ÍNDICE

Introducción 27

CAPÍTULO I. Requisitos legales y organizativos básicos para el tratamiento de la información y de los datos personales en la UE 33

I. LA CALIDAD LEGAL DE LOS DATOS 33

1. La información y los datos 33
   1.1. Los datos exactos 34
   1.2. Los datos adecuados 35
   1.3. Los datos pertinentes 36
   1.4. Los datos no excesivos con respecto a las finalidades para las que han sido recogidos 37
   1.5. Las finalidades determinadas, explícitas y legítimas para las que se obtienen los datos 38
   1.6. La compatibilidad de las finalidades de la recogida 39
   1.7. Las finalidades históricas, científicas o estadísticas 40
   1.8. La actualización de los datos 41
   1.9. La conservación de los datos 42
2. La longitud de los datos. Concepto y requisitos 43
3. La legitimación para el tratamiento de datos y de información referida a personas identificadas o identificables 44
4. Derecho de información del interesado en la recogida de datos 49
   4.1. Cuando los datos se recaben del propio interesado 49
   4.2. Cuando los datos no se recaben del propio interesado 55
5. La solicitud del consentimiento al interesado 57
   5.1. La revocación del consentimiento 59
   5.2. Capacidad legal para tratar datos de terceros 60

CAPÍTULO II. Modelo de documento de seguridad para la empresa en general 61

I. ÁMBITO DE APLICACIÓN 61

II. LEGALIZACIÓN Y LEGITIMACIÓN DE LA BASE DE DATOS 62

1. Legalización 62
   1.1. Notificación para la inscripción de ficheros 62
   1.2. Inscripción de los ficheros 63
   1.3. Modificación y cancelación de la inscripción 63
2. Legitimación de los datos para poder ser tratados con los procedimientos de la empresa 64
   2.1. Requisitos previos para proceder al tratamiento 64
   2.2. Condiciones que se han de dar para poder iniciar la recogida de datos de personas 64
      2.2.1. La información a los afectados 64
      2.2.2. Consentimiento 66
      2.2.3. Tarjeta «Alfa» para obtener datos de carácter personal 67
      2.2.4. Calidad de los datos 69
      2.2.5. Finalidad concreta antes de proceder a la recogida 69
      2.2.6. Exactitud de la información contenida en los datos 69
      2.2.7. Sustitución directa en caso de inexactitud 70
      2.2.8. Cancelación cuando se haya terminado el objeto que hizo precisa su recogida 70
      2.2.9. Conservación 70
   2.3. La entrada de información en la base de datos 70
      2.3.1. El archivo documental de accesos 70
      2.3.2. El archivo documental transitorio 71
   2.4. Tratamiento y mantenimiento de los datos 72
      2.4.1. Forma de tratamiento 72
      2.4.2. El acceso a la base de datos general de administración de la empresa 72
      2.4.3. Conservación 72

III. MEDIDAS ENCAMINADAS A GARANTIZAR LOS NIVELES DE SEGURIDAD 73

1. Identificación y autenticación del personal autorizado a acceder a los datos personales 73
   1.1. Medidas de seguridad físicas 73
   1.2. Medidas de seguridad informáticas 75
2. Control de acceso 77
   2.1. Medidas de seguridad físicas 77
   2.2. Medidas de seguridad informáticas 78
   2.3. Responsabilidad de los autorizados 78
3. Gestión de soportes 80

   3.1. Identificación, inventariado y almacenamiento de soportes informáticos con datos de carácter personal 80
   3.2. Identificación 80
   3.3. Inventario de soportes 80
   3.4. Almacenamiento 81
   3.5. Modelo de etiqueta adhesiva para la identificación de los soportes informáticos con datos personales 81
   3.6. Control de salida de soportes 82
   3.7. Control de entrada de soportes 82
   3.8. Medidas adicionales 82
4. Acceso a datos a través de redes de comunicaciones 82
5. Régimen de trabajo fuera de los locales de la ubicación del fichero 83
6. Ficheros temporales 83
7. Copias de seguridad 84
   7.1. Procedimientos de recuperación 84
   7.2. Medios físicos para efectuar las copias de seguridad y lugar de custodia 84
8. Pruebas con datos reales 84

