPACTO EN INTELIGENCIA ARTIFICIAL COMO ELEMENTO DE DEFENSA Y VENTAJA COMPETITIVA 449

10. CONCLUSIONES 450

11. BIBLIOGRAFÍA 450

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 1.25.

LA SUPERVISIÓN HUMANA DE LOS SISTEMAS DE IA

XAVIER RIBAS 453

1. UNA FUNCIÓN NUEVA CON CUATRO ATRIBUTOS 453

2. LAS OBLIGACIONES DEL PROVEEDOR: TRANSPARENCIA Y CONTROL 453

3. LAS CAPACIDADES EXIGIDAS AL SUPERVISOR 454

4. LA POLÍTICA DE CUATRO OJOS 454

5. LOS NIVELES DE SUPERVISIÓN: UNA RESPUESTA PROPORCIONAL AL RIESGO 455

6. LA SUPERVISIÓN COMO OPORTUNIDAD PROFESIONAL 456

7. CONCLUSIONES 456

CAPÍTULO 1.26.

ANÁLISIS DE LA JURISPRUDENCIA SOBRE MODELO DE PREVENCIÓN DE DELITOS

AMEDEO MARCHELLI 457

1. INTRODUCCIÓN 457

2. EL PUNTO DE PARTIDA: STS 514/2015 458

3. LA SENTENCIA FUNDACIONAL: STS 154/2016 458

3.1. La Cultura de Respeto al Derecho 458

3.2. El Núcleo de la Responsabilidad 458

3.3. El Debate sobre la Carga de la Prueba 459

4. CONSOLIDACIÓN DEL MODELO: STS 221/2016 459

4.1. El Concepto de Delito Corporativo 459

4.2. Rechazo de la Presunción de Defecto Organizativo 459

5. DESARROLLO JURISPRUDENCIAL (2016-2022) 460

6. STS 298/2024: EL «GIRO» 460

6.1. Los Elementos de la Responsabilidad 460

6.2. Carga de alegación y prueba 460

6.3. Encaje con 2025 460

Si quieres adquirir esta obra haz click aquí

Página

7. JURISPRUDENCIA DE 2025 461

7.1. STS 372/2025 461

7.2. SAN 17 de septiembre de 2025 461

7.3. STS 768/2025 461

7.4. STS de 10-14 de octubre de 2025 462

7.5. STS 836/2025 462

7.6. AAN de 23 de octubre de 2025 462

7.7. AAN de 19 de noviembre de 2025 463

7.8. AAN 9159/2025 463

8. RELEVANCIA DE LOS MODELOS DE PREVENCIÓN 463

8.1. La Exención de Responsabilidad 463

8.2. Los Criterios de la Fiscalía 464

8.3. La Distinción entre Núcleo Típico y Eximente 464

9. IMPLICACIONES PRÁCTICAS 465

9.1. Para el Diseño de Modelos de Prevención 465

9.2. Para la Defensa en un Proceso Penal 465

9.3. Para la Mejora Continua 465

10. CONCLUSIONES 466

2

RIESGOS CON MAYOR PROBABILIDAD EN 2026

CAPÍTULO 2.1.

DELITOS COMETIDOS CON SISTEMAS DE IA

VÍCTOR MANUEL ANTUNES RIVERA 469

1. PROBLEMAS PRÁCTICOS DE LOS DELITOS COMETIDOS CON SISTEMAS DE IA 469

2. ¿CUÁLES SON LOS DELITOS MÁS COMUNES QUE SE PUEDEN COMETER CON SISTEMAS DE IA? 471

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 2.2.

DEEPFAKES Y SUPLANTACIÓN DE IDENTIDAD: EL CASO ARUP

XAVIER RIBAS 475

1. UNA VIDEOLLAMADA DE 25 MILLONES DE DÓLARES ... 475
2. LOS ATAQUES DE PRESENTACIÓN 476
3. LA IA COMO HERRAMIENTA DEL ATAQUE Y DE LA DEFENSA 476
4. LA RESPUESTA PENAL A LOS DEEPFAKES 476
5. MEDIDAS PREVENTIVAS PARA LA EMPRESA 477
6. CONCLUSIONES 477

CAPÍTULO 2.3.

PROMPT INJECTION EN DOCUMENTOS JURÍDICOS

XAVIER RIBAS 479

1. EL DOCUMENTO JURÍDICO COMO VECTOR DE ATAQUE. 479
2. LOS CANALES DE ENTRADA 479
3. LA MECÁNICA DEL ATAQUE 480
4. LAS ACCIONES QUE EL PROMPT PUEDE DESENCADENAR 480
5. RIESGOS JURÍDICOS Y REGULATORIOS 481
6. MEDIDAS TÉCNICAS PREVENTIVAS 481
7. MEDIDAS ORGANIZATIVAS PREVENTIVAS 482
8. CONCLUSIONES 482

CAPÍTULO 2.4.

SHADOW AI Y BRECHAS DE SEGURIDAD

XAVIER RIBAS 483

1. EL ATAJO QUE SE CONVIERTE EN BRECHA 483
2. LAS PRIMERAS ACCIONES DEL COMITÉ DE CRISIS 483
3. LOS LAMENTOS DEL DÍA DESPUÉS 484
4. LAS MEDIDAS QUE PODÍAN HABER EVITADO LA BRECHA 485
5. CONCLUSIONES 485

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 2.5.
RIESGOS PENALES EN MATERIA DE SALUD PÚBLICA 2026
REBECA VELASCO 487
1. INTRODUCCIÓN 488
1.1. Concepto de salud pública en el ámbito penal 488
1.2. Relevancia en los programas de compliance penal 488
1.3. Proyección del riesgo en el escenario 2026 489
1.4. Sectores especialmente expuestos 489
2. MARCO NORMATIVO APLICABLE 490
2.1. Delitos contra la salud pública en el Código Penal 490
3. TIPOLOGÍAS DELICTIVAS RELEVANTES 492
3.1. Elaboración, despacho o suministro de sustancias nocivas 492
3.2. Delitos relativos a medicamentos 492
3.3. Delitos en materia de alimentos 493
3.4. Tráfico de drogas y sustancias estupefacientes 493
3.5. Supuestos imprudentes y agravados 493
3.6. Consideraciones comunes desde la perspectiva de compliance 493
4. RIESGOS CON MAYOR PROBABILIDAD EN 2026 494
4.1. Digitalización del mercado sanitario 494
4.2. Incremento de canales de distribución no controlados 494
4.3. Globalización de la cadena de suministro 494
4.4. Riesgos en marketplaces y plataformas intermediarias 495
4.5. Greenwashing y healthwashing en productos de consumo 495
4.6. Incremento de inspecciones y presión regulatoria 495
5. FACTORES DE RIESGO PENAL EN LA ORGANIZACIÓN 496
5.1. Fallos en controles de calidad 496
5.2. Deficiencias en homologación de proveedores 496
5.3. Falta de trazabilidad documental 496
5.4. Incentivos comerciales agresivos 497
5.5. Externalización sin control 497
5.6. Cultura de cumplimiento insuficiente 497

Si quieres adquirir esta obra haz click aquí

Página

6. MEDIDAS DE PREVENCIÓN Y CONTROL 497
6.1. Evaluación específica del riesgo de salud pública 497
6.2. Protocolos de control de productos 498
6.3. Due diligence de proveedores y distribuidores 498
6.4. Sistemas de trazabilidad 498
6.5. Controles sobre publicidad y marketing 498
6.6. Canal interno de información y gestión de incidentes 498
6.7. Formación específica del personal 499
7. SISTEMAS DE DETECCIÓN Y RESPUESTA 499
7.1. Indicadores de riesgo 499
7.2. Auditorías internas y externas 499
7.3. Gestión de alertas sanitarias 499
7.4. Protocolos de retirada de productos 500
7.5. Coordinación con autoridades 500
8. CONSECUENCIAS PENALES Y REPUTACIONALES 500
8.1. Penas aplicables a personas físicas 500
8.2. Responsabilidad penal de la persona jurídica 501
8.3. Impacto reputacional y económico 501
9. INTEGRACIÓN EN EL MODELO DE COMPLIANCE 502
9.1. Mapa de riesgos penales 502
9.2. Supervisión por el órgano de compliance 502
9.3. Revisión periódica del riesgo 503
10. CONCLUSIONES 503

CAPÍTULO 2.6.

DERECHOS DE LOS TRABAJADORES

QUERALT GARCÍAS 505
1. INTRODUCCIÓN GENERAL 505
1.1. Objeto y metodología 505

Si quieres adquirir esta obra haz click aquí

Página

1.2. Digitalización del trabajo, precariedad y tutela de los derechos fundamentales 506

1.3. Fuentes normativas básicas 507

2. RESPONSABILIDAD PENAL DE LAS EMPRESAS POR VULNERACIÓN DE DERECHOS LABORALES 511

2.1. Delito contra los derechos de los trabajadores 511

2.2. Responsabilidad penal de la persona jurídica (art. 31 bis CP) aplicada al ámbito laboral 512

2.3. Conexión entre ilícitos penales laborales e infracciones administrativas en materia de protección de datos 512

2.4. Supuestos prácticos 513

3. FALSOS AUTÓNOMOS Y LABORALIZACIÓN DE LAS RELACIONES DE TRABAJO EN PLATAFORMAS 515

3.1. El concepto de trabajador por cuenta ajena frente al autónomo 515

3.2. Los «riders» como paradigma: el Caso Glovo 516

3.2.1. Caso Glovo 516

3.2.2. Conexión entre la sentencia del TS y la posterior reforma normativa («Ley *Rider*») 517

3.2.3. El giro hacia la contratación laboral 518

3.2.4. Flotas subcontratadas y nuevos problemas de laboralidad. 518

3.2.5. Gestión de datos y algoritmos en el nuevo modelo 519

3.3. Génesis y objetivos de la Directiva (UE) 2024/2831 520

3.3.1. Mejora de las condiciones laborales en el trabajo en plataformas: lucha contra la precariedad y «falsos autónomos digitales» 520

3.3.2. Gestión algorítmica del trabajo y transparencia 521

3.3.3. Protección de datos personales en el trabajo en plataformas 522

3.3.4. Retos para la transposición en España 522

4. REGISTRO HORARIO, PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL 523

4.1. La obligación de registro de jornada 523

4.2. El nuevo registro digital de jornada 524

4.3. Registro horario y tutela de derechos 524

Si quieres adquirir esta obra haz click aquí

Página

4.4. Protección de datos y automatización en el registro horario 525
4.4.1. Licitud de tratamiento y proporcionalidad 525
4.4.2. Información a las personas trabajadoras 526
4.4.3. Usos de sistemas automatizados y algoritmos de control de jornada 526
5. CONCLUSIONES 527
5.1. Convergencia entre derecho laboral, penal y protección de datos en la empresa digital 527
5.2. Propuestas de futuro 528
6. BIBLIOGRAFÍA 529
6.1. Registro horario 529
6.2. Falsos autónomos 529

CAPÍTULO 2.7.
PROTECCIÓN DE DATOS PERSONALES
QUERALT GARCÍAS 531
1. INTRODUCCIÓN 531
2. DATOS BIOMÉTRICOS Y CONTROL DE PRESENCIA 532
2.1. Naturaleza de los datos biométricos como categoría especial 532
2.2. Criterios fijados por la AEPD 533
2.3. Primeras sanciones e impacto del caso AENA 535
2.4. Criterios de diseño de sistemas lícitos de control de presencia 537
3. VIDEOVIGILANCIA 538
3.1. Legitimación y proporcionalidad 538
3.2. Videovigilancia en el ámbito laboral 539
3.3. Obligaciones del responsable del tratamiento en el ámbito laboral 539
4. USO DE IMÁGENES DE TERCEROS EN SISTEMAS DE INTELIGENCIA ARTIFICIAL 540
4.1. Riesgos del tratamiento 541
4.2. Riesgos menos visibles 543
4.3. Políticas internas de casos de uso de IA, PIAs y FRIAs 543

Si quieres adquirir esta obra haz click aquí

Página

5. BRECHAS DE SEGURIDAD DE DATOS PERSONALES 544
5.1. Obligación de notificación 545
5.2. Especial atención en tratamientos biométricos 545
5.3. Documentación y gestión interna 546
6. EVALUACIONES DE IMPACTO Y GESTIÓN DEL RIESGO . 546
6.1. Supuestos de realización obligatoria 546
6.2. Contenido mínimo y fases 547
6.3. Privacidad desde el diseño y por defecto 548
6.4. Papel del delegado de Protección de Datos 548
7. CONCLUSIÓN 548

CAPÍTULO 2.8.

GEOPOLÍTICA, MERCADO Y CONSUMIDORES: PRINCIPALES RIESGOS

VÍCTOR MANUEL ANTUNES RIVERA 551

1. CONFLICTOS GEOECONÓMICOS 551
2. CONFLICTOS ENTRE ESTADOS 552
3. ESG (ENVIROMENT, SOCIAL AND GOVERNANCE) 553
4. CAMBIOS TECNOLÓGICOS 554
5. CONCLUSIONES 554

CAPÍTULO 2.9.

PROPIEDAD INTELECTUAL E INDUSTRIAL EN LA ERA DE LA IA

ALBA MORENO 555

1. INTRODUCCIÓN 555
2. LA TRANSFORMACIÓN DEL PROCESO INVENTIVO EN LA ERA DE LA INTELIGENCIA ARTIFICIAL 556
3. LA TITULARIDAD DE LAS INVENCIONES EN UN ESCENARIO DE INTELIGENCIA ARTIFICIAL 557
3.1. ¿Puede una IA ser autora? Debate dogmático y práctico 557
3.2. Obras generadas de forma autónoma vs. obras asistidas por IA ... 557

Si quieres adquirir esta obra haz click aquí

Página

3.3. Titularidad de derechos: programadores, usuarios, empresas 558
3.4. Modelos de explotación y licencias de contenidos generados por IA .. 559
4. INVENCIONES, PATENTES E INTELIGENCIA ARTIFICIAL 559
4.1. IA como herramienta del inventor humano 559
5. PROPIEDAD INDUSTRIAL, MARCAS Y FENÓMENOS DERIVADOS DE LA IA 560
5.1. Marcas en entornos digitales automatizados 560
5.2. Uso de marcas ajenas en prompts, metadatos y resultados de IA .. 561
5.3. Responsabilidad de plataformas y desarrolladores 561
6. RESPONSABILIDAD, INFRACCIÓN Y ENFORCEMENT EN CONTEXTOS DE IA 562
6.1. ¿Quién responde por la infracción cometida mediante IA? 562
6.2. Sistemas de notice & takedown y resolución de disputas en línea . 564
7. MEDIDAS TECNOLÓGICAS DE PROTECCIÓN Y GESTIÓN DE DERECHOS 566
8. IMPACTO EN LA INDUSTRIA CULTURAL Y CREATIVA 567
9. TRANSPARENCIA DEL ENTRENAMIENTO VS. SECRETO EMPRESARIAL 569
10. CREATIVIDAD HUMANA Y «DESPLAZAMIENTO» LABORAL: RESPUESTAS JURÍDICAS POSIBLES 571

CAPÍTULO 2.10.

RIESGOS GEOPOLÍTICOS

MARC RIUS 573
1. INTRODUCCIÓN 573
2. ESCENARIOS GEOPOLÍTICOS DE RIESGO E INCERTIDUMBRE 574
2.1. El retorno de la inestabilidad 574
2.2. Conflictos armados y su impacto en la empresa 574
2.3. Sanciones y restricciones comerciales 575
2.4. Fragmentación regulatoria 575

Si quieres adquirir esta obra haz click aquí

Página

3. INTELIGENCIA ARTIFICIAL 576
3.1. El estado actual 576
3.2. La hegemonía estadounidense 576
3.3. La estrategia china 577
3.4. Europa 578
4. IMPLICACIONES PARA EL CUMPLIMIENTO NORMATIVO 578
4.1. Sanciones internacionales 579
4.2. Responsabilidad penal de administradores y alta dirección 579
4.3. Cadena de suministro 580
4.4. Blanqueo de capitales y financiación del terrorismo 580
4.5. Ciberseguridad 581
4.6. Materias primas críticas y tierras raras 581
5. CONCLUSIONES 582
6. CASO PRÁCTICO 582
6.1. Descripción del supuesto 583
6.2. Análisis de riesgos identificados 583
6.3. Evaluación de evidencias y controles disponibles 584
6.4. Recomendaciones y plan de actuación 585

CAPÍTULO 2.11.

LA EXPLICABILIDAD DE LOS ALGORITMOS Y MODELOS DE IA Y SU TRASCENDENCIA EN LOS MODELOS DE GOBERNANZA

JULEN DOUSSINAGUE OYARZABAL 587

1. INTRODUCCIÓN 587
2. CONCEPTOS TÉCNICOS 588
2.1. Algoritmos y modelos de inteligencia artificial 588
2.2. Opacidad y explicabilidad 589
2.3. La opacidad de los algoritmos 591
2.4. Ejemplo práctico 591
3. RIESGOS JURÍDICOS 592
3.1. Riesgos en el tratamiento de datos personales 592

Si quieres adquirir esta obra haz click aquí

Página

3.1.1. Toma de decisiones automatizadas 593
3.1.2. Deber de transparencia 594
3.2. Riesgos del Reglamento de Inteligencia Artificial 595
3.2.1. Obligaciones aplicables a Proveedores para sistemas de alto riesgo 595
3.2.2. Obligaciones aplicables a Responsables de Despliegue para sistemas de alto riesgo 596
3.3. Riesgos en el ámbito laboral 597
3.4. Riesgos penales 598
3.5. Riesgos de la propiedad intelectual e industrial 599
4. USO DE ALGORITMOS EN EL SECTOR PÚBLICO 599
4.1. El derecho de acceso a la información pública 600
4.2. Límites al derecho de acceso a la información pública 601
4.3. Deber de transparencia algorítmica 602

3

MAPA DE RIESGOS Y OBLIGACIONES LEGALES 2026

CAPÍTULO 3.1.

ANÁLISIS DE RIESGOS CON UNA APLICACIÓN INFORMÁTICA

JUAN PABLO TORNOS 605

1. INTRODUCCIÓN 605
2. DIGITALIZACIÓN DE LA GESTIÓN DE RIESGOS 605
3. ACREDITACIÓN DE PRUEBA MEDIANTE APLICACIONES DE COMPLIANCE 606
4. OBJETIVOS DE UNA APLICACIÓN DE COMPLIANCE 607
5. ELEMENTOS CLAVE DE UNA APLICACIÓN DE COMPLIANCE 608
5.1. Filtros de contexto 608
5.2. Fichas base precargadas 608
5.3. Información interconectada 609
5.4. Asignación de responsables 610

Si quieres adquirir esta obra haz click aquí

Página

5.5. Subida de evidencias 611
5.6. Envío de alertas automáticas 612
5.7. Extracción de información 613
5.8. Histórico de información 614
5.9. Registro de cambios 615
5.10. Seguridad de la información y tipología de usuarios 616

CAPÍTULO 3.2.

