

# Índice

## PRÓLOGO

La cualificación del delegado de protección de datos personales .	43
---	----

## NORMATIVA GENERAL DE PROTECCIÓN DE DATOS

### CAPÍTULO 1.1

Contexto normativo.....	51
1.1.1. Privacidad y protección de datos en el panorama internacional	51
Antecedentes .....	51
El Modelo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).....	51
El modelo europeo/useño.....	52
Normativa .....	53
1.1.2. La protección de datos en Europa .....	54
Convenio Europeo de Derechos Humanos .....	54
Convenio 108.....	54
Directiva 95/46/CE.....	55
Principios. ....	55
Comité Europeo de Protección de Datos .....	57
Reglamento Europeo de Protección de Datos .....	58
Principios esenciales.....	58
1.1.3. La protección de datos en España.....	58

LORTAD 1992 .....	59
LOPD 1999.....	59
Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de Los Derechos Digitales (LOPD-GDD).....	60
1.1.4. Estándares y buenas prácticas.....	61

### CAPÍTULO 1.2

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Fundamentos.....	63
1.2.1. Ámbito de Aplicación.....	63
Ámbito Material.....	63
Ámbito Territorial .....	64
1.2.1 (bis). Ámbito de Aplicación LOPD-GDD.....	65
1.2.2. Definiciones.....	66
Nuevas Definiciones RGPD.....	67
1.2.3. Sujetos obligados.....	71
Personas Físicas .....	71
Personas Jurídicas.....	71
Autoridades Públicas .....	71

### CAPÍTULO 1.3

El Reglamento Europeo de Protección De Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Principios.....	73
1.3.1. El binomio derecho/deber en la protección de datos.....	73
RGPD .....	73
LOPD-GDD .....	74
1.3.2. Licitud del tratamiento.....	74

Consentimiento .....	74
Ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.....	75
Cumplimiento de una obligación legal aplicable al Responsable del tratamiento .....	76
Protección de intereses vitales del interesado o de otra persona física.....	76
Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al Responsable de tratamiento .....	77
Interés legítimo.....	78
1.3.3. Lealtad y transparencia .....	80
Principio de Lealtad.....	80
Principio de Transparencia.....	81
1.3.4. Limitación de la finalidad. ....	81
1.3.5. Exactitud.....	82
1.3.6. Integridad y confidencialidad.....	83

**CAPÍTULO 1.4**

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Legitimación .....	85
1.4.1. El consentimiento: otorgamiento y revocación. ....	85
Concepto y definición.....	85
Obtención del consentimiento mediante una declaración .....	86
Obtención del consentimiento mediante una clara acción afirmativa .....	86
Revocación o retirada del consentimiento.....	87
Prueba.....	87
Validez en el contexto de declaración escrita que también se refiera a otros asuntos.....	88

1.4.2. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado .....	88
1.4.3. Consentimiento de los niños.....	89
Ámbito de protección .....	89
Parámetro de la edad.....	89
Norma española .....	90
Modo de informar .....	90
Verificación de la edad .....	90
1.4.4. Categorías especiales de datos.....	92
Enumeración .....	92
Datos genéticos.....	92
Datos relativos a la salud. ....	93
Datos biométricos. ....	93
Actos de violencia de género. ....	93
Datos de infracciones y condenas penales.....	94
Prohibición de tratamiento .....	94
Excepciones a la prohibición para el tratamiento.....	94
Consentimiento explícito. ....	94
Cumplimiento de obligaciones.....	95
Intereses vitales.....	95
Fundación o Asociación. ....	95
Datos públicos.....	95
Reclamaciones.....	96
Interés público esencial.....	96
Medicina. ....	96
Salud Pública.....	96
Investigación científica. ....	97
Margen de maniobra legislativo a nivel nacional.....	97
1.4.5. Datos relativos a infracciones y condenas penales. ....	97
Limitaciones .....	97

Exclusión .....	98
Infracciones administrativas.....	99
Regulación específica del legislador español.....	99
1.4.6. Tratamiento que no requiere identificación.....	99
1.4.7. Bases jurídicas distintas del consentimiento.....	100
<b>CAPÍTULO 1.5</b>	
Derechos de los individuos.....	101
1.5.1. Transparencia e información.....	101
Aspectos comunes al procedimiento de ejercicio de derechos de los interesados .....	102
Facilidad.....	102
Gratuidad.....	102
Independencia.....	102
Información.....	102
Colaboración.....	103
Plazo .....	103
Negativa.....	103
Subsanación.....	103
Prueba.....	103
Concisión.....	104
Comprensión.....	104
Menores.....	104
Iconos.....	104
Información .....	104
Información que deberá facilitarse en todo caso.....	104
Información que deberá facilitarse si se dan determina- dos supuestos de hecho .....	105
Momento en que se ha de informar al interesado .....	105
Supuestos en los que no es preciso informar.....	106
Como informar a los interesados.....	106

