Nota 9
Introducción. 15

1. La Internet de las Cosas 19
1.1. De qué hablamos cuando hablamos de IoT 20
1.2. Componentes e interrelaciones 24
1.3. La transformación cognitiva. 27
1.3.1. Sistemas ciberfísicos 31

2. La quiebra de la responsabilidad de producto 35

3. Los problemas de la limitación de responsabilidad del software 47
3.1. La limitación de responsabilidad: la cláusula «as is» 47
3.2. La seguridad del *software* y el específico tratamiento del *software* inseguro 54
3.3. Responsabilidad en el *software* embebido 57

4. Seguridad y responsabilidad ¿Y ahora qué? 59
4.1. ¿Quién es el responsable de garantizar la seguridad de un producto? Inseguridad desde el diseño. 59
4.1.1. Ataques físicos 66
4.1.1.1. Puertos de conexión del dispositivo 66
4.1.1.2. Firmware 67
4.1.2. Ataque sobre las comunicaciones. 68
4.1.2.1. Comunicaciones entre el dispositivo y la nube 68
4.1.2.2. Comunicaciones entre dispositivos y aplicaciones móviles . . 70
4.1.2.3. Comunicaciones inalámbricas del dispositivo 72
4.1.2.4. Interfaz web u otros interfaces de gestión del dispositivo . . . 73
4.1.3. Ataque a almacenamiento local de datos 74
4.2. Estándares, buenas prácticas y proyectos normativos 75
4.2.1. Buenas Prácticas IoT de CCN 76

4.2.2. Recomendaciones del Grupo de trabajo de amenazas y sensibilización del Centro de Estudios en Movilidad e IoT (CEM) . . . 78
4.2.3. La seguridad en los sistemas ciberfísicos: principios éticos 81
4.2.4. La «Internet of Things (IoT) Cybersecurity Improvement Act». 87
4.3. Evaluación de conformidad y marcas de garantía. 91
4.3.1. La Directiva RED 92
4.3.2. Productos sanitarios 93
4.3.3. La marca de garantía propuesta por la «Cybersecurity act». 96
4.5. ¿Quién es el responsable de la seguridad una vez puesto en el mercado? La gestión de los dispositivos médicos IoT durante todo su ciclo de vida 102
4.5.1. La Guía FDA de gestión de la ciberseguridad de dispositivos médicos 105
4.5.1.1. Alcance 106
4.5.1.2. Definiciones 107
4.5.1.3. Principios generales 110
4.5.1.4. Consideraciones previas a la comercialización 110
4.5.1.5. Consideraciones tras la comercialización 111
4.5.1.6. Mantenimiento de la seguridad y el rendimiento esencial . . 113
4.5.1.7. Gestión de riesgos de ciberseguridad de dispositivos médicos. 114
4.5.1.8. Remediando y reportando vulnerabilidades de ciberseguridad 120
4.6. Reparto de responsabilidad por daños en la IoT insegura: estado de la cuestión 124
4.6.1. Revisión del clásico esquema culpabilístico desde la perspectiva del IoT básico 125
4.7. Propuestas sobre la responsabilidad por IoT y sistemas ciberfísicos inseguros 136

5. Casos de uso 141
5.1. El transporte inteligente 141
5.1.1. Transporte inteligente. 142
5.1.2. El coche autónomo y conectado 146
5.1.2.1. Definición y componentes 147
5.1.2.2. Clasificación de los coches autónomos 154
5.1.2.3. Seguridad de los coches autónomos y conectados. 158
5.1.2.3.1. Informe Intel-McAfee 159
5.1.2.3.2. Principios de ciberseguridad para coches conectados y autónomos Departamento de Transporte de Reino Unido 161
5.1.2.3.3. Guía ENISA 163
5.1.2.4. Legislación y principios éticos 189
5.1.2.4.1. España. 191
5.1.2.4.2. EEUU: el software es el conductor. 193
5.1.2.4.3. Reino Unido 199
5.1.2.4.4. Alemania. 199
5.1.2.5. Aproximación a la responsabilidad por daños 202

5.1.3. Aeropuertos inteligentes 205
5.2. Las casas inteligentes 242
5.3. Hospitales inteligentes 243
5.4. Uso de IoT y sistemas ciberfísicos en entornos de bienestar personal, salud y cuidado de mayores 271
5.5. Las ciudades inteligentes 274
5.5.1. Definición 274
5.5.2. Procesamiento e interacción de datos en la ciudad inteligente . . 278
5.5.2.1. El ciclo de datos en las ciudades inteligentes 278
5.5.3. La plataforma de servicios de las ciudades inteligentes 286
5.5.4. Ciberseguridad en las ciudades inteligentes: el sistema de transporte público 293
5.6. Drones 313
5.6.1. Definición 313
5.6.2. Situación en España 314
5.6.3. La seguridad de los sistemas de aeronaves no tripuladas 319

6. Responsabilidad empresarial por la IoT 323
6.1. Responsabilidad penal de las personas jurídicas (artículo 33 bis CP) 323
6.1.1. Identificación de los riesgos del uso de cosas conectadas (daños por ataques de denegación de servicio) 324
6.1.2. Integración y mitigación de los riesgos en el programa de compliance 327
6.2. Responsabilidad por la recogida y análisis de datos en la IoT 330
6.2.1. El dictamen 8/2014 del WG 29 sobre la IoT 332
6.2.2. El tratamiento de grandes datos en la IoT 338
6.2.3. Privacidad desde el diseño en la IoT: la propuesta de Reglamento de ePrivacy 348
6.2.4. La privacidad en los coches autónomos 350