FINALIDAD INSTRUMENTAL Y FINALIDAD ESENCIAL DE LOS SISTEMAS DE IA

XAVIER RIBAS 619

1. EL ROL DEL SISTEMA DETERMINA SU CALIFICACIÓN JURÍDICA 619
2. LAS DOS FINALIDADES 620
3. LOS SISTEMAS DE IA CON FINALIDADES CONSECUTIVAS. 620
4. LAS TRES VERIFICACIONES 620
5. LA EXCEPCIÓN DEL ARTÍCULO 6.3 DEL RIA 621
6. LAS CONSECUENCIAS JURÍDICAS DE LA CALIFICACIÓN 621
7. CONCLUSIONES 622

CAPÍTULO 3.3.

DATA ACT

ALBA MORENO Y MARC RIUS 623

1. INTRODUCCIÓN 623
1.1. ¿Qué cambia para mi empresa con el Data Act? 624
1.2. Quién está obligado y quién no: test de aplicabilidad rápido 625
2. LA FUNCIÓN DEL COMPLIANCE 627
2.1. Programa de compliance del Data Act 627
2.1.1. Fase 1. Inventario de datos y activos 627
2.1.2. Fase 2. Gap analysis 627
2.1.3. Fase 3. Plan de acción 628

Si quieres adquirir esta obra haz click aquí

Página

2.1.4. Fase 4. Implementación 628
2.1.5. Fase 5. Monitorización continua 629
3. EL ROL DEL COMPLIANCE OFFICER ANTE EL DATA ACT 629
4. EL MODELO DE LAS TRES LÍNEAS DE DEFENSA APLICADO AL DATA ACT 630
4.1. Los controles internos del programa de compliance 631
5. CULTURA DE CUMPLIMIENTO: EL FACTOR DIFERENCIAL 632
6. EL DATA ACT EN LA ESTRATEGIA DE DATOS DE LA EMPRESA 632
6.1. El mapa de riesgos 633
6.2. Matriz de riesgos 635
6.3. Políticas y procedimientos internos: qué documentos debe tener la empresa 635
6.3.1. La documentación como columna vertebral del compliance 635
7. CONTROLES PREVENTIVOS, DETECTIVOS Y CORRECTIVOS 636
7.1. Controles preventivos 636
7.2. Controles detectivos 637
7.3. Controles correctivos 637
8. INTERACCIÓN CON OTROS MARCOS DE CUMPLIMIENTO 638
8.1. Relación con el Reglamento General de Protección de Datos (RGPD) 638
8.2. Relación con normativa de ciberseguridad (NIS2, ISO 27001, ENS) .. 639
8.3. Relación con normativa contractual y derecho de la competencia .. 640
8.4. Relación con regulación cloud y portabilidad de servicios 640

CAPÍTULO 3.4.

MAPA DE OBLIGACIONES DE DILIGENCIA DEBIDA

XAVIER RIBAS 643
1. ÁMBITOS PROTEGIDOS 643
1.1. Derechos humanos 643
1.2. Medio ambiente 644

Si quieres adquirir esta obra haz click aquí

Página

2. CANALES DE SUMINISTRO Y DE DISTRIBUCIÓN 645
3. MAPA DE OBLIGACIONES DE DILIGENCIA DEBIDA 646
4. POLÍTICA DE DILIGENCIA DEBIDA 647
5. ANÁLISIS DE RIESGOS 647
6. PRIORIZACIÓN DE RIESGOS 648
7. PREVENCIÓN DE RIESGOS 648
8. ELIMINACIÓN DE EFECTOS ADVERSOS 649
9. REPARACIÓN DE EFECTOS ADVERSOS 650
10. COLABORACIÓN CON LAS PARTES INTERESADAS 650
11. MECANISMO DE NOTIFICACIÓN 650
12. PROCEDIMIENTO DE RECLAMACIÓN 651
13. SUPERVISIÓN 652
14. COMUNICACIÓN 652
15. DOCUMENTACIÓN 652

CAPÍTULO 3.5.
LEY DE ATENCIÓN DE LA CLIENTELA
REBECA VELASCO Y ALBA MORENO 653
1. INTRODUCCIÓN Y CONTEXTO NORMATIVO 653
1.1. Finalidad de la Ley 10/2025 653
1.2. Ámbito de aplicación 654
1.3. Relevancia desde la perspectiva de compliance 655
2. FORMACIÓN Y CULTURA DE CUMPLIMIENTO 655
2.1. La formación como pilar del cumplimiento 655
2.2. Alcance y colectivos afectados 656
2.3. Contenido de la formación 656
2.4. Frecuencia, actualización y trazabilidad 657
2.5. Cultura de cumplimiento en la atención a la clientela 657
2.6. Evaluación y mejora continua 658

Si quieres adquirir esta obra haz click aquí

Página

3. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE CUMPLIMIENTO 658
3.1. Riesgos en la atención a la clientela 659
3.2. Riesgos derivados de la automatización y los canales digitales 659
3.3. Riesgos en la gestión de reclamaciones 660
3.4. Riesgo reputacional asociado 660
3.5. Evaluación y priorización de riesgos 660
4. INTEGRACIÓN EN EL MODELO DE COMPLIANCE 661
4.1. Incorporación en políticas y procedimientos 661
4.2. Alineación con otros riesgos (consumo, datos, digital) 661
4.3. Mejora continua del sistema 662

4

MAPA DE RIESGOS Y OBLIGACIONES LEGALES 2026 POR SECTORES

CAPÍTULO 4.1.

NORMAS DE MAYOR INCIDENCIA EN 2026 PARA EL SECTOR FINANCIERO Y AQUELLAS RELATIVAS A LA FUNCIÓN DE COMPLIANCE Y A SUS RIESGOS SI LAS HUBIERA

ELISABET ESCAYOLA 665

CAPÍTULO 4.2.

ESPACIO EUROPEO DE DATOS DE SALUD: HACIA UN EMPODERAMIENTO REAL DEL PACIENTE

ALEJANDRA SALAT FRAGA 699

1. QUÉ ES EL REEDS Y QUÉ PROBLEMAS TRATA DE SOLUCIONAR 700
2. CUANDO Y A QUIÉN APLICA 702
2.1. Ámbito temporal 702
2.2. A qué y a quién aplica 702
3. ¿EL FIN DEL PAPEL? 703

Si quieres adquirir esta obra haz click aquí

Página

4. USO PRIMARIO (CAPÍTULO II) 704

4.1. Qué es uso primario 704

4.2. Categorías prioritarias de datos de salud electrónicos personales .. 704

4.3. Registro de categorías prioritarias en HCE 705

5. DERECHOS DE LOS PACIENTES EN CUANTO AL USO PRIMARIO 705

5.1. Derecho de acceso (art. 3) 706

5.2. Servicios de acceso salud y representantes (art. 4) 707

5.3. Derecho del paciente a introducir información en su propia HCE (art. 5) 707

5.4. Derecho del paciente a solicitar la rectificación (art. 6) 707

5.5. Derecho de los pacientes a la portabilidad de los datos (art. 7 REEDS) 708

5.6. Derecho a limitar el acceso (art. 8 REEDS) 708

5.7. Derecho a obtener información sobre el acceso a datos (art. 9) 709

5.8. Opt-out opcional (art. 10) 709

5.9. Cuadro comparativo derechos REEDS y RGPD 710

6. ACCESO POR PROFESIONALES (TAMBIÉN DESDE OTRO EM) 712

7. MYHEALTH@EU 713

8. GOBERNANZA USO PRIMARIO 713

9. USO SECUNDARIO (CAPÍTULO IV) 714

9.1. Qué es el uso secundario 714

9.2. Quien debe facilitar datos de salud electrónicos 714

9.3. Sujetos exentos 715

9.4. Fines permitidos (art. 53) 715

9.5. Fines prohibidos (art. 54) 716

9.6. Categorías mínimas de datos 717

9.7. Cómo funciona a la práctica 717

9.8. Calidad y utilidad de los datos 718

Si quieres adquirir esta obra haz click aquí

Página

9.9. Vías de acceso: permiso o petición 718

9.9.1. En caso de solicitud de acceso para permiso 719

9.9.2. En caso de petición de datos (formato estadístico anonimizado) 721

9.10. Publicación de resultados 721

9.11. Usuarios de datos y terceros países 721

9.12. Derecho de opt-out en uso secundario 721

9.12.1. Qué efecto jurídico produce el opt-out (y sus límites) .. 722

9.12.2. Cómo se implementa en la práctica: dónde se «filtra» el opt-out 722

9.12.3. Excepciones posibles por interés público (opcional para EEMM) 722

10. PROPIEDAD INTELECTUAL E INDUSTRIAL («IP») Y SECRETOS COMERCIALES (ART. 52) 722

11. INCUMPLIMIENTOS, MULTAS Y OTRAS SANCIONES 723

11.1. Supervisión en uso primario: autoridades de salud digital y autoridades RGPD 723

11.2. Supervisión en uso secundario: OADS 724

11.3. Discrecionalidad para EEMM 724

12. CONCLUSIONES 724

5

RETOS DE FUTURO

CAPÍTULO 5.1.

INTELIGENCIA ARTIFICIAL, TRANSFORMACIÓN Y FUTURO

CARLA CASAS 729

1. ¿CUÁL FUE TU PRIMER CONTACTO CON LA IA Y QUÉ IMPACTO TUVO EN TI? 730

2. HAS MENCIONADO RIESGOS PSICOLÓGICOS EN PERSONAS QUE INTERACTÚAN INTENSAMENTE CON LA IA. ¿CUÁLES SON LOS PRINCIPALES? 730

Si quieres adquirir esta obra haz click aquí

Página

3. ¿CÓMO VINCULAS LA IA CON TÉCNICAS DE MANIPULACIÓN Y PERSUASIÓN? 730

4. ¿CÓMO VES EL MERCADO LABORAL Y LA SOCIEDAD EL IMPACTO ECONÓMICO DE LA IA? 731

5. SI EL CONOCIMIENTO PIERDE VALOR, ¿QUÉ ES LO QUE SÍ LO TIENE? 731

6. MENCIONASTE QUE MUCHOS PRODUCTOS DE IA SE CONVERTIRÁN EN ELEMENTOS BÁSICOS POCO RELEVANTES. ¿QUÉ ESTÁ PASANDO CON EL MERCADO DE HERRAMIENTAS? 731

7. PONGAMOS COMO EJEMPLO UNA AUDITORÍA DE COMPLIANCE. ¿POR QUÉ EL FACTOR HUMANO SIGUE SIENDO INSUSTITUIBLE? 732

8. ¿HACIA DÓNDE APUNTAN LAS ESPECULACIONES SOBRE INTELIGENCIA GENERAL Y CONSCIENCIA? 732

9. HABLAS DE SOLEDAD INTELECTUAL: LA MAYORÍA NO QUIERE HABLAR DE ESTO. ¿CÓMO NOS PUEDE AFECTAR? 732

10. USAS LA METÁFORA DEL TRACTOR PARA HABLAR DE COMPETITIVIDAD. EXPLÍCALA 732

11. MENCIONASTE UNA CRISIS DE IDENTIDAD PROFESIONAL. ¿ES REALMENTE TAN GRAVE? 733

12. ¿CUÁL ES TU PROPUESTA PARA QUE LAS EMPRESAS GESTIONEN ESTE RETO? 733

13. ¿QUÉ ELEMENTOS CONSIDERAS ESENCIALES EN EL PROCESO DE FORMACIÓN Y TRANSFORMACIÓN DE UN PROFESIONAL Y DE UNA EMPRESA EN LOS PRÓXIMOS CINCO AÑOS? 733

14. PARA ACABAR, ¿PUEDES DARME TU OPINIÓN SOBRE LOS ASPECTOS ÉTICOS? 734

CAPÍTULO 5.2.

NEURODERECHOS Y PRIVACIDAD COGNITIVA: NUEVOS DESAFÍOS PARA EL COMPLIANCE

AGUSTINA BARISONE 737

1. INTRODUCCIÓN 737

Si quieres adquirir esta obra haz click aquí

Página

2. MARCO CONCEPTUAL: NEURODERECHOS Y PRIVACIDAD COGNITIVA. FUNDAMENTOS HUMANOS, ÉTICOS Y PSICOLÓGICOS 739

2.1. Transformación del concepto de privacidad 739

2.2. Neurodatos: definición y características 739

2.3. Privacidad cognitiva: delimitación y alcance 740

2.4. Neuroderechos: fundamentos y principios 740

2.5. Implicaciones para el Compliance 741

3. MARCO NORMATIVO VIGENTE EN ESPAÑA Y LA UNIÓN EUROPEA 741

3.1. Protección de datos personales y derechos digitales 742

3.2. Regulación de la inteligencia artificial y tecnologías emergentes ... 742

3.3. Derechos fundamentales y protección de la esfera mental 743

3.4. Límites del marco normativo actual 743

4. DESAFÍOS PARA EL COMPLIANCE Y LA GOBERNANZA ÉTICA 744

5. RETOS ÉTICOS Y PSICOSOCIALES 745

5.1. Manipulación, vigilancia y autonomía psicológica 745

5.2. Impacto en la salud mental y el bienestar 746

5.3. El rol del psicólogo en la gestión del riesgo cognitivo 747

6. CONCLUSIONES 747

CAPÍTULO 5.3.

PRODUCTOS SANITARIOS Y TERAPIAS DIGITALES

VÍCTOR MANUEL ANTUNES RIVERA 749

1. DEFINICIÓN DE PRODUCTOS SANITARIOS Y DE TERAPIAS DIGITALES 749

2. MAPA LEGISLATIVO DE LOS PRODUCTOS SANITARIOS Y TERAPIAS DIGITALES. OBLIGACIONES NORMATIVAS 750

3. NORMATIVA ESPECÍFICA Y RETOS PARA EL COMPLIANCE EN LAS TERAPIAS DIGITALES 754

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 5.4.

COMPUTACIÓN CUÁNTICA, CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

XAVIER RIBAS 759

1. CAMBIO TECNOLÓGICO DISRUPTIVO 759

2. RIESGO ACTUAL DIFERIDO: CAPTURA AHORA Y DESCIFRA EN EL FUTURO 760

3. SISTEMA ACTUAL BASADO EN LA DIFICULTAD DEL CÁLCULO 761

4. ROBUSTEZ ACTUAL DE LAS CONTRASEÑAS Y DEL CIFRADO 762

5. FUERZA BRUTA CLÁSICA VERSUS LÍMITES FÍSICOS 764

6. LA DISRUPCIÓN CUÁNTICA 764

7. RIESGOS PARA LA CIBERSEGURIDAD 765

8. RIESGOS PARA LAS IDENTIDADES DIGITALES 766

9. IMPACTO EN COMPLIANCE 767

10. IMPACTO EN MATERIA DE PROTECCIÓN DE DATOS 768

10.1. Obligaciones en materia de seguridad 768

10.2. Responsabilidad proactiva 769

10.3. Evaluaciones de impacto 770

10.4. Conservación de datos y riesgo diferido 770

10.5. Conclusiones 771

11. DEBER DE PREPARACIÓN 771

12. LA CRIPTOGRAFÍA POST-CUÁNTICA 773

13. LOS ALGORITMOS POST-CUÁNTICOS 773

14. LOS SISTEMAS HÍBRIDOS E INTELIGENTES 774

15. LAS VENTAJAS FUTURAS DE LOS SISTEMAS BIOMÉTRICOS EN EL CONTROL DE ACCESO 775

16. EFECTOS JURÍDICOS TRANSVERSALES 775

17. RESPONSABLES DE LA GESTIÓN DE ESTE RIESGO 776

Si quieres adquirir esta obra haz click aquí

Página

CAPÍTULO 5.5.

GENERAR CULTURA DE CUMPLIMIENTO EN LA ERA DE LA IA

ALBA MORENO 779

1. INTRODUCCIÓN 779

2. DE LA MERA OBSERVANCIA NORMATIVA A LA CULTURA DE CUMPLIMIENTO 780

3. IDENTIFICACIÓN DE RIESGOS LEGALES Y ÉTICOS EN PROYECTOS DE IA 781

4. EVALUACIONES DE IMPACTO Y ANÁLISIS DE RIESGOS 782

5. SENSIBILIZACIÓN GENERAL DE LA PLANTILLA 783

6. INTEGRAR LA CULTURA DE CUMPLIMIENTO EN LOS INCENTIVOS Y PROCESOS INTERNOS 784

6.1. Evaluación del desempeño incorporando el cumplimiento en IA ... 785

6.2. Reconocimiento de buenas prácticas y liderazgo responsable 785

6.3. Consecuencias internas del uso indebido de sistemas de IA 786

7. CONTRATOS, RELACIONES CON TERCEROS Y CADENA DE VALOR DE LA IA 788

7.1. Requisitos de cumplimiento en la selección de proveedores de IA .. 788

7.2. Cláusulas de compliance en contratos de IA 789

7.3. Gestión del cumplimiento en ecosistemas colaborativos de datos y modelos 790

8. INDICADORES, AUDITORÍA Y MEJORA CONTINUA DE LA CULTURA DE CUMPLIMIENTO 791

8.1. Definición de indicadores clave de cumplimiento en IA 791

8.2. Auditorías internas y externas de sistemas de IA 792

9. SUPERVISIÓN HUMANA Y CONTROL OPERACIONAL DEL SISTEMA 793

9.1. Modelos de supervisión humana (HITL, HOTL, human override). 793

9.2. Gestión de incidentes en IA 794

9.3. Monitorización en producción 794

9.4. Mecanismos de parada y rollback 795

Si quieres adquirir esta obra haz click aquí

Página

10. GESTIÓN DE RECLAMACIONES, DERECHOS Y RELACIÓN CON AFECTADOS CON ESPECIAL ATENCIÓN A COLECTIVOS VULNERABLES Y CONTEXTO SOCIAL 796

10.1. Gestión de reclamaciones y canales de atención 796

10.2. Garantía de derechos frente a decisiones automatizadas 797

10.3. Atención reforzada a colectivos vulnerables 798

10.4. Criterios de cuidado reforzado en contextos sensibles 798

CAPÍTULO 5.6.

