

Índice General

Página

PRÓLOGO

JOSÉ MIGUEL GORDILLO LUQUE.....	17
---------------------------------	----

CAPÍTULO 1.

MARCO REGULATORIO DE LA CIBERSEGURIDAD

I

LA ESTRATEGIA EUROPEA DE CIBERSEGURIDAD: LA LEGISLACIÓN DE LA UE QUE LA DESARROLLA

LETICIA LÓPEZ-LAPUENTE	25
1. Introducción: una transformación digital europea ciberse- gura en un entorno de amenazas complejo	25
2. Los principios rectores de la Estrategia Europea de Ciberse- guridad	27
3. La principal legislación en ciberseguridad de la UE	31
3.1. <i>Directivas sobre medidas para un alto nivel común de ciberse- guridad en la Unión (Directivas NIS1 y NIS2).....</i>	31
3.2. <i>ENISA y el Reglamento de Ciberseguridad</i>	35
3.3. <i>El Reglamento de Ciberresiliencia.....</i>	36
3.4. <i>El Reglamento de Ciberresiliencia</i>	37
3.5. <i>Reglamento DORA</i>	37
3.6. <i>Directiva Europea sobre la Resiliencia de Entidades Críticas.</i>	37

NORMATIVA COMUNITARIA PARA LA CIBERSEGURIDAD EN EL SECTOR ELÉCTRICO

ROBERTO FERNÁNDEZ CASTILLA.....	39
1. Introducción: El sector eléctrico y su exposición a un mundo digitalizado	39
2. Regulación en materia de ciberseguridad en el sector de la electricidad	41
2.1. <i>Reglamento 2019/941: Preparación frente a los riesgos en el sector de la electricidad.....</i>	43
a. Razonamiento detrás del enfoque basado en riesgos.....	43
b. Evaluación y análisis de riesgos: los planes de preparación.....	44
c. Integración de la ciberseguridad en la seguridad del suministro.....	45
d. Conclusión: la importancia del Reglamento 2019/941 en la ciberseguridad del sistema eléctrico .	45
2.2. <i>Reglamento (UE) 2019/943: Mercado interior de la electricidad</i>	46
a. Consideraciones en materia de ciberseguridad	47
b. Conclusión	48
2.3. <i>Reglamento Delegado (UE) 2024/1366: Complemento del Reglamento (UE) 2019/943 en materia de ciberseguridad.....</i>	49
a. Objetivos específicos y medidas que implementa .	49
b. <i>Ámbito</i> subjetivo de aplicación	50
c. Disposiciones específicas en materia de ciberseguridad	52
d. Conclusión: Relevancia y aportación al sistema eléctrico europeo	54

II

LEGISLACIÓN NACIONAL ESPECÍFICA EN MATERIA DE SEGURIDAD NACIONAL, CIBERSEGURIDAD, RESILIENCIA OPERATIVA

ROSA ORTUÑO	55
-------------------	----

LEGISLACIÓN PENAL ESPECÍFICA CON IMPACTO EN CIBERSEGURIDAD

DAVID VELÁZQUEZ	81
1. Normativa aplicable	81
2. Delitos que afectan a la ciberseguridad en la legislación penal española	87
2.1. Acceso ilegal a sistemas informáticos	87
2.2. Interceptación ilegal de datos informáticos	90
2.3. Daños en datos, programas informáticos o documentos electrónicos	90
2.4. Delitos de abuso de dispositivos (artículos 197 ter y 264 ter).	92
2.5. Otros delitos relacionados con la ciberseguridad	94

III

OTRAS NORMATIVAS DISTINTAS DE CIBERSEGURIDAD CON IMPACTO EN LA REGULACIÓN DE LA SEGURIDAD DE LAS EMPRESAS

ROSA ORTUÑO.....	95
1. Datos: protección de datos (RGPD) y Estrategia Europea de Datos (Data Act, Data Governance Act)	95
2. Seguridad de la información: Cyber resilience Act.....	106
3. Inteligencia artificial: IA Act.....	106
4. El nuevo Reglamento sobre Seguridad de los Productos	110
5. Ejemplo de normativa específica de productos por sector: Sector sanitario: Reglamento de productos sanitarios	111
6. Responsabilidad por daños por productos defectuosos	112
7. Nota Final	113

IV

ESTRATEGIAS Y MARCO NORMATIVO DE CIBERSEGURIDAD DE ESTADOS UNIDOS, AUSTRALIA, REINO UNIDO, BRASIL Y MÉXICO

NOHAILA EL MOUDEN JAADOUNI.....	117
1. Introducción.....	117
2. Estrategias nacionales de ciberseguridad: análisis comparado.	118
2.1. <i>La relevancia del análisis de las Estrategias Nacionales de Ciberseguridad</i>	118
a) Estados Unidos: <i>The National Cybersecurity Strategy</i> (2023)	119
b) Australia: <i>The 2023-2030 Australian Cyber Security Strategy</i> (2023-2030).....	122
c) Reino Unido: <i>The Government Cyber Security Strategy</i> (2022-2030)	124
d) Brasil: <i>Política Nacional de Cibersegurança (PNCiber)</i> (2023)	126
e) México: <i>La Estrategia Nacional de Ciberseguridad</i> (2017).....	127
2.2. <i>Sobre la necesidad de una mayor cooperación internacional...</i>	129

CAPÍTULO 2.

