

ÍNDICE GENERAL

ABREVIATURAS	5
DOMINIO I. NORMATIVA GENERAL DE PROTECCIÓN DE DATOS	7
CAPÍTULO 1. CONTEXTO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES, por ADRIÁN PALMA ORTIGOSA	9
1. Introducción	9
2. La protección de datos en el ámbito internacional	10
2.1. OCDE.....	11
2.2. ONU.....	12
2.3. EEUU.....	12
3. La protección de datos en Europa	12
3.1. Consejo de Europa.....	13
3.2. Unión Europea	14
3.2.1. <i>Directiva 95/46 CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995</i>	14
3.2.2. <i>Carta de derechos fundamentales de la Unión Europea</i>	16
3.2.3. <i>Tratado de Funcionamiento de la Unión Europea</i>	16
3.2.4. <i>Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016</i>	16
4. La protección de datos en España	18
4.1. Constitución Española	18
4.2. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal.....	19
4.3. Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos	19
4.4. Proyecto de Ley Orgánica de Protección de datos.....	20
5. Estándares y buenas prácticas	20
CAPÍTULO 2. ÁMBITO DE APLICACIÓN Y DEFINICIONES DEL RGPD, por ADRIÁN PALMA ORTIGOSA	25
1. Ámbito de aplicación material	25

1.1. Ámbito de aplicación positivo	25
1.2. Ámbito de aplicación negativo (exclusiones)	25
2. Ámbito de aplicación territorial	28
3. Definiciones del RGPD	29
3.1. Introducción	29
3.2. Definiciones básicas	30
3.3. Definiciones novedosas	33
CAPÍTULO 3. PRINCIPIOS RELATIVOS AL TRATAMIENTO DE DATOS PERSONALES, por ADRIÁN PALMA ORTIGOSA	39
1. El binomio derecho/deber en la protección de datos	39
2. Los principios relativos al tratamiento de datos	40
2.1. Licitud del tratamiento	41
2.2. Lealtad y transparencia	42
2.3. Limitación de la finalidad	43
2.3.1. <i>Fin legítimo</i>	44
2.3.2. <i>Fin determinado</i>	44
2.3.3. <i>Fin explícito</i>	44
2.3.4. <i>Incompatibilidad de los fines tratados ulteriormente</i>	44
2.4. Minimización de datos	45
2.5. Exactitud	46
2.6. Limitación del plazo de conservación	46
2.7. Integridad y confidencialidad (seguridad de los datos)	47
2.8. Responsabilidad proactiva (<i>accountability</i>)	47
2.9. Principio de proporcionalidad	48
CAPÍTULO 4. LAS BASES DE LEGITIMACIÓN DEL TRATAMIENTO DE DATOS PERSONALES. EN ESPECIAL, EL CONSENTIMIENTO, por CARLOS TRUJILLO CABRERA	51
1. Introducción	51
2. El consentimiento: otorgamiento y revocación	53
2.1. Consentimiento y autodeterminación informativa	53
2.2. Requisitos para el otorgamiento del consentimiento	54
2.2.1. <i>Manifestación de voluntad libre</i>	55
2.2.2. <i>Manifestación de voluntad específica</i>	56
2.2.3. <i>Manifestación de voluntad informada</i>	57
2.2.4. <i>Manifestación de voluntad inequívoca</i>	59
2.2.5. <i>Mediante una declaración o una clara acción afirmativa</i> ..	60
2.3. Revocación del consentimiento	62
3. El consentimiento de los niños	63
4. Categorías especiales de datos	65
5. Datos relativos a infracciones y condenas penales	69
6. Tratamiento que no requiere identificación	69
7. Bases jurídicas distintas del consentimiento	70