ÉTICA EN LA EVALUACIÓN DE IMPACTO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

REBECA VELASCO 801

1. MARCO NORMATIVO DE REFERENCIA 802

2. PRINCIPIOS ÉTICOS DE APLICACIÓN TRANSVERSAL 802

2.1. Beneficencia y no maleficencia 803

2.2. Autonomía y supervisión humana 803

2.3. Equidad y no discriminación 803

2.4. Explicabilidad y transparencia 804

2.5. Privacidad y protección de datos desde el diseño 804

2.6. Bienestar social y medioambiental 804

2.7. Responsabilidad y rendición de cuentas 806

3. ANÁLISIS ÉTICO DIFERENCIADO POR NIVEL DE RIESGO 806

3.1. Sistemas de IA prohibidos 806

3.2. Sistemas de alto riesgo (Anexo III RIA) 807

a) Sistema de gestión de riesgos (Art. 9 RIA) 807

b) Gobernanza de datos (Art. 10 RIA) 807

c) Documentación técnica y trazabilidad (Arts. 11 y 12 RIA) 807

d) Transparencia e información a los usuarios (Art. 13 RIA) 808

e) Supervisión humana (Art. 14 RIA) por personal capacitado 808

f) Evaluación de conformidad y registro (Arts. 43 y 49 RIA) 808

Si quieres adquirir esta obra haz click aquí

Página

3.3. Sistemas de riesgo limitado (Arts. 50 y 53 RIA) 808
3.4. Modelos de IA de uso general 809
4. EVALUACIÓN DE IMPACTO EN DERECHOS FUNDAMENTALES (EIDF) 809
4.1. Contenido mínimo de la Evaluación de Impacto en Derechos Fundamentales o (EIDF) 810
4.2. Coordinación con la EIPD (Art. 35 RGPD) 810
5. GOBERNANZA INTERNA 811
5.1. Roles y responsabilidades 811
5.2. Proceso de evaluación ética: fases 812
5.3. Registro de sistemas y documentación 812
6. SUPUESTOS DE ESPECIAL ATENCIÓN ÉTICA 812
6.1. Sistemas que toman decisiones con efectos jurídicos significativos .. 812
6.2. Sistemas que afectan a grupos vulnerables 813
6.3. Sistemas de generación de contenido (IA generativa) 813
6.4. Sistemas de IA en el sector de la salud 813
7. INCUMPLIMIENTO Y CONSECUENCIAS 813
8. CONCLUSIONES Y RECOMENDACIONES 814

CAPÍTULO 5.7.

ÉTICA Y GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR

CARMEN LÓPEZ RUIZ 815

1. LA TRANSFORMACIÓN DEL SECTOR ASEGURADOR MEDIANTE LA IA 815
1.1. Principales marcos internacionales 816
1.2. Qué es y qué no es un sistema de IA: aclarando conceptos clave 817
2. ÉTICA EN LA IA 820
2.1. Principios éticos 820
2.2. Los riesgos de una IA sin ética en el sector asegurador 821
3. GOBERNANZA DE LA IA EN LA ENTIDAD ASEGURADORA. 824
3.1. Estructura organizativa: Comité de IA, roles clave y ubicación 826

Si quieres adquirir esta obra haz click aquí

Página

3.2. Gestión de los sistemas de IA 830
3.3. Registro de usos de sistemas de IA 833
3.4. La IA como herramienta de trabajo y alfabetización 834
4. REFLEXIÓN FINAL 836
5. BIBLIOGRAFÍA 837

CAPÍTULO 5.8.

AUMENTO DEL AHORRO Y LA INVERSIÓN EN LAS EMPRESAS; CMU (MERCADO ÚNICO DE CAPITALES) RIS (RETAIL RISK STRATEGY ENTRE OTRAS) + EURO DIGITAL

ELISABET ESCAYOLA 839

1. MERCADO ÚNICO DE CAPITALES 839
2. RETAIL RISK STRATEGY 854
2.1. Definición y alcance de la norma 854
3. EURO DIGITAL 865

CAPÍTULO 5.9.

BLOCKCHAIN Y SU USO EN LAS FINANZAS. TOKENIZACIÓN DE ACTIVOS

VÍCTOR MANUEL ANTUNES RIVERA 869

1. DEFINICIÓN DE BLOCKCHAIN. USO EN LAS FINANZAS: VENTAJAS Y RIESGOS 869
2. TOKENIZACIÓN DE ACTIVOS 872
2.1. Definición 872

CAPÍTULO 5.10.

ANÁLISIS DAFO DEL DIRECTIVO FRENTE A LA INTELIGENCIA ARTIFICIAL

AGUSTINA BARISONE 877

1. INTRODUCCIÓN 877
2. SESGOS COGNITIVOS 878
3. SOBRECARGA COGNITIVA 879

Si quieres adquirir esta obra haz click aquí

Página

4. RESISTENCIA AL CAMBIO O DIFICULTAD PARA DESAPRENDER MODELOS DE GESTIÓN TRADICIONALES..... 879

5. BRECHA DE COMPETENCIA DIGITAL PARA EVALUAR CRÍTICAMENTE LOS RESULTADOS DE LA IA..... 880

6. DIFICULTAD PARA DELEGAR DECISIONES A SISTEMAS ALGORÍTMICOS SIN PERDER EL CONTROL ESTRATÉGICO 881

7. RIESGO DE DEPENDENCIA EXCESIVA DE LA IA, EROSIONANDO EL PENSAMIENTO CRÍTICO PROPIO 881

8. PARÁLISIS POR ANÁLISIS FRENTE A LA HIPER-DISPONIBILIDAD DE DATOS 882

9. COMUNICACIÓN DE DECISIONES BASADAS EN IA A EQUIPOS CON BAJA ALFABETIZACIÓN DIGITAL..... 883

10. OBSOLESCENCIA DE HABILIDADES DIRECTIVAS CLÁSICAS ANTE LA VELOCIDAD DEL CAMBIO TECNOLÓGICO 883

11. PÉRDIDA DE AUTORIDAD PERCIBIDA SI LOS MODELOS DE IA SUPERAN AL DIRECTIVO EN PREDICCIONES..... 884

12. MODIFICACIÓN DE LA PIRÁMIDE DIRECTIVA 884

13. PRESIÓN CULTURAL POR ADOPTAR LA IA 885

14. VENTAJA DE LOS COMPETIDORES CON IA..... 886

15. RIESGO REPUTACIONAL EN DECISIONES CON IA QUE RESULTAN ERRÓNEAS O ÉTICAMENTE CUESTIONABLES 886

16. DIFICULTAD PARA MANTENER LOS VALORES CORPORATIVOS EN ENTORNOS DOMINADOS POR MÉTRICAS ALGORÍTMICAS..... 887

17. DEVALUACIÓN DEL CRITERIO EXPERTO HUMANO FRENTE A LA PERCEPCIÓN DE OBJETIVIDAD DE LA IA. 887

18. TYPOMAXXING Y LA HUMANIZACIÓN DE LA IA..... 888

Si quieres adquirir esta obra haz click aquí

Página

19. LOS PERFILES SENIOR COMO VENTAJA ESTRATÉGICA ANTE LA IA 889

20. IMPACTO DE LA ELIMINACIÓN DE PERFILES JUNIOR POR LA IA 889

21. DECISIONES BASADAS EN EL PRECIO ACTUAL DE LA IA. 890

22. RALENTIZACIÓN DEL DESARROLLO 891

23. CONCLUSIONES 891

Si quieres adquirir esta obra haz click aquí

Capítulo 1.16

Formación obligatoria en materia de IA

XAVIER RIBAS

SUMARIO: 1. EL PUNTO DE PARTIDA DEL CUMPLIMIENTO EN IA. 2. EL MARCO NORMATIVO: ARTÍCULOS 4 Y 3.56 Y CONSIDERANDO 20. 3. QUIÉN ESTÁ OBLIGADO Y QUÉ SE SANCIONA. 4. LOS DOS REQUISITOS DE ADAPTACIÓN QUE EXIGE EL ARTÍCULO 4. 5. ESTRUCTURA MODULAR. 6. ADAPTACIÓN AL PERFIL DEL DESTINATARIO DE LA FORMACIÓN. 7. OBJETIVOS Y CONTENIDOS EXIGIBLES. 8. TRAZABILIDAD, EVIDENCIA Y VERIFICACIÓN. 9. LA FORMACIÓN DE LA FUNCIÓN DE SUPERVISIÓN HUMANA. 10. CARÁCTER DINÁMICO DEL PLAN. 11. CONCLUSIONES.

1. EL PUNTO DE PARTIDA DEL CUMPLIMIENTO EN IA

Todo programa de cumplimiento normativo en materia de inteligencia artificial empieza por las personas. Antes de inventariar sistemas, clasificar riesgos o diseñar controles, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, RIA), impone una obligación que opera como condición habilitante de todas las demás: garantizar que quienes desarrollan, despliegan, operan o se ven afectados por sistemas de IA dispongan de un nivel suficiente de competencia para comprenderlos. Es el deber de alfabetización en IA, recogido en el artículo 4 del RIA.

La ubicación del precepto no es casual. El artículo 4 se integra en las disposiciones generales del Reglamento y precede a todo el régimen sustantivo de prohibiciones, clasificación de riesgo y obligaciones de los operadores. El legislador europeo sitúa así la competencia humana como fundamento previo del resto del articulado. Para la función de compliance, la formación se convierte e en la primera evidencia documentada de diligencia en el uso de la IA que la organización puede crear.

2. EL MARCO NORMATIVO: ARTÍCULOS 4 Y 3.56 Y CONSIDERANDO 20

El artículo 4 del RIA obliga a proveedores y responsables del despliegue a adoptar medidas para garantizar, en la mayor medida posible, un nivel suficiente de alfabetización

Si quieres adquirir esta obra haz click aquí

en materia de IA de su personal y de las demás personas que se ocupen del funcionamiento y la utilización de los sistemas de IA en su nombre.

El artículo contiene tres elementos a tener en cuenta:

1. Es una obligación de medios y no de resultado, es decir, basta acreditar acciones razonables y proporcionadas, no garantizar un dominio individual.
2. El perímetro subjetivo es amplio, ya que alcanza a la plantilla y a los terceros que operan los sistemas de IA por cuenta de la organización.
3. No existe umbral de tamaño, es decir, afecta por igual a la pequeña y la gran empresa. La norma ajusta el alcance y la profundidad, pero no modifica la existencia del deber.

El contenido material lo fija el artículo 3, apartado 56, que define la alfabetización como las capacidades, los conocimientos y la comprensión que permiten a proveedores, responsables del despliegue y personas afectadas llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades, los riesgos y los perjuicios que la IA puede causar. El Considerando 20 añade la finalidad, que consiste en dotar a los agentes de los conceptos para decidir de forma fundamentada, y aclara que la competencia exigible no es uniforme, sino dependiente del contexto.

La obligación es plenamente exigible desde el 2 de febrero de 2025.

3. QUIÉN ESTÁ OBLIGADO Y QUÉ SE SANCIONA

El deber recae sobre dos categorías de operadores: los proveedores de sistemas de IA y los responsables del despliegue, es decir los usuarios profesionales de dichos sistemas.

Los destinatarios de la formación, por su parte, son el personal propio y las personas que, en nombre del operador, se encarguen del funcionamiento y la utilización de los sistemas, lo que incorpora a proveedores externos y colaboradores. Esta extensión del perímetro a terceros es uno de los puntos que con más frecuencia se descuida en la práctica.

El incumplimiento de las obligaciones de formación constituirá una infracción grave del Reglamento de IA en los siguientes casos:

Artículo del RIA	**Obligaciones cuyo incumplimiento puede constituir una infracción grave del Reglamento de IA**
Formación asociada al uso de los sistemas de IA Artículo 26.1	Adoptar, por parte de los responsables del despliegue, las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de IA de alto riesgo con arreglo a las instrucciones de uso que los acompañen.
Formación asociada a la supervisión humana Artículo 26.2	Asignación de la supervisión humana de los sistemas de IA de alto riesgo a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

Si quieres adquirir esta obra haz click aquí

Artículo del RIA	**Obligaciones cuyo incumplimiento puede constituir una infracción grave del Reglamento de IA**
Conocimientos asociados a la supervisión humana Artículo 14.4 Artículo 26.4 Artículo 25.5	1. Suministrar los conocimientos necesarios para entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento. 2. Suministrar los conocimientos necesarios para ser consciente de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»). 3. Suministrar los conocimientos necesarios para interpretar correctamente los resultados de salida del sistema de IA de alto riesgo. 4. Suministrar los conocimientos necesarios para decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que éste genere. 5. Suministrar los conocimientos necesarios para intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura. 6. Suministrar los conocimientos necesarios para verificar que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo.

Tabla. Obligaciones cuyo incumplimiento puede constituir una infracción grave del Reglamento de IA.

4. LOS DOS REQUISITOS DE ADAPTACIÓN QUE EXIGE EL ARTÍCULO 4

El artículo 4 del RIA exige que la formación esté adaptada, y esa adaptación opera sobre dos requisitos que conviene tener en cuenta. El primero es el perfil del destinatario: sus conocimientos técnicos, su experiencia, su nivel de educación y su formación previa. El segundo es el contexto previsto de uso de los sistemas de IA, que a su vez se descompone en el sector al que pertenece la empresa, el rol o posición que ocupa en la cadena de valor de la IA, el departamento del usuario, las finalidades y casos de uso previstos, y los modelos o sistemas concretos que se van a utilizar.

A estos dos requisitos el Reglamento suma una tercera exigencia, con frecuencia olvidada: la adaptación a las personas afectadas por el uso de los sistemas. Usuario y persona afectada sujetos diferentes, y el plan debe contemplar a los dos. La tabla siguiente ilustra esa distinción.

Si quieres adquirir esta obra haz click aquí

Sistema de IA	Trabajadores del proveedor	Usuarios del sistema	Personas afectadas
Chatbot	Proveedor del chatbot	Empresa que lo integra en su web	Usuarios del chatbot
Análisis de currículums	Proveedor del sistema	Departamento de RR. HH.	Candidatos
Diagnóstico de enfermedades	Proveedor del sistema	Equipo médico	Pacientes

Tabla. Diferenciación entre usuarios del sistema y personas afectadas según el tipo de sistema de IA.

5. ESTRUCTURA MODULAR

La forma más eficaz de cumplir los requisitos en un curso es desarrollarlo de manera modular, combinando contenidos intercambiables que se ensamblan según el sector, el rol, el departamento y el sistema de cada organización. El modelo se puede dividir en cinco módulos:

- Módulo transversal. - Contenido común a todos los cursos, con independencia de sector o rol: conceptos básicos de la IA, su ciclo de vida, la distinción entre modelo y sistema de IA, las oportunidades y los perjuicios que puede causar, y los contenidos éticos y jurídicos esenciales, de acuerdo con la regulación de la IA en la Unión, obligaciones de los usuarios, riesgos jurídicos y medidas preventivas.
- Módulo de sector. - Casos de uso más habituales, riesgos y controles específicos y oportunidades del sector de actividad.
- Módulo de rol. - Adaptado a la posición de la empresa en la cadena de valor de la IA según las categorías del Reglamento: proveedor, importador, distribuidor y responsable del despliegue o usuario.
- Módulo de departamento. - Casos de uso, riesgos, controles y oportunidades propios del área que utiliza el sistema.
- Módulo de sistema de IA. - Casos de uso, riesgos específicos, medidas que el usuario debe aplicar y oportunidades de cada modelo o sistema concreto que la empresa vaya a utilizar.

Las ventajas de esta arquitectura es que satisface el doble eje del artículo 4 sin multiplicar cursos, ya que el módulo transversal cubre la base común y los módulos de sector, rol, departamento y sistema cubren el contexto previsto de uso. Esta combinación concreta de piezas, junto con el nivel de profundidad, permite adaptar la formación al perfil del destinatario.

6. ADAPTACIÓN AL PERFIL DEL DESTINATARIO DE LA FORMACIÓN

Si los módulos son las columnas del curso, el perfil del destinatario determina el nivel de adaptación o la profundidad con que se imparte cada uno. La estrategia recomendada

Si quieres adquirir esta obra haz click aquí

combina un nivel básico y un nivel avanzado dentro del propio curso, de modo que un mismo módulo pueda impartirse con distinta profundidad. No es lo mismo formar a un ingeniero de datos que diseña modelos que a personal administrativo que utiliza un asistente generativo, o que a un director jurídico que debe validar decisiones con impacto en derechos. La tabla orientativa siguiente cruza los dos planos.

Perfil	Contenido	Profundidad
Dirección y Consejo	Gobernanza, marco normativo, riesgos estratégicos y deberes de supervisión.	Media-alta.
Función jurídica y compliance	Módulos transversales y de rol; RIA, RGPD y normativa sectorial; documentación.	Alta.
Perfiles técnicos	Módulo de sistema de IA; funcionamiento de modelos, sesgos, calidad de datos.	Alta.
Usuarios de negocio	Módulos de departamento y sistema; uso informado y detección de resultados anómalos.	Media.

Tabla. Cruce entre el modelo modular (columnas) y el perfil del destinatario (profundidad).

7. OBJETIVOS Y CONTENIDOS EXIGIBLES

Cualquiera que sea la combinación modular, el curso debe perseguir un conjunto de objetivos que traducen directamente la definición del artículo 3.56, es decir:

1. Mejorar las capacidades, los conocimientos y el nivel de comprensión de la IA del usuario.
2. Prepararlo para un uso informado y responsable de los sistemas
3. Hacerle tomar conciencia de las oportunidades, los riesgos y los perjuicios que la IA puede causar, así como de los aspectos éticos y jurídicos de su uso.

Estos objetivos coinciden con los atributos que valorará la autoridad competente al medir la suficiencia de la formación.

8. TRAZABILIDAD, EVIDENCIA Y VERIFICACIÓN

El RIA es un reglamento basado en la rendición de cuentas, por lo que no basta con formar, hay que poder demostrarlo. Un curso sin registro de asistencia, sin evaluación y sin evidencia de aplicación no satisface el artículo 4 aunque se haya impartido. Desde la perspectiva del compliance, la formación que no deja rastro documental es, a efectos probatorios, una formación que no ha existido. Por ello el curso debe ser auditable, ofrecer trazabilidad sobre la actividad de cada alumno, contemplar la emisión de un certificado de finalización y, en su grado óptimo, permitir generar una evidencia indubitada con sello de tiempo que acredite la fecha en la que la empresa impartió la formación. La formación es, por lo tanto, la primera pieza de la evidencia defensiva.

Si quieres adquirir esta obra haz click aquí

Para verificar si un curso cumple el artículo 4 y los criterios de las FAQ de la Comisión Europea, resulta útil una lista de comprobación. Los puntos esenciales son los siguientes:

1. ¿El curso está adaptado a los conocimientos, experiencia, educación y formación del usuario (p. ej., con nivel básico y avanzado)?
2. ¿Está adaptado al contexto previsto de uso de los sistemas de IA?
3. ¿Tiene en cuenta el rol de la empresa en la cadena de valor de la IA?
4. ¿Contempla los casos de uso y riesgos específicos del sector?
5. ¿Contempla los casos de uso y riesgos específicos del departamento?
6. ¿Contempla los casos de uso y riesgos específicos del sistema de IA utilizado?
7. ¿Tiene en cuenta el perfil de las personas o colectivos afectados (clientes, candidatos, trabajadores, pacientes)?
8. ¿Mejora las capacidades, los conocimientos y el nivel de comprensión del usuario?
9. ¿Prepara para un uso informado y responsable de los sistemas de IA?
10. ¿Genera conciencia de las oportunidades, los riesgos y los perjuicios que la IA puede causar?
11. ¿Aborda los aspectos éticos y jurídicos del uso de la IA?
12. ¿Es auditable, ofrece trazabilidad de la actividad del alumno y emite certificado de finalización?
13. ¿Permite crear una evidencia con sello de tiempo que acredite la fecha de impartición?

