Abreviaturas 19

Presentación 23

1 Panorama actual y normativa sobre protección de datos personales 25

1.1 Comunitaria ... 27

1.1.1 Convenio de 28 de enero de 1981, del Consejo de Europa, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ... 27

1.1.2 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ... 27

1.1.3 Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones ... 28

1.1.4 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 ... 29

1.1.5 Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativa a la conservación de datos generados o tratados con relación a la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones ... 30

1.1.6 Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ... 30

1.2 Nacional ... 31

1.2.1 Constitución Española, de 27 de diciembre de 1978 ... 31

1.2.2 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal ... 31

1.2.3 Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal ... 32

Página

1.2.4 Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal 32
1.2.5 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 33
1.2.6 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 34
1.2.7 Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico 35
1.2.8 Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones 35
1.2.9 Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios 36
1.2.10 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones 36
1.2.11 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos 37

2 Contenido y principios de la normativa 39

2.1 Definiciones 47
2.1.1 Definiciones de la LOPD 47
2.1.2 **Definiciones del Real Decreto** 1720/2007, de desarrollo de la LOPD 50
2.2 Objeto y ámbito de aplicación 54
2.2.1 Objeto 54
2.2.2 Ámbito Subjetivo 54
2.2.2.1 Personas físicas 54
2.2.2.2 Datos personales de empresarios 55
2.2.3 Ámbito territorial 56
2.2.4 Ficheros excluidos 56
2.2.5 Tratamientos regulados específicamente 57
2.2.6 Cómputo de plazos 57
2.3 Principios de la LOPD 58
2.3.1 **Calidad de los Datos** 58
2.3.1.1 Finalidad 59
2.3.1.2 Utilización no abusiva 59
2.3.1.3 Exactitud 59
2.3.1.4 Lealtad 60
2.3.1.5 Cancelación 60
2.3.1.6 **Tratamiento con fines estadísticos, históricos o científicos** . 60
2.3.2 Deber de **Información** 61
2.3.2.1 Datos recabados del propio interesado 62
2.3.2.2 Datos recabados de terceros 63
2.3.2.3 Acreditación del cumplimiento del deber de información . 63
2.3.2.4 Datos recabados de fuentes accesibles al público 64
2.3.2.5 Deber de información a menores de edad 64
2.3.2.6 Supuestos especiales. Deber de información en casos de reestructuraciones societarias 64
2.3.2.7 Excepciones al deber de información 65
2.3.3 Consentimiento del afectado 66
2.3.3.1 Principios generales. Forma de recabar el consentimiento . 68
2.3.3.2 Tratamiento de datos de menores de edad 70
2.3.3.3 Excepciones 71
2.3.3.4 **Consentimiento en el marco** de una relación contractual para fines no relacionados directamente con la misma 71
2.3.3.5 Consentimiento para el tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas 72
2.3.3.6 Revocación del consentimiento 72
2.3.4 Datos especialmente protegidos 72
2.3.5 Seguridad de los Datos 74
2.3.6 Deber de Secreto 74
2.3.7 Comunicación de los datos 75
2.3.7.1 Comunicación de datos a terceros 75
2.3.7.2 Comunicación de datos **entre** empresas de un mismo Grupo 76
2.3.7.3 Comunicación de datos y el artículo **27** de la LOPD 76
2.3.7.4 Excepciones al consentimiento 77
2.3.7.5 Comunicación de datos disociados 78
2.3.8 Acceso a los datos por cuenta de terceros 78
2.4 Derechos de los interesados 82
2.4.1 Contenido y finalidad de cada derecho. Legislación aplicable 82
2.4.1.1 Derecho de impugnación de valoraciones 82
2.4.1.2 Derecho de consulta al Registro General de Protección de Datos 83
2.4.1.3 Derecho de acceso 83
2.4.1.4 Derecho de rectificación y cancelación 85
2.4.1.5 Derecho de oposición 86
2.4.1.6 Derecho de acceso, rectificación, cancelación y oposición con relación a ficheros de información sobre solvencia patrimonial y crédito 87
2.4.1.7 Derecho de acceso, rectificación, cancelación y oposición con relación a tratamientos para actividades de publicidad y prospección comercial 88
2.4.1.8 Derecho de oposición con relación a tratamientos realizados a través de los motores de búsqueda 89
2.4.1.9 Ejercicio de derechos en los nuevos Servicios de Administración Electrónica 91
2.4.2 Carácter personalísimo y condiciones generales para el ejercicio de los derechos de los interesados 91
2.4.3 Requisitos para el ejercicio de los derechos 92
2.5 Notificación e inscripción registral de ficheros 94
2.5.1 Objetivos de la inscripción de ficheros 94
2.5.1.1 Objetivos perseguidos por la Agencia de Protección de Datos 94
2.5.1.2 Objetivos perseguidos por las Entidades Privadas 94