7.1. La existencia de una relación contractual en la que el interesado sea parte o la existencia de una obligación legal para el responsable	70
7.2. La necesidad de proteger intereses vitales del interesado o de otras personas	71
7.3. El interés legítimo como base del tratamiento.....	71
CAPÍTULO 5. DERECHOS DE LOS INDIVIDUOS, por JUAN PABLO MURGA FERNÁNDEZ.....	77
1. Transparencia e información	78
1.1. El principio de transparencia (Sección 1, Capítulo III RGPD).....	78
1.1.1. Origen y naturaleza del principio de transparencia	78
1.1.2. Concepto del principio de transparencia	79
1.1.3. Transparencia, corresponsabilidad y menores: Considerando 58 RGPD.....	80
1.1.4. Requisitos de la transparencia: art. 12 RGPD (transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado)	80
1.2. El deber de información (arts. 13 y 14 RGPD).....	86
1.2.1. Información que deberá facilitarse cuando los datos personales se obtengan del interesado (art. 13 RGPD).....	87
1.2.2. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado (art. 14 RGPD)..	88
2. Acceso, rectificación, supresión (olvido)	91
2.1. Derecho de acceso (art. 15 RGPD).....	91
2.2. Derecho de rectificación (art. 16 RGPD).....	93
2.3. Derecho de supresión (el “derecho al olvido”): art. 17 RGPD.....	94
2.3.1. El derecho de supresión.....	94
2.3.2. El derecho al olvido.....	96
3. Derecho de oposición (art. 21 RGPD)	100
3.1. Oposición a tratamientos basados en el interés público o interés legítimo	101
3.2. Oposición a tratamientos que tengan por objeto la mercadotecnia directa	102
3.3. El derecho de oposición en el caso de tratamientos con fines de investigación: un caso excepcional.....	102
3.4. Ejercicio del derecho de oposición, efectos del ejercicio y comunicación de su existencia.....	102
4. Decisiones individuales automatizadas (art. 22 RGPD)	103
5. Derecho a la portabilidad (art. 20 RGPD).....	105
5.1. Introducción y concepto.....	105
5.2. Operaciones de tratamiento y datos cubiertos por el derecho a la portabilidad	105
5.3. ¿Cómo deben proporcionarse los datos que deben portarse?	108

5.4. Plazo en que debe facilitarse la portabilidad	109
5.5. Excepciones al derecho a la portabilidad.....	109
6. Limitación del tratamiento (art. 23 RGPD)	109

CAPÍTULO 6. POSICIÓN JURÍDICA DE LOS INTERVINIENTES EN EL TRATAMIENTO DE DATOS PERSONALES. MEDIDAS DE CUMPLIMIENTO, por SARA LORENZO CABRERA

1. Las políticas de protección de datos	115
1.1. Aproximación a las políticas de protección de datos	115
1.2. Clasificación de las distintas políticas de protección de datos	116
2. Posición jurídica de los intervinientes en el tratamiento de datos	117
2.1. Responsable del tratamiento: definición y régimen jurídico	117
2.2. Elementos configuradores del concepto de responsable del tratamiento	119
2.2.1. Fuentes de atribución del poder de determinación	120
2.2.2. ¿Sobre qué elementos recae el poder de determinación? ...	121
2.2.3. Finalidad del tratamiento	122
2.2.4. Medios del tratamiento	122
2.3. Responsabilidad del responsable del tratamiento	123
2.3.1. Consideraciones generales: cambio de paradigma	123
2.3.2. Las obligaciones del responsable del tratamiento	125
2.4. Régimen de corresponsabilidad	128
2.4.1. Delimitación del supuesto de «corresponsabilidad»	128
2.4.2. Relación entre corresponsables y su formalización	129
2.5. Encargado y subencargado del tratamiento	130
2.5.1. Aproximación a la figura del «encargado del tratamiento»	130
2.5.2. Relación entre el responsable y el encargado. Breve referencia a los subencargados del tratamiento.....	132
2.6. Representante del responsable o del encargado del tratamiento y las relaciones entre ellos.....	135
3. El registro de actividades de tratamiento	136
3.1. Introducción	136
3.2. Configuración legal de la obligación de llevanza de un registro de actividades	137