9. LA FORMACIÓN DE LA FUNCIÓN DE SUPERVISIÓN HUMANA

La obligación general del artículo 4 tiene un nivel superior cuando entran en juego los sistemas de IA de alto riesgo. Para ellos, el Reglamento exige una formación cualificada vinculada a la función de supervisión humana, cuyo incumplimiento puede constituir una infracción grave. Conviene tratarla de forma separada, porque su régimen, sus destinatarios y sus consecuencias difieren de los de la formación general.

Pueden distinguirse tres capas:

1. La primera es la formación asociada al uso. - El artículo 26, apartado 1, del RIA obliga a los responsables del despliegue a adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de alto riesgo con arreglo a las instrucciones de uso que los acompañan.
2. La segunda es la asignación de la supervisión. - El artículo 26, apartado 2, exige encomendar la supervisión humana de esos sistemas a personas físicas que tengan la competencia, la formación y la autoridad necesarias. La formación deja de ser, así, un mero contenido para convertirse en un requisito de idoneidad del supervisor.

Si quieres adquirir esta obra haz click aquí

3. La tercera capa, y la más exigente, son los conocimientos asociados a la supervisión, que resultan de la lectura conjunta de los artículos 14, apartado 4, 26, apartado 4, y 25, apartado 5, del RIA. El supervisor debe disponer de los conocimientos necesarios para:
   - Entender adecuadamente las capacidades y limitaciones del sistema de alto riesgo y vigilar debidamente su funcionamiento.
   - Ser consciente de la tendencia a confiar de forma automática o excesiva en los resultados del sistema, es decir, el llamado *sesgo de automatización.*
   - Interpretar correctamente los resultados de salida del sistema.
   - Decidir, en cada situación concreta, no utilizar el sistema o descartar, invalidar o revertir sus resultados.
   - Intervenir en el funcionamiento del sistema o interrumpirlo mediante un botón de parada o un procedimiento similar que permita detenerlo de forma segura.
   - Verificar que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema.

La tabla siguiente resume estas obligaciones:

Obligación formativa	**Artículo RIA**	**Contenido**
Formación asociada al uso	Art. 26.1	Usar los sistemas de alto riesgo conforme a las instrucciones de uso que los acompañan.
Asignación de la supervisión	Art. 26.2	Encomendar la supervisión a personas físicas con la competencia, la formación y la autoridad necesarias.
Conocimientos para la supervisión	Arts. 14.4, 26.4 y 25.5	Comprender capacidades y límites del sistema, reconocer el sesgo de automatización, interpretar las salidas, descartar o revertir resultados, intervenir o detener el sistema y verificar la idoneidad de los datos de entrada.

Tabla. Obligaciones de formación vinculadas a la supervisión humana de sistemas de IA de alto riesgo.

La consecuencia práctica para la función de compliance es doble. En el plano del diseño, el modelo modular debe incorporar, para las organizaciones que desplieguen sistemas de alto riesgo, un módulo de supervisión humana dirigido específicamente a las personas designadas como supervisoras, con un nivel de profundidad superior al del usuario ordinario. En el plano del riesgo, la omisión o insuficiencia de esta formación en el terreno de las infracciones graves del Reglamento, lo que eleva tanto la exposición

Si quieres adquirir esta obra haz click aquí

sancionadora como la importancia de documentar de forma indubitada que el supervisor reunía la competencia y la formación exigidas antes de asumir la función.

10. CARÁCTER DINÁMICO DEL PLAN

La obligación no se limita a una acción formativa única. Dado que las herramientas de inteligencia artificial evolucionan con rapidez y que cada nuevo sistema incorporado genera su propia necesidad de competencias, el plan debe prever una actualización periódica, con revisión de contenidos y sesiones de actualización recurrentes, y un mecanismo que vincule la adopción de cualquier sistema de IA nuevo con la actualización del módulo correspondiente. No se puede formar sobre lo que no se ha inventariado, de modo que el registro de casos de uso alimenta de forma natural el módulo de sistema de IA del curso.

Si tomamos el ejemplo de una empresa farmacéutica que despliega tres sistemas: uno de selección de centros para ensayos clínicos, un asistente de farmacovigilancia y una herramienta de cribado de candidaturas en RRHH. El curso se crearía combinando el módulo transversal, el módulo de sector farmacéutico, el módulo de rol, en este caso responsable del despliegue, los módulos de departamento para el equipo clínico y para RRHH y los módulos de sistema correspondientes a cada una de las tres herramientas.

La dirección recibiría el conjunto con énfasis en gobernanza y supervisión, dado que el cribado de candidaturas puede encajar en la categoría de alto riesgo del Anexo III del RIA, mientras los equipos técnicos aprenderían con mayor profundidad el módulo de sistema.

Cada acción quedaría registrada con trazabilidad por alumno, certificado y sello de tiempo, y el plan se revisaría al incorporar cualquier sistema nuevo.

El resultado facilita a la empresa utilizar la IA con criterio y poder demostrarlo.

11. CONCLUSIONES

La formación en materia de IA se integra en los programas de compliance existentes. El modelo modular es una forma eficiente de organizar un curso y al mismo tiempo un mecanismo que permite demostrar, módulo a módulo y alumno a alumno, que la formación se ha ajustado al perfil, al sector, al rol y al sistema concretos.

Acreditar un plan segmentado, proporcionado al riesgo, auditable y fechado de forma indubitada, permite cumplir una obligación legal vigente, reduce la probabilidad de incidentes derivados de la impericia en el uso de la IA y construye la primera capa de evidencia defensiva frente a una eventual exigencia de responsabilidad, también en relación con el artículo 31 bis del Código Penal.

La formación es, en sentido estricto, el punto en el que empieza la acreditación de la diligencia.

Si quieres adquirir esta obra haz click aquí

Capítulo 1.17

Control de terceros, proveedores y cadena de suministro

AMEDEO MARCHELLI

SUMARIO: 1. INTRODUCCIÓN. 2. ESTRUCTURA DE LA CADENA DE VALOR. 2.1. CANALES DE SUMINISTRO Y DISTRIBUCIÓN. 3. POR QUÉ CONTROLAR A LOS TERCEROS. *3.1. Riesgos Legales. 3.2. Riesgos Reputacionales. 3.3. Riesgos Financieros.* 4. MARCO LEGAL. *4.1. Normativa Española. 4.2. Normativa Europea.* 5. ENFOQUE BASADO EN RIESGOS. *5.1. Principios Generales. 5.2. Factores de Riesgo. 5.3. Niveles de Diligencia Debida.* 6. LAS TRES FASES DE LA DILIGENCIA DEBIDA. *6.1. Fase de Selección y Evaluación. 6.2. Fase de Formalización. 6.3. Fase de Seguimiento y Reevaluación.* 7. CONTROLES ESPECÍFICOS POR TIPO DE TERCERO. *7.1. Agentes Comerciales e Intermediarios. 7.2. Proveedores de Bienes y Servicios. 7.3. Socios en Joint Ventures y Alianzas. 7.4. Contratistas y Subcontratistas.* 8. DOCUMENTACIÓN. 9. ORGANIZACIÓN Y RESPONSABILIDADES. *9.1. Responsabilidades por Función. 9.2. Flujo de Aprobación.* 10. SEÑALES DE ALERTA. 11. CONCLUSIONES.

1. INTRODUCCIÓN

Las relaciones con terceros amplían el perímetro de riesgo de la empresa: sus decisiones pueden proyectarse en nuestro nombre o beneficio y generar consecuencias legales, financieras y reputacionales. Por ello, gestionar estos riesgos con un enfoque sistemático no es accesorio; es una condición de eficacia del sistema de compliance.

Este tema ofrece una guía breve y práctica para identificar, evaluar y controlar riesgos derivados de la cadena de suministro y de los canales de distribución. Partimos de un hecho operativo: la cadena de valor no es lineal, sino una red donde los impactos pueden aflorar más allá del primer nivel visible. En ese contexto, la diligencia debida sobre terceros es la herramienta que permite prevenir, detectar y responder ante situaciones como corrupción, vulneraciones de derechos humanos o daño medioambiental.

Si quieres adquirir esta obra haz click aquí

2. ESTRUCTURA DE LA CADENA DE VALOR

2.1. CANALES DE SUMINISTRO Y DISTRIBUCIÓN

Es preciso entender que los canales de suministro y distribución no siguen un patrón lineal, sino ramificado donde cada socio comercial mantiene múltiples vínculos con otros que, a su vez, replican ese esquema[1].

Esta estructura implica que los riesgos pueden originarse en niveles muy alejados de la empresa, en proveedores de proveedores o en distribuidores de distribuidores. La diligencia debida debe tener en cuenta esta complejidad y no limitarse al primer nivel de la cadena.

El canal de suministro incluye a todos los terceros que proporcionan bienes o servicios a la empresa: proveedores directos, subcontratistas, fabricantes de componentes, proveedores de materias primas y otros. El canal de distribución incluye a quienes llevan los productos o servicios de la empresa al mercado: distribuidores, franquiciados, licenciatarios, agentes comerciales y otros.

Las obligaciones de diligencia debida se aplican a ambos canales. Un distribuidor que soborna a funcionarios para obtener contratos genera los mismos riesgos para la empresa que un proveedor que utiliza trabajo forzoso. Ambas situaciones deben prevenirse y, si se producen, deben abordarse con la misma seriedad.

3. POR QUÉ CONTROLAR A LOS TERCEROS

3.1. RIESGOS LEGALES

La normativa española e internacional establece que las empresas pueden ser responsables por actos de terceros que actúan en su nombre o en su beneficio.

En el ámbito penal, la responsabilidad de la persona jurídica (art. 31 bis del Código Penal) exige que el delito lo cometa una persona física que actúe por cuenta y en beneficio de la empresa, y la exención/atenuación depende de un modelo eficaz previo. Un agente comercial que soborna a un funcionario para obtener un contrato puede generar responsabilidad penal para la empresa si esta no tenía controles adecuados.

En el ámbito de la corrupción, normativas como el UK *Bribery Act* (s.7) delito corporativo de falta de prevención con defensa de procedimientos adecuados o el FCPA estadounidense (anti-soborno y libros/registros e controles internos) tienen alcance extraterritorial y pueden aplicarse a empresas españolas que operan en determinados mercados o que tienen conexiones con el Reino Unido o Estados Unidos.

En el ámbito de los derechos humanos y el medio ambiente, la Directiva europea de diligencia debida obliga a las grandes empresas a identificar, prevenir y mitigar los impactos adversos en toda su cadena de valor.

1. CHOI, T., DOOLEY, K. & RUNGTUSANATHAM, M., «Supply networks and complex adaptive systems: Control versus emergence», *Journal of Operations Management* (ELSEVIER), 19(3), 2021-5, pp. 351-366. https://doi.org/10.1016/S0272-6963(00)00068-1

Si quieres adquirir esta obra haz click aquí

3.2. RIESGOS REPUTACIONALES

La asociación con terceros que actúan de forma poco ética puede dañar gravemente la reputación de la empresa. En la era de la información instantánea, las noticias sobre prácticas abusivas en la cadena de suministro se difunden rápidamente y pueden afectar a la percepción de la marca por parte de clientes, inversores y la sociedad.

Campañas de organizaciones no gubernamentales, reportajes periodísticos o publicaciones en redes sociales pueden exponer prácticas de proveedores que la empresa desconocía, pero que se le atribuyen por la relación comercial existente.

3.3. RIESGOS FINANCIEROS

Los incumplimientos de terceros pueden tener consecuencias financieras directas para la empresa: sanciones administrativas o penales, indemnizaciones a perjudicados, costes de investigación y defensa legal, pérdida de contratos o licencias, y exclusión de procesos de contratación pública.

Además, la interrupción de la cadena de suministro por problemas legales de un proveedor puede generar pérdidas operativas significativas.

4. MARCO LEGAL

4.1. NORMATIVA ESPAÑOLA

El Código Penal establece la responsabilidad penal de las personas jurídicas por delitos cometidos por quienes actúan por cuenta de la empresa. La existencia de controles adecuados sobre terceros forma parte del modelo de prevención que puede eximir de responsabilidad.

La Ley 11/2018 obliga a informar anualmente sobre políticas, riesgos, procedimientos de diligencia debida y resultados. La ley modifica el Código de Comercio para exigir que las grandes empresas informen sobre sus prácticas de diligencia debida en la cadena de suministro, incluyendo medidas para prevenir impactos adversos en derechos humanos y medio ambiente.

La Ley 2/2023 de protección del informante obliga a las empresas a disponer de canales de denuncia accesibles para terceros que mantienen relación con la empresa, como proveedores, clientes o socios comerciales, con confidencialidad y posibilidad de anonimato.

4.2. NORMATIVA EUROPEA

La Directiva de diligencia debida en materia de sostenibilidad (CSDDD) establece obligaciones vinculantes para las grandes empresas de la Unión Europea. Estas empresas deben integrar la diligencia debida en sus políticas, identificar impactos adversos reales y potenciales, prevenir y mitigar impactos potenciales, poner fin a impactos reales, establecer mecanismos de reclamación y comunicar públicamente sobre sus actuaciones. Tras el **acuerdo de diciembre 2025**, la Directiva eleva los umbrales de aplicación: mayor

Si quieres adquirir esta obra haz click aquí

o igual a 5.000 empleados y mayor o igual a □1.500m de facturación, con transposición hasta 26/07/2028 y aplicación desde 07/2029; mantiene el enfoque de debida diligencia basada en riesgo a lo largo de la cadena de actividades. En la antigua propuesta originaria del año 2022, se aplicaba a empresas de la UE con más de 500 empleados y facturación mundial superior a 150 millones de euros.

Desde el 1 de enero 2021 el Reglamento sobre minerales de zonas de conflicto exige diligencia debida a los importadores en la Unión Europea de estaño, tantalio, wolframio y oro (3TG) procedentes de zonas afectadas por conflictos o de alto riesgo, conforme a la Guía OCDE.

El Reglamento contra la deforestación (EUDR 2023/1115) obliga a realizar diligencia debida (geolocalización, legalidad y *deforestation-free*) sobre productos que puedan contribuir a la deforestación, como soja, aceite de palma, cacao, café, madera, caucho y ganado. Tras las decisiones 2024-2025, este Reglamento aplica desde 30/12/2026 (grandes/medianas empresas) y 30/06/2027 (micro/pequeñas empresas).

5. ENFOQUE BASADO EN RIESGOS

5.1. PRINCIPIOS GENERALES

No todos los terceros presentan el mismo nivel de riesgo. La diligencia debida debe ser proporcional al riesgo que representa cada relación comercial. Este enfoque permite concentrar recursos en las situaciones más críticas y evita que los procedimientos se conviertan en una carga burocrática desproporcionada.

Los procedimientos de diligencia debida deben ser consistentes para el mismo nivel de riesgo. Terceros similares en términos de riesgo deben someterse a controles similares, garantizando un tratamiento equitativo y evitando arbitrariedades.

Cuando existen muchos riesgos que no pueden abordarse simultáneamente, debe establecerse una priorización. Los criterios de priorización son la probabilidad de que el impacto adverso se materialice y la gravedad del impacto si se produce. Los riesgos más probables y más graves deben abordarse en primer lugar.

5.2. FACTORES DE RIESGO

Al evaluar el riesgo asociado a un tercero, deben considerarse múltiples factores.

Respecto al propio tercero, es relevante el tipo de actividad que realiza para la empresa, si actúa en nombre de la empresa o la representa ante otros, si tiene contacto con funcionarios públicos, su historial de cumplimiento y reputación, su estructura de propiedad y control, y si dispone de su propio sistema de compliance.

Respecto a la geografía, deben considerarse los países donde opera el tercero, los índices de corrupción y estado de derecho de esos países, y los riesgos específicos de derechos humanos o medio ambiente en las zonas de operación.

Respecto a la relación comercial, son relevantes el volumen económico, la duración prevista, el nivel de dependencia mutua y la capacidad de influencia de la empresa sobre el tercero.

Si quieres adquirir esta obra haz click aquí

5.3. NIVELES DE DILIGENCIA DEBIDA

En función del nivel de riesgo identificado, se aplicará un nivel de diligencia debida proporcional.

Para terceros de riesgo bajo, se aplicará una diligencia debida simplificada que incluya verificaciones básicas sobre identidad, actividad y reputación general.

Para terceros de riesgo medio, se aplicará una diligencia debida estándar con verificaciones más detalladas, incluyendo estructura de propiedad, referencias comerciales y búsquedas en bases de datos de riesgos.

Para terceros de riesgo alto, se aplicará una diligencia debida reforzada con investigaciones en profundidad, verificación de beneficiarios finales, posibles visitas presenciales y aprobación por niveles superiores de la organización.

6. LAS TRES FASES DE LA DILIGENCIA DEBIDA

El proceso de diligencia debida sobre terceros se estructura en tres fases que se suceden a lo largo de la relación comercial.

6.1. FASE DE SELECCIÓN Y EVALUACIÓN

Antes de iniciar una relación comercial con un tercero, la empresa debe realizar una evaluación inicial para conocer quién es el tercero y qué riesgos puede presentar.

Los objetivos de esta fase son identificar al tercero y verificar su identidad legal, conocer su actividad, estructura y propiedad, evaluar el nivel de riesgo que representa, y decidir si se procede con la relación y qué nivel de diligencia debida adicional se requiere.

Las acciones típicas incluyen solicitar documentación básica como escrituras, poderes e identificación de administradores; verificar la existencia legal del tercero en registros públicos; realizar búsquedas en bases de datos de sanciones, riesgos y noticias adversas; identificar a los beneficiarios finales; evaluar si existen vínculos con personas políticamente expuestas; solicitar información sobre el sistema de compliance del tercero si existe; y documentar la evaluación realizada y la decisión adoptada.

Deben vigilarse señales de alerta como la reticencia del tercero a proporcionar información básica, estructuras de propiedad opacas o excesivamente complejas, presencia en países de alto riesgo sin justificación comercial clara, noticias adversas sobre corrupción, fraude u otras irregularidades, vínculos con personas políticamente expuestas sin justificación, y solicitudes de pagos inusuales o en jurisdicciones distintas a las de la operación.

6.2. FASE DE FORMALIZACIÓN

Una vez decidido que se procede con la relación comercial, esta debe formalizarse mediante un contrato que incluya compromisos de cumplimiento.