IV. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL 85

1. Funciones y obligaciones de carácter general 85
2. Funciones y obligaciones específicas 85
   2.1. Responsable del fichero 85
   2.2. Responsable de seguridad 86
   2.3. Jefe de personal-encargado del subfichero de personal 87
   2.4. Administrador de sistemas 88
   2.5. Responsable del tratamiento 88
   2.6. Responsable de atención a los afectados 89
   2.7. Responsable de registros 90
   2.8. Encargados 91
   2.9. Obligaciones de los usuarios del sistema de información de empresa 92
      2.9.1. Números de identificación y claves de acceso 92
      2.9.2. Confidencialidad de la información 93
      2.9.3. Uso del correo electrónico 94
      2.9.4. Acceso a internet 95
      2.9.5. Propiedad intelectual e industrial 95
      2.9.6. Incidencias 95
      2.9.7. Protección de datos 96

V. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS 96

VI. SALIDA DE INFORMACIÓN. LOS ENCARGADOS DEL TRATAMIENTO 97

1. Consideraciones previas 97

2. Régimen de tratamiento de la información con acceso a terceros 98
3. La cesión de información 99
4. Acceso a la base de datos por parte del personal 102
5. Personal de la empresa sin acceso autorizado a la base de datos 103
5.1. Prohibición de acceso 103
6. Destrucción de los soportes 103
7. Salida de los datos a través de la red 104
8. Responsabilidad en caso de incumplimiento 105

VII. Los derechos de acceso, rectificación, cancelación y oposición 105

1. Derecho de acceso 105
1.1. Carácter personal de los derechos 105
1.2. Derecho de acceso y/o consulta 105
1.3. Contenido de la información 106
1.4. Denegación del acceso 106
2. Derecho de rectificación o cancelación 107
2.1. Bloqueo de los datos 107
3. El derecho de oposición 107

VIII. Tratamientos con fines de publicidad y de prospección comercial. El censo promocional 108

IX. Régimen específico del uso de videocámaras 109

1. Objeto 109
2. Legitimación de la información 109
3. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición 110
4. Conservación de las imágenes 110
5. Ubicación de las cámaras 110
6. Tratamiento de las imágenes 111

X. Tratamiento de la información sanitaria (sólo para grandes empresas con servicio médico sanitario propio) 111

1. Ámbito de aplicación 111
2. Definiciones 111
3. Funciones y obligaciones específicas 112
3.1. Médico responsable 112
3.2. El centro sanitario 113
3.3. Personal del centro (departamento de Empresa) 114
4. Documentación clínica 115
4.1. Historia clínica 115
4.1.1. Definición y archivo 115
4.1.2. Contenido 116
4.1.3. Conservación 117

4.1.4. Apertura de la historia clínica 117
4.1.5. Acceso a la historia clínica 118
4.2. Consentimiento informado 120
4.2.1. Definición y contenido 120
4.2.2. Autonomía de la voluntad del paciente 121
4.2.3. Excepciones a la necesidad de solicitud de consentimiento informado al paciente 121
4.3. Instrucciones previas 122
4.3.1. Definición y regulación 122
4.3.2. Contenido 123
4.3.3. Formalización 124
4.4. Informe de alta 124
4.4.1. Definición 124

XI. Comercio electrónico 125

1. Datos de oficiales del nombre de dominio 125
2. Ámbito de aplicación 126
3. Usos prohibidos 127
4. Obligación de publicidad 127
4.1. El registro del nombre de dominio 127
4.2. Obligación de información 128
5. Comunicaciones comerciales 129
5.1. Requisitos para la realización de comunicaciones comerciales 129
5.1.1. Principio de legitimación 129
5.1.2. Principio de identificación 130
5.1.3. Principio de legalidad 130
5.2. Externalización del servicio de comunicaciones comerciales 130
6. Contratación por vía electrónica 131
6.1. Obligaciones previas al inicio del procedimiento de contratación 131
6.2. Obligaciones posteriores a la recepción del contrato 132
7. Infracciones y sanciones 133
7.1. Infracciones 133
7.1.1. Son infracciones muy graves 133
7.1.2. Son infracciones graves 134
7.1.3. Son infracciones leves 135
7.2. Sanciones 136
7.2.1. Por la comisión de las infracciones recogidas en el punto anterior, se impondrán las siguientes sanciones 136
7.2.2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el «Boletín Oficial del Estado», o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración pública o en la página de inicio

del sitio de internet del prestador, una vez que aquélla tenga carácter firme 136