CAPÍTULO 7. RESPONSABILIDAD PROACTIVA, por SARA LORENZO CABRERA, ADRIÁN PALMA ORTIGOSA Y CARLOS TRUJILLO CABRERA

1. Privacidad desde el diseño y por defecto. Principios fundamentales.	143
1.1. Introducción	143
1.2. Principios fundamentales.....	145
1.3. Implementación en el artículo 25 del Reglamento General de Protección de Datos.....	147
1.3.1. Privacidad desde el diseño.....	147
1.3.2. Privacidad por defecto	149

2. Evaluación de impacto de protección de datos y los tratamientos de alto riesgo	150
2.1. Consideraciones generales	150
2.2. Obligación de realizar una evaluación de impacto: ¿en qué supuestos?.....	150
2.3. ¿Quién es el sujeto obligado a realizar la EIPD y cuándo debe hacerlo?.....	155
2.4. Ámbito y contenido mínimo de la EIPD	155
2.5. Revisión de la evaluación de impacto.....	156
2.6. Consulta previa	157
2.6.1. <i>Supuestos de consulta previa</i>	157
2.6.2. <i>Sujeto obligado y procedimiento de consulta</i>	157
3. Seguridad de los datos personales	158
3.1. Introducción.....	158
3.2. Medidas técnicas y organizativas relativas a la seguridad del tratamiento	158
4. Las violaciones de seguridad. Notificación y comunicación de las violaciones de seguridad	161
4.1. Notificación de una violación de seguridad. Art 33. RGPD.	161
4.1.1. Sujeto al que se ha de notificar y deber de notificación	161
4.1.2. Contenido mínimo de la notificación	162
4.1.3. Otras obligaciones	162
4.2. Comunicación de una violación de seguridad. Art 34	162
4.2.1. <i>Sujeto al que se ha de comunicar y deber de comunicación</i>	162
4.2.2. <i>Contenido mínimo de la comunicación</i>	163
4.2.3. <i>Otras obligaciones</i>	163
4.2.4. <i>Justificación de las comunicaciones</i>	163
5. Códigos de conducta y certificaciones	164
5.1. Códigos de conducta.....	164
5.2. Certificaciones	168

CAPÍTULO 8. EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS. DELEGADOS DE PROTECCIÓN DE DATOS (DPD, DPO O DATA PRIVACY OFFICER), por SALVADOR TOMÁS TOMAS..... 173

1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses	173
1.1. Consideraciones previas.....	173
1.2. Designación	174
1.3. Proceso de toma de decisión y cualificación	178
1.4. Formalidades en la designación, nombramiento y cese.....	180
1.5. Análisis de conflicto de intereses.....	181
2. Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección	183

2.1. Obligaciones	183
2.2. Responsabilidades.....	185
2.3. Independencia	185
2.4. Reporte a dirección	187
3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones	189
3.1. Colaboración.....	189
3.2. Autorizaciones previas	191
3.3. Relación con los interesados	192
3.4. Gestión de reclamaciones	192
4. Comunicación con la autoridad de protección de datos.....	193
CAPÍTULO 9. TRANSFERENCIAS INTERNACIONALES DE DATOS, por SARA LORENZO CABRERA.....	195
1. Introducción	195
2. Principio general de transferencias internacionales de datos	196
3. Concepto de «transferencia internacional de datos». Breve referencia al «tratamiento transfronterizo de datos»	197
4. Transferencias basadas en una decisión de adecuación	200
4.1. La decisión de adecuación como primera fuente de legitimación de las transferencias internacionales de datos	200
4.2. ¿Qué se entiende por «nivel de protección adecuado»?	201
4.3. Competencia y objeto de adecuación	202
4.4. Procedimiento para adoptar la decisión de adecuación	204
4.4.1. <i>Iniciativa</i>	204
4.4.2. <i>Evaluación</i>	205
4.4.3. <i>Aprobación de la adecuación</i>	206
4.4.4. <i>Publicación</i>	208
4.4.5. <i>Decisiones de adecuación adoptadas bajo el régimen de la Directiva 95/46/CE</i>	208
4.5. Principales efectos jurídicos de la decisión de adecuación	208
5. Transferencias internacionales mediante garantías adecuadas.....	210
5.1. La aportación de garantías adecuadas como segunda fuente de legitimación de las transferencias internacionales de datos.....	210
5.2. Clasificación de los diferentes cauces legales para aportar las garantías adecuadas	211
5.2.1. <i>Primera modalidad de garantías adecuadas</i>	211
5.2.2. <i>Segunda modalidad de garantías adecuadas</i>	213
5.3. Especial atención a las «normas corporativas vinculantes» y a las «cláusulas contractuales tipo» como garantías adecuadas.....	215
5.3.1. <i>Normas corporativas vinculantes</i>	215
5.3.2. <i>Cláusulas contractuales tipo</i>	218
5. Excepciones al principio general de transferencias	219
6. Otros supuestos específicos de transferencias internacionales de datos	223

