

Índice General

	<i>Página</i>
ASPECTOS JURÍDICOS DE LA CIBERSEGURIDAD Y SU CERTIFICACIÓN: ANÁLISIS DE LAS NORMAS ISO Y SU IMPACTO EN EL CUMPLIMIENTO LEGAL	
MARÍA LUISA GARCÍA TORRES.....	23
1. Introducción.....	23
2. El nuevo marco normativo europeo en ciberseguridad: análisis de la Directiva NIS2, del Reglamento DORA, y de la <i>Cyber Resilience Act</i>.....	27
2.1. <i>La Directiva NIS2</i>	27
2.2. <i>El Reglamento DORA</i>	29
2.3. <i>Cyber Resilience Act</i>	29
3. Certificaciones ISO: concepto y naturaleza	30
4. Normas y certificaciones ISO en materia de ciberseguridad, privacidad y <i>compliance</i>: utilidad organizativa y jurídica ...	31
4.1. <i>Normas ISO sobre SGSI: ISO/IEC 27001 e ISO/IEC 27002</i>	31
4.2. <i>Normas ISO sobre PIMS: ISO/IEC 27701, ISO/IEC 27018 e ISO/IEC 27005</i>	32
4.3. <i>Norma ISO en SGC: ISO 37301 e ISO 37001</i>	32
4.4. <i>Norma ISO sobre ciberseguridad: ISO/IEC 27032</i>	33
4.5. <i>El EU Cybersecurity Certification Framework y los esquemas europeos de certificación: relación con las normas ISO</i>	33
4.6. <i>Convergencia entre el ENS y los estándares ISO/IEC</i>	34

5.	Las certificaciones ISO como mecanismos de gobernanza, diligencia debida y gestión jurídica del riesgo.....	34
6.	Ventajas estratégicas y jurídicas de las certificaciones ISO frente a sus costes de implementación: análisis de casos reales	35
7.	Conclusiones.....	38

SOFT LAW Y CIBERSEGURIDAD: HACIA UNA GOBERNANZA JURÍDICA MULTINIVEL

	BÁRBARA CORTÉS CABRERA.....	41
1.	Construcción de la gobernanza del ciberespacio a partir del soft law.....	41
2.	Evolución normativa de la UE del soft law al hard law	45
	2.1. <i>Soft law fundacional y prelegislación (1992-2005).....</i>	46
	2.2. <i>Estrategias comunitarias y prelegislación avanzada (2013-2020)</i>	47
	2.3. <i>Consolidación jurídica al hard law (2016-2024).....</i>	48
3.	Contribución del soft law en la gobernanza multinivel de la ciberseguridad.....	51
4.	Desafíos constitucionales y demográficos del soft law en el ciberespacio.....	53
5.	Conclusiones.....	54

INTERSECCIÓN ENTRE LA NORMATIVA DE PROTECCIÓN DE DATOS Y LA CIBERSEGURIDAD. DESAFÍOS Y ESTRATEGIAS PARA LA EFICIENCIA OPERATIVA DIGITAL

	VERÓNICA JULIANA CAICEDO BUITRAGO.....	57
1.	Introducción.....	57
2.	Marco Normativo Internacional en privacidad y seguridad de datos	59
	2.1. <i>Ámbito Europeo.....</i>	59
	2.2. <i>Ámbito Español.....</i>	61
	2.3. <i>California — Estados Unidos</i>	65

	<i>Página</i>
3. Desafíos para las empresas. Cumplimiento sin comprometer la seguridad ni la eficiencia.....	66
3.1. <i>Equipos multidisciplinares.....</i>	<i>66</i>
3.2. <i>Requisitos potencialmente conflictivos</i>	<i>68</i>
3.3. <i>Costes operativos y recursos humanos</i>	<i>69</i>
4. Conclusiones.....	75

ALGUNOS ASPECTOS PROBLEMÁTICOS SOBRE LA RESPONSABILIDAD CIVIL POR INFRACCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS EN CASOS DE CIBERATAQUE

FELIPE OYARZÚN VARGAS.....	77
1. Introducción.....	77
2. ¿Cuál es el plazo de prescripción por los daños derivados por un ciberataque?.....	80
3. En cuanto al criterio de imputación en casos de ciberataques: ¿régimen objetivo o subjetivo?	83
4. En cuanto a la causalidad: ¿el hecho de un tercero (como un hacker) exonera de responsabilidad al responsable del tratamiento?	86
5. En cuanto al daño resarcible: ¿Qué daños se pueden producir por una brecha de seguridad?.....	87
6. Conclusiones.....	92

EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL: ¿UNA REGULACIÓN ÉTICA Y EFICAZ DE LOS SISTEMAS DE GESTIÓN DE RIESGOS?