Información por Capas.....	107
Información Adicional.....	108
1.5.2. Acceso, rectificación, supresión (olvido).....	108
Acceso.....	108
Definición.....	108
Información que comprende el derecho de acceso.....	108
Formas de acceso.....	109
Rectificación .....	110
Definición.....	110
Supresión (Olvido) .....	111
Definición.....	111
Requisitos.....	111
Exclusiones.....	112
Derechos LOPD-GDD .....	113
Derecho al olvido en búsquedas de Internet (LOPD-GDD).....	113
Derecho al olvido en servicios de redes sociales y servicios equivalentes.....	113
1.5.3. Oposición.....	114
Información .....	114
Interés legítimo cumplimiento de un deber .....	114
Mercadotecnia directa.....	115
Investigación científica o histórica o fines estadísticos .....	115
1.5.4. Decisiones individuales automatizadas.....	115
Definición .....	115
Excepciones .....	116
1.5.5. Portabilidad.....	116
Definición .....	116
Supuestos exclusivos .....	117
Aspectos técnicos y formato.....	117

LOPD-GDD .....	117
1.5.6. Limitación del tratamiento.....	117
Definición.....	117
Supuestos.....	118
Impugnación.....	118
Tratamiento ilícito.....	118
Reclamaciones.....	118
Oposición.....	118
1.5.7. Excepciones a los derechos.....	119
Materias que pueden limitarse .....	119
Limitaciones RGPD.....	120
Arte y periodismo.....	120
Interés público.....	120

**CAPÍTULO 1.6**

El Reglamento Europeo de Protección de Datos y la Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Medidas de cumplimiento .....	121
1.6.1. Las políticas de protección de datos.....	121
Programa de cumplimiento normativo de protección de datos y privacidad.....	121
Sistemas de Gestión de Seguridad de la Información (SGSI) ..	122
1.6.2. Posición jurídica de los intervinientes. Responsables, <i>Corresponsables</i> , Encargados, Encargado del tratamiento y sus representantes. Relaciones entre ellos y formalización.....	123
Responsable del Tratamiento .....	123
Corresponsable .....	124
Encargado de tratamiento.....	124
Especialidades Sector Público.....	125
Deber de diligencia <i>in eligendo</i> e <i>in vigilando</i> del Responsable en la elección del Encargado y en supervisar su cumplimiento .	126

Posibilidad del Encargado de subcontratar .....	126
Necesidad de formalización de un contrato u otro acto jurídico .....	126
Proveedores con acceso a instalaciones, pero que no requieren realizar un tratamiento de datos. Prestadores de servicios sin acceso a datos.....	126
Representante de Responsables o Encargados no establecidos en la Unión Europea.....	127
Otras figuras recogidas en el ENS .....	128
Responsable de la información.....	128
Responsable del servicio.....	128
Responsable de la seguridad.....	128
Responsable del sistema .....	129
Formalización de la relación entre los diferentes actores. Responsables y Encargados del tratamiento .....	129
Forma .....	129
Contenido.....	130
Cláusulas contractuales tipo.....	131
Plazo para formalizar la relación con los Encargados del tratamiento.....	131
1.6.3. El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.....	132
Excepciones .....	132
Contenido.....	133
RAT Responsables de tratamiento.....	133
RAT Encargados y Representante .....	134

## CAPÍTULO 1.7

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Responsabilidad proactiva.....	135
1.7.1. Privacidad desde el diseño y por defecto. Principios fundamentales.....	135

Legitimación de la PbD.....	135
Los siete principios de la PbD .....	136
Respeto por el individuo.....	136
Suma positiva (sostenibilidad del proyecto).....	136
Proactivo no reactivo / preventivo no correctivo.....	136
Privacidad por defecto.....	137
Privacidad embebida en el diseño.....	137
Visibilidad y transparencia.....	137
Sujetos obligados a la protección de datos desde el diseño.....	137
Objetivos de privacidad y seguridad.....	138
Desvinculación (Unlinkability).....	138
Transparencia (Transparency).....	138
Control (Intervenability).....	138
Seguridad, extremo a extremo (end to end).....	139
Ingeniería en privacidad.....	139
Estrategias orientadas al tratamiento de los datos.....	140
Estrategias orientadas a los procesos .....	142
Patrones de diseño de la privacidad.....	146
Privacy enhancing technologies (PETs).....	147
1.7.2. Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo.....	149
Concepto .....	149
Supuestos RGPD .....	149
Listas Autoridades de Control.....	150
Lista positiva AEPD (6 de mayo de 2019) .....	150
Lista negativa AEPD (9 de septiembre de 2019) .....	152
Elementos/Fases de la EIPD .....	154
Ciclo de vida del dato.....	154
Análisis de la necesidad y proporcionalidad del tratamiento.....	154
Gestión de Riesgos.....	156