Los objetivos de esta fase son establecer por escrito las obligaciones de cumplimiento del tercero, obtener su compromiso con los valores y políticas de la empresa,

Si quieres adquirir esta obra haz click aquí

prever mecanismos de control y supervisión, y establecer consecuencias en caso de incumplimiento.

Las cláusulas recomendadas para incluir en los contratos son las siguiente:

- La **cláusula de cumplimiento normativo** establece el compromiso del tercero de cumplir todas las leyes aplicables, incluyendo normativa anticorrupción, de competencia, laboral, medioambiental y de protección de datos.
- La **cláusula anticorrupción** recoge la declaración del tercero de que no ha ofrecido ni ofrecerá pagos, regalos o ventajas indebidas a funcionarios públicos o empleados de la empresa para obtener o mantener negocios.
- La **cláusula de derechos humanos** establece el compromiso del tercero de respetar los derechos humanos y mantener condiciones laborales dignas, prohibiendo el trabajo forzoso, el trabajo infantil y la discriminación.
- La **cláusula medioambiental** recoge el compromiso del tercero de cumplir la normativa medioambiental y minimizar el impacto de sus operaciones.
- La **cláusula de auditoría** reserva a la empresa el derecho de auditar al tercero o solicitar información sobre su cumplimiento de las obligaciones contractuales.
- La **cláusula de subcontratación** establece el compromiso del tercero de aplicar requisitos equivalentes a sus propios subcontratistas.
- La **cláusula de resolución** permite a la empresa resolver el contrato en caso de incumplimiento de las obligaciones de compliance, sin perjuicio de otras acciones legales.
- La **cláusula de canal de denuncias** recoge el compromiso del tercero de informar de cualquier indicio de incumplimiento y de utilizar el canal de denuncias si es necesario.

Cuando un tercero ejecute procesos críticos o servicios continuados, el contrato incorporará acuerdos de nivel de servicio que especifiquen obligaciones de compliance (derechos de auditoría, reglas de subcontratación, notificación de incidentes y conservación de registros) y métricas para verificar su cumplimiento. Antes de firmar, se completará una diligencia debida eficaz sobre la capacidad del proveedor para sostener estos compromisos.

Está claro que, dependiendo del contexto, de los profesionales y equipos de negociación, no siempre es posible incluir todas las cláusulas recomendadas. En relaciones donde la empresa tiene poco poder de negociación, puede resultar difícil imponer condiciones al tercero. En estos casos, la imposibilidad de incluir ciertas cláusulas debe considerarse como un factor de riesgo adicional, la reticencia del tercero a aceptar cláusulas de cumplimiento debe tratarse como una señal de alerta, si se decide continuar sin las cláusulas debe documentarse la razón y las medidas alternativas adoptadas, y puede ser necesario aplicar controles compensatorios adicionales.

6.3. FASE DE SEGUIMIENTO Y REEVALUACIÓN

La diligencia debida no termina con la firma del contrato. Durante toda la relación comercial, la empresa debe supervisar al tercero y reevaluar periódicamente el riesgo.

Si quieres adquirir esta obra haz click aquí

Los objetivos de esta fase son detectar cambios en el perfil de riesgo del tercero, identificar posibles incumplimientos de las obligaciones contractuales, actualizar la evaluación de riesgos cuando sea necesario, y decidir sobre la continuidad de la relación.

El seguimiento continuo incluye supervisar el desempeño del tercero en la ejecución del contrato, estar atento a señales de alerta durante la relación, verificar que las facturas y pagos corresponden a servicios reales, y atender cualquier denuncia o queja relacionada con el tercero.

Las revisiones periódicas comprenden actualizar las búsquedas en bases de datos de riesgos, solicitar información actualizada sobre estructura y propiedad, revisar el cumplimiento de las obligaciones contractuales, y reevaluar el nivel de riesgo y ajustar los controles si es necesario.

La frecuencia de las revisiones debe ser de al menos cada doce meses para terceros de alto riesgo, cada dos o tres años para terceros de riesgo medio, y al renovar el contrato o ante cambios significativos para terceros de bajo riesgo.

Indicadores mínimos de desempeño (ejemplos indicativos):

- **Formación**: cobertura y eficacia en terceros relevantes.
- **Tiempo de reacción**: días hasta acción sobre alertas/señales.
- **Excepciones e incidentes**: por tipología y área.
- **Planes correctivos**: porcentaje de acciones cerradas en plazo.
- **Tendencias predictivas**: evolución del riesgo residual en categorías críticas.

Existen circunstancias que exigen reevaluación inmediata: cambio en la propiedad o dirección del tercero, noticias adversas sobre el tercero, indicios de incumplimiento o irregularidades, cambios en la normativa aplicable, expansión de la relación a nuevos países o actividades, y denuncias recibidas a través del canal de denuncias.

7. CONTROLES ESPECÍFICOS POR TIPO DE TERCERO

7.1. AGENTES COMERCIALES E INTERMEDIARIOS

Los agentes comerciales presentan un perfil de riesgo elevado porque actúan en nombre de la empresa y pueden comprometerla con sus actuaciones. El riesgo es especialmente alto cuando el agente tiene contacto con funcionarios públicos o interviene en procesos de decisión de compra donde puede existir la tentación de ofrecer incentivos indebidos.

Los controles recomendados incluyen diligencia debida reforzada antes de su contratación, verificación de que la comisión propuesta es razonable y acorde con el mercado, cláusulas anticorrupción específicas en el contrato, prohibición de subcontratar sin autorización previa, aprobación de la contratación por niveles superiores de la organización, y supervisión activa de su actividad durante toda la relación.

Si quieres adquirir esta obra haz click aquí

7.2. PROVEEDORES DE BIENES Y SERVICIOS

El nivel de diligencia debida sobre proveedores dependerá del riesgo que presente cada uno. Los factores a considerar incluyen el sector de actividad, el país de operación, el tipo de productos o servicios suministrados y el volumen de la relación.

Para proveedores de alto riesgo, los controles recomendados incluyen evaluación de sus prácticas laborales y medioambientales, verificación de que disponen de los permisos y licencias necesarios, inclusión de cláusulas de auditoría y acceso a instalaciones, auditorías presenciales si el riesgo lo justifica, y exigencia de que apliquen requisitos similares a sus subcontratistas.

7.3. SOCIOS EN JOINT VENTURES Y ALIANZAS

Las joint ventures y alianzas requieren especial atención porque la empresa puede ser responsable de actos de su socio en el ámbito de la asociación. La reputación de la empresa queda vinculada a la del socio.

Los controles recomendados incluyen diligencia debida exhaustiva sobre el socio antes de formalizar la asociación, acuerdos claros sobre gobierno corporativo y toma de decisiones, implementación de un sistema de compliance propio en la joint venture, derecho de auditoría sobre las operaciones de la alianza, y mecanismos de salida en caso de incumplimiento grave del socio.

7.4. CONTRATISTAS Y SUBCONTRATISTAS

Los contratistas que trabajan en instalaciones de la empresa o que realizan trabajos en su nombre deben someterse a controles específicos.

Las verificaciones necesarias incluyen comprobar que cumplen la normativa laboral y de seguridad, que sus trabajadores están debidamente contratados y asegurados, y que no utilizan prácticas de subcontratación en cadena que diluyan los controles. Durante la ejecución del trabajo, debe supervisarse que las condiciones de trabajo son adecuadas.

8. DOCUMENTACIÓN

El proceso de diligencia debida debe documentarse adecuadamente. Esta documentación es esencial para demostrar que la empresa actuó con la diligencia exigida en caso de que surjan problemas.

La documentación mínima recomendada incluye la evaluación de riesgos realizada sobre cada tercero, la información recopilada durante la diligencia debida, la decisión adoptada y la persona que la aprobó, el contrato firmado con las cláusulas de compliance, los registros de las revisiones periódicas realizadas, los incidentes detectados y las medidas adoptadas, y las comunicaciones relevantes con el tercero sobre temas de cumplimiento.

Si quieres adquirir esta obra haz click aquí

La documentación debe conservarse durante el plazo establecido por ley (por ejemplo, el art. 30 del Código de Comercio exige seis años (salvo régimen especial)), desde su elaboración u obtención.

La documentación debe incluir pruebas justificativas que demuestren el cumplimiento de las obligaciones. No basta con tener políticas escritas; debe poder demostrarse que se aplicaron en la práctica.

9. ORGANIZACIÓN Y RESPONSABILIDADES

9.1. RESPONSABILIDADES POR FUNCIÓN

Generalmente hablando, hay varias unidades con varios actores en las empresas y cada una de estas tiene objetivos y organización diferente:

- las **unidades de negocio** son responsables de identificar las necesidades de contratación de terceros, proporcionar información sobre la naturaleza de la relación propuesta, supervisar el desempeño del tercero durante la relación, y comunicar cualquier señal de alerta o incidencia.
- El **departamento de compras** es responsable de aplicar los procedimientos de diligencia debida establecidos, recopilar la documentación necesaria del tercero, incluir las cláusulas de compliance en los contratos, y gestionar el proceso de homologación de proveedores.
- La **función de Compliance** (si hay) diseña los procedimientos de diligencia debida, fija los criterios de evaluación de riesgos, asesora en casos complejos o de alto riesgo, verifica la correcta aplicación de los procedimientos y administra el canal de denuncias y notificaciones vinculadas a terceros.
- El **departamento legal** (si hay y no es externalizado) es generalmente responsable de revisar y aprobar las cláusulas contractuales de compliance, asesorar sobre requisitos legales aplicables, y gestionar incidentes legales relacionados con terceros.
- La **alta dirección** es responsable de aprobar relaciones con terceros de alto riesgo cuando sea necesario, asegurar que existen recursos suficientes para la diligencia debida, y establecer el tono desde arriba sobre la importancia del control de terceros.

9.2. FLUJO DE APROBACIÓN

Debe establecerse un flujo de aprobación que defina quién puede autorizar la contratación de terceros según el nivel de riesgo.

- Para terceros de **riesgo bajo**, la aprobación puede corresponder al responsable del área que solicita la contratación.
- Para terceros de **riesgo medio**, la aprobación requiere la validación de compliance además de la del responsable del área.

Si quieres adquirir esta obra haz click aquí

– Para terceros de **riesgo alto**, la aprobación debe corresponder a la alta dirección, con informe previo de compliance.

10. SEÑALES DE ALERTA

Durante la diligencia debida y la relación con terceros deben vigilarse determinadas señales de alerta.

En la fase de selección, las señales de alerta incluyen reticencia a proporcionar información básica, inconsistencias en la documentación presentada, estructura de propiedad inusualmente compleja u opaca, falta de presencia física o instalaciones reales, noticias adversas en medios de comunicación, y vínculos no explicados con funcionarios públicos.

Durante la relación, las señales de alerta incluyen solicitud de pagos inusuales o en jurisdicciones diferentes a las de la operación, facturación que no corresponde con los servicios efectivamente prestados, solicitud de cambios en las condiciones de pago sin justificación clara, reticencia a someterse a auditorías acordadas, cambios frecuentes en la propiedad o dirección, y denuncias o quejas sobre el tercero.

Ante cualquier señal de alerta, la respuesta adecuada es no ignorarla ni minimizarla, documentar la situación, comunicarla a compliance para su evaluación, no proceder con la operación hasta que se aclare la situación, y considerar la terminación de la relación si no se resuelve satisfactoriamente.

11. CONCLUSIONES

El control de terceros, proveedores y cadena de suministro es un elemento esencial de cualquier sistema de compliance porque la empresa responde por riesgos que no controla directamente, pero que pueden materializarse en su nombre o beneficio. Por ello, conocer a los socios de negocio y poner límites claros no es accesorio: es una condición de sostenibilidad jurídica y operativa.

La cadena de valor no es lineal; funciona como una red ramificada en la que los impactos pueden surgir lejos del primer eslabón visible. Esa realidad exige una diligencia debida estructurada, que abarque selección y evaluación antes de contratar, formalización con cláusulas y salvaguardas proporcionadas al riesgo y, después, seguimiento y reevaluación periódicos. La proporcionalidad guía el esfuerzo: concentramos recursos donde el riesgo es más alto (agentes e intermediarios con contacto público, sectores/países críticos).

En paralelo, el marco regulatorio europeo eleva las expectativas sobre derechos humanos y medio ambiente en la cadena de valor, lo que convierte la transparencia y la trazabilidad en un estándar de mercado. Prepararse implica alinear procesos, evidencias y cultura con esos requisitos y con las expectativas de clientes, inversores y sociedad.

Nada de lo anterior funciona sin un liderazgo visible: la alta dirección debe asignar recursos, reforzar la gobernanza (roles, independencia y escalado) y medir la ejecución. Este sistema debe operar con un ciclo de Planificar-Hacer-Verificar-Actuar (PHVA), revisando riesgos, controles e indicadores para aprender y mejorar de forma continua. Solo así la compañía convierte el control de terceros en una ventaja de cumplimiento y de negocio.

Si quieres adquirir esta obra haz click aquí

Capítulo 1.18

Certificaciones de compliance ISO-UNE

JUAN PABLO TORNOS

SUMARIO: 1. INTRODUCCIÓN. 2. CONCEPTO DE CERTIFICACIÓN DE COMPLIANCE. 3. OBJETIVO Y UTILIDAD DE LAS CERTIFICACIONES. 4. ALCANCE Y DURACIÓN DE LAS CERTIFICACIONES. 5. PRINCIPALES NORMAS DE COMPLIANCE ISO-UNE CERTIFICABLES. *5.1. ISO 37001 – Sistema de gestión antisoborno. 5.2. UNE 19601 – Sistema de gestión de compliance penal. 5.3. ISO 37001 – Sistema de gestión de compliance.* 6. ESTRUCTURA DE UNA CERTIFICACIÓN ISO-UNE. *6.1. Contexto de la organización.* 6.1.1. Alcance, contexto y partes interesadas. 6.1.2. Obligaciones de compliance. 6.1.3. Evaluación de riesgos. *6.2. Liderazgo. 6.3. Planificación. 6.4. Apoyo. 6.5. Operación. 6.6. Evaluación del desempeño. 6.7. Mejora.* 7. SINERGIAS E INTEGRACIÓN ENTRE NORMAS. 8. INTERPRETACIONES, SESGOS Y ZONAS GRISES DE LAS NORMAS CERTIFICABLES. 9. PREPARACIÓN PARA LA OBTENCIÓN DE UNA CERTIFICACIÓN ISO-UNE. *9.1. Planificación y revisión inicial. 9.2. Auditoría previa de la organización. 9.3. Evaluación previa de la entidad certificadora. 9.4. Auditoría de la entidad certificadora.*

1. INTRODUCCIÓN

Uno de los objetivos de los modelos de compliance es evitar la materialización de riegos y ayudar al cumplimiento de las distintas obligaciones legales. No obstante, estas cuestiones deben poder evidenciarse de alguna forma, es decir, se puede disponer de un buen modelo de compliance, no obstante, de poco sirve si no se puede demostrar esa eficacia, por ejemplo, frente a terceros.

Asimismo, muchas legislaciones garantizan la exoneración o atenuación de la responsabilidad legal si la organización acredita la existencia, previa a la comisión de esa infracción, de un modelo de compliance idóneo y eficaz para prevenir la materialización de riesgos.

A lo largo de estos años se han ido desarrollando distintos marcos de referencia, como las normas ISO-UNE, que establecen cuales son los requisitos mínimos que debería cumplir un modelo de compliance (denominado «sistema de gestión de compliance» en estas normas) para ser idóneo y eficaz.

Si quieres adquirir esta obra haz click aquí

A su vez, estas normas ISO-UNE pueden ser certificadas por auditores externos, con objeto de verificar que un modelo de compliance cumple con las disposiciones contenidas en estas y, en consecuencia, dejar evidencia de que ese modelo de compliance es eficaz mediante esta certificación.

Sin perjuicio de que en la actualidad existen muchas normas y certificaciones, en el presente apartado nos centraremos en las ISO-UNE al ser de las más comunes en el ámbito del compliance penal.

2. CONCEPTO DE CERTIFICACIÓN DE COMPLIANCE

Previamente a entrar a analizar las distintas certificaciones de compliance, resulta necesario explicar en que consisten.

Una certificación de compliance es un reconocimiento formal que acredita que una organización cumple con una normativa determinada.

En el caso de los modelos de compliance, implica verificar la implantación de un sistema de cumplimiento normativo que previene, detecta y gestiona riesgos legales. Estas certificaciones suelen basarse en estándares internacionales, como la ISO 37301 (sistemas de compliance) o la ISO 37001 (antisoborno).

Es decir, una cuestión es la norma (como las ISO previamente mencionadas) y otra la certificación, otorgada por un tercero externo tras verificar que la organización cumple con esa norma.

3. OBJETIVO Y UTILIDAD DE LAS CERTIFICACIONES

El objetivo principal de las certificaciones es **verificar que la organización actúa conforme a unas buenas prácticas contenidas en la norma sobre la que se certifique**. En otras palabras, que dispone de un modelo de compliance que cumple con los requisitos de la norma certificada.

El asumir las buenas prácticas contenidas en una norma tiene por objeto reducir riesgos de incumplimiento y, en consecuencia, mejorar la reputación y generar confianza a terceros, como clientes, proveedores y socios de negocio, así como entre los propios empleados, directivos y órganos de gobierno. Gracias a estas certificaciones se puede evidenciar este cumplimiento.

No obstante, la obtención de una certificación, o la aplicación de unas buenas prácticas contenidas en una norma como las ISO-UNE, no asegura completamente que no se hayan producido en la organización incumplimientos, ni que no vayan a producirse en el futuro, es decir, **no brinda una garantía absoluta de eliminación del riesgo** de comisión de incumplimientos que afronta una organización.

Asimismo, la certificación **no asegura la exoneración o atenuación** automática de la responsabilidad de la persona jurídica. Entre otros, la Circular 1/2016 de Fiscalía General del Estado acogía este criterio:

> *Las certificaciones sobre la idoneidad del modelo expedidas por empresas, corporaciones o asociaciones evaluadoras y certificadoras de cumplimiento de obligaciones, mediante las*

Si quieres adquirir esta obra haz click aquí

que se manifiesta que un modelo cumple las condiciones y requisitos legales, podrán apreciarse como un elemento adicional más de su observancia, pero en modo alguno acreditan la eficacia del programa, ni sustituyen la valoración que de manera exclusiva compete al órgano judicial.

El hecho de certificar un modelo de compliance o, al menos, de seguir las disposiciones de una norma de referencia:

a) **Ayuda en el cumplimiento de las exigencias legales**, al cumplir con una serie de buenas prácticas contenidas en la norma certificada.

b) **Fomenta las expectativas de terceros depositadas en las organizaciones**, es decir, como decíamos mejora la reputación y genera confianza en que la organización cumple con la normativa vigente.

c) **Contribuye en la prevención, detección y gestión de riesgos e incumplimientos**, mitigando la probabilidad de que se materialicen infracciones gracias a la implantación de una serie de medidas contenidas en una norma.

d) **Fomenta una cultura de compliance**, asegurando que la empresa cumpla y aplique una serie de principios y buenas prácticas.