Página

2.5.1.2.1 Evitar la imposición de sanciones ... 94
2.5.1.2.2 Buena imagen exterior ... 95
2.5.1.2.3 Labores de control interno ... 95
2.5.1.3 Objetivos perseguidos por las Entidades Públicas ... 96
2.5.2 Principios que rigen la inscripción de ficheros ... 96
2.5.3 El Registro General de Protección de Datos ... 97
2.5.3.1 Concepto ... 97
2.5.3.2 Los Registros de Protección de Datos Autonómicos ... 97
2.5.3.3 El derecho de Consulta en el Registro ... 98
2.5.3.4 Actualización de los datos contenidos en el Registro ... 98
2.5.4 Inscripción de ficheros en el Registro ... 99
2.5.4.1 El Procedimiento de inscripción de la creación, modificación o supresión de ficheros ... 100
2.5.4.2 Las inscripciones de ficheros de titularidad privada ... 100
2.5.4.2.1 De creación de ficheros ... 101
2.5.4.2.2 De modificación de ficheros ... 101
2.5.4.2.3 De supresión de ficheros ... 102
2.5.4.3 Las inscripciones de ficheros de titularidad pública ... 103
2.5.4.3.1 Elaboración de las disposiciones generales para la creación, modificación o supresión de ficheros públicos ... 104
2.5.4.3.2 De creación de ficheros ... 105
2.5.4.3.3 De modificación de ficheros ... 105
2.5.4.3.4 De supresión de fichero ... 105
2.6 Movimiento internacional de datos ... 106
2.6.1 Conceptos relevantes ... 106
2.6.1.1 Transferencia Internacional de Datos ... 106
2.6.1.2 Nivel adecuado de protección ... 107
2.6.1.3 Importador de Datos ... 108
2.6.1.4 Exportador de Datos ... 108
2.6.1.5 Establecimiento ... 109
2.6.2 Régimen Jurídico ... 109
2.6.2.1 Directiva 95/46, de 14 de octubre de 1995 ... 109
2.6.2.1.1 La libre circulación de datos personales entre Estados ... 109
2.6.2.1.2 Principios generales ... 109
2.6.2.1.3 Regulación general ... 110
2.6.2.1.4 Excepciones ... 111
2.6.2.2 Reglamento 45/2001, de 18 de diciembre de 2000 ... 112
2.6.2.3 LOPD y su Reglamento de desarrollo ... 113
2.6.2.3.1 Excepciones ... 113
2.6.2.3.2 Transferencia a países que no ofrezcan nivel de protección adecuado ... 114
2.6.2.3.3 Suspensión temporal de las transferencias ... 117
2.6.2.4 La Instrucción 1/2000 de la AEPD. La Sentencia de la AN de 15 de marzo de 2002 y la Sentencia del TS de 25 de septiembre de 2006 ... 118
2.6.2.4.1 Normas de aplicación general ... 120
2.6.2.4.2 Normas de aplicación particular a ciertas transferencias ... 122
2.6.2.5 Las Decisiones de la Comisión relativas a cláusulas contractuales tipo ... 127
2.6.2.5.1 Principios generales comunes a las Decisiones ... 127
2.6.2.5.2 Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001: Cláusulas Contractuales tipo para la Transferencia Internacional de Datos Personales ... 128
2.6.2.5.3 Decisión 2010/87/UE, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo ... 131
2.7 Los Códigos Tipo ... 136
2.7.1 Concepto ... 136
2.7.2 Clasificación de los Códigos Tipo ... 136
2.7.2.1 Acuerdos privados ... 137
2.7.2.2 Estándares de confidencialidad ... 137
2.7.2.3 Sellos de confidencialidad ... 137
2.7.3 Naturaleza y ámbito de aplicación ... 137
2.7.3.1 Contenido del Código Tipo ... 138
2.7.3.2 Garantías del cumplimiento de los Códigos Tipo ... 139
2.7.3.3 Depósito y publicación de los Códigos Tipo ... 140
2.7.3.4 Obligaciones de las entidades promotoras de los Códigos Tipo ... 140
2.7.3.5 Grado de vinculación de los Códigos Tipo ... 140
2.7.4 Procedimiento de inscripción de Códigos Tipo ... 141
2.7.4.1 Iniciación ... 141
2.7.4.2 Tramitación ... 141
2.7.4.3 Resolución ... 142
2.7.4.4 Duración ... 142
2.7.5 Ventajas de la adopción de un Código Tipo ... 142
2.7.6 Algunos Códigos Tipo inscritos en el RGPD ... 143
2.8 El procedimiento sancionador ... 144
2.8.1 Fase de actuaciones previas ... 145
2.8.1.1 Iniciación ... 145
2.8.1.2 Personal competente ... 145
2.8.1.3 Obtención de información ... 146
2.8.1.4 Actuaciones presenciales ... 146
2.8.1.5 Resultado ... 146
2.8.2 Fases de instrucción y resolución ... 147
2.8.3 Recursos contra la resolución sancionadora ... 148
2.8.4 Plazos y caducidad del procedimiento administrativo sancionador, de las infracciones y de las sanciones ... 149
2.8.4.1 «Prescripción» de la acción para sancionar ... 150
2.8.4.2 Caducidad ... 150
2.8.4.3 Prescripción de las infracciones ... 151