Identificación del riesgo.....	156
Análisis del riesgo.....	157
Cálculo del Riesgo.....	159
Evaluación del Riesgo.....	160
Informe EIPD .....	161
Contenido mínimo.....	161
Deber de Consulta .....	162
Supervisión y revisión de la EIPD .....	162
Supervisión.....	162
Revisión.....	162
1.7.3. Las violaciones de la seguridad. Notificación de violaciones de seguridad.....	163
Contexto Normativo.....	163
Privacidad.....	163
Seguridad de la información en el sector público.....	164
Infraestructuras críticas. ....	164
Actores adicionales.....	164
Evento, incidente y brecha .....	165
Definiciones. ....	165
Requisitos ENS.....	165
Taxonomía de amenazas.....	167
Valoración de incidentes.....	168
Detección y recogida de información para la valoración..	168
Proceso de gestión de incidentes .....	170
Fase de Preparar y Planificar.....	170
Investigación, comunicación y coordinación de los medios internos/externos implicados. ....	171
Puesta en marcha del plan de respuesta.....	171
Puesta en marcha del proceso de notificación.....	171
Estudio y activación de las posibles medidas a adoptar....	172
Proceso de Respuesta .....	172

Contención.....	172
Solución.....	172
Recuperación.....	173
Notificación a la Autoridad de Control.....	173
Notificación a los interesados. ....	173
Seguimiento y cierre .....	173
1.7.4. El Delegado de Protección de Datos (DPD). Marco normativo.	174

**CAPÍTULO 1.8**

El Reglamento Europeo de Protección de Datos. Delegados de Protección de Datos (DPD, DPO, o Data Privacy Officer).....	175
1.8.1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses .....	175
Supuestos de nombramiento obligatorio RGPD.....	175
Autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial. ....	175
Sector Privado. ....	176
Supuestos de nombramiento obligatorio LOPD-GDD.....	178
DPD en el Encargado del tratamiento .....	179
Supuestos especiales de nombramiento de DPD.....	180
Grupo de Empresas.....	180
Autoridades u organismos públicos.....	180
Asociaciones y colectivos.....	181
Supuestos de designación voluntaria de DPD .....	181
La contratación externa del DPD.....	181
DPD unipersonal o colectivo.....	181
Notificación.....	182
Despido o sanción por realizar tareas de DPD.....	182
Compatibilidad con otras funciones. Análisis de conflicto de intereses .....	183

1.8.2. Obligaciones y responsabilidades. Independencia. Identificación y reporte a la dirección .....	184
Independencia.....	184
Obligaciones .....	184
Deber de secreto.....	184
Responsabilidad.....	185
1.8.3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones.....	185
Aspectos generales .....	185
Funciones del DPD (RGPD) .....	186
Interpretación de la AEPD .....	187
Funciones adicionales del DPD según la LOPD-GDD: Gestión de reclamaciones.....	188
1.8.4. Comunicación con la autoridad de protección de datos.....	189
Comunicación con la autoridad de protección de datos.....	189
1.8.5. Competencia profesional. Negociación. Comunicación. Presupuestos. ....	190
1.8.6. Formación.....	191
1.8.7. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.....	191

## CAPÍTULO 1.9

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Transferencias internacionales de datos .....	193
1.9.1. El sistema de decisiones de adecuación.....	193
Introducción a las transferencias internacionales de datos .....	193
El sistema de decisiones de adecuación.....	194
Criterios para la decisión.....	194
Revisión.....	195

Decisiones de adecuación vigentes.....	196
Sentencia del TJUE (16/07/2020) asunto C-311/18. ....	196
1.9.2. Transferencias mediante garantías adecuadas.....	197
Definición.....	197
Garantías adecuadas que NO requieren autorización .....	197
Garantías adecuadas que SÍ requieren autorización .....	198
1.9.3. Normas corporativas vinculantes.....	198
Definición .....	198
Requisitos .....	199
1.9.4. Excepciones.....	200
Definición.....	200
Excepciones .....	201
Interés legítimo Imperioso.....	202
1.9.5. Autorización de la autoridad de control.....	203
Aplicación del Mecanismo de Coherencia.....	203
Autorización bajo la LOPD-GDD .....	204
1.9.6. Suspensión temporal.....	205
1.9.7. Cláusulas contractuales. ....	205

**CAPÍTULO 1.10**

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Autoridades de control.....	207
1.10.1. Autoridades de Control.....	207
Independencia.....	207
Garantías formales. ....	208
Garantías materiales.....	209
Funciones.....	210
Funciones que afectan al interesado .....	210