XII. PROCEDIMIENTOS DE REVISIÓN 136

1. *Check-list* para verificación del control periódico interno 137
   1.1. Control de la aplicación del documento de seguridad 137
   1.2. Control del sistema de identificación y autenticación 138
   1.3. Control del sistema de control de acceso 138
   1.4. Control del cumplimiento de las normas de confidencialidad y secreto. 138
   1.5. Control del cumplimiento de las normas internas y las funciones del personal 138
   1.6. Control de los procedimientos de gestión de soportes 139
   1.7. Control antivirus 139
   1.8. Control del cumplimiento de las normas de propiedad intelectual ... 139
   1.9. Control del procedimiento de copias de respaldo 139
   1.10. Control del procedimiento de incidencias 139

CAPÍTULO III. Modelo de documento de seguridad para los centros docentes 141

I. EL MANUAL DE FUNCIONES DEL PERSONAL DEL CENTRO 141

CUADRO DE RESPONSABLES DEL FICHERO Y DEL TRATAMIENTO 141

1. Responsable del fichero 141
   1.1. Ámbito 141
   1.2. Finalidad del fichero 142
   1.3. Usos del fichero 142
   1.4. Aplicaciones del fichero 142
2. Encargado del fichero 143
   2.1. Ámbito 143
   2.2. Funciones propias 143
   2.3. Responsabilidad 143
   2.4. Tareas propias 144
      2.4.1. Legalización de ficheros 144
         a) Notificación para la inscripción de ficheros 144
         b) Inscripción de los ficheros 144
         c) Modificación y cancelación de la inscripción 145
      2.4.2. Legitimación de los datos para el tratamiento 145
         a) El tratamiento de los datos personales sólo puede efectuarse cuando 145
         b) Requisitos para la obtención del consentimiento de los afectados. Información del interesado 146
      2.4.3. La Entrada de la información y de los datos en el fichero (los archivos documentales de accesos y transitorio) 146

2.4.3.1. El archivo documental de accesos 146
2.4.3.2. El archivo documental transitorio 147
2.4.3.3. Inclusión en el fichero de administración general 148
2.4.4. El mantenimiento de los datos y del fichero 149
2.4.4.1. El registro de incidencias 150
2.4.4.2. Identificación, autenticación y control de acceso 150
2.4.4.3. Procedimiento de gestión, archivo y respaldo 152
2.4.4.4. Registro de soportes 153
3. Encargado del tratamiento 154
   3.1. Ámbito 154
   3.2. Tratamiento y mantenimiento de los datos 155
      A) Tratamiento 155
      B) Recogida 155
      C) Ubicuidad, adecuación y longitud 155
      D) Calidad 155
      E) Conservación 155
4. El responsable de seguridad 156
   4.1. Concepto legal 156
   4.2. Niveles de seguridad 156
   4.3. Aplicación de los niveles de seguridad 157
   4.4. Ejercicio y tutela de los derechos de los afectados 162
   4.5. Archivos y registros 164
      4.5.1. El Registro general de archivos 165
      4.5.2. Registro general de accesos físicos 166
      4.5.3. Registro de copias de seguridad 166
      4.5.4. El registro de incidencias 168

II. EL MAESTRO INFORMÁTICO DEL DOCUMENTO DE SEGURIDAD 168

1. Ámbito de aplicación del documento de seguridad 169
   1.1. Ámbito jurídico 169
   1.2. Ámbito personal 169
   1.3. Ámbito material 169
2. Medidas de seguridad informáticas 169
   2.1. Plan de seguridad 170
      2.1.1. Fundamentos 170
      2.1.2. Sistema de seguridad para el acceso a las dependencias donde se trate información sobre personas identificadas o identificables 170
      2.1.3. Sistema de alarma en las oficinas 170
   2.2. Identificación y autenticación 171
      2.2.1. Descripción del procedimiento de identificación y autenticación de usuarios 171
      2.2.2. Asignación, distribución y almacenamiento de contraseñas 172
      2.2.3. Normas generales de cumplimiento obligatorio en el uso de los códigos de acceso («las contraseñas») 173