Página

2.8.4.4 Prescripción de las sanciones 151
2.8.4.5 Algunos principios del procedimiento sancionador: legalidad, tipicidad, seguridad jurídica, defensa, presunción de inocencia y proporcionalidad 152
2.8.4.5.1 Tipicidad y reserva de ley: referencias jurisprudenciales 152
2.8.4.5.2 Presunción de inocencia: referencias jurisprudenciales 154
2.8.4.5.3 ¿Es necesaria la intencionalidad en la comisión de la infracción? 154
2.8.5 El derecho del interesado a ser indemnizado 154
2.8.6 Repertorio de sentencias de interés sobre Protección de Datos 155
2.8.6.1 **Validez de las Instrucciones de la Agencia Española** de Protección de Datos 155
2.8.6.2 ¿Son datos de carácter personal los relativos a profesionales o autónomos? Sanción existente 155
2.8.6.3 ¿Cuándo se aplica la posible rebaja del art. 45.5 LOPD? Confirmación de Sanción 156
2.8.6.4 Cómputo de la prescripción de las infracciones consistentes en hechos continuados. Mantener datos personales inexactos. Confirmación de sanción 157
2.8.6.5 Facultades del Director de la AEPD de adoptar medidas cautelares para ordenar el cese del tratamiento 157
2.8.6.6 Sanción por infracción del deber de secreto, pese a que el Responsable del Fichero fue «engañado» para la obtención de los datos. Sanción a título de mera o simple inobservancia 158
2.8.6.7 Forma en que ha de figurar el contrato de encargo de tratamiento. Encargo de tratamiento de «Scoring» 158
2.8.6.8 Omisión de trámite de alegaciones en el procedimiento. Generación de indefensión formal y no material que no anula la resolución 159
2.8.6.9 Sanción por obstruir la actividad inspectora 160
2.8.6.10 Sanción por tratar un dato de afiliación política de persona que pública y notoriamente es sabido que pertenece a dicho grupo político, sin consentimiento de dicha persona .. 160
2.8.6.11 Diferenciación entre el responsable del fichero y el responsable del tratamiento. Posición del beneficiario de la publicidad 161
2.8.6.12 Control disciplinario por uso incorrecto del ordenador. Exigencia de determinar previamente que el uso está controlado 162
2.9 Las Medidas de Seguridad en el tratamiento de datos de carácter personal .. 162
2.9.1 El principio de seguridad de la información en materia de datos personales 162
2.9.2 ¿Qué es la Seguridad de la Información? 163
2.9.2.1 Confidencialidad 163
2.9.2.2 Integridad 163
2.9.2.3 Disponibilidad 163
2.9.3 ¿Por qué es importante asegurar la Información? 164
2.9.4 El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 164
2.9.5 Alcance 164
2.9.6 Concepto de medida organizativa 164
2.9.7 Concepto de medida técnica 165
2.9.8 Ámbito de aplicación 165
2.9.8.1. Ficheros automatizados 165
2.9.8.2 Ficheros no automatizados 166
2.9.8.3 Centros de Tratamiento 166
2.9.8.4 Locales 166
2.9.8.5 Equipos 166
2.9.8.6 Sistemas y programas informáticos 166
2.9.8.7 Personas 166
2.9.9 Definiciones 166
2.9.9.1 Sistemas de información 166
2.9.9.2 Usuario 167
2.9.9.3 Recurso 167
2.9.9.4 Accesos autorizados 167
2.9.9.5 Identificación 167
2.9.9.6 Autenticación 167
2.9.9.7 Control de acceso 167
2.9.9.8 Contraseña 168
2.9.9.9 Incidencia 168
2.9.9.10 Soporte 168
2.9.9.11 Responsable de seguridad 168
2.9.9.12 Copia de respaldo 168
2.9.10 Las Medidas de Seguridad. Consideraciones previas 168
2.9.10.1 Nivel básico 169
2.9.10.2 Nivel medio 169
2.9.10.3 Nivel alto 169
2.9.11 Las Medidas de Seguridad comunes 170
2.9.11.1 Encargado del Tratamiento 170
2.9.11.2 Prestaciones de servicios sin acceso a datos personales 171
2.9.11.3 Delegación de autorizaciones 171
2.9.11.4 Régimen de trabajo fuera de los locales del Responsable del Fichero o Encargado del Tratamiento 171
2.9.11.5 Ficheros temporales o copias de trabajo de documentos ... 171
2.9.11.6 Documento de Seguridad 171
2.9.12 Medidas de seguridad aplicables a Ficheros Automatizados 173
2.9.12.1 Nivel básico 173
2.9.12.1.1 Funciones y obligaciones del personal 173
2.9.12.1.2 Registro de incidencias 173
2.9.12.1.3 Control de acceso 174
2.9.12.1.4 Gestión de soportes 176
2.9.12.1.5 Identificación y autenticación 176
2.9.12.1.6 Copias de respaldo y recuperación 177
2.9.12.2 Nivel medio 178
2.9.12.2.1 El Responsable de seguridad 178