7. Cooperación internacional en el ámbito de la protección de datos personales	224
8. Suspensión temporal de los flujos internacionales de datos.....	225
CAPÍTULO 10. LAS AUTORIDADES DE CONTROL, por M^a DE LOS ÁNGELES FERNÁNDEZ SCAGLIUSI	229
1. Autoridades de control independientes	229
1.1. Concepto	229
1.2. Independencia	231
2. Competencias, funciones y poderes	233
2.1. Competencias	233
2.2. Funciones	235
2.3. Poderes.....	237
3. Régimen sancionador	240
3.1. Consideraciones previas.....	240
3.2. Sujetos responsables	241
3.3. Infracciones.....	241
3.3.1. <i>Clases de infracciones</i>	241
3.3.1.1. Clases de infracciones según el RGPD	241
3.3.1.2. Clases de infracciones según el Proyecto de LOPD.	242
3.3.2. <i>Prescripción de infracciones</i>	248
3.4. Sanciones y medidas coercitivas.....	248
3.4.1. <i>Clases de sanciones</i>	248
3.4.2. <i>Criterios de graduación de las sanciones y multas coercitivas</i>	248
3.4.3. <i>Prescripción de las sanciones</i>	249
3.4.4. <i>Multas administrativas</i>	250
3.4.5. <i>Multas administrativas a autoridades y organismos públicos</i>	250
4. Comité Europeo de Protección de Datos	251
4.1. Concepto	251
4.2. Principios	251
4.3. Organización y funcionamiento	253
4.4. Funciones	254
4.5. Recursos frente a las resoluciones	257
5. Procedimientos seguidos por la AEPD	258
5.1. Régimen jurídico.....	258
5.2. Iniciación de los procedimientos	259
5.3. Medidas provisionales	260
5.4. Plazo de tramitación de los procedimientos	261
6. La tutela jurisdiccional.....	261
7. El derecho de indemnización	262

CAPÍTULO 11. DIRECTRICES DE INTERPRETACIÓN DEL RGPD , por CARLOS TRUJILLO CABRERA	265
1. Directrices del Grupo de Trabajo del artículo 29	265
1.1. Directrices en materia de notificación de violaciones de seguridad	266
1.2. Directrices en materia de decisiones automatizadas y elaboración de perfiles	267
1.3. Directrices en materia de establecimiento e imposición de multas administrativas	268
1.4. Directrices en materia de consentimiento	269
1.5. Directrices en materia de transparencia	269
2. El Comité Europeo de Protección de Datos	270
3. Criterios de órganos jurisprudenciales	273
CAPÍTULO 12. NORMATIVAS SECTORIALES AFECTADAS POR LA PROTECCIÓN DE DATOS , por M ^a DE LOS ÁNGELES FERNÁNDEZ SCAGLIUSI, SARA LORENZO CABRERA, JUAN PABLO MURGA FERNÁNDEZ Y ADRIÁN PALMA ORTIGOSA	275
1. Sanitaria, farmacéutica e investigación	275
1.1. Introducción y contexto normativo	275
1.2. Los principios del tratamiento en el ámbito sanitario	277
1.3. Los derechos de los interesados. Los pacientes	278
1.4. Investigación	279
2. Solvencia patrimonial	281
2.1. Importancia de la materia y conceptos introductorios	281
2.2. Características de los SIC en España y marco normativo	283
2.3. Régimen jurídico vigente de la CIRBE y los SIC privados	283
2.3.1. Régimen jurídico de la CIRBE: la Ley 44/2002	284
2.3.2. Régimen jurídico de los SIC privados	285
2.4. Régimen jurídico venidero de los SIC privados: art. 20 PLOPD	289
3. Telecomunicaciones	290
4. Videovigilancia	292
4.1. Introducción y contexto normativo	292
4.2. La videovigilancia y el derecho a la protección de datos	293
4.2.1. Ámbito de aplicación	293
4.2.2. Requisitos generales aplicables al tratamiento de datos basado en técnicas de videovigilancia	294
4.2.3. Derechos de los interesados. Especial referencia al derecho/deber de información	296
4.2.4. Cancelación/Supresión de las imágenes	298
4.2.5. Partes implicadas en la videovigilancia	298
4.2.6. Uso de la videovigilancia en el lugar de trabajo	298
5. Seguros	300
5.1. Consideraciones previas	300
5.2. Corredores o mediadores de seguros	300