2.3. Control de accesos y confidencialidad de la información 173
2.3.1. Control de acceso al sistema 174
2.3.2. Control de acceso al programa que gestione la base de datos 174
2.4. Gestión de soportes 175
2.5. Uso del correo electrónico 176
2.6. Acceso a Internet 176
3. Funciones y obligaciones de todos los usuarios que tienen autorización para acceder al uso del sistema informático 177
3.1. Obligaciones y funciones comunes a todo el personal del centro 177
3.1.1. Números de identificación y claves de acceso 177
3.1.2. Actividades expresamente prohibidas 177
3.1.3. Confidencialidad de la información 179
3.1.4. Incidencias 179
3.1.5. Actos especialmente prohibidos en materia de protección de datos 180
3.2. Obligaciones y funciones específicas para los responsables 180
3.2.1. El responsable de la base de datos 180
3.2.2. El responsable de seguridad, responsables del tratamiento de la información y jefes de niveles 181
3.2.3. El jefe de personal 182
4. Estructura de los ficheros informatizados del centro y descripción de los sistemas de información que los tratan 182
4.1. Longitud y calidad de los datos. Composición de la información ... 182
4.2. Sistema de tratamiento 184
4.2.1. Configuración 185
4.2.2. Procedimiento de notificación, gestión y respuesta ante las incidencias 185
4.2.3. Procedimiento de realización de copias de respaldo y de recuperación de datos 187
5. Protocolos aplicables al tratamiento documental de la información en los centros docentes 187
5.1. Principios y derechos 187
5.1.1. Principio de identidad 187
5.1.2. Principio de legalidad 187
5.1.3. Principio de legitimación 188
5.2. Los protocolos de acceso al centro 188
5.2.1. Preinscripción 188
5.2.2. Inscripción 194
5.2.2.1. Inadmisión 194
5.2.2.2. Admisión 194
5.2.2.3. La formalización de la matrícula 194
5.2.2.3.1. Las condiciones particulares de la matriculación 195
5.3. Gestión interna de los documentos y de la información 201
5.3.1. El registro general de accesos documentales 201

5.3.2. El acceso a datos aportados por el propio interesado. Inicio del camino para el tratamiento interno 202
5.3.3. Los destinos internos 202
5.3.3.1. La dirección del centro 203
5.3.3.1.1. Protocolo de tratamiento sanitario 203
5.3.3.1.2. Protocolo de permisos extraordinarios 205
5.3.3.2. Los departamentos del centro como destinatarios de la información externa 207
5.4. La salida de información del centro 207
5.4.1. La cesión y la transmisión 207
5.4.2. La dirección del centro como emisor de información dirigida al exterior del centro 208
5.4.2.1. Protocolo de notificaciones, reclamaciones y amonestaciones a los padres o a los representantes de los menores 208
5.5. La tenencia de información posterior al tratamiento 213
III. EL SISTEMA DE AUTOCONTROL 215
1. FORMULARIO GUÍA DE UNA TOMA DE DATOS PARA AUTOCONTROL O AUDITORÍA INTERNA DEL CENTRO 215
A) TOMA DE DATOS 215
1. Titularidad del centro 215
2. Enseñanzas impartidas 216
3. Los servicios y estructura del centro 217
4. La matrícula 218
5. Proceso de admisión de alumnos 218
5.1. Normativa aplicable 218
5.2. Los formularios de solicitud de inscripción 219
5.3. Los protocolos 219
5.4. La baremación 219
5.5. Los listados de preinscripción 220
5.6. Periodo de reclamaciones 220
5.7. Tratamiento de la documentación 221
6. Proceso de matriculación 221
6.1. Regulación 221
6.2. Admisión 221
6.3. Protocolo para matriculación 221
6.4. Documentación anexa 222
6.5. Documentos obligatorios para alumnos de otros centros 222
6.6. El expediente académico de alumnos de otros centros 222
6.7. El expediente académico del centro 223
6.8. Datos de las nuevas incorporaciones 223
6.9. Procedimiento del tratamiento informatizado 223
7. El final de la escolarización 223

7.1. La expedición de titulación 224
7.2. Procedimiento para obtención del título 224
7.3. Prueba de selectividad 224
7.4. Distribución y abono de las fichas de selectividad 225
7.5. El Resguardo 225
7.6. Resultados 225
8. El archivo histórico de expedientes académicos 225
9. La inspección educativa 226
9.1. La Revisión de protocolos 226
9.2. Revisión directa de un ciclo 226
9.3. Verificación de reclamaciones 227
10. Departamento de orientación 227
10.1. Objeto del departamento 227
10.2. Funciones 227
10.3. El plan de acción tutorial 228
10.4. Actuación 228
10.5. Elaboración de programas 228
10.6. Procedimientos 228
10.7. La orientación psicológica 229
10.8. Tratamiento externo 229
10.9. El Equipo Psicopedagógico de la Conselleria d'Ensenyament-Ente Público 229
10.10. Fichas de seguimiento 229
11. Departamento de enfermería 230
11.1. Funciones 230
11.2. Procedimientos 231
11.3. Servicio de vacunación 231
11.4. Infraestructura informática 231
11.5. Seguro de Accidentes 231
11.6. Procedimiento en caso de accidente 232
12. Biblioteca 232
12.1. El préstamo de libros 232
12.2. Acceso a los datos 233
12.3. Legitimación para el acceso 233
13. Actividades extraescolares 233
13.1. Procedimientos 233
13.2. Inscripción 233
13.3. Informe periódico 234
13.4. El Consejo escolar de Deportes 234
13.5. Tratamiento informatizado de las actividades 234
14. La APA (asociación de padres, madres y tutores legales) 234
14.1. Presentación 235
14.2. Las Comunicaciones 235
14.3. Ficheros propios 235