Página

2.9.12.2.2 Auditoría 179
2.9.12.2.3 Gestión de soportes 180
2.9.12.2.4 Identificación y autenticación 181
2.9.12.2.5 Control de acceso físico 181
2.9.12.2.6 Registro de incidencias 181
2.9.12.3 Nivel alto 182
2.9.12.3.1 Distribución de soportes 182
2.9.12.3.2 Copias de respaldo y recuperación 182
2.9.12.3.3 Registro de accesos 183
2.9.12.3.4 Transmisión de datos por redes de telecomunicaciones 184
2.9.12.4 Plazos de Implantación de las medidas de seguridad 184
2.9.13 Medidas de seguridad aplicables a Ficheros no automatizados 185
2.9.13.1 Niveles de seguridad 185
2.9.13.2 Nivel básico 185
2.9.13.2.1 Criterios de archivo 185
2.9.13.2.2 Dispositivos de almacenamiento 186
2.9.13.2.3 Custodia de los soportes 186
2.9.13.3 Nivel medio 186
2.9.13.3.1 Responsable de seguridad 186
2.9.13.3.2 Auditoría 186
2.9.13.4 Nivel alto 186
2.9.13.4.1 Almacenamiento de la información 186
2.9.13.4.2 Copia o reproducción 187
2.9.13.4.3 Acceso a la documentación 187
2.9.13.4.4 Traslado de documentación 187
2.9.13.5 Plazos de implantación de las medidas de seguridad para ficheros no automatizados 187

3 Fases y procedimiento de actuación en un proyecto de adecuación a la normativa de protección de datos 189

3.1 Introducción 191
3.1.1 Normativa específica y normativa general 191
3.1.2 Inconvenientes para el cumplimiento de la normativa de protección de datos 191
3.2 Motivaciones e impulso del inicio del proyecto 192
3.2.1 Ley que exige su cumplimiento 192
3.2.2 La imposición de sanciones económicas 192
3.2.3 Afectación a la imagen en caso de multa. El «riesgo reputacional» ... 192
3.2.4 Mejora de la imagen y percepción de seguridad por los clientes y los empleados 193
3.2.5 Mejora de gestión y los procedimientos internos 194
3.2.6 Gran volumen de información confidencial, gran concienciación y buena disponibilidad 194
3.2.7 Escasa concienciación a nivel directivo 195
3.2.8 Bloqueo de ficheros como sanción 195
3.3 Determinación de los objetivos a alcanzar 196

Página

3.3.1 Necesidad de un Proyecto de Adecuación 196
3.3.2 Diferentes enfoques de un Proyecto de Adecuación 196
3.3.3 Fijación de los objetivos finales de un Proyecto de Adecuación 196
3.4 Fases del proyecto y metodología 197
3.4.1 Estructuración del Proyecto 197
3.4.2 Fases del Proyecto de Adecuación 197
3.4.3 Metodología del Proyecto de Adecuación 201

4 Fase preliminar 203

4.1 La formación del equipo de trabajo, del comité de seguimiento y del personal colaborador 205
4.1.1 El Equipo de Trabajo 205
4.1.2 El Personal Colaborador 205
4.1.3 El Comité de Seguimiento 206
4.2 Perfil de los profesionales que van a participar en el proyecto 207
4.2.1 El Equipo de Trabajo 207
4.2.2 El Personal Colaborador 209
4.2.3 El Comité de Seguimiento 209
4.3 Definición de las funciones y responsabilidades de los miembros del equipo ... 210
4.3.1 Casuística 210
4.3.2 Esquema general 210
4.4 Premisas básicas para comenzar el proyecto 213
4.4.1 Determinación del ámbito institucional del proyecto 213
4.4.2 Dificultades e imprevistos 213