Funciones que afectan al Responsable y al Encargado del tratamiento.....	210
Funciones que afectan a las garantías de cumplimiento...	211
1.10.2. Potestades.....	211
Poderes de investigación .....	211
Potestades de regulación. Circulares de la AEPD .....	213
Poderes correctivos.....	214
Poderes de autorización y consultivos .....	215
Autoridades de Control Autonómicas .....	215
Poderes y funciones. ....	215
Deber de cooperación institucional. ....	216
Tratamientos contrarios al RGPD.....	217
Comunicaciones entre las autoridades autonómicas de protección de datos y el Comité Europeo de Protección de Datos.....	217
Tratamientos transfronterizos.....	217
1.10.3. Régimen sancionador.....	218
Sujetos Responsables .....	218
Infracciones-Tipicidad.....	218
Catálogo de infracciones.....	218
Interrupción de la prescripción de la infracción. ....	219
Sanciones y Medidas correctivas .....	219
Sanciones.....	219
Criterios de graduación.....	220
Medidas correctivas .....	221
Publicidad de las Sanciones .....	221
Régimen aplicable a determinadas categorías de Responsables o Encargados del tratamiento .....	222
Prescripción de las sanciones.....	224
1.10.4. Comité Europeo de Protección de Datos.....	224
Orígenes y naturaleza jurídica.....	224

Composición del Comité.....	225
Independencia.....	225
Funciones.....	226
Cooperación internacional sobre protección de datos personales.....	229
Conceptos.....	229
Procedimiento de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.....	230
Procedimiento de Operaciones conjuntas de las autoridades de control.....	232
Cooperación entre la autoridad supervisora europea y las demás autoridades supervisoras interesadas.....	233
Dictamen del Comité.....	233
Resolución de conflictos por el Comité.....	235
Plazos y mayorías para tomar la decisión por parte del Comité.....	236
Notificaciones al Responsable o al Encargado y a los interesados.....	237
Procedimiento de Urgencia.....	237
Solicitud de dictamen urgente o decisión vinculante.....	238
Plazo de adopción de los dictámenes urgentes o decisiones vinculantes.....	238
Asistencia mutua.....	238
1.10.5. Procedimientos seguidos por la AEPD.....	240
Procedimientos en caso de posible vulneración de la normativa de protección de datos.....	240
Forma de iniciación y duración.....	240
Falta de atención de una solicitud de ejercicio de los derechos.....	240
Determinación de la posible existencia de una infracción.....	240
Plazo de caducidad.....	241
Suspensión del procedimiento.....	241

Admisión a trámite de las reclamaciones .....	241
Causas de inadmisión.....	241
Tramitación de la admisión.....	242
Decisión sobre la admisión.....	242
Determinación del alcance territorial.....	243
Actuaciones previas de investigación.....	244
Acuerdo de inicio del Procedimiento para el ejercicio de la potestad sancionadora .....	244
Medidas provisionales y de garantía de los derechos.....	245
1.10.6. La tutela jurisdiccional.....	246
Derecho a la tutela judicial efectiva frente Responsables y Encargados .....	246
Representación de los interesados.....	246
Competencia.....	247
Suspensión de procedimientos .....	247
1.10.7. El Derecho de indemnización.....	248
Responsable .....	248
Encargado.....	248
Inversión de la carga de la prueba .....	248
Corresponsabilidad .....	248
Competencia.....	249
<b>CAPÍTULO 1.11</b>	
Directrices de interpretación del RGPD .....	251
1.11.1. Guías del GT29.....	251
1.11.2. Opiniones del Comité Europeo de Protección de Datos .....	251
Capacidad de emitir dictámenes .....	251
1.11.3. Criterios de órganos jurisdiccionales.....	252
La sentencia Google Spain (C-131/12).....	253
La sentencia Schrems I (C-362/14).....	253

La sentencia Tele2 Serie (C-203/15 y C-698/15).....	253
La sentencia Schrems II (C-311/18) .....	253
La sentencia Bellacón (C-520/19) .....	253
<b>CAPÍTULO 1.12</b>	
Normativas sectoriales afectadas por la protección de datos.....	255
1.12.1. Sanitaria, Farmacéutica, Investigación.....	255
RGPD .....	255
Datos genéticos. ....	255
Datos de salud.....	256
Salud pública.....	256
Ley 14/1986, de 25 de abril, General de Sanidad .....	257
Ley 33/2011, de 4 de octubre, General de Salud Pública.....	257
Derecho a la intimidad confidencialidad y respeto de la dignidad .....	257
Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.....	258
Derecho a la intimidad.....	258
Consentimiento informado. ....	259
Historia clínica.....	259
Acceso a la Historia clínica. ....	259
Plazos de conservación.....	260
Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.....	260
Ley 14/2007, de 3 de julio, de Investigación biomédica .....	261
Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación .....	262
Otra normativa relacionada.....	262
1.11.2. Protección de los menores.....	262