GOBIERNO DE LA CIBERSEGURIDAD

I

LA CIBERSEGURIDAD Y LA DIRECTIVA NIS 2

RAFAEL SEBASTIÁN	133
1. Introducción.....	133
1.1. <i>La amenaza fantasma: cómo actúan los piratas informáticos .</i>	135
1.2. <i>Tendencias en materia de ciberseguridad</i>	139
1.3. <i>La ciberseguridad. Una defensa activa</i>	140
1.4. <i>Una mirada al futuro</i>	142
2. El marco normativo	143

	<i>Página</i>
2.1. <i>Legislación aplicable</i>	143
2.2. <i>Panorama institucional</i>	147
2.3. <i>El código de buen gobierno</i>	148
3. Ciberseguridad y gobierno corporativo	150
3.1. <i>Notificación de ciberincidentes</i>	151
3.2. <i>La gobernanza de la ciberseguridad y la Directiva NIS 2</i>	153
3.3. <i>Los deberes de los administradores en materia de ciberseguridad</i>	155
3.4. <i>Asignación de la ciberseguridad a una comisión especializada</i>	158
3.5. <i>Responsabilidad del Consejo</i>	159
3.6. <i>Responsabilidad de la Comisión de Auditoría</i>	161
4. Conclusiones	162
Bibliografía	165

CAPÍTULO 3. COLABORACIÓN PÚBLICO-PRIVADA EN MATERIA DE CIBERSEGURIDAD

I

MODELOS DE COLABORACIÓN PARA LA PREVENCIÓN Y LA RESPUESTA COORDINADA ANTE INCIDENTES DE SEGURIDAD

DAVID VELÁZQUEZ	171
-----------------------	-----

II

LA CIBERSEGURIDAD DESDE LA PERSPECTIVA DE LA ADMINISTRACIÓN PÚBLICA: PARTICULARIDADES EXISTENTES Y ESTADÍSTICAS RELEVANTES. RESPONSABILIDAD Y COLABORACIÓN DE LOS ÓRGANOS DE SUPERVISIÓN Y CONTROL Y LA PROMOCIÓN DE LA SEGURIDAD. NOVEDADES Y CAMBIOS DERIVADOS DEL ANTEPROYECTO DE LA LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD

DAVID FRANCISCO BLANCO	183
------------------------------	-----

1. La Ciberseguridad desde la Perspectiva de la Administra- ción Pública: Particularidades Existentes	184
--	------------

	<i>Página</i>
1.1. <i>Introducción</i>	184
1.2. <i>Particularidades existentes</i>	185
1.3. <i>Estadísticas relevantes</i>	189
2. Responsabilidad y Colaboración de los Órganos de Supervisión, Control y la Promoción de la Seguridad	191
2.1. <i>Centro Criptológico Nacional</i>	191
2.2. <i>Centro Nacional de Protección de Infraestructuras y Ciberseguridad</i>	195
2.3. <i>Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos</i>	197
2.4. <i>Mando Conjunto del Ciberespacio</i>	198
2.5. <i>Instituto Nacional de Ciberseguridad de España</i>	199
3. Novedades y cambios derivados del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad	204

CAPÍTULO 4

GESTIÓN Y RESPUESTA ANTE INCIDENTES DE CIBERSEGURIDAD

MARIO MONTES SANTAMARÍA	211
1. Reacción penal frente a los incidentes de ciberseguridad	211
2. Riesgos penales asociados al pago en casos de <i>ransomware</i>.	218

CAPÍTULO 5

IMPLICACIONES DE CIBERSEGURIDAD EN LA CONTRATACIÓN DE PRODUCTOS Y SERVICIOS TECNOLÓGICOS

FRANCISCO JAVIER GARCÍA Y MARC CALVO CARMONA.....	225
1. La digitalización del sector eléctrico y la creciente importancia de la ciberseguridad	225
2. El papel de los proveedores en la ciberseguridad de los operadores eléctricos	228

	<i>Página</i>
3. Pautas a seguir por los operadores eléctricos en la contratación de proveedores tecnológicos	229
3.1. <i>Primer paso: determinación del régimen aplicable en materia de ciberseguridad</i>	<i>230</i>
3.2. <i>Segundo paso: redacción del contrato.....</i>	<i>233</i>
a) Cláusulas contractuales en cumplimiento del RD 2024/1366.....	233
b) Cláusulas contractuales de conformidad con el RGPD.....	235
c) Garantías de cumplimiento	236
d) Definición de las medidas de seguridad	237
e) Facultades de supervisión	238
f) Asunción de responsabilidad	238
g) Confidencialidad.....	239
h) Restricciones a la subcontratación	239
i) Notificación de incidentes y deber de colaboración	239
j) Facultad de terminación.....	241
k) Jurisdicción	241
4. Conclusiones.....	245

CAPÍTULO 6

CIBERAMENAZAS EN EL SECTOR ELÉCTRICO

JOSEP PEGUEROLES VALLÉS, FCO. JAVIER GARCÍA PÉREZ Y ROBERTO FERNÁNDEZ CASTILLA.....	249
1. La red eléctrica como infraestructura crítica. Seguridad IT y seguridad OT	250
2. La generación, distribución y comercialización inteligente de energía eléctrica. Vulnerabilidades intrínsecas de la Smart Grid	251

	<i><u>Página</u></i>
3. Agentes implicados, atacantes, amenazas híbridas, geopolíticas	254
4. Cumplimiento en medidas de ciberseguridad.....	259
5. Medidas de ciberseguridad para la <i>Smart Grid</i>	261
6. Conclusiones.....	262
7. Referencias	263