5 Fase 1: análisis inicial 217

5.1 Documentación básica de necesaria revisión 219
5.1.1 El papel del Equipo de Trabajo en la revisión 219
5.1.2 Naturaleza de la documentación a revisar 220
5.2 Documentación jurídica con incidencia directa en protección de datos 220
5.2.1 Contratos con clientes 221
5.2.1.1 Volumen de información y diversidad de los contratos 221
5.2.1.2 Objetivos del Equipo de Trabajo 221
5.2.2 Contratos con empleados 222
5.2.2.1 Aspectos a tener en cuenta 222
5.2.2.2 Compromisos de confidencialidad 222
5.2.2.3 Obtención del consentimiento del empleado 223
5.2.3 Contratos con proveedores 223
5.2.4 Contratos de encargo del tratamiento 224
5.2.4.1 Detección de los supuestos de encargo del tratamiento 224
5.2.4.2 Aspectos analizados 225
5.2.5 Contratos de cesión de datos 225
5.2.6 Acuerdos marco internacionales. Las multinacionales 226
5.2.7 Comunicaciones con carácter informativo o para recabar el consentimiento 227

Página

5.2.8 Políticas o procedimientos internos 229
5.2.9 Procedimiento para el respeto de los derechos de acceso, rectificación, cancelación y oposición que hayan sido ejercitados 230
5.2.10 Las inscripciones ya realizadas previamente por la entidad ante el Registro General de Protección de Datos 230
5.2.10.1 Funciones de orientación para el Equipo de Trabajo 231
5.2.10.2 Solicitud de los documentos acreditativos 231
5.2.10.3 Documentos acreditativos de la modificación de ficheros 231
5.2.10.4 Documentos acreditativos de relaciones mantenidas con la AEPD 232
5.2.11 Informes jurídicos previos 232
5.3 Documentación técnica con incidencia directa en protección de datos 233
5.3.1 Organigrama de redes y sistemas de información 233
5.3.2 Documento de Seguridad existente 233
5.3.3 Informes de Auditoría realizados de los ficheros automatizados y no automatizados 234
5.3.4 Procedimientos de seguridad existentes 234
5.3.4.1 Enumeración de Procedimientos de Seguridad 235
5.3.5 Perfiles de acceso a la información 236
5.4 Documentación jurídica y técnica conexa 237
5.4.1 Formularios de recogida de datos 237
5.4.2 Documentación de campañas de marketing 238
5.4.2.1 Compraventa de Bases de Datos 238
5.4.3 Otra 238
5.5 Documentación conexa de carácter organizativo: procedimientos internos, composición y organigrama 238
5.6 Análisis de la situación 239
5.6.1 Inventario de la documentación recogida y analizada 240
5.6.1.1 Finalidad de la elaboración del Inventario 240
5.6.2 Contrato de encargo de tratamiento entre el Equipo de Trabajo de carácter externo y la entidad 240
5.6.3 Evaluación del panorama actual de la empresa 241
5.6.4 Informe de estado de situación 242
5.6.5 Informe de recomendaciones previas 243

6 Fase 2: localización e identificación de ficheros 245

6.1 Posibles panoramas existentes 248
Entidad con ficheros ya detectados y declarados 249
6.1.2 Entidad sin ficheros localizados 249
Información necesaria a recabar de cada fichero 250
6.2.1 Introducción 250
6.2.1.1 Objetivo y finalidad 250
6.2.1.2 Determinación de los departamentos afectados 250
6.2.1.3 La vida del dato 250
6.2.2 Origen y procedencia de los datos 252
6.2.2.1 Origen de los datos: otro fichero de la propia entidad 252