14.4. Ejercicio de derechos 235
14.5. La prohibición de uso 236
15. Becas 236
15.1. Los impresos de solicitud 236
15.2. Gestión de la información 237
15.3. Notificación de resoluciones sobre gastos de matriculación 237
15.4. Notificación de resoluciones sobre gastos de material 237
15.5. Protocolo de tramitación de Becas 237
16. Formación en empresas 237
16.1. Determinación de la empresa 238
16.2. Cuando la empresa se interesa 238
16.3. Procedimientos 238
16.4. Control académico en la empresa 238
16.5. Homologación 239
16.6. Control de convenios firmados 239
16.7. Archivo documental 239
16.8. Cesión de datos a las empresas 239
16.9. Notificación administrativa 240
17. Los programas de garantía social 240
17.1. Los beneficiarios 240
17.2. La preinscripción 240
17.3. La inscripción 241
17.4. El control periódico 241
17.5. Convenios para realizar prácticas en empresas 241
17.6. La Certificación oficial 241
17.7. La entrega del Certificado Oficial 242
17.8. Pruebas de acceso a los ciclos formativos de grado medio 242
18. Cursos ocupacionales y de reciclaje 242
18.1. Diseño de los programas 242
18.2. Notificación de la expedición de títulos 243
19. Intercambios 243
19.1. Crédito variable 243
19.2. Selección de alumnos candidatos 243
19.3. Notificación al colegio receptor 244
19.4. Cesión de Datos 244
19.5. Fórum con otros centros 244
19.6. Estancias en el extranjero 245
19.7. Notificación y cesión de datos 245
19.8. Seguro adicional 246
20. Tutores, profesores, absentismo escolar y conflictos profesor-alumno 246
20.1. Acceso a los datos de los alumnos 246
20.2. Absentismo en «infantil» y «primaria» 246
20.3. Absentismo en ESO y Bachillerato 246
20.4. Notificación de incidencias de asistencia 247

20.5. Notificaciones por agenda escolar ... 247
20.6. Control de la lista de control de asistencia ... 248
20.7. El informe de incidentes ... 248
21. Cesión de datos ... 248
22. Información a padres separados ... 248
23. La red informática del centro ... 249
23.1. El Reglamento interno de seguridad ... 249
23.2. La red ... 249
23.3. Los identificadores de los alumnos ... 249
23.4. Los identificadores de los profesores ... 249
23.5. La conexión externa ... 250
B) EL PROCESO DE VERIFICACIÓN OCULAR ... 250
24. Las comprobaciones. El proceso de verificación ocular ... 250
24.1. El acceso al PAC Documental ... 250
24.2. Acceso a la agenda escolar ... 250
24.3. El archivo documental general ... 251
24.3.1. El archivo de expedientes del curso ... (en vigencia) ... 251
24.3.2. El archivo documental histórico ... 251
24.4. Las Solicitudes de inscripción ... 252
24.4.1. Ciclos Formativos Superiores ... 252
24.4.3. Primaria admitido ... 252
24.4.4. Infantil admitido ... 252
24.5. Aplicación que regula el fichero de alumnos del Centro ... 253
24.5.1. La entrada de datos a la aplicación ... 253
24.5.2. Datos de solicitudes sin concierto ... 253
24.5.3. Arranque del programa ... 253
24.5.4. Acceso a listado de infantil ... 254
24.5.5. Comprobación de datos antiguos ... 254
24.5.6. Impresión de la longitud de la información que consta informatizada respecto de la documental ... 254
24.6. La Secretaría ... 254
24.6.1. Libro Registro de Entrada ... 255
24.6.2. Libro Registro de Salida ... 255
24.7. Libro Registro Manual de expedición de títulos ... 255
24.8. Centros Sanitarios ... 256
24.9. Enfermería ... 256
24.9.1. Acceso al fichero documental ... 256
24.9.2. Infraestructura informática ... 256
24.9.3. Prestación asistencial ... 257
24.10. Departamento de Orientación ... 257
24.10.1. Despacho de la Responsable ... 257
24.10.2. Despacho del psicopedagogo ... 258
24.10.3. Fichero informático del departamento de Orientación ... 258
24.11. Acceso al programa de ... (la Generalitat) para expedición de títulos 258