5.3. Agentes de seguros y colaboradores externos	302
5.4. Entidades aseguradoras en la Ley 20/2015, de 14 de julio de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras	303
5.5. Breve apunte de la instrucción 2/1995, de 4 de mayo de la AEPD sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo bancario o personal	305
6. Publicidad	305
CAPÍTULO 13. NORMATIVA ESPAÑOLA CON IMPLICACIONES EN PROTECCIÓN DE DATOS, por CARLOS TRUJILLO CABRERA, M^a DE LOS ÁNGELES FERNÁNDEZ SCAGLIUSI, SARA LORENZO CABRERA.....	313
1. LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico	313
2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones	315
3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica	315
CAPÍTULO 14. NORMATIVA EUROPEA CON IMPLICACIONES EN PROTECCIÓN DE DATOS, por ADRIÁN PALMA ORTIGOSA Y SALVADOR TOMÁS TOMAS	317
1. La Directiva e-Privacy	317
1.1. Introducción y contexto normativo	317
1.2. Análisis legal: Directiva e-Privacy.....	319
2. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo	322
2.1. Objeto y ámbito de aplicación de la Directiva	322
2.2. Principios relativos al tratamiento y plazos de conservación y revisión.....	324
2.3. Categorías de interesados	325
2.4. Distinción entre datos personales y verificación de la calidad de los datos personales	325
2.5. Licitud del tratamiento y consentimiento del interesado	326
2.6. Condiciones de tratamiento específicas, tratamiento de categorías especiales de datos personas y mecanismo de decisión individual automatizado	326
2.7. Derechos de los interesados	328
2.7.1. <i>Comunicación y modalidades del ejercicio de los derechos de los interesados</i>	<i>328</i>
2.7.2. <i>Información a disposición del interesado, derecho de acceso y limitaciones</i>	<i>328</i>