Página

6.2.2.2 Origen de los datos: una fuente exterior diferente a la propia entidad 253
6.2.2.3 Manera en la que han sido recabados 254
6.2.2.4 El procedimiento de recogida de datos 255
6.2.2.5 El soporte utilizado para la obtención 255
6.2.2.6 Origen y procedencia de los datos: implicaciones en materia de protección de datos 256
6.2.3 Los tratamientos de los datos que se realizan dentro de la entidad 257
6.2.3.1 Tratamientos de datos en la entidad: implicaciones en materia de protección de datos 257
6.2.4 La cancelación de los datos o su salida de la entidad 258
6.2.4.1 Cancelación y salida de datos: implicaciones en materia de protección de datos 258
6.3 Métodos para la identificación de ficheros. El enfoque del proyecto para conseguir la colaboración con el personal 259
6.3.1 Introducción 259
6.3.1.1 Pasos previos 259
6.3.1.2 Labor del personal colaborador en la Fase II 259
6.3.2 Las entrevistas personales 260
6.3.2.1 Metodología óptima 260
6.3.2.2 Determinación de la composición del personal colaborador 261
6.3.2.3 La elaboración de actas tras las entrevistas 261
6.3.3 La utilización de formularios 262
6.3.4 La revisión presencial de los ficheros y los tratamientos 262
6.3.5 Optimización de los recursos para conseguir la máxima colaboración 263
6.3.5.1 Página web de la empresa externa especializada 263
6.3.5.2 Software 263
6.3.5.3 Intranet de la propia entidad 264
6.3.5.4 Conference call 264
6.4 Aspectos más problemáticos en los diferentes departamentos de una entidad 264
6.4.1 Departamento de Recursos Humanos y Servicio Médico 264
6.4.1.1 Dictamen del Grupo de Trabajo del Artículo 29 sobre el tratamiento de datos personales en el contexto laboral 264
6.4.1.1.1 Finalidad 265
6.4.1.1.2 Transparencia 265
6.4.1.1.3 Legitimidad 265
6.4.1.1.4 Proporcionalidad 265
6.4.1.1.5 Exactitud y conservación de los datos 265
6.4.1.1.6 Formación del personal 265
6.4.1.1.7 Consentimiento 265
6.4.1.1.8 Vigilancia y control 266
6.4.1.2 Selección de Personal 266
6.4.1.2.1 Implicaciones de los principios establecidos en la LOPD: Calidad de los datos, Derecho de Información, Consentimiento y Cesión 266
6.4.1.2.2 Empresas de Selección de Personal y ETT's 271
6.4.1.3 Trabajadores de la Entidad 272

Página

6.4.1.3.1 Implicaciones jurídicas: calidad de los datos, deber de información, consentimiento y cesión 272
6.4.1.3.2 Deber de secreto y compromiso de confidencialidad 277
6.4.1.3.3 Control del trabajador: potestad de vigilancia del empresario 277
6.4.1.3.4 Datos de afiliación sindical 282
6.4.1.3.5 Datos de Salud. Servicio Médico 284
6.4.1.3.6 Prestaciones de servicios 288
6.4.1.3.7 Ejercicio de derechos 289
6.4.2 Departamento Comercial y Marketing 289
6.4.2.1 Utilización de datos de carácter personal con la finalidad de marketing: cumplimiento de los principios establecidos en la Ley 289
6.4.2.1.1 Datos procedentes del propio interesado 290
6.4.2.1.2 Datos procedentes de fuentes accesibles al público o de ficheros con fines de publicidad 292
6.4.2.2 Arrendamiento de bases de datos 294
6.4.2.3 Contratación de empresas especializadas: prestaciones de servicios y cesiones de datos 295
6.4.3 Otros Departamentos con implicaciones en materia de protección de datos 296
6.4.3.1 Atención al Cliente 296
6.4.3.1.1 Call Center 297
6.4.3.1.2 Atención ejercicio de derechos 297
6.4.3.2 Sistemas e Informática 298
6.4.3.3 Departamento de Administración y Financiero 298
6.4.3.4 Asesoría Jurídica 299
6.4.3.4.1 Tratamiento de datos de las partes en un procedimiento judicial 299
6.4.3.5 Seguridad física 301
6.4.3.5.1 Control de acceso al edificio 301
6.4.3.5.2 Utilización de videocámaras en los controles de acceso a edificios 301

7 Fase 3: clasificación y análisis legal de los ficheros identificados 303

7.1 Introducción 305
7.2 Clasificación e inventario de ficheros físicos y lógicos 305
7.2.1 Concepto de fichero físico y lógico 305
7.2.1.1 Concepto de fichero en la LOPD 305
7.2.1.2 Concepto de fichero físico 306
7.2.1.3 Concepto de fichero lógico 306
7.2.1.4 Concepto de fichero temporal 307
7.2.1.5 La elaboración del inventario de ficheros 308
7.2.2 Ventajas y finalidad de la elaboración del Inventario 308
7.2.3 Claves para la correcta agrupación de ficheros físicos en ficheros lógicos 309
7.3 Análisis legal. Aspectos importantes objeto de estudio 310

Página

7.4 Fuentes y recursos para llevar a cabo el estudio 310
7.4.1 Normativa vigente 310
7.4.2 Las Instrucciones de la AEPD 311
7.4.3 Guías de la AEPD 311
7.4.4 Planes sectoriales de oficio 312
7.4.5 Resoluciones AEPD y jurisprudencia 312
7.4.6 Documentos del Grupo del art. 29 de la Directiva 313
7.4.7 Códigos Tipo 313
7.5 Estudio de supuestos especialmente problemáticos. Las consultas a la AEPD 313