CARLOS ÁLVARO PERIS.....	93
1. Los sistemas de gestión de riesgos y la ciberseguridad	93
2. La regulación de los sistemas de gestión de riesgos en el Reglamento Europeo de Inteligencia Artificial	94
2.1. <i>Análisis normativo.....</i>	<i>95</i>

	<i>Página</i>
2.2. <i>Análisis técnico</i>	97
2.3. <i>Análisis ético</i>	104
3. La complementariedad de los sistemas de <i>compliance</i> penal	108
4. Conclusiones	109

EL USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

HÉCTOR AYLLÓN SANTIAGO.....	111
1. Introducción	111
2. Ventajas de aplicar la IA en la ciberseguridad	113
3. Riesgos e inconvenientes del uso de la IA en la ciberseguridad	116
4. Regulación ética de los sistemas de IA	120
4.1. <i>Internacional</i>	120
4.2. <i>Nacional</i>	122
5. Principales aspectos éticos del uso de IA en ciberseguridad .	123
6. Conclusiones	127

LA UTILIZACIÓN DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL EN LA GOBERNANZA DEL FUTURO: OPORTUNIDADES Y RIESGOS PARA LA CIBERSEGURIDAD DESDE LA PERSPECTIVA CONSTITUCIONAL

JOSÉ LUIS MATEOS CRESPO.....	129
1. Introducción	129
2. La interrelación entre la gobernanza y la inteligencia artificial	130
3. ¿Nos dirigimos hacia una democracia algorítmica?	135
4. La protección de los Derechos Fundamentales ante los avances de la IA en la gobernanza	137
5. La ciberseguridad como elemento central de una buena gobernanza	139

	<i>Página</i>
6. La necesaria actualización del plan nacional de ciberseguridad en España como respuesta ante los nuevos riesgos.....	141
7. Conclusiones.....	143

GOBERNANZA ALGORÍTMICA DE LA CIBERSEGURIDAD: DESAFÍOS PARA EL ESTADO CONSTITUCIONAL EN LUCHA CONTRA LA DESINFORMACIÓN Y LA CIBERDELINCUENCIA

EMILIO FERRERO GARCÍA	147
1. Introducción.....	147
2. Ciberseguridad en un mundo complejo	148
3. Ciberdesinformación y ciberdelincuencia.....	150
4. Ciber gobernanza algorítmica ante la crisis de representación	152
5. La respuesta del estado	154
6. Algunas propuestas y perspectivas de abordaje a modo de conclusiones.....	156
6.1. Coordinación orgánica y alineación de acción	156
6.2. Reformas legislativas e institucionales.....	158
6.3. Refuerzo presupuestario y compromiso institucional	159
7. Anexo	162

PREVENCIÓN DE LA FINANCIACIÓN DEL TERRORISMO EN EL CIBERESPACIO: EL ENFOQUE DE LA UNIÓN EUROPEA

LUIS MIGUEL SÁNCHEZ-GIL.....	165
1. Introducción.....	165
2. Instrumentos y medidas de la unión europea en materia de fintech del terrorismo	166
2.1. Evolución legislativa de la Unión Europea	167
2.2. La creación de la Autoridad de Lucha Contra el Blanqueo de Capitales y la Financiación del Terrorismo: arquitectura operativa y competencias.....	173

	<i>Página</i>
3. Reflexión final	174
3.1. <i>Conclusiones</i>	174
3.2. <i>Prospectiva</i>	176

POLÍTICAS DE CIBERSEGURIDAD PARA PREVENIR LA FINANCIACIÓN DEL TERRORISMO Y DELITOS MEDIANTE NORMATIVAS, TECNOLOGÍA Y COOPERACIÓN