2.7.3.	<i>Derecho de rectificación o supresión de datos personales y limitación de su tratamiento</i>	330
2.7.4.	<i>Ejercicio de los derechos del interesado, comprobación por la autoridad de control y derechos en investigaciones y procesos penales</i>	330
2.8.	Responsable del tratamiento y encargado del tratamiento	331
2.8.1.	<i>Obligaciones generales</i>	331
2.8.1.1	Obligaciones del responsable del tratamiento, protección de datos desde el diseño y por defecto y corresponsable del tratamiento.....	331
2.8.1.2.	Encargado y tratamiento bajo la autoridad del responsable o del encargado	331
2.8.1.3.	Registro de las actividades de tratamiento y registro de operaciones	331
2.8.1.4.	Cooperación con la autoridad de control, evaluación de impacto relativa a la protección de datos y consulta previa.....	332
2.9.	Seguridad de los datos personales	333
2.9.1.	<i>Seguridad del tratamiento</i>	333
2.9.2.	<i>Notificación a la autoridad de control de una violación de la seguridad de los datos personales y su comunicación al interesado</i>	334
2.10.	Delegado de protección de datos	334
2.11.	Transferencias de datos personales a terceros países u organizaciones internacionales.....	335
2.11.1.	<i>Principios generales de las transferencias de datos personales</i>	335
2.11.2.	<i>Transferencias basadas en una decisión de adecuación y transferencias mediante garantías apropiadas</i>	336
2.11.3.	<i>Excepciones para situaciones específicas</i>	337
2.11.4.	<i>Transferencias de datos personales a destinatarios establecidos en terceros países</i>	337
2.11.5.	<i>Cooperación internacional en el ámbito de la protección de datos personales</i>	338
2.12.	Autoridades de control independientes.....	339
2.12.1.	<i>Independencia, condiciones generales aplicables a sus miembros y normas relativas a su establecimiento</i>	339
2.12.2.	<i>Competencia, funciones y poderes</i>	339
2.13.	Cooperación	341
2.14.	Recursos, responsabilidad y sanciones	341
2.14.1.	<i>Derecho a presentar una reclamación ante una autoridad de control</i>	341
2.14.2.	<i>Derecho a la tutela judicial efectiva</i>	341
2.14.3.	<i>Representación de los interesados, derecho a indemnización y sanciones</i>	342

2.15. Actos de ejecución.....	342
2.16. Disposiciones finales.....	342
2.16.1. Derogación de la Decisión Marco 2008/977/JAI.....	343
2.16.2. Actos jurídicos de la Unión en vigor y relación con acuerdos internacionales celebrados con anterioridad en el ámbito de la cooperación en materia penal y de la cooperación policial.....	343
2.16.3. Trasposición y entrada en vigor.....	344
DOMINIO II. RESPONSABILIDAD ACTIVA	347
CAPÍTULO 1. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS TRATAMIENTOS DE DATOS PERSONALES, por DIEGO DE LA PRADA ESPINA.....	349
1. Introducción. Marco General de la evaluación y gestión de riesgos. Conceptos generales.....	349
2. Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración de amenazas.....	353
2.1. Inventario de activos.....	354
2.2. Valoración de activos (Para este apartado y saber más consultar Magerit).....	355
2.2.1. Dimensiones.....	356
2.2.2. Valoración de los activos.....	356
2.2.3. Valoración cualitativa.....	357
2.2.4. Valoración cuantitativa.....	358
2.2.5. El valor de la interrupción del servicio.....	358
2.3. Identificación y valoración de amenazas.....	358
2.4. Identificación de vulnerabilidades.....	360
2.5. Impacto.....	360
3. Riesgo por amenaza del activo.....	360
4. Valores especiales globales de ajuste de resultados.....	361
4.1. Identificación de las amenazas.....	362
4.2. Valoración de las amenazas.....	362
4.3. Determinación del impacto potencial.....	363
4.4. Impacto acumulado.....	363
4.5. Impacto repercutido.....	364
4.6. Agregación de valores de impacto.....	364
5. Determinación del riesgo potencial.....	365
6. Gestión del riesgo.....	366
6.1. Salvaguardas.....	366
6.2. Efecto de las salvaguardas.....	366
6.3. Tipo de protección.....	366
7. Catálogo de salvaguardas.....	368
7.1. Protecciones generales u horizontales.....	369
7.2. Protección de los datos / información.....	369
7.3. Protección de las claves criptográficas.....	369
7.4. Protección de los servicios.....	369