8 Fase 4: realización de la auditoría de las medidas de seguridad 315

8.1 Obligación del reglamento de la LOPD 317
8.2 Objeto 317
8.3 Enfoque de la auditoría 318
8.3.1 Enfoque técnico 318
8.3.2 Enfoque organizativo 318
8.3.3 Enfoque jurídico 318
8.4 Metodología de trabajo en la realización de la auditoría 318
8.4.1 Obtención de información escrita 318
8.4.2 Obtención de información no escrita 319
8.4.3 Revisión presencial de los sistemas de información 319
8.4.4 Componentes a revisar presencialmente en la realización de la auditoría 319
8.4.4.1 Identificación y autenticación 319
8.4.4.2 Control y registro de acceso 320
8.4.4.3 Pruebas con datos reales 320
8.4.4.4 Procedimiento de notificación y gestión de incidencia 320
8.4.4.5 Análisis de otros procedimientos generales 320
8.4.5 Fases de la Auditoría 321
8.5 Relación de aplicaciones y sistemas a auditar 321
8.6 Equipo de trabajo 322
8.6.1 Auditor solitario 322
8.6.2 Auditores en pareja 323
8.6.3 Auditores en equipo 323
8.7 Cualificaciones de los auditores 323

9 Fase 5: elaboración del informe de adecuación y del documento de seguridad 325

9.1 El informe de adecuación a la Normativa en materia de protección de datos 327
9.1.1 Diferencia entre el Informe de Auditoría y el Informe de Adecuación a la normativa en materia de protección de datos 327
9.1.2 Objetivos perseguidos en el Informe de Adecuación a la normativa en materia de protección de datos 328
9.1.3 Metodología seguida 328
9.1.3.1 Informe general *vs* Informes departamentales 328

Página

9.1.3.2 Aspectos a tener en cuenta ... 329
9.1.4 Contenido del Informe ... 330
9.1.4.1 Introducción ... 330
9.1.4.2 Bloque Normativo ... 330
9.1.4.3 Aspectos detectados y recomendaciones ... 330
9.1.4.4 Conclusiones del Informe ... 331
9.1.4.5 Anexos ... 332
9.1.5 ¿Quién debe elaborarlo? ... 332
9.1.6 ¿A quién va dirigido? ... 333
9.2 El Documento de seguridad ... 333
9.2.1 Introducción ... 333
9.2.2 Objetivos del Documento de Seguridad ... 335
9.2.3 Metodología seguida ... 335
9.2.4 Contenido del Documento de Seguridad ... 336
9.2.4.1 Introducción y objeto del Documento de Seguridad ... 336
9.2.4.2 Ámbito de aplicación del Documento de Seguridad ... 336
9.2.4.3 Medidas, normas, procedimientos, reglas y estándares de seguridad ... 337
9.2.5 ¿Quién debe elaborarlo? ... 338
9.2.6 ¿A quién va dirigido? ... 338
9.2.7 Modelo de documento de seguridad ... 339

10 Fase 6: implantación de medidas correctoras y concienciación del personal 363

10.1 Funciones y obligaciones del personal: el Manual «Data Use Policy» ... 365
10.1.1 Introducción ... 365
10.1.2 Objetivos del Manual ... 365
10.1.3 Contenido del Manual ... 365
10.1.4 ¿Quién debe elaborarlo? ... 366
10.1.5 ¿A quién va dirigido? ... 366
10.1.6 Modelo de Manual Data Use Policy ... 366