24.12. Departamento de Formación-Trabajo ... 258
24.12.1. Convenio con una empresa ... 259
24.12.2. Programa de Garantía social ... 259
24.12.3. Acceso al programa del Departament de Treball ... 259
24.12.4. Solicitud de subvenciones ... 259
24.13. Departamento de Actividades Extraescolares ... 260
24.13.1. Alumnos inscritos en cada deporte ... 260
24.13.2. Acceso a los datos de los alumnos del centro ... 260
24.13.3. Hoja de inscripción de un equipo ... 260
25. Trituradoras de papel ... 260
26. Consentimiento a la inspección para recibir documentación con datos de carácter personal ... 260
26.1. Doc. 45 ... 261
26.2. Doc. 46 ... 261
27. Medidas de seguridad ... 261
27.1. Comunicación de las normas reglamentarias al personal del centro ... 261
27.2. Registro de Incidencias ... 262
27.3. Identificación y Autenticación ... 262
27.4. Perfiles ... 263
27.5. Locales ... 263
27.6. Registro de copias de recuperación y de respaldo ... 263
27.8. Responsable de Seguridad ... 264
27.9. Auditorías de verificación del cumplimiento ... 264
27.10. Pruebas con datos reales ... 265
27.11. Cifrado de los datos que viajan por la red ... 265
27.12. Trabajo externo con datos personales ... 265
28. Documentación a remitir a la agencia española de protección de datos ... 265

2. CLÁUSULAS REGULADORAS Y CONTRATOS PERIMETRALES ... 266

2.1. Ficha de prohibición de uso de la información de los trabajadores ... 266
2.2. Cláusula para los padres que gestionan el ampa ... 267
2.3. Cláusula para monitores de colonias ... 268
2.4. Carta para antiguos alumnos ... 268
2.5. Cláusula para personal temporal o subcontratado ... 269
2.6. Contrato perimetral tipo ... 269

CAPÍTULO IV. Modelo de Código tipo regulador del tratamiento deontológico de la información personal en los centros docentes ... 271

I. EXPOSICIÓN DE MOTIVOS ... 271

1. Antecedentes ... 271
2. Principios legales que fundamentan el código ... 272
De Derecho Comunitario. Normas imperativas de derecho positivo. ... 272

De derecho español ... 272
3. Valores añadidos que aporta el cumplimiento del Código ... 273

II. Objeto ... 274

III. Ámbito de aplicación ... 274

IV. Principios específicos del código deontológico ... 275

1. Principio de legitimación inequívoca ... 275
2. Principio de actividad única ... 276
3. Principio de unidad de actuación frente a los derechos de los afectados ... 276
4. Principio de legalización de las bases de datos ... 276
5. Principio de nivel ... 276

V. Normas de conducta y medidas de seguridad ... 277

Capítulo V. El tratamiento de la información sanitaria ... 331
1. Los medios y los profesionales ... 331
   1.1. El médico responsable ... 331
   1.2. El centro sanitario ... 331
   1.3. Personal del servicio ... 332
2. La documentación clínica ... 332
   2.1. La historia clínica ... 332
      2.1.1. Definición y archivo ... 332
      2.1.2. Contenido ... 333
         2.1.2.1. Tipos de datos de inclusión obligatoria ... 333
         2.1.2.2. La apertura de la historia clínica ... 334
         2.1.2.3. Acceso por el personal del servicio ... 335
         2.1.2.4. Acceso por el paciente ... 335
         2.1.2.5. Acceso por terceros ... 335
         2.1.2.6. Para fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia ... 336
   2.2. El consentimiento informado ... 336
      2.2.1. Definición y contenido ... 336
      2.2.2. Menores de edad e incapaces ... 337
      2.2.3. Información al paciente ... 337
      2.2.4. Excepciones a la obligatoriedad de consentir ... 338
   2.3. Instrucciones previas ... 339
      2.3.1. Definición y regulación ... 339
      2.3.2. Contenido ... 339
      2.3.3. Formalización ... 340
   2.4. Informe de alta ... 341
      2.4.1. Definición ... 341
      2.4.2. Hoja de informe de alta ... 341
      2.4.3. Hoja de continuación de informe de alta ... 341
      2.4.4. Hoja de petición de alta voluntaria ... 342