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.....	262
Medios de comunicación.....	263
No necesidad del consentimiento del menor.....	263
Acogimiento familiar del menor.....	264
Acogimiento residencial.....	265
Ley 54/2007, de 28 de diciembre, de Adopción internacional	265
Sujeción a la legislación.....	265
Limitación de la finalidad.....	265
Transferencia internacional.....	265
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	266
Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia .....	266
Deber de comunicación cualificado.....	266
Formación en materia de derechos, seguridad y responsabilidad digital .....	267
Protocolos de actuación.....	267
Uso seguro y Responsable de Internet.....	267
De la Agencia Española de Protección de Datos.....	267
1.11.3. Solvencia Patrimonial.....	268
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	268
Presunción de licitud.....	268
Corresponsables.....	269
Cuantía.....	270
Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero.....	270
Conservación de los datos.....	270
1.12.4. Telecomunicaciones.....	271
Ley 11/2022, de 28 de junio, General de Telecomunicaciones	271

Intercepción de las comunicaciones.....	271
Medidas técnicas y de gestión a implantar por los operadores.....	271
Derechos de los usuarios finales. ....	273
Con relación a los datos de tráfico y los datos de localización. ....	273
En relación con las guías de abonados.....	274
1.12.5. Videovigilancia.....	274
Regulación .....	275
Ámbito laboral.....	275
Obligaciones.....	276
1.12.6. Seguros.....	278
Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.....	278
1.12.7. Prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Publicidad, etc. ....	279
Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.....	279
Objeto. ....	279
Ámbito de aplicación.....	279
Autoridades competentes. ....	280
Plazos de conservación y revisión.....	280
Distinción entre categorías de interesados.....	281
Verificación de la calidad de los datos personales. ....	281

Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad. ....	282
Régimen disciplinario.....	283
Restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.....	283
Ejercicio de los derechos del interesado a través de la autoridad de protección de datos.....	284
Registro de operaciones.....	285
Transferencias internacionales. Excepciones para situaciones específicas. ....	285
Comunicaciones comerciales por vía electrónica. Publicidad ..	286
Sistemas teóricos.....	286
Sistema del legislador español.....	287
Regla General: Consentimiento expreso.....	287
Información en materia de cookies .....	288
Obligaciones de los Responsables.....	288

### **CAPÍTULO 1.13**

Normativa española con implicaciones en protección de datos ....	291
1.13.1. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.....	291
Ámbito de aplicación y generalidades .....	291
Páginas web.....	291
Ámbito territorial.....	292
Obligaciones de los prestadores de servicios.....	292
1.13.2. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones ...	293
1.13.3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica/Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza....	293
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza .....	293

Funciones.....	294
Firma electrónica avanzada.....	294
Firma electrónica cualificada.....	294
Protección de datos.....	295
1.13.4. Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial.....	296
Objeto.....	296
Ámbito de Aplicación.....	296
Protección de datos personales.....	296
<b>CAPÍTULO 1.14</b>	
Normativa europea con implicaciones en protección de datos.....	299
1.14.1. Directiva <i>e-Privacy</i> : Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.....	299
1.14.2. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE.....	300
Ámbito de aplicación subjetivo y exclusiones objetivas....	300
1.14.3. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 comunicaciones.....	302
Guía de Abonados.....	302
Información.....	302
Información en contratos y transparencia.....	302
1.14.4. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27.....	303

1.14.5. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión .....	304
Definiciones y alcance.....	304
Clasificación de los sistemas de IA como prácticas prohibidas y de alto riesgo de la IA .....	305
Excepciones de aplicación de la ley .....	306
Sistemas de IA de propósito general y modelos básicos.....	306
Transparencia y protección de los derechos fundamentales.....	307
Entrada en vigor .....	307

## RESPONSABILIDAD ACTIVA

### CAPÍTULO 2.1

Análisis y gestión de riesgos de los tratamientos de datos personales.....	311
2.1.1. Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales.....	311
Conceptos Generales .....	312
Alcance, contexto, criterios.....	312
Contexto externo.....	312
Contexto Interno.....	312
Evaluación del riesgo .....	313
Identificación del riesgo.....	313
Análisis del Riesgo. ....	314
Valoración del riesgo.....	314
Tratamiento del riesgo .....	315
Registro e informe.....	315
Comunicación y consulta.....	316
Seguimiento y revisión.....	316

2.1.2. Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante.....	317
Concepto de tratamiento .....	317
Inventario y valoración de activos .....	317
Actividades de tratamiento sobre los datos de carácter personal.....	318
Riesgo de cumplimiento normativo.....	319
Riesgo para los derechos y libertades.....	319
Análisis de riesgo.....	319
Tipos de amenaza contra el flujo de información .....	322
Riesgo Inherente.....	324
Salvaguardas existentes y valoración de su protección.....	326
2.1.3. Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible. ..	327
Conceptos.....	327
Estrategias .....	327
Aceptar.....	327
Evitar.....	328
Reducir.....	328
Transferir.....	328
Riesgo residual, riesgo aceptable y riesgo inasumible .....	328
Puntos de decisión.....	328
Análisis de cumplimiento.....	329
Selección y asignación de salvaguardas a amenazas: valoración de la protección.....	331
NIST Cybersecurity Framework.....	331