11 Fase 7: inscripción de los ficheros en el registro de protección de datos 391

11.1 El registro de protección de datos ... 393
11.1.1 Consideraciones más relevantes de la Memoria del año 2008 ... 393
11.2 La agrupación de ficheros físicos y lógicos ... 395
11.2.1 Agrupación de ficheros físicos en ficheros lógicos ... 395
11.2.2 Esquema explicativo de la agrupación de ficheros ... 396
11.2.3 Nivel de seguridad de los ficheros lógicos ... 397
11.3 Declaraciones en el Registro de Protección de Datos ... 399
11.3.1 Sistema de notificaciones NOTA ... 399
11.3.1.1 Obtención del formulario y presentación ... 399
11.3.1.2 Consideraciones iniciales del asistente NOTA ... 399
11.3.2 Creación ... 400
11.3.2.1 Ficheros de titularidad privada ... 400
11.3.2.1.1 Persona física que actúa en representación del responsable del fichero ante la AEPD ... 400
11.3.2.1.2 Responsable del Fichero o del Tratamiento ... 401
11.3.2.1.3 Servicio o Unidad concreto ante el que se podrán ejercitar los derechos de acceso, rectificación, cancelación u oposición ... 401
11.3.2.1.4 Encargado del Tratamiento ... 401
11.3.2.1.5 Identificación y finalidad del fichero ... 402
11.3.2.1.6 Origen y procedencia de los datos ... 403
11.3.2.1.7 Estructura básica y descripción de los tipos de datos ... 404
11.3.2.1.8 Medidas de seguridad ... 405
11.3.2.1.9 Cesión o Comunicación de Datos ... 406
11.3.2.1.10 Transferencias Internacionales de Datos ... 406
11.3.2.2 Ficheros de Titularidad Pública ... 407
11.3.2.2.1 Responsable del Fichero o Tratamiento ... 407
11.3.2.2.2 Disposición general de creación, modificación y supresión del fichero ... 408
11.3.2.2.3 Finalidad del fichero y usos previstos ... 408
11.3.3 Modificación ... 409
11.3.3.1 Ficheros de titularidad privada ... 409
11.3.3.2 Ficheros de titularidad pública ... 410
11.3.4 Supresión ... 410
11.3.4.1 Ficheros de titularidad privada ... 410
11.3.4.2 Ficheros de titularidad pública ... 410
11.4 Los formularios oficiales vigentes ... 411
11.4.1 Resolución de 12 de julio del 2006 ... 411
11.4.2 Cumplimentación y envío de los mismos ... 411
11.4.2.1 Formularios en formato papel ... 412
11.4.2.2 Formularios en formato telemático. Presentación con certificado de firma reconocido ... 412
11.4.2.3 Formularios en formato telemático. Presentación sin certificado de firma reconocido ... 412
11.4.2.4 Formularios en formato telemático. Notificaciones simplificadas o notificaciones tipo ... 413
11.4.3 Quién debe rellenarlos ... 413
11.4.3.1 Grupos empresariales ... 414
11.4.3.2 Sucursales ... 415
11.4.3.3 Inscripciones por el encargado del tratamiento ... 415
11.5 Repercusión jurídica de la declaración de ficheros ... 416

12 Mantenimiento y seguimiento 417

12.1 ¿Cuándo se cumple definitivamente con la normativa? La necesidad de un seguimiento ... 419
12.2 El Comité de Seguimiento LOPD ... 420
12.2.1 Creación del Comité de Seguimiento LOPD. Personal integrante y funciones de sus miembros ... 420
12.2.2 Objetivos ... 421

Página

12.2.3 Ámbito y acciones a desarrollar por el Comité de Seguimiento 421
12.2.4 Funcionamiento general. Las normas y las juntas 422

13 Particularidades de la protección de datos de carácter personal para médicos y clínicas y/o centros asistenciales 425

13.1 Obligaciones para médicos y clínicas/centros sanitarios derivadas de la normativa de protección de datos personales 427
13.1.1 Obligación de información en la recogida de datos 428
13.1.2 Obligación de recabar el consentimiento de la persona afectada 429
13.1.3 Obligación de garantizar la seguridad de los datos de salud 430
13.1.4 Obligación de secreto 431
13.2 Cesión/comunicación de datos y acceso a datos por cuenta de terceros 432
13.3 Garantías de los afectados 433
13.4 Contratos entre centro médico y facultativos 435
Anexo I 436
Anexo II 437
Anexo III 438
Anexo IV 439
Anexo V 440

14 La externalización de los servicios TIC de una organización. El caso práctico del outsourcing del servicio de atención a usuarios 443

14.1 Introducción: la externalización de servicios TIC: modalidades y riesgos de seguridad asociados 445
14.2 Modalidades de externalización y aspectos de protección de datos a considerar en cada una 448
14.2.1 Out-tasking in house: subcontratación de personal 448
14.2.2 Outsourcing convencional 449
14.2.3 Business Process Outsourcing: Externalización completa 449
14.2.4 Offshoring: deslocalización y transferencias internacionales 450
14.3 Exposición de un caso práctico: la externalización del servicio de atención a usuarios: impacto de la normativa de protección de datos 452
14.4 Aspectos LOPD en la externalización del SAU 452
14.4.1 Aspectos jurídicos 452
14.4.1.1 Aspectos relativos a la regulación del encargo de tratamiento con el proveedor 453
14.4.1.2 Aspectos relativos a la regulación de la confidencialidad en el manejo de información de la entidad por parte del personal del proveedor 456
14.4.2 Aspectos técnicos 456
14.4.2.1 Medidas de seguridad a cumplir por el proveedor del servicio 457
14.4.2.2 Medidas de seguridad a cumplir por la entidad contratante 459
14.5 Otros aspectos adicionales al contrato de externalización 460

Página

Anexo legislativo 467

Glosario 1057

Índice analítico 1059

Índice cronológico de disposiciones citadas 1067