4. ALCANCE Y DURACIÓN DE LAS CERTIFICACIONES

Es importante destacar el alcance de la certificación, es decir, la auditoría de la certificación debe definirse previamente: puede extenderse a toda la organización o varias organizaciones, a un área o actividad concreta, etc.



En el propio documento de la certificación se indica el alcance. Es habitual encontrar organizaciones, por ejemplo, que indican que disponen de la certificación en toda la organización, no obstante, al revisar el documento se indica que se auditó únicamente un departamento o un proceso.

Este aspecto es importante, ya que el modelo de compliance a certificar debe alcanzar los ámbitos que se quieren auditar, por ejemplo, si se va a certificar el modelo de compliance para todo el grupo empresarial, en todas las empresas del grupo deberá estar implementado el modelo de compliance.

En consecuencia, previo a certificar el modelo de compliance, se debería tener en cuenta su alcance en los siguientes ámbitos:

Si quieres adquirir esta obra haz click aquí

a) **Tamaño y estructura de la organización**: el modelo de compliance alcanza a toda la organización, solo a la sociedad matriz o solo a algunas entidades.

b) **Ubicaciones geográficas**: el modelo de compliance alcanza a las entidades de todos los territorios o tan solo a entidades locales.

c) **Sector de actividad donde se opera**: el modelo de compliance alcanza todos los sectores donde opera la organización o solo a una parte.

d) **Actividades de la organización**: el modelo de compliance alcanza a todas las actividades de la organización o tan solo aplica a una parte.

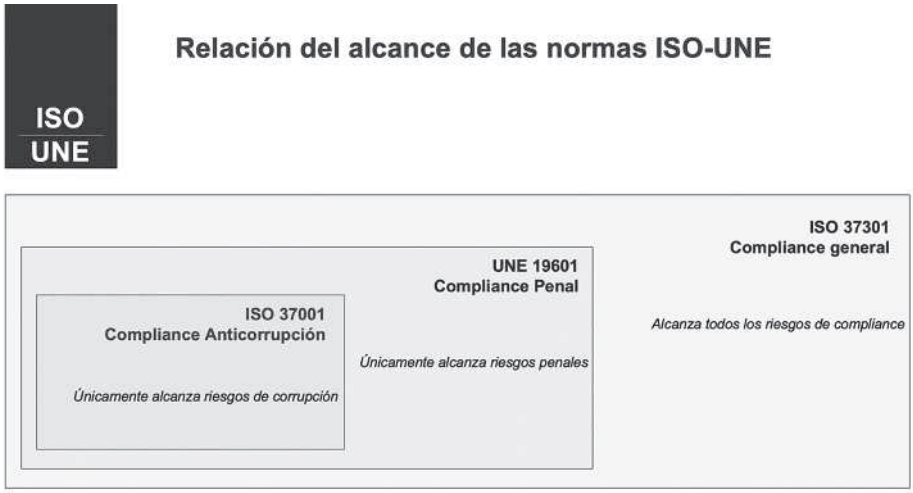
Finalmente, se destaca que las certificaciones disponen de una d**uración temporal**, normalmente de tres años, por lo que se deben ir renovando periódicamente cada tres años, sin perjuicio de que anualmente se realice una revisión de la misma por parte de lo auditores externos para verificar, entre otros, que se han ido solventando las no conformidades detectadas y se continua cumpliendo con los requisitos establecidos.

5. PRINCIPALES NORMAS DE COMPLIANCE ISO-UNE CERTIFICABLES

En el presente apartado describiremos tres de las principales normas certificables de compliance. Concretamente, nos centraremos en la norma ISO 37001, ISO 37301 e UNE 19601.

Cabe mencionar una cuestión importante sobre los estándares internacionales ISO-UNE: aquellas normas que terminan con el número «0» no son certificables, mientras que las que finalizan en el número «1» pueden certificarse.

El siguiente recuadro expone las diferencias de forma resumida entre estas tres certificaciones:



Si quieres adquirir esta obra haz click aquí

5.1. ISO 37001 – SISTEMA DE GESTIÓN ANTISOBORNO

La ISO 37001 es una norma internacional publicada en 2021, que fue actualizada en 2025, que establece los requisitos para implementar, mantener y mejorar un sistema de gestión de compliance antisoborno en una organización.

Su objetivo es ayudar a prevenir, detectar y responder al soborno, tanto en el sector público como privado. Aplica a empresas de cualquier tamaño y sector, e incluye medidas como como evaluación de riesgos de corrupción, diligencia debida a terceros y controles financieros y no financieros.

5.2. UNE 19601 – SISTEMA DE GESTIÓN DE COMPLIANCE PENAL

La UNE 19601 es una norma española que establece los requisitos para implantar, desarrollar y mejorar un Sistema de Gestión de Compliance Penal en las organizaciones, la cual parte de la ISO 19600, no obstante, a diferencia de esta última se puede certificar.

Su objetivo principal es ayudar a prevenir la comisión de delitos dentro de la organización, así como detectar y gestionar posibles incumplimientos, en línea con el Código Penal español.

5.3. ISO 37001 – SISTEMA DE GESTIÓN DE COMPLIANCE

La ISO 37301 es una norma internacional publicada en 2021 y que establece los requisitos para implantar, mantener y mejorar un Sistema de Gestión de Compliance en una organización.

Su objetivo es ayudar a prevenir y gestionar riesgos legales y regulatorios, asegurando que cumplen con leyes, normas internas y compromisos éticos. Es aplicable a cualquier tipo de organización, independientemente de su tamaño o sector.

6. ESTRUCTURA DE UNA CERTIFICACIÓN ISO-UNE

Las certificaciones ISO-UNE se dividen en varios apartados, normalmente coincidentes entre ellas. En el caso de las tres analizadas, disponen en general de una misma estructura que describiremos brevemente en el presente apartado:

a) Contexto de la organización.

b) Liderazgo.

c) Planificación.

d) Apoyo.

e) Operación.

f) Evaluación del desempeño.

g) Mejora.

Asimismo, en cada uno de los apartados analizaremos las principales cuestiones que tener en cuenta para adaptar el modelo de compliance a la norma.

Si quieres adquirir esta obra haz click aquí

6.1. CONTEXTO DE LA ORGANIZACIÓN

6.1.1. Alcance, contexto y partes interesadas

Las normas ISO-UNE acostumbran a solicitar que se documente una serie de información relativa a la organización y de su modelo de compliance, información que, salvo el alcance, normalmente las organizaciones no tienen documentada, por lo que se trata de un punto que toca desarrollarlo de cara a obtener la certificación.

Primero de todo se debe **describir la organización**, su actividad y el sector en el que opera, para facilitar el poder identificar los riesgos que le pueden afectar, bien sea a través de factores externos destacando, entre otros, el mercado, la normativa, etc., o bien a través de factores internos destacando, entre otros, la estructura de la organización, su actividad, objetivos de negocio, etc. Normalmente la propia norma indica algunos factores a describir, como el tamaño o estructura de la organización o bien el modelo de negocio.

También se solicita identificar y describir cuales son las **necesidades y expectativas de las partes interesadas** (stakeholders) de la organización, tanto internas (empleados, directivos, órgano de gobierno, etc.) como externas (clientes, proveedores, administraciones públicas, etc.). Esta identificación se debe hacer en ambos sentidos, es decir, que espera la organización de la parte interesada y viceversa, que espera la parte interesada de la organización.

Finalmente, también se solicita como cuál es el **alcance del modelo de compliance**. El alcance se puede dividir en varios ámbitos, por ejemplo, se tendría que especificar:

- **Alcance societario**: a que sociedades del grupo alcanza el modelo de compliance.
- **Alcance material**: a que actividades de la organización alcanza el modelo de compliance.
- **Alcance personal:** a que personas, departamentos o áreas alcanza el modelo de compliance.
- **Alcance relacional:** a que terceros, como proveedores o clientes, alcanza el modelo de compliance.
- **Alcance geográfico**: a que sociedades de un territorio alcanza el modelo de compliance, es decir, solo entidades nacionales, internacionales, de determinados territorios, etc.

Toda esta información descrita, pese a pertenecer a tres subgrupos diferentes, se puede agrupar en un mismo documento, dado que se encuentra relacionada entre ella. No obstante, si se prefiere también puede documentarse en diferentes documentos, dependiendo de las necesidades de la organización.

6.1.2. Obligaciones de compliance

Se trata de una obligación contenida en la ISO 37301 consistente en identificar las obligaciones de compliance de la organización para garantizar su cumplimiento, es decir, no solo las de carácter legal, sino también las asumidas voluntariamente, por ejemplo, mediante contratos o convenios.

Si quieres adquirir esta obra haz click aquí

Asimismo, se debe evaluar el impacto de estas obligaciones tendrán en la organización, es decir, no se refiere a la sanción que pudiera conllevar no cumplir con la obligación, sino qué impacto tendrá cumplir con esta obligación en la organización, por ejemplo, recursos necesarios para implementar la obligación, tiempo de implementación, procesos que deberán actualizarse, etc.

6.1.3. Evaluación de riesgos

Será necesario analizar los riesgos que correspondan a cada norma (de soborno, penales o de compliance) que afectan a la organización. La siguiente tabla muestra un resumen del proceso de evaluación de riesgos basado en la ISO 31000 de gestión de riesgos.

Proceso de evaluación de riesgos	
Identificación de riesgos	Identificar los distintos riesgos de aplicación en la organización.
Análisis de riesgos *(riesgo inherente)*	Determinación de la probabilidad de producirse el riesgo y el impacto que ello supondría en la organización en caso de materializarse un riesgo.
Identificación y evaluación de controles y evidencias *(riesgo residual)*	Definición del tratamiento de los riesgos mediante la implementación de controles para evitar o reducir su materialización.
Elaboración del plan de acción *(tratamiento del riesgo)*	Elaboración de un plan de acción con objeto de aplicar las recomendaciones que surjan del presente informe, cuya finalidad es evitar o reducir la materialización del riesgo.
Seguimiento y revisión	Mantener un seguimiento de lo dispuesto en el presente informe y el plan de acción, con objeto de asegurar su cumplimiento y, en su caso, realizar los ajustes oportunos (controles no eficaces, cambios de contexto, nuevos riesgos, etc.).

Es importante definir una metodología de análisis que cumpla con los estándares previstos en la norma de referencia. Por ejemplo, fijar la escala a aplicar (se recomienda que sea mínimo de 3) incluir probabilidad e impacto en la evaluación del riesgo, etc.

6.2. LIDERAZGO

En este punto se describen cuáles son las distintas funciones que deben, como mínimo ostentar cada órgano de la organización respecto al modelo de compliance, normalmente dividido entre órgano de gobierno, alta dirección, función de compliance, y personal.

Asimismo, en este punto se describe el contenido mínimo que debe ostentar la política de compliance del modelo de compliance.

Si quieres adquirir esta obra haz click aquí

6.3. PLANIFICACIÓN

En este punto se destacan los **objetivos de compliance**, entendidos como aque llos objetivos que se fija la organización para mejorar el modelo. Vamos a desarrollar esta cuestión ya que en la práctica genera confusión.

Normalmente los objetivos de compliance parten de cuestiones que se detectan y que buscan mejorar el modelo de compliance pese a no ser una obligación en sí mismos. Este punto es importante, no hay que confundir obligación y objetivo: si existe una obligación no puede ser un objetivo.

Para facilitar su diferenciación, es mejor utilizar el concepto «mejora» que objetivo, por ejemplo, existe la obligación de disponer de un canal de denuncias conforme la Ley de protección del informante o bien por la propia ISO-UNE al asumirse el compromiso de cumplir con ella (como hemos comentado antes, por obligación entendemos tanto los imperativos legales como aquellas asumidas voluntariamente), no obstante, si se ha detectado que se reciben pocas denuncias, pudiéramos asumir como objetivo de compliance («mejora») acrecentar la cultura de cumplimiento aumentando el número de denuncias recibidas.

Una vez identificado el objetivo, hay que establecer los baremos para su medición, que deben ser lo más objetivos y medibles, por ejemplo, denuncias del anterior ejercicio respecto al actual.

Finalmente, es necesario desarrollar un plan de acción para asumir el objetivo, con una o varias acciones: aumentar las acciones de sensibilización respecto al canal de denuncias (por ejemplo, enviando una píldora trimestral recordando su existencia), facilitar el acceso al canal de denuncias (por ejemplo, haciéndolo más visible en la página web o intranet interna), etc.

A continuación, mostramos un resumen del ejemplo anterior:

- Obligación: disponer de un canal de denuncias
    - Objetivo de compliance (mejora): acrecentar la cultura de cumplimiento aumentando el número de denuncias recibidas.
        * Plan de acción:
            - Aumentar las acciones de sensibilización respecto al canal de denuncias.
            - Facilitar el acceso al canal de denuncias.
        * Baremo de medición: denuncias recibidas en el anterior ejercicio vs denuncias recibidas al final del actual ejercicio.

Por otro lado, en este apartado de la norma se establece la **planificación** para actualizar o mejorar el modelo de compliance, por ejemplo, en caso de detectar no conformidades. En otras palabras, que en caso de realizar acciones de revisión o actualización del modelo es necesario planificarlas mediante un plan de acción que debe reunir unos requisitos mínimos establecidos en la norma.

Si quieres adquirir esta obra haz click aquí

6.4. APOYO

Este apartado se centra en la asignación de recursos al modelo de compliance, las acciones relacionadas con la formación, concienciación y comunicación, así como la información documentada.

Una cuestión que establece las normas ISO-UNE es la necesidad de documentar cierta información, es decir, exige que determinadas cuestiones queden documentadas (por ejemplo, la evaluación de riesgos o la política de compliance), no obstante, otras no lo exige, aunque en determinados casos es recomendable para evidenciar su existencia, habrá que valorarlo caso a caso.

Se debe tener en cuenta lo siguiente:

- **Se puede documentar más allá de lo estipulado en la norma**: a pesar de que la norma solo establece ciertas cuestiones a documentar, ello no impide que se puedan documentar muchas más cuestiones, por ejemplo, para tener evidencia de su existencia, idoneidad y eficacia.
- **Se puede documentar distinta información en un mismo documento**: a la hora de documentar la información, especialmente aquella que pueda estar relacionada entre sí, la norma no impide que se recoja en un mismo documento (tal como mencionábamos en el apartado de 6.1 por ejemplo) facilitando con ello su gestión.

6.5. OPERACIÓN

Este apartado de la norma se centra en las cuestiones de diligencia debida, controles para evitar la materialización de riesgos, así como los canales de denuncias y procesos de investigación interna. Cabe decir, sobre este último punto, que tras la entrada en vigor de la Ley de protección del informante es posible que existan obligaciones legales que antes solo se contemplaban en estos apartados, incluso que la ley haya establecido obligaciones que vayan más allá que lo establecido en la norma de referencia.

6.6. EVALUACIÓN DEL DESEMPEÑO

En este apartado se centra el seguimiento del estado del modelo de compliance, auditorías periódicas del modelo, así como las obligaciones de informar sobre el modelo de compliance, por ejemplo, a la alta dirección y órganos de gobierno.

6.7. MEJORA

Este apartado final se centra en la actualización y mejora del modelo, así como la gestión de las no conformidades detectadas y acciones correctivas al respecto.

7. SINERGIAS E INTEGRACIÓN ENTRE NORMAS

Sin perjuicio de que cada norma dispone de su ámbito, al seguir una estructura similar como hemos visto en el apartado anterior: mismos capítulos (contexto, lide-

Si quieres adquirir esta obra haz click aquí

razgo, planificación, etc.), lenguaje afín y enfoque basado en riesgos, ello permite que se pueden integrar entre ellas, es decir, compartir los mismos documentos e incluso realizar auditorías integradas de forma que no deba duplicarse el trabajo cada vez.

En consecuencia, una vez integrada una norma ISO-UNE en el modelo de compliance, es más fácil integrar otras normas, especialmente si son de la misma rama como las tres analizadas previamente.

8. INTERPRETACIONES, SESGOS Y ZONAS GRISES DE LAS NORMAS CERTIFICABLES

Aunque las normas certificables buscan ser objetivas y estandarizadas, su redacción suele ser bastante general, permitiendo interpretaciones o enfoques diferentes. Esto puede generar discrepancias entre la interpretación de la organización y el auditor externo.

Entre otros, **las organizaciones tienden a interpretar la norma de forma más flexible**, adaptándola a su contexto y buscando ser más eficientes, es decir, aplicar el principio lo «mínimo necesario» para cumplir.

Por otro lado, **el auditor puede priorizar su criterio personal**, por ejemplo, según prácticas vistas en otras organizaciones, asumiéndolas como obligaciones, aunque no sean obligatorias según la norma, **o bien aplicar un criterio de «rigor excesivo»** que puede provocar exigencias más allá de lo que la norma requiere, en resumen, en ambos casos confundir buenas prácticas con requisitos obligatorios.

Estas diferencias pueden generar tensiones, no conformidades discutibles y la necesidad de justificar de forma excesiva cada interpretación de la norma.

9. PREPARACIÓN PARA LA OBTENCIÓN DE UNA CERTIFICACIÓN ISO-UNE

De cara a obtener la certificación podemos dividir el proceso en dos grandes fases:

- **Preparación de la auditoría**: fase preparatoria de la certificación, en la que se debe verificar y, en su caso, actualizar el modelo de compliance a los requisitos exigidos en la certificación. A su vez, esta fase la podemos dividir en dos subfases que describiremos en los siguientes subapartados: a) Planificación y revisión inicial y b) Auditoría previa de la organización3
- **Auditoría con entidad de certificación**: fase en que la entidad oficial acude para analizar el modelo de compliance y verificar si cumple con los requisitos de la certificación. A su vez, esta fase se puede dividir en dos subfases que describiremos más adelante: a) Evaluación previa de la entidad certificadora y b) Auditoria de la entidad certificadora.

En los siguientes subapartados desarrollamos cada uno de estos puntos.

Si quieres adquirir esta obra haz click aquí

9.1. PLANIFICACIÓN Y REVISIÓN INICIAL

Esta primera fase, como hemos indicado previamente, se trata de verificar el cumplimiento de los requisitos establecidos en el marco de referencia seleccionado, es decir, verificar si el modelo de compliance cumple con las cuestiones previstas en la norma.

Se trata de hacer una checklist previa de los distintos requisitos de la norma y si estos ya se encuentran incluidos y/o desarrollados en nuestro modelo de compliance.

Normalmente los puntos que las organizaciones deben abordar con más profundidad en esta primera fase son los relacionados principalmente con el punto 6.1 y los objetivos de compliance descritos en el apartado 6.3 ya que normalmente no se dispone de estos. Asimismo, es recomendable revisar la información documentada que exige disponer la norma, ya que en ocasiones las organizaciones ya realizan determinadas cuestiones contenidas en la norma, no obstante, están pendientes de documentar.