M. ^a OLIVIA GALÁN AZOFRA.....	179
1. Introducción	179
2. Justificación	180
3. Objetivo	182
3.1. <i>Objetivo General</i>	182
3.2. <i>Objetivos Específicos</i>	182
4. Regulación y marco normativo en ciberseguridad	182
5. Estrategias de prevención del blanqueo de capitales y financiación del terrorismo	185
6. Uso de tecnologías avanzadas en la lucha contra el cibercrimen	186
7. Colaboración internacional en la ciberseguridad y lucha contra el terrorismo	187
8. Amenazas y vulnerabilidades en el ciberespacio	188
9. Responsabilidad de las entidades financieras en la detección de operaciones sospechosas	189
10. Impacto del cibercrimen en la seguridad nacional	190
11. Protección de infraestructuras críticas frente a ataques cibernéticos	191
12. Big data e inteligencia artificial en la identificación de patrones delictivos	191
13. Desafíos éticos y legales en la ciberseguridad	192
14. Conclusiones	192

EL IMPACTO DE LAS CRIPTOMONEDAS EN EL DELITO DE BLANQUEO DE CAPITALES: ¿UN RIESGO EN UN MUNDO DIGITALIZADO?

DIEGO GONZÁLEZ LÓPEZ	195
1. Introducción.....	195
2. ¿Cómo se utilizan las criptomonedas?.....	196
3. El delito de blanqueo de capitales y las monedas virtuales.	198
4. Las criptomonedas como facilitadoras del blanqueo de capitales	203
4.1. <i>Exchanges no sujetos a regulación</i>	203
4.2. <i>Cold wallets</i>	204
4.3. <i>Privacy Coins</i>	204
4.4. <i>Coin Mixers.....</i>	205
4.5. <i>Deepweb y Darknet</i>	206
4.6. <i>Juegos y apuestas online.....</i>	206
5. Conclusiones.....	207

ARMONIZACIÓN DE LA PROTECCIÓN DE ACTIVOS Y LA GESTIÓN DE RIESGOS EN PYMES COLOMBIANAS MEDIANTE ESTÁNDARES INTERNACIONALES DE GOBERNANZA DE TI Y CIBERSEGURIDAD

YENNY STELLA NÚÑEZ ALVAREZ	209
1. Introducción.....	211
2. Escenario Actual de las PYMES en Colombia.....	212
3. Riesgos en las PYMES y Consecuencias de una Gobernanza Deficiente.....	214
4. Estándares y Marcos de Gobernanza TI y Ciberseguridad ..	215
5. Resultados y Discusión	217
6. Conclusiones.....	221

LA NECESIDAD REGULATORIA DE LOS SMARTS CONTRACTS A LA LUZ DE SU INCIPIENTE CRECIMIENTO EN EL SECTOR LEGAL

BLANCA APARICIO ARAQUE.....	223
1. Introducción.....	223
2. El impacto de la IA generativa en los contratos.....	223
3. Definición de los contratos inteligentes.....	227
4. Regulación de los contratos inteligentes.....	228
5. Influencia en las diferentes etapas contractuales.....	231
5.1. <i>La etapa precontractual.....</i>	231
5.2. <i>La prestación del consentimiento contractual.....</i>	232
5.3. <i>La forma del contrato.....</i>	235
5.4. <i>El objeto del contrato.....</i>	236
5.5. <i>La causa del contrato.....</i>	236
6. La formación de los contratos inteligentes.....	237
7. La ejecución de los contratos.....	237
8. Desafíos y perspectivas futuras.....	238
9. Conclusiones.....	239

DESAFÍOS CIBERJURÍDICOS EN LOS ALBORES DE LA ERA POST-CUÁNTICA

RODRIGO E. BIONDA.....	241
1. Amanecer cuántico.....	241
2. Dimensión técnica: ¿Qué es la Computación Cuántica?.....	243
3. Diferencias entre clásicas y cuánticas.....	245
4. El «Q» Day.....	245
5. Riesgo actual: «Steal Now, Decrypt Later».....	246
6. Preguntas, no respuestas.....	247
7. El Imperativo Cuántico.....	251
8. Logout.....	252