Capítulo VI. Modelo de documento de seguridad para los consultorios sanitarios ... 343

I. Objeto, ámbito de aplicación, recursos protegidos y estructura del sistema de seguridad ... 343

1. Objeto del documento ... 343
2. Ámbito de aplicación ... 343
3. Recursos protegidos (gerencia, personal, seguridad, mantenimiento e informática) ... 344
4. Estructura funcional del sistema de seguridad ... 345
5. El plan de seguridad ... 346

II. Medidas de seguridad ... 346

1. Medidas de seguridad en los edificios ... 347
   1.1. Clasificación de las zonas por el tipo de información que contienen ... 347
   1.2. Sistema de alarma en los edificios ... 348
      1.2.1. Armado del sistema ... 348
      1.2.2. Desarmado del sistema ... 348
      1.2.3. Durante y/o después de una alarma ... 349
   1.3. Régimen de uso de las videocámaras ... 349
   1.4. Procedimiento de gestión de llaves, claves, contraseñas o códigos de acceso físico a los lugares ... 349
      1.4.1. Gestión del acceso físico por llave única ... 349
      1.4.2. Control de acceso físico por adjudicación de llaves codificadas ... 350
   1.5. Los puestos de trabajo ... 350
2. Medidas de seguridad aplicables a los aparatos y soportes informáticos ... 351
   2.1. El sistema informático ... 351
      2.1.1. Aplicaciones de acceso a la base de datos ... 351
   2.2. Acceso al sistema nivel de usuario por contraseñas propias ... 353
      2.2.1. Asignación de identificadores ... 353
      2.2.2. Diseño de las autorizaciones y construcción del identificador ... 353
      2.2.3. Construcción del autenticador ... 354
      2.2.4. Asignación del autenticador provisional y asunción del código de acceso (password) definitivo ... 354
      2.2.5. Otros usos de las contraseñas ... 355
      2.2.6. Régimen legal y responsabilidad de los adjudicatarios de contraseñas. ... 355
   2.3. Identificación, inventariado y almacenamiento de soportes informáticos con datos de carácter personal ... 356
   2.4. Infraestructura de seguridad informática ... 360
      2.4.1. Roles y responsabilidades ... 360
      2.4.2. Copias de seguridad ... 360
      2.4.3. Gestión de incidencias ... 361
3. Uso de los medios en la entrada y la salida de los datos a través de la red ... 363

4. Controles periódicos de verificación del cumplimiento 364
4.1. Check-list para verificación del control periódico interno 364
5. El tratamiento de la información 367
5.1. Capacidad legal para tratar información de terceros 367
5.1.1. Legalización de los ficheros 367
5.1.1.1. Notificación para la inscripción de ficheros 367
5.1.1.2. Inscripción de los ficheros 367
5.1.1.3. Modificación y cancelación de la inscripción 368
5.1.2. Legitimación de los datos para poder ser tratados 368
5.1.2.1. Requisitos previos para proceder al tratamiento 368
5.1.2.2. Requisitos para la obtención del consentimiento de los afectados. Información del interesado 369
5.1.3. Régimen de tratamiento de la información con acceso a terceros 371
5.2. La entrada de información en la base de datos 373
5.2.1. El archivo documental de accesos 373
5.2.2. El archivo documental transitorio 373
5.3. Tratamiento y mantenimiento de los datos 374
5.3.1. Forma de tratamiento 374
5.3.2. El acceso a la base de datos general de administración del centro 374
5.3.3. Ubicuidad, adecuación y longitud 375
5.3.4. Calidad 375
5.3.5. Conservación 375
5.3.6. Destrucción 375
5.4. La cesión de información 375
5.4.1. El contrato perimetral 376

III. NORMAS DE CONDUCTA OBLIGATORIA COMÚN PARA TODO EL PERSONAL SANITARIO QUE INTERVENGA EN EL TRATAMIENTO DE LA INFORMACIÓN SOBRE PERSONAS FÍSICAS 377

1. Requisitos legales para el tratamiento de la información 377
1.1. Condiciones que se han de dar para poder iniciar la recogida de datos de personas 377
1.1.1. Calidad de los datos 377
1.1.2. Finalidad concreta antes de proceder a la recogida 378
1.1.3. Exactitud de la información contenida en los datos 378
1.1.4. Sustitución directa en caso de inexactitud 378
1.1.5. Cancelación cuando se haya terminado el objeto que hizo precisa su recogida 378
1.1.6. Conservación 378
1.2. Derecho de información del afectado en la recogida de datos 379
1.2.1. Modo en que hay que informar cuando los datos sean solicitados al afectado 379
1.2.2. Información obligatoria que hay que darle al afectado antes de pedirle los datos 379