**CAPÍTULO 2.2**

Metodologías de análisis y gestión de riesgos .....	333
---	-----

2.2.1. Metodologías de análisis de gestión de riesgos .....	333
2.2.2. MAGERIT V3.....	334
Objetivos.....	334
Metodología/Fases.....	335
Identificación y Valoración de activos relevantes, su interrelación y su valor.....	335
Determinar a qué amenazas están expuestos los activos identificados.....	335
Estimar el riesgo actual.....	335
Obtener el riesgo residual.....	335
Identificación y valoración de activos.....	336
Secuencia de actuaciones.....	336
Identificación y valoración de amenazas .....	338
Identificación.....	338
Valoración.....	338
Determinación del riesgo.....	339
Riesgos acumulados y repercutidos .....	340
Riesgo actual vs residual. Plan de tratamiento.....	341
Eficacia de las medidas de seguridad .....	342
Cálculo del riesgo residual .....	343
2.2.3. Otras metodologías de análisis de riesgos.....	344
Octave Allegro.....	344
Fases.....	344
Pasos .....	345

### CAPÍTULO 2.3

Programa de cumplimiento de protección de datos y seguridad en una organización.....	347
2.3.1. El Diseño y la implantación del programa de protección de datos en el contexto de la organización.....	347

Fase 1: Conocer la situación actual .....	347
Actividades previas.....	347
Análisis de cumplimiento.....	349
2.3.2. Accountability: La trazabilidad del modelo de cumplimiento ..	350
<b>CAPÍTULO 2.4</b>	
Seguridad de la información.....	351
2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS .....	351
Esquema Nacional de Seguridad .....	351
Directiva NIS.....	351
Ámbito de Aplicación. ....	351
Operadores de servicios esenciales.....	352
Proveedores de servicios digitales. ....	352
Objetivos.....	352
Elementos principales. ....	353
Requisitos mínimos.....	354
Seguridad de los sistemas e instalaciones.....	354
Gestión de incidentes.....	354
Gestión de la continuidad de las actividades. ....	355
Supervisión, Auditorías y pruebas, .....	355
Cumplimiento de las normas internacionales.....	355
2.4.2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.....	356
Concepto de Ciberseguridad y de Seguridad de la Información (SI).....	356
Marco ciberseguridad del NIST .....	356
Ámbito de aplicación.....	357
Objetivos.....	357

Elementos principales.....	357
Principios básicos.....	359
Gobierno de la Seguridad de la Información - ISO/IEC 27014:2020.....	360
Ámbito de Aplicación.....	360
Objetivos:.....	361
Elementos principales.....	361
Principios básicos.....	362
Requisitos mínimos.....	364
Métricas del Gobierno de la SI.....	364
Proceso de monitorización en la Norma ISO/IEC 27014/2020.....	364
Tipos de métricas e indicadores.....	364
Métricas e indicadores en el ENS.....	366
Estado de la SI.....	367
Estrategia de SI.....	368
2.4.3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.....	369
El ciclo de vida de los servicios.....	369
Estrategia del Servicio.....	369
Diseño del Servicio.....	369
Transición del Servicio.....	369
Operación del Servicio.....	370
Mejora continua del Servicio.....	370
El ciclo de vida de los sistemas de información.....	370
Fases del ciclo de vida.....	371
Metodologías Ágiles (SCRUM).....	373
Seguridad desde el diseño y por defecto (PBD).....	375
El control de calidad de los SI.....	375

Integración de la Seguridad y la Privacidad en el Ciclo de la Vida .....	376
Metodologías Ágiles en el diseño de un sistema de información.....	377
Intervención del DPO en el diseño del sistema de información.....	378

**CAPÍTULO 2.5**

Evaluación de impacto de protección de datos “EIPD” .....	379
---	-----

**TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS**

**CAPÍTULO 3.1**

La auditoría de protección de datos .....	383
3.1.1. El proceso de Auditoría. Cuestiones generales y aproximación a la Auditoría. Características básicas de la Auditoría.....	383
Conceptos generales ISO 19011:2018 .....	383
Criterios de auditoría. ....	384
Alcance.....	384
Objetivos.....	384
Evidencias objetivas.....	384
Hallazgos de Auditoría.....	385
Limitaciones en el alcance.....	386
Tipos de auditoría.....	387
Auditorías de primera parte.....	387
Auditorías de segunda parte.....	387
Auditorías de tercera parte. ....	387
Elementos .....	387
Programa de Auditoría.....	387
Contacto inicial/Preparación/Revisión documental .....	388