7.5. Protección de las aplicaciones (software)	370
7.6. Protección de equipos (hardware)	370
7.7. Protección de las comunicaciones	370
7.8. Protección en los puntos de interconexión con otros sistemas	371
7.9. Protección de los soportes de información	371
7.10. Protección de los elementos auxiliares	371
7.11. Seguridad física – Protección de las instalaciones	371
7.12. Salvaguardas relativas al personal	371
7.13. Salvaguardas de tipo organizativo	372
7.14. Continuidad de operaciones	372
7.15. Externalización	372
7.16. Adquisición y desarrollo	372
8. Gestión del Riesgo Residual	373
8.1. Riesgo residual	373
CAPÍTULO 2. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS, por	
DIEGO DE LA PRADA ESPINA	375
1. Introducción, marco general de la evaluación y gestión de riesgos.	
Conceptos generales.....	376
2. ¿Qué nos aporta un análisis de riesgos?	376
3. Antecedentes	376
3.1. ISO 3100-2009. Gestión de riesgos, principios y guías.....	377
3.2. UNE-ISO; 27001-2013/IEC. Sistemas de gestión para la seguridad de la información (SGSI).....	378
4. Metodologías.....	378
4.1. Metodología Prest.....	378
4.2. Método Mosler (Método Navarrete) Siguiendo a Juan Francisco Gómez Velasco)	379
4.3. MAGERIT.3.....	380
4.4. Guía de Análisis de Riesgos de la Agencia Española de Protección de Datos Personales	381
CAPÍTULO 3. PROGRAMA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS Y	
SEGURIDAD EN UNA ORGANIZACIÓN, por DIEGO DE LA PRADA ESPINA ...	385
1. El diseño y la implantación del programa de protección de datos en una organización	385
1.1. Introducción.....	385
1.2. Diseño de un programa o política de protección de datos	386
1.2.1.Llevar un registro de las actividades de tratamiento.....	387
1.2.2.Realizar una Evaluación de Impacto en la Protección de Datos personales	387
1.2.3.Incrementar la transparencia	387
1.2.4.Aplicar los principios de Privacidad desde el diseño y por defecto	387
1.2.5.Designar un Delegado de Protección de Datos.....	388

1.2.6. Notificar las violaciones de seguridad de los datos que se produzcan a la autoridad competente e interesados	388
1.2.7. La evidencia del cumplimiento	390
2. Objetivos del programa de cumplimiento	391
3. Accountability: la trazabilidad del modelo de cumplimiento	391
3.1. Definición, nociones generales	391
3.2. Modelo de listado de documentos en vigor	394
3.3. Elaboración de documentos para gestionar y evidenciar el cumplimiento	395
CAPÍTULO 4. SEGURIDAD DE LA INFORMACIÓN, por M^a CARMEN ROMERO TERNERO.....	401
1. Seguridad de la información	401
2. Marco normativo.....	405
2.1. Directiva NIS	406
2.1.1. <i>Ámbito de aplicación</i>	408
2.1.2. <i>Objetivos</i>	409
2.1.3. <i>Elementos principales</i>	410
2.1.4. <i>Principios</i>	416
2.1.5. <i>Requisitos mínimos</i>	417
2.2. Esquema Nacional de Seguridad	421
2.2.1. <i>Ámbito de aplicación</i>	423
2.2.2. <i>Objetivos</i>	424
2.2.3. <i>Elementos principales</i>	424
2.2.4. <i>Principios básicos</i>	430
2.2.5. <i>Requisitos mínimos</i>	430
3. Ciberseguridad y gobierno de la seguridad de la información.....	440
3.1. Generalidades.....	442
3.2. Misión.....	444
3.3. Gobierno efectivo de la Seguridad de la Información	444
3.4. Conceptos de Seguridad de la Información	447
3.5. Alcance	451
3.6. Métricas del gobierno de la Seguridad de la Información	452
3.7. Estado de la Seguridad de la Información	453
3.8. Estrategia de Seguridad de la Información	455
4. Puesta en práctica de la seguridad de la información	458
4.1. Seguridad desde el diseño y por defecto.....	460
4.2. El ciclo de vida de los Sistemas de Información	461
4.3. Integración de la seguridad y la privacidad en el ciclo de vida	468
4.4. El control de calidad de los Sistemas de Información	470
CAPÍTULO 5. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS “EIPD”, por DIEGO DE LA PRADA ESPINA	477
1. Introducción y fundamento de las “EIPD”: origen, concepto y característica de las “EIPD”. Alcance y necesidad	477