Una vez identificadas estas cuestiones que pudieran faltar, se recomienda realizar un plan de acción para solventarlas y pasar a continuación a la siguiente fase.

9.2. AUDITORÍA PREVIA DE LA ORGANIZACIÓN

Posteriormente, la propia certificación indica que se debe realizar una auditoría del modelo para verificar que cumple con los requisitos de la norma.

Esta «preauditoría» a la de la certificación puede ser realizada por un departamento independiente de la entidad, como puede ser Auditoría Interna, siempre y cuando no fuera la certificación sobre esta función, o bien se debe contratar a un experto externo.

Normalmente en esta segunda fase se muestran algunas «no conformidades» (explicaremos este concepto en el apartado 8.4) que deben ser solventadas previo a la auditoría de la certificación. En consecuencia, se debe elaborar un plan de acción para solventar estas no conformidades que se hubieran detectado.

La ventaja de haber realizado la fase anterior es que en esta fase ya tenemos gran parte del trabajo realizado y evitamos tener que alargar esta auditoría o retrasar más el proceso de certificación.

9.3. EVALUACIÓN PREVIA DE LA ENTIDAD CERTIFICADORA

Una vez finalizada la auditoría previa, la entidad certificadora realiza un análisis preliminar del modelo de compliance para verificar si este puede superar la auditoría de la certificación.

Si se han solventado las no conformidades detectadas en las fases anteriores en principio se avanza a la certificación. En caso negativo, normalmente se acuerda aplazar la certificación hasta solventar las no conformidades que se hubieran detectado.

En esta misma fase, pese a realizar un análisis superficial, la propia certificadora puede facilitar algunas conclusiones preliminares de cuestiones que haya podido detectar. En este caso se pueden abordar previamente a la auditoría para evitar nuevas no conformidades en el informe de la certificadora.

Si quieres adquirir esta obra haz click aquí

9.4. AUDITORÍA DE LA ENTIDAD CERTIFICADORA

Finalmente, superadas las fases anteriores, la entidad certificadora realiza la auditoría para verificar si el modelo de compliance cumple con los requisitos de la norma objeto de certificación.

Estas auditorías pueden durar algunos días, incluso semanas, dependiendo de la norma a certificar y el alcance que se quiera auditar. Es recomendable informar a los distintos departamentos y áreas de la organización que fueran a participar en la auditoría de que estén disponibles y que faciliten la información que requiera el auditor. También es recomendable preparar, por ejemplo, en una misma carpeta de forma ordenada, los distintos documentos del modelo de compliance para facilitar su revisión por parte del auditor externo.

Una vez realizada la auditoría, la entidad certificadora emite un informe en el que explica el desarrollo de la auditoría y los distintos hallazgos encontrados, los cuales se dividen en los siguientes:

- **No conformidad mayor**: incumplimiento grave de un requisito de la norma, el cual puede consistir en una ausencia total de un requisito, fallo sistemático del modelo o que falta alguna cuestión clave. Suele requerir acciones correctivas urgentes, normalmente debe corregirse en un plazo corto y que, en caso de no hacerlo, pueden impedir obtener la certificación.
- **No conformidad menor**: desviación puntual o de bajo impacto de la norma, que no compromete el modelo de compliance, pero que debe corregirse antes de la siguiente auditoría. Indica que el sistema funciona, aunque con cuestiones a subsanar.
- **Observación**: comentarios del auditor sobre una situación que, aunque se cumple la norma, podría convertirse en no conformidad en el futuro o que presenta margen de mejora. No obliga a acción correctiva formal, aunque debe abordarse en el plan de acción, aunque sea para descartar su implementación y justificar por qué se ha descartado.
- **Oportunidad de mejora**: recomendación para optimizar el sistema, aumentar su eficacia o eficiencia. Se trata de sugerencias basadas en buenas prácticas.

Las cuestiones anteriores deben abordarse mediante un plan de acción para subsanarlas que debe ser presentado a la entidad certificadora. Una vez presentado, si la entidad certificadora esta conforme emite la certificación, la cual deberá ser renovada periódicamente como indicamos anteriormente.

Si quieres adquirir esta obra haz click aquí

Capítulo 1.19

Diseño e implementación de un sistema de Trade Compliance: una guía práctica para Compliance Officers

ANA CANET ARANDA

SUMARIO: 1. INTRODUCCIÓN. *1.1. Consideraciones iniciales y tesis interpretativas sobre el Trade Compliance. 1.2. El Trade Compliance en un entorno de enforcement creciente.* 2. CONCEPTO Y ALCANCE DEL TRADE COMPLIANCE. 3. EL TRADE COMPLIANCE COMO SUB-PROGRAMA DEL COMPLIANCE MANAGEMENT SYSTEM. 4. AUTORIDADES COMPETENTES Y MARCO INSTITUCIONAL DEL TRADE COMPLIANCE. *4.1. Autoridades Aduaneras. 4.2. Autoridades de control a la exportación. 4.3. Autoridades responsables de sanciones y embargos internacionales. 4.4. Autoridades con competencias indirectas.* 5. ESTÁNDARES INTERNACIONALES, GUÍAS Y SOFT LAW DE REFERENCIA. 6. PRINCIPALES ÁMBITOS DE RIESGO EN TRADE COMPLIANCE. 7. LA PRIMERA Y LA SEGUNDA LÍNEA DE DEFENSA EN TRADE COMPLIANCE. 8. SINERGIAS CON OTROS PROGRAMAS DE COMPLIANCE. 9. DISEÑO DE UN MODELO PROPORCIONAL DE TRADE COMPLIANCE. *9.1. Particularidades del Trade Compliance en PYMES.* 10. SUPERVISIÓN, INDICADORES Y MEJORA CONTINUA EN TRADE COMPLIANCE. 11. ENFORCEMENT Y RÉGIMEN SANCIONADOR EN TRADE COMPLIANCE. 12. EL VALOR DEL COMPLIANCE EN LA PREVENCIÓN Y MITIGACIÓN DE SANCIONES EN TRADE COMPLIANCE. 13. TECNOLOGÍA, AUTOMATIZACIÓN Y USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL EN TRADE COMPLIANCE. 14. IMPLEMENTACIÓN DESDE CERO DE UN PROGRAMA DE TRADE COMPLIANCE. *14.1. Alcance y encaje organizativo. 14.2. Evaluación de riesgos. 14.3. Elaboración de estándares internos. 14.4. Implementación de controles. 14.5. Formación y comunicación. 14.6. Supervisión, mejora continua y reporting.* 15. CONCLUSIONES. ANEXO I. CHECKLIST DE ARRANQUE Y ROADMAP DE 90 DÍAS PARA LA IMPLANTACIÓN DE UN PROGRAMA DE TRADE COMPLIANCE. ANEXO II. ERRORES FRECUENTES EN LA IMPLANTACIÓN DEL TRADE COMPLIANCE. ANEXO III. INDICADORES BÁSICOS RECOMENDADOS (KPIS Y KRIS) EN TRADE COMPLIANCE.

Si quieres adquirir esta obra haz click aquí

1. INTRODUCCIÓN

1.1. CONSIDERACIONES INICIALES Y TESIS INTERPRETATIVAS SOBRE EL TRADE COMPLIANCE

Este capítulo tiene por finalidad ofrecer un marco interpretativo inicial para el análisis del Trade Compliance, formulado desde una perspectiva prudente, práctica y estratégica. Las consideraciones que se exponen no pretenden establecer postulados cerrados, sino aportar criterios de lectura que faciliten al Compliance Officer la contextualización del diseño, la implantación y la supervisión de este subprograma dentro del Compliance Management System (CMS).

Desde una primera aproximación, puede sostenerse que uno de los principales riesgos en materia de Trade Compliance no se limita al incumplimiento normativo en sentido estricto, sino a la existencia de una percepción interna de control que no siempre refleja la realidad operativa. La presencia formal de políticas, procedimientos o herramientas puede generar una sensación de cumplimiento que, en ausencia de una supervisión efectiva y de una asignación clara de responsabilidades, oculte debilidades estructurales del sistema.

En este contexto, el valor del Trade Compliance no residiría tanto en la acumulación de controles como en la capacidad de la organización para comprender con precisión quién interviene en las operaciones de comercio internacional, bajo qué criterios y con qué responsabilidades. Esta aproximación conecta directamente con el modelo de líneas de defensa y con la necesidad de evitar solapamientos o vacíos que comprometan la eficacia del programa.

Asimismo, cabe considerar que la proporcionalidad constituye un elemento crítico del diseño del Trade Compliance. Un nivel de robustez desalineado con el perfil de riesgo real de la organización puede generar ineficiencias, favorecer incumplimientos sistemáticos y dificultar la identificación de desviaciones relevantes.

Finalmente, estas reflexiones sugieren la conveniencia de analizar el Trade Compliance no solo desde una perspectiva preventiva, sino también desde la capacidad de la organización para explicar y defender su sistema en caso de incidente.

1.2. EL TRADE COMPLIANCE EN UN ENTORNO DE ENFORCEMENT CRECIENTE

El comercio internacional se desarrolla en un contexto de creciente complejidad normativa y refuerzo sostenido del *enforcement* por parte de autoridades nacionales y supranacionales. La globalización de las cadenas de suministro, la fragmentación de los procesos productivos y la interdependencia entre jurisdicciones han incrementado de forma significativa la exposición de las organizaciones a riesgos de incumplimiento en materia de comercio exterior.

En este escenario, el Trade Compliance ha dejado de concebirse como una función meramente operativa o técnica para consolidarse como un ámbito de riesgo relevante desde la perspectiva del Compliance corporativo. Las consecuencias del incumplimiento trascienden hoy el plano administrativo u operativo y pueden derivar en sanciones

Si quieres adquirir esta obra haz click aquí

económicas relevantes, restricciones de actividad, responsabilidades penales y daños reputacionales de alto impacto.

El refuerzo del *enforcement* en ámbitos como las sanciones internacionales, los controles a la exportación, el fraude aduanero o la supervisión de la cadena de suministro ha elevado de forma sustancial las expectativas de diligencia exigibles a las empresas que operan en mercados internacionales, incluidas aquellas sometidas a regímenes sancionadores con alcance extraterritorial.

Desde esta realidad, el Trade Compliance debe abordarse de forma sistemática e integrada en el CMS, configurándose como un subprograma específico y no como un conjunto aislado de controles técnicos. Ello exige una adecuada delimitación de funciones entre la primera y la segunda línea de defensa, así como la articulación de sinergias con otros programas de Compliance existentes.

En este marco, el Compliance Officer actúa como segunda línea de defensa, con un rol centrado en la identificación y evaluación de riesgos, el diseño del marco normativo interno, la supervisión de la eficacia de los controles y el *reporting* al órgano de administración, sin sustituir a las funciones operativas responsables de la ejecución diaria de las operaciones de comercio exterior.

El propósito de este artículo es ofrecer una aproximación doctrinal y práctica al Trade Compliance que permita comprender su encaje como riesgo estratégico de Compliance y como herramienta de gestión preventiva y defensiva frente al riesgo sancionador. El enfoque adoptado no pretende sustituir a los manuales técnicos del comercio internacional, sino proporcionar un marco conceptual que facilite su integración coherente en un sistema de cumplimiento corporativo orientado a la sostenibilidad, la reputación y la viabilidad a largo plazo de la organización.

2. CONCEPTO Y ALCANCE DEL TRADE COMPLIANCE

El Trade Compliance puede definirse como el conjunto estructurado de principios, políticas, procedimientos y controles destinados a asegurar que las operaciones de comercio internacional de una organización se desarrollan de conformidad con la normativa aplicable en materia aduanera, controles a la exportación, sanciones y embargos internacionales, así como con otros requisitos regulatorios vinculados al movimiento transfronterizo de bienes, servicios, tecnología y conocimiento.

Desde la perspectiva del Compliance corporativo, el Trade Compliance trasciende una concepción meramente técnica u operativa y se configura como un ámbito preventivo y sistémico, orientado a la identificación, evaluación y mitigación de riesgos legales, administrativos, penales y reputacionales asociados a la actividad internacional.

Su alcance es transversal. Normativamente, implica la aplicación concurrente de normas de distinto origen cuya interacción sobre una misma operación constituye una fuente relevante de complejidad y riesgo. Organizativamente, se materializa en procesos ejecutados por funciones de primera línea como logística, compras, ventas internacionales o *legal export*, y en el diseño y supervisión, desde la función de Compliance, de un marco de control alineado con las expectativas razonables de las autoridades.

Si quieres adquirir esta obra haz click aquí

En este contexto, resulta esencial distinguir el Trade Compliance de la función de Legal Export. Mientras esta se centra en el análisis jurídico-técnico de operaciones concretas, el Trade Compliance adopta una visión integradora y basada en riesgos, alineada con el CMS y orientada a la prevención estructural de incumplimientos.

La eficacia del modelo exige una delimitación clara de responsabilidades: las áreas operativas y técnicas actúan como primera línea de defensa, ejecutando los procesos de comercio exterior, mientras que la función de Compliance, como ya hemos explicado actúa como segunda línea, define el marco normativo interno, supervisa la eficacia de los controles y articula los mecanismos de escalado y *reporting* sin asumir funciones ejecutivas.

Desde la perspectiva sancionadora, el Trade Compliance adquiere una relevancia particular, al poder los incumplimientos dar lugar a sanciones económicas significativas, restricciones operativas, pérdida de autorizaciones o, en determinados ordenamientos, responsabilidades penales. En este marco, las autoridades valoran de forma expresa la existencia y efectividad de programas de Compliance adecuados al graduar sanciones o evaluar la diligencia debida.

Quedan fuera del alcance de este análisis los aspectos puramente técnicos u operativos del comercio exterior, salvo en la medida en que constituyan fuentes de riesgo que deban ser identificadas y supervisadas desde la segunda línea de defensa.

Así entendido, el Trade Compliance se configura como un ámbito especializado del cumplimiento normativo, integrado en el CMS, que permite gestionar de forma ordenada y proporcional los riesgos derivados de la actividad internacional en organizaciones de cualquier tamaño.

3. EL TRADE COMPLIANCE COMO SUB-PROGRAMA DEL COMPLIANCE MANAGEMENT SYSTEM

En el contexto actual de creciente complejidad regulatoria y refuerzo del *enforcement*, el Trade Compliance no puede abordarse como una función aislada o meramente operativa. Su gestión exige una integración coherente en el Compliance Management System, como subprograma especializado alineado con los principios, estructuras y mecanismos generales del sistema de cumplimiento.

Desde esta perspectiva, el Trade Compliance comparte con otros ámbitos del Compliance una aproximación basada en riesgos, la exigencia de controles proporcionales y la necesidad de una gobernanza clara. Su integración en el CMS evita silos normativos, reduce duplicidades y permite aprovechar controles transversales, reforzando la coherencia y eficacia global del sistema.

La claridad en la asignación de responsabilidades y la existencia de un sistema de control interno bien gobernado son elementos especialmente valorados por las autoridades supervisoras y sancionadoras. La confusión de roles o la falta de supervisión efectiva suelen operar como factores negativos en escenarios de *enforcement.*

Concebir el Trade Compliance como subprograma del CMS implica su sujeción a los mecanismos generales de gobernanza, incluida la implicación del órgano de administración, la evaluación periódica de riesgos y la mejora continua. Este enfoque refuerza su

Si quieres adquirir esta obra haz click aquí

legitimidad interna y permite demostrar externamente que el cumplimiento en materia de comercio internacional forma parte de un sistema sólido, coherente y alineado con los estándares internacionales de Compliance.

4. AUTORIDADES COMPETENTES Y MARCO INSTITUCIONAL DEL TRADE COMPLIANCE

El Trade Compliance se desarrolla en un entorno institucional complejo y multinivel, en el que concurren autoridades con competencias de supervisión, control y sanción que operan de forma coordinada y en ocasiones solapada. Para el Compliance Officer, comprender este marco no es un ejercicio descriptivo ni académico, sino un elemento operativo esencial para identificar riesgos relevantes, diseñar controles proporcionados y anticipar las expectativas razonables de diligencia debida por parte de los reguladores.

Desde una perspectiva práctica, las autoridades con impacto en Trade Compliance pueden agruparse en cuatro grandes categorías: autoridades aduaneras; autoridades de control a la exportación; autoridades responsables de sanciones y embargos internacionales; y autoridades con competencias indirectas cuyos ámbitos de actuación se ven afectados por incumplimientos en el comercio internacional.

Desde la perspectiva del Compliance Officer, la utilidad de este mapa institucional no reside en dominar los procedimientos administrativos de cada autoridad, sino en comprender cómo este entramado incide en la evaluación del riesgo y en el diseño del sistema de control interno. La multiplicidad de actores, unida a la intensificación del enforcement y a la creciente interconexión entre áreas regulatorias, hace inviable un enfoque fragmentado y exige un Trade Compliance estructurado, basado en riesgos y plenamente integrado en un sistema de Compliance robusto y transversal.

4.1. AUTORIDADES ADUANERAS

Las autoridades aduaneras constituyen el primer nivel de control institucional sobre las operaciones de comercio exterior. Son las responsables de verificar aspectos esenciales como la clasificación arancelaria, el valor en aduana, el origen de las mercancías y la correcta aplicación de los regímenes aduaneros, así como de realizar controles *ex post* y ejercer la potestad sancionadora. En el caso español, estas funciones corresponden a la Agencia Tributaria, a través del Departamento de Aduanas e Impuestos Especiales. A nivel de la Unión Europea, la Comisión Europea desempeña un papel central en la armonización normativa y en la supervisión de la aplicación del Código Aduanero de la Unión, influyendo de forma directa en los criterios interpretativos que deben aplicar las autoridades nacionales. Para el Compliance Officer, este ámbito se traduce en riesgos recurrentes asociados a errores sistemáticos de clasificación, infravaloración, uso indebido de regímenes especiales o deficiencias en la documentación de origen.

4.2. AUTORIDADES DE CONTROL A LA EXPORTACIÓN

En segundo lugar, intervienen las autoridades de control a la exportación, con competencias sobre operaciones relativas a productos, tecnologías y conocimientos sujetos a

Si quieres adquirir esta obra haz click aquí

restricciones específicas, en particular los bienes y tecnologías de doble uso. En España, estas funciones se ejercen bajo la coordinación de la Secretaría de Estado de Comercio, a través de la Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso (JIMDDU). Estas autoridades supervisan la necesidad de licencias, autorizaciones o comunicaciones previas y pueden imponer sanciones severas o restricciones a la actividad empresarial en caso de incumplimiento. Desde la óptica del Trade Compliance, el riesgo no se limita a la exportación directa, sino que alcanza la transferencia intangible de tecnología, la asistencia técnica o la participación de filiales y socios en terceros países.