Plan de Auditoría.....	388
Checklist.....	388
Reunión de apertura.....	388
Control / Controles.....	388
Auditor.....	389
Auditoría.....	389
Informe resumen .....	390
Reunión de cierre .....	390
Informe de Auditoría.....	390
Plan de Acciones Correctivas (PAC).....	390
Principios de segregación de funciones.....	390
Evidencia de Auditoría.....	391
Suficiencia de las evidencias .....	391
Clases de Auditorías .....	391
Inicial.....	391
Auditoría de seguimiento.....	393
Auditoría combinada.....	393
Auditoría de sistemas de información.....	394
Auditoría de renovación.....	394
Auditorías extraordinarias.....	395
Marco jurídico .....	395
Características básicas de la Auditoría .....	396
Pre-Auditoría.....	396
Ejecución.....	398
Entrega de resultados.....	398
3.1.2. Elaboración del informe de Auditoría. Aspectos básicos e importancia del informe de Auditoría.....	398
Definición .....	398
3.1.3. Ejecución y seguimiento de acciones correctoras.....	400
Introducción al Plan de Acciones Correctivas (PAC) .....	400

Fases .....	401
Detección.....	401
Análisis causal.....	402
Búsqueda de soluciones.....	402
Acciones de mejora.....	402
Monitorización y reevaluación.....	403
<b>CAPÍTULO 3.2</b>	
Auditoría de sistemas de información.....	405
3.2.1. La Función de la Auditoría en los Sistemas de Información.	
Conceptos básicos. Estándares y Directrices de Auditoría de SI.	405
Concepto .....	405
Consideraciones generales .....	406
Definición del Alcance y objeto de la Auditoría.....	406
Requisitos para el Equipo Auditor. ....	406
Incorporación de expertos técnicos al equipo de Auditoría..	407
Estándares.....	408
ISO 19011.....	410
Buenas prácticas ENS (ANEXO II).....	410
Marco organizativo.....	411
Marco operacional.....	411
Marco de protección de las infraestructuras. ....	411
Buenas prácticas ISO 27002:2022 .....	411
Directrices de Auditoría de SI. (ISACA).....	412
Guía de Seguridad de las TICCCN-STIC 802.....	412
3.2.2. Control interno y mejora continua. Buenas prácticas. Integra- ción de la auditoria de protección de datos en la auditoria de SI.	413
Control Interno .....	413
Elementos. ....	413
Modelo de control interno basado en tres líneas de defensa.....	415

Primera línea.....	415
Segunda línea.....	415
Tercera línea.....	416
3.2.3. Planificación, ejecución y seguimiento.....	416
Planificación de la Auditoría.....	416
Evidencias de Auditoría.....	416
Elaboración y presentación de los hallazgos de la Auditoría.....	418
Presentación del informe de Auditoría.....	419

### CAPÍTULO 3.3

La gestión de la seguridad de los tratamientos.....	421
3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI).....	421
Esquema Nacional de Seguridad.....	421
Objetivos.....	421
Ámbito de aplicación.....	423
Sistemas de información que traten datos personales.....	423
Principios básicos.....	424
La seguridad como un proceso integral.....	425
Gestión de la seguridad basada en los riesgos.....	425
Prevención, detección, respuesta y conservación.....	426
Existencia de líneas de defensa.....	426
Vigilancia continua y reevaluación periódica.....	426
Diferenciación de responsabilidades.....	427
Política de seguridad.....	428
Requisitos mínimos de seguridad.....	429
Capacidad de respuesta a incidentes de seguridad.....	430
ISO/IEC 27001:2022 (UNE ISO/IEC 27001:2014).....	431
Cláusula 4. Contexto.....	431

Cláusula 5. Liderazgo.....	431
Cláusula 6. Planificación.....	432
Tratamiento de los Riesgos.....	433
3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación.....	434
Concepto .....	434
Medidas .....	434
3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.....	435
Elementos del PCN.....	435
Planificación y alcance .....	435
Análisis del Impacto en el Negocio ( <i>Business Impact Analysis-BIA</i> )	436
Respuesta a la contingencia.....	437
Plan de Respuesta a Incidentes. ....	437
Procedimientos Operativos de Recuperación. ....	437
Instrucciones y procedimientos técnicos.....	438
Pruebas, Mantenimiento y Formación.....	438
<b>CAPÍTULO 3.4</b>	
Otros conocimientos.....	439
3.4.1. El cloud computing.....	439
Tecnología .....	439
Características esenciales .....	439
Modalidades de contratación de servicios de cloud computing	440
Requerimientos jurídicos y de seguridad que deben reunir los proveedores .....	441
Aspectos para tener en cuenta. ....	441
Accesos de usuarios con privilegios. ....	422
Localización de los datos.....	422