1.1. Introducción y origen.....	477
1.2. Fundamento de las EIDP	478
1.3. Concepto y características de las EIPD	481
1.4. Alcance y necesidad.....	482
2. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, desarrollo de la evaluación y consultas	483
2.1. Aspectos preparatorios y organizativos	483
2.2. Realización de la EIPD y consultas previas.....	487
2.2.1. Contexto.....	489
2.2.2. Gestión de riesgos	493
2.2.3. Conclusión.....	498
2.2.4. Comunicación y consulta a la Agencia Española de Protección de Datos.....	500
2.2.5. Supervisión y revisión de la implantación.....	500
DOMINIO III. TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS.....	503
CAPÍTULO 1. LA AUDITORÍA DE PROTECCIÓN DE DATOS, por DIEGO DE LA PRADA ESPINA	505
1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la auditoría.....	505
1.1. Cuestiones generales. Aproximación a la auditoría.....	505
1.2. Características básicas de la auditoría	509
2. Elaboración del informe de auditoría: aspectos básicos e importancia del informe de auditoría	511
3. Ejecución y seguimiento de acciones correctoras	517
CAPÍTULO 2. AUDITORÍA DE SISTEMAS DE INFORMACIÓN, por DIEGO DE LA PRADA ESPINA.....	529
1. La función de la auditoría en los Sistemas de Información. Conceptos básicos. Estándares y directrices de auditoría de sistemas de información	529
1.1. Conceptos básicos.....	529
1.2. Estándares.....	532
1.3. Directrices de la auditoría del Sistema de Información.....	533
2. Control interno y mejora continua	535
3. Buenas prácticas e integración de la auditoría de protección de datos en la auditoría del SGSI	539
3.1. Obligación de secreto.....	541
3.2. Política de Control de acceso a datos.....	542
3.3. Equipo de usuario desatendido	544
3.4. Puesto despejado y pantalla limpia.....	544
3.5. Uso de los recursos	544
3.6. Soportes	545

3.7. Incidencias	546
3.8. Puesto de trabajo	546
3.9. Confidencialidad	546
3.10. Ordenadores portátiles y teletrabajo	546
4. Planificación, ejecución y seguimiento	547
4.1. Planificación.....	547
4.2. Implementación de programa de auditoría	549
4.3. Preparación de las actividades de la auditoría	549
4.4. Realización de actividades de auditoría.....	551
4.5. Preparación y distribución del informe de la auditoría.....	552
4.6. Auditoría de seguimiento.....	553
CAPÍTULO 3. LA GESTIÓN DE LA SEGURIDAD DE LOS TRATAMIENTOS, por DIEGO DE LA PRADA ESPINA	555
1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/ IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información	555
2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los pro- cedimientos. Seguridad aplicada a las TI y la documentación	558
3. Recuperación de desastres y continuidad del negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la re- cuperación del desastre.....	562
3.1. Objeto y ámbito de aplicación	562
3.2. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.....	564
3.3. Pruebas de mantenimiento y evaluación de los planes de continui- dad del negocio	564
3.4. Contenido de un Plan de Continuidad	565
3.5. Eventos catastróficos.....	569
3.5.1. <i>Eventos catastróficos que afectan a la seguridad física de</i> <i>los equipos.....</i>	<i>569</i>
3.5.2. <i>Eventos catastróficos que afectan a la seguridad física de</i> <i>los soportes.....</i>	<i>569</i>
3.5.3. <i>Eventos catastróficos que afectan a la seguridad del soft-</i> <i>ware</i>	<i>570</i>
CAPÍTULO 4. OTROS CONOCIMIENTOS, por M^a CARMEN ROMERO TERNERO	571
1. El <i>cloud computing</i> o la computación en la nube	571
2. Los <i>Smartphones</i>	572
3. Internet de las cosas (IoT)	574
4. <i>Big data</i> y elaboración de perfiles	576
5. Redes sociales	577
6. Tecnologías de seguimiento de usuario	578
7. <i>Blockchain</i> y últimas tecnologías	580