4.3. AUTORIDADES RESPONSABLES DE SANCIONES Y EMBARGOS INTERNACIONALES

Una relevancia especialmente sensible adquieren las autoridades responsables de sanciones y embargos internacionales. En el ámbito de la Unión Europea, los regímenes sancionadores se aprueban a nivel del Consejo y se aplican de forma directa en los Estados miembros, afectando tanto a exportaciones como a importaciones, inversiones, servicios y flujos financieros. Sin embargo, desde una perspectiva de riesgo, resulta imprescindible considerar también la actuación de autoridades extranjeras con capacidad de enforcement extraterritorial, como la Office of Foreign Assets Control (OFAC). La práctica de estas autoridades demuestra que el riesgo no se limita al incumplimiento directo de una prohibición, sino que se extiende a la insuficiencia de controles frente a operaciones indirectas, triangulaciones o el uso de intermediarios y terceros. Este factor explica por qué muchas organizaciones adoptan estándares de diligencia más exigentes que los estrictamente derivados de su normativa nacional o europea.

4.4. AUTORIDADES CON COMPETENCIAS INDIRECTAS

Finalmente, intervienen autoridades con competencias indirectas, cuyo impacto en Trade Compliance es cada vez más relevante. En este grupo se incluyen autoridades penales y fiscales, autoridades de defensa de la competencia —como la Comisión Nacional de los Mercados y la Competencia—, autoridades anticorrupción y, de forma creciente, organismos vinculados a derechos humanos, sostenibilidad y diligencia debida en la cadena de suministro. Aunque estas autoridades no supervisan el comercio internacional en sentido estricto, sus actuaciones pueden activarse a partir de incumplimientos relacionados con mercados de destino, terceros, agentes comerciales o estructuras de distribución internacional, generando riesgos significativos de carácter sancionador, reputacional o incluso penal.

5. ESTÁNDARES INTERNACIONALES, GUÍAS Y SOFT LAW DE REFERENCIA

El diseño y la supervisión de un programa de Trade Compliance no pueden sustentarse exclusivamente en la normativa jurídicamente vinculante aplicable en cada jurisdicción. En la práctica, las expectativas de autoridades y tribunales se configuran también a partir de estándares internacionales, guías técnicas y normas de *soft law*

Si quieres adquirir esta obra haz click aquí

que, aun careciendo de fuerza obligatoria directa, operan como criterios de referencia para valorar la diligencia debida de las organizaciones, sirviendo como referencia para evaluar la solidez de los programas de cumplimiento. Este marco se apoya, por un lado, en estándares transversales de gestión y Compliance, como los desarrollados por la ISO, que proporcionan la arquitectura del sistema; y, por otro, en guías especializadas en aduanas, control de exportaciones y sanciones, emitidas por organismos como la World Customs Organization, la Comisión Europea y autoridades con fuerte capacidad de *enforcement* extraterritorial, como la Office of Foreign Assets Control (OFAC). A ello se suman las directrices de diligencia debida y cadena de suministro responsable de la Organisation for Economic Co-operation and Development (OCDE) y las guías sectoriales de la International Chamber of Commerce (ICC), que conectan el Trade Compliance con ámbitos como terceros, sostenibilidad y derechos humanos. En conjunto, estos instrumentos no imponen obligaciones nuevas, pero condicionan de forma decisiva cómo las autoridades valoran la adecuación, proporcionalidad y eficacia de los sistemas de Trade Compliance.

Desde la perspectiva del Compliance Officer como segunda línea de defensa, estos marcos cumplen una función estructural de orientación y *benchmarking*, al permitir diseñar sistemas de control coherentes, identificar buenas prácticas reconocidas y justificar, en contextos de supervisión o enforcement, que el modelo adoptado es razonable, proporcional y alineado con las expectativas internacionales de gobernanza y cumplimiento.

La utilización de estándares internacionales y *soft law* no implica una adopción literal igual que en el resto de los ámbitos de Compliance. Su valor reside en servir como criterio de apoyo para el diseño, la evaluación y la mejora continua del sistema, mediante una adaptación razonada al perfil de riesgo y a la estructura de cada organización.

La referencia expresa y documentada a estos marcos refuerza, además, la posición de la organización en escenarios de inspección o procedimiento sancionador, al permitir acreditar que el programa de Trade Compliance ha sido concebido conforme a buenas prácticas ampliamente aceptadas. En este sentido, los estándares internacionales y el *soft law* deberían constituir un componente estructural del Trade Compliance y una herramienta clave para la prevención y mitigación del riesgo sancionador en el comercio internacional.

6. PRINCIPALES ÁMBITOS DE RIESGO EN TRADE COMPLIANCE

Desde la óptica del Compliance corporativo, el Trade Compliance constituye un ámbito específico de gestión de riesgos integrado en el Compliance Management System. La identificación y priorización de los focos de riesgo resulta esencial para un diseño eficaz de controles, una adecuada asignación de responsabilidades entre líneas de defensa y la acreditación de la diligencia debida ante las autoridades.

El enfoque basado en riesgos es particularmente relevante en el comercio internacional, donde la exposición varía en función del sector, los productos o tecnologías, los mercados de destino, el uso de intermediarios y la complejidad de la cadena de suministro. Ello exige soluciones proporcionadas y adaptadas al perfil concreto de cada organización.

Entre los principales ámbitos de riesgo destacan, en primer lugar, los riesgos aduaneros, asociados a la clasificación arancelaria, el valor en aduana, el origen o la aplicación

Si quieres adquirir esta obra haz click aquí

de regímenes especiales, cuya gestión deficiente puede dar lugar a regularizaciones económicas, sanciones y pérdida de beneficios. En segundo término, los riesgos vinculados a los controles a la exportación, que afectan a bienes, tecnologías o transferencias de conocimiento sujetos a restricciones y suelen ser objeto de un *enforcement* especialmente riguroso.

Especial complejidad presentan los riesgos derivados de sanciones y embargos internacionales, caracterizados por su dinamismo y por la extensión de las prohibiciones a operaciones indirectas y a través de terceros, lo que exige mecanismos de control reforzados para identificar beneficiarios finales y prevenir desvíos de uso o destino.

A estos se añaden los riesgos asociados a terceros y a la cadena de suministro, así como los riesgos organizativos y de gobernanza, vinculados a una deficiente delimitación de responsabilidades, ausencia de políticas y procedimientos adecuados, carencias formativas o mecanismos de escalado ineficaces, que suelen actuar como factores agravantes.

Desde la perspectiva sancionadora, la valoración del incumplimiento atiende tanto a la infracción material como al contexto organizativo. La identificación previa y documentada de los principales riesgos y la implantación de controles razonables y proporcionales constituyen, por ello, el punto de partida imprescindible para un sistema de Trade Compliance eficaz, coherente y creíble.

7. LA PRIMERA Y LA SEGUNDA LÍNEA DE DEFENSA EN TRADE COMPLIANCE

La eficacia del Trade Compliance exige una delimitación clara de funciones entre las líneas de defensa, conforme al modelo de las tres líneas, hoy consolidado como estándar de referencia en gobernanza y control interno y plenamente aplicable a los riesgos del comercio internacional.

La primera línea de defensa está integrada por las funciones operativas directamente implicadas en las actividades de comercio exterior. A estas áreas corresponde la gestión directa de los riesgos inherentes a su operativa y la aplicación efectiva de los controles, apoyadas en procedimientos claros, herramientas adecuadas y formación específica.

La segunda línea de defensa recae en la función de Compliance. Su papel no es operativo, sino estructural: definir el marco normativo interno del Trade Compliance, asesorar a la primera línea y supervisar de forma independiente la eficacia del sistema de control, asegurando su coherencia con el CMS.

La segregación clara de responsabilidades entre ambas líneas resulta esencial tanto para la eficacia del programa como para responder a las expectativas de las autoridades, que valoran de forma creciente la claridad organizativa y la existencia de mecanismos de supervisión efectivos.

La interacción entre ambas líneas debe articularse mediante mecanismos formales de coordinación, escalado y reporting, así como mediante acciones de formación y sensibilización que refuercen una cultura de cumplimiento en el comercio internacional.

En conjunto, la correcta articulación de la primera y la segunda línea de defensa constituye un pilar estructural del Trade Compliance, al permitir una gestión proporcionada

Si quieres adquirir esta obra haz click aquí

del riesgo, reforzar la credibilidad del sistema y garantizar que la función de Compliance ejerza su labor de supervisión sin asumir responsabilidades operativas.

8. SINERGIAS CON OTROS PROGRAMAS DE COMPLIANCE

La integración del Trade Compliance en el Compliance Management System permite aprovechar sinergias con otros subprogramas de Compliance, reforzando la coherencia del sistema y su eficacia preventiva, al tiempo que se evitan duplicidades y cargas innecesarias para las funciones operativas.

Los riesgos asociados al comercio internacional presentan una clara interrelación con otros ámbitos de cumplimiento, en particular con el Compliance penal, las sanciones internacionales, la anticorrupción, la competencia y, de forma creciente, la sostenibilidad y la diligencia debida en la cadena de suministro. Esta convergencia justifica un enfoque integrado, apoyado en controles y procesos transversales.

La utilización de herramientas comunes, como la evaluación de riesgos, la due diligence de terceros, el screening, la formación y los mecanismos de reporting, permite reforzar la capacidad de detección y prevención, facilitar la supervisión por la segunda línea de defensa y mejorar la acreditación de la diligencia debida ante autoridades y terceros.

La integración no debe implicar una dilución de responsabilidades ni una pérdida de especialización. El Trade Compliance mantiene especificidades propias que exigen un tratamiento diferenciado dentro de un marco común de control.

Desde la perspectiva sancionadora, las autoridades valoran positivamente los sistemas de Compliance integrados y coherentes. En este sentido, las sinergias entre el Trade Compliance y otros programas constituyen un elemento estructural para un sistema de cumplimiento eficaz y creíble en el ámbito del comercio internacional.

9. DISEÑO DE UN MODELO PROPORCIONAL DE TRADE COMPLIANCE

El diseño del Trade Compliance debe partir del principio de proporcionalidad, entendido como la adecuación del sistema al perfil de riesgo real de la organización. Este enfoque, propio del Compliance corporativo, evita tanto modelos insuficientes como estructuras excesivamente complejas e ineficaces.

La proporcionalidad no implica una rebaja de los estándares de cumplimiento, sino su adaptación razonada al tamaño, sector, complejidad de las operaciones internacionales, mercados de destino y grado de utilización de terceros. Desde esta lógica, el Trade Compliance puede articularse de forma escalable, distinguiendo entre modelos básicos y modelos más robustos en función de la exposición al riesgo.

Un modelo mínimo se centra en la identificación de riesgos clave, la existencia de políticas y procedimientos esenciales, la asignación clara de responsabilidades y una supervisión adecuada por parte de la segunda línea de defensa. Un modelo más avanzado incorpora evaluaciones de riesgo detalladas, controles de segundo nivel reforzados, apoyo

Si quieres adquirir esta obra haz click aquí

tecnológico y mecanismos de supervisión continua, siendo adecuado para organizaciones con mayor complejidad operativa.

En todo caso, la sofisticación del sistema debe responder a riesgos reales. Un programa desproporcionado o desconectado de la operativa puede resultar tan ineficaz como uno insuficiente.

Las autoridades valoran de forma creciente la adecuación del programa de Trade Compliance al perfil de riesgo de la organización. En este sentido, el diseño proporcional del sistema constituye un elemento clave para acreditar diligencia debida y reforzar la credibilidad del Compliance Management System en el ámbito del comercio internacional.

9.1. PARTICULARIDADES DEL TRADE COMPLIANCE EN PYMES

Las PYMES están sujetas, en términos sustantivos, a los mismos marcos regulatorios que las grandes organizaciones, aunque presentan particularidades estructurales que condicionan la forma en que el cumplimiento debe diseñarse e implementarse.

Desde una primera aproximación, puede interpretarse que el principal reto del Trade Compliance en las PYMES no reside tanto en la complejidad normativa como en la concentración de funciones y responsabilidades. En muchas PYMES, las decisiones relacionadas con el comercio internacional se adoptan por un número reducido de personas, lo que incrementa la dependencia de perfiles clave y dificulta la segregación formal de funciones propia de organizaciones de mayor tamaño.

Esta concentración funcional no implica necesariamente un mayor riesgo de incumplimiento, pero sí exige un enfoque distinto en el diseño del programa. En este contexto, la proporcionalidad no debe entenderse como una reducción del cumplimiento, sino como una priorización clara y consciente de los riesgos más relevantes, acompañada de mecanismos mínimos de trazabilidad y supervisión.

Puede sostenerse, desde esta óptica, que en las PYMES el riesgo más significativo en materia de Trade Compliance no es la ausencia de controles formales, sino la falta de claridad sobre quién asume la responsabilidad última de determinadas decisiones. La informalidad en los procesos, habitual en organizaciones de menor tamaño, puede dificultar la demostración *ex post* de la diligencia debida, incluso cuando las decisiones adoptadas han sido razonables.

Desde la perspectiva del Compliance Officer, cuando esta función existe formalmente en la PYME o se ejerce de manera compartida, el énfasis debe situarse en el establecimiento de reglas claras de decisión, escalado y documentación, más que en la creación de estructuras complejas. La capacidad de explicar de forma sencilla cómo se gestionan los riesgos de comercio internacional adquiere especial relevancia en escenarios de inspección o requerimientos de información por parte de autoridades.

Otro elemento característico de las PYMES es su mayor dependencia de terceros, tales como agentes, distribuidores, transitarios o asesores externos. Desde un punto de vista interpretativo, esta dependencia no exime de responsabilidad, pero sí refuerza la necesidad de adoptar criterios mínimos de selección, supervisión y documentación de la relación con dichos terceros, adaptados a los recursos disponibles.

Si quieres adquirir esta obra haz click aquí

En relación con la implantación práctica, puede considerarse adecuado que las PYMES adopten modelos de Trade Compliance basados en un número limitado de controles esenciales, claramente definidos y comprendidos por las personas clave de la organización. La eficacia del sistema dependerá menos del volumen de documentación y más de la coherencia entre riesgos identificados, controles aplicados y decisiones adoptadas.

Desde una perspectiva sancionadora, las autoridades suelen analizar la conducta de las PYMES atendiendo a criterios de razonabilidad y diligencia contextualizada. La existencia de un programa sencillo, pero bien pensado, alineado con el perfil de riesgo y correctamente aplicado, puede resultar más defendible que un sistema formalmente sofisticado, pero inoperante.

En este sentido, la formación en Trade Compliance en las PYMES adquiere una dimensión especialmente estratégica. La formación dirigida a perfiles clave, centrada en riesgos reales y escenarios concretos, puede generar un impacto preventivo superior al de programas formativos extensos, pero genéricos.

El Trade Compliance en las PYMES no debe concebirse como una versión reducida del cumplimiento aplicable a grandes organizaciones, sino como un modelo adaptado, claro y defendible. La clave reside en identificar los riesgos críticos, asignar responsabilidades de forma explícita y documentar de manera razonable las decisiones adoptadas, integrando el Trade Compliance en la cultura y en la operativa real de la empresa.

10. SUPERVISIÓN, INDICADORES Y MEJORA CONTINUA EN TRADE COMPLIANCE

Un programa de Trade Compliance solo puede considerarse eficaz y defendible si incorpora mecanismos estructurados de supervisión, medición y mejora continua. Estos elementos, integrados en el Compliance Management System, permiten verificar la eficacia real de los controles, identificar debilidades o desviaciones y asegurar la adaptación del sistema a la evolución de los riesgos, del entorno regulatorio y del modelo de negocio.

La supervisión del Trade Compliance es una función propia de la segunda línea de defensa y corresponde al Compliance Officer. Su cometido consiste en evaluar de forma periódica el diseño, la implantación y la eficacia de los controles definidos por la primera línea, sin asumir funciones operativas, con el objetivo de obtener una seguridad razonable sobre el nivel de cumplimiento y la exposición al riesgo de la organización.

Para el adecuado ejercicio de esta función resulta esencial la definición de indicadores que permitan medir el funcionamiento del programa. Los indicadores clave de rendimiento (KPIs) y de riesgo (KRIs) deben seleccionarse de forma coherente con el perfil de riesgo, la complejidad de las operaciones internacionales y el grado de madurez del programa. En el ámbito del Trade Compliance, estos indicadores pueden referirse, entre otros aspectos, a la cobertura de la formación específica, las incidencias detectadas, los tiempos de resolución de consultas o escalados, el volumen de operaciones sometidas a controles reforzados o los resultados de revisiones internas y externas. Su valor reside en su capacidad para aportar información relevante y accionable, no en su número.

El uso de indicadores debe complementarse con procesos periódicos de revisión del programa, como autoevaluaciones, revisiones temáticas, auditorías internas o evalua-

Si quieres adquirir esta obra haz click aquí

Si quieres adquirir esta obra haz click aquí

EL COMPLIANCE EN LA ERA DE LA IA

La gestión de los riesgos jurídicos tras la irrupción de la IA en las empresas

El Compliance se ha consolidado como una prioridad para las personas jurídicas. Si en sus inicios muchos directivos y órganos de gobierno lo percibían como un obstáculo para el negocio, hoy forma parte de la gestión ordinaria de las empresas. La irrupción de la inteligencia artificial abre ahora una nueva etapa: su uso cotidiano, a menudo sin autorización ni supervisión, genera riesgos jurídicos que los modelos de prevención tradicionales no contemplaban.

Esta obra, heredera del *Practicum Compliance*, actualiza desde un punto de vista práctico los elementos de un modelo de cumplimiento eficaz e incorpora los nuevos controles que exige la IA: el registro de casos de uso, la evaluación de impacto y la supervisión humana. Analiza además los riesgos con mayor probabilidad, como los delitos cometidos con IA, los deepfakes o el shadow AI, y ofrece mapas de riesgos y obligaciones legales.

Desde la anterior edición, los cambios han sido numerosos. En 2021 se publicó la ISO 37301, que sustituyó a la ISO 19600. En 2023 llegaron la Ley 2/2023 de protección de las personas informantes y la norma ISO/IEC 42001 sobre sistemas de gestión de la IA. En 2024 se aprobó el Reglamento Europeo de Inteligencia Artificial. En paralelo han surgido nuevas exigencias en materia de datos, ciberseguridad y diligencia debida, como el Data Act, DORA o la Directiva europea sobre diligencia debida de las empresas en materia de sostenibilidad.

Además de las cuestiones relacionadas con el cumplimiento normativo en general, el *Compliance en la era de la IA* pretende ser una herramienta para identificar, valorar y gestionar los riesgos jurídicos a los que se enfrenta una persona jurídica al integrar la inteligencia artificial en su actividad y en su modelo de organización y gestión.

ISBN: 979-13-7061-022-7

AENOR GESTIÓN DE LA CALIDAD ISO 9001 ER-0280/2005
IQNET RECOGNIZED CERTIFICATION
AENOR GESTIÓN AMBIENTAL ISO 14001 GA-2005/0100

ARANZADI