3.4.2. Los Smartphones.....	422
Tecnología .....	422
Funcionalidades.....	422
Datos que pueden recopilar.....	443
APPS.....	443
Fabricantes de sistemas operativos y de dispositivos .....	444
Tiendas de aplicaciones.....	444
Tratamientos adicionales.....	444
Terceras partes.....	444
Geolocalización.....	445
Riesgos específicos en materia de protección de datos .....	446
3.4.3. Internet de las cosas (IoT).....	447
Tecnología .....	447
Riesgos específicos en materia de protección de datos .....	447
Rastreo.....	447
Elaboración de perfiles.....	447
Seguridad de la IoT .....	448
Retos.....	448
Privacidad de la IoT.....	449
Propuesta de Reglamento de ePrivacy .....	449
3.4.4. Big data y elaboración de perfiles.....	450
Tecnología .....	450
Beneficios de Big Data.....	450
Riesgos.....	451
Anonimización .....	452
Política de anonimización.....	453
Riesgos específicos en materia de protección de datos .....	454
Transparencia.....	454
Base jurídica del tratamiento.....	454
3.4.5. Redes sociales.....	456

Tecnología .....	456
Transferencias internacionales y ámbito de aplicación. ....	456
Terceras partes .....	457
Usuarios. ....	458
Obligaciones de la red social. ....	459
Tratamiento de categorías especiales de datos. ....	460
Datos de NO miembros de la red social. ....	460
Conservación de los datos. ....	461
3.4.6. Tecnologías de seguimiento de usuario. ....	461
Tecnología .....	461
Funciones. ....	462
Riesgos específicos en materia de protección de datos .....	462
El Marco Revisado .....	463
Recomendaciones. ....	463
Riesgos asociados. ....	464
3.4.7. Blockchain y últimas tecnologías. ....	464
Tecnología .....	464
Riesgos específicos en materia de protección de datos .....	465

## APÉNDICES

### APÉNDICE 1

Especialidades LOGPD-GDD .....	469
A1.1. Ámbito de aplicación de los títulos I a IX y de los artículos 89 a 94 .....	469
Ámbito de aplicación general. ....	469
Exclusiones .....	469
Aplicación subsidiaria .....	469
Poder Judicial y Ministerio Fiscal .....	470
A1.2. Consentimiento de los menores de edad. ....	470

Edad .....	470
Complemento de la capacidad .....	471
A1.3. Datos de las personas fallecidas.....	471
Ejercicio por los causahabientes.....	471
Testamento Digital .....	471
Menores o discapacitados .....	472
A1.4. Categorías especiales de datos.....	472
A1.5. Tratamiento .....	473
A1.6. Sistemas de información crediticia.....	474
A1.7. Tratamientos relacionados con la realización de determinadas operaciones mercantiles.....	476
A1.8. Tratamientos con fines de videovigilancia.....	476
A1.9. Sistemas de exclusión publicitaria .....	478
A1.10. Sistemas de información de denuncias internas. ....	479
A1.11. Tratamiento de datos en el ámbito de la función estadística pública.....	481
A1.12. Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.....	482
A1.13. Tratamiento de datos relativos a infracciones y sanciones ad- ministrativas.....	483
A1.14. Actuaciones de investigación a través de sistemas digitales .....	484
A1.15. Los derechos en la era digital.....	484
A1.16. Derecho a la neutralidad de Internet.....	485
A1.17. Derecho de acceso universal a Internet. ....	485
A1.18. Derecho a la seguridad digital.....	486
A1.19. Derecho a la educación digital. ....	486
A1.20. Derecho de rectificación en Internet.....	487
A1.21. Derecho a la actualización de informaciones en medios de co- municación digitales.....	487

A1.22. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. ....	488
A1.23. Derecho a la desconexión digital en el ámbito laboral.....	489
A1.24. Derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonidos en el lugar de trabajo.....	490
A1.25. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. ....	491
A1.26. Derechos digitales en la negociación colectiva. ....	491
A1.27. Protección de datos de los menores en Internet. ....	492
A1.28. Derecho al olvido en búsquedas de Internet.....	492
A1.29. Derecho al olvido en servicios de redes sociales y servicios equivalentes.....	493
A1.30. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.....	494
A1.31. Derecho al testamento digital. ....	494

**APÉNDICE 2**

Catálogo de infracciones LOPD-GDD.....	497
Faltas Muy Graves LOGPD-GDD (Art. 72).....	497
Prescripción 3 años .....	497
Faltas Graves LOGPD-GDD (Art. 73).....	499
Prescripción 2 años .....	499
Faltas Leves LOGPD-GDD (Art. 74) .....	502
Prescripción 1 años .....	502

**APÉNDICE 3**

Glosario de términos de seguridad (ENS).....	507
--	-----

**APÉNDICE 4**

Controles anexo III del ENS .....	515
-----------------------------------	-----

**APÉNDICE 5**

Controles ISO 27001:2022 .....	519
A5 Controles organizacionales .....	519
A6 Controles personales .....	520
A7 Controles físicos.....	520
A8 Controles tecnológicos.....	520

**APÉNDICE 6**

Amenazas y medidas seguridad gestiona AEPD .....	523
Medidas organizativas .....	523
Medidas técnicas.....	528
Medidas jurídico-organizativas.....	533

**APÉNDICE 7**

Códigos de conducta aprobados bajo la LOPD .....	537
Índice de voces.....	539
Bibliografía .....	553