1.2.3. Cuando los datos de carácter personal no hayan sido recabados del interesado 380
1.3. Obligación de solicitar el consentimiento al afectado 380
1.3.1. La obligación legal 380
1.3.2. Casos en los que no es preciso pedir el consentimiento por escrito 380
1.3.3. Revocación del consentimiento 380
1.3.4. Oposición 381
1.4. La comunicación de datos 381
1.4.1. Límites legales 381
1.4.2. Casos en los que no es preciso el consentimiento previo 381
1.4.3. Consentimiento nulo 382
1.4.4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable 382
1.4.5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la Ley de protección de datos. 382
1.4.6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores. 382
1.5. Acceso a los datos por cuenta de terceros 382
1.6. La seguridad de los datos 383
1.7. Los derechos de acceso, rectificación y cancelación 383
1.8. Tratamientos con fines de publicidad y de prospección comercial. El censo promocional 384
1.9. Tipos de infracciones 385
1.9.1. Infracciones leves 385
1.9.2. Infracciones graves 385
1.9.3. Infracciones muy graves 386
1.10. Niveles de seguridad 387
1.10.1. Aplicación de los niveles de seguridad 387
2. Normas obligatorias para los usuarios de los dominios, red, soportes y medios de telecomunicación, así como de tratamiento audiovisual de la información 388
2.1. Obligaciones de todo el personal dependiente del sanitario 388
2.1.1. Números de identificación y claves de acceso 388
2.1.2. Confidencialidad de la información 390
2.1.3. Uso del correo electrónico 390
2.1.4. Acceso a internet 391
2.1.5. Propiedad intelectual e industrial 391
2.1.6. Incidencias 392
2.1.7. Protección de datos 392
2.2. Funciones específicas de los responsables y encargados del fichero y del tratamiento de la información y de los datos 392
2.2.1. Funciones específicas del responsable del fichero 393
2.2.2. Funciones específicas del responsable de seguridad 393

2.2.3. Funciones del jefe de personal-encargado del subfichero de personal 394

CAPÍTULO VII. Modelo de documento de seguridad. Manual de funciones técnicas y jurídicas del servicio de teleasistencia 395

I. OBJETO, ÁMBITO DE APLICACIÓN, RECURSOS PROTEGIDOS Y ESTRUCTURA DEL SISTEMA DE SEGURIDAD 395

1. Objeto del documento 395
2. Ámbito de aplicación 395
3. Recursos protegidos 396
4. Estructura funcional del sistema de seguridad 397
5. El plan de seguridad 398

II. MEDIDAS DE SEGURIDAD 399

1. Medidas de seguridad en los edificios 399
   1.1. Clasificación de las zonas por el tipo de información que contienen 399
   1.2. Sistema de alarma en los edificios 401
      1.2.1. Armado del sistema 401
      1.2.2. Desarmado del sistema 401
      1.2.3. Durante y/o después de una alarma 401
   1.3. Régimen de uso de las videocámaras 401
   1.4. Procedimiento de gestión de llaves, claves, contraseñas o códigos de acceso físico a los lugares 401
      1.4.1. Gestión del acceso físico por llave única en la sede central en donde se coordina el servicio 401
      1.4.2. Las llaves de acceso a los domicilios de los usuarios del servicio 402
   1.5. Los puestos de trabajo 405
2. Medidas de seguridad aplicables a los aparatos y soportes informáticos 406
   2.1. El sistema informático 406
      2.1.1. Aplicaciones de acceso a la base de datos 406
   2.2. Acceso al sistema nivel de usuario por contraseñas propias 408
      2.2.1. Asignación de identificadores 408
      2.2.2. Diseño de las autorizaciones y construcción del identificador 408
      2.2.3. Construcción del autenticador 409
      2.2.4. Asignación del autenticador provisional y asunción del código de acceso (password) definitivo 409
      2.2.5. Otros usos de las contraseñas 410
      2.2.6. Régimen legal y responsabilidad de los adjudicatarios de contraseñas 410
   2.3. Identificación, inventariado y almacenamiento de soportes informáticos con datos de carácter personal 411
   2.4. Infraestructura de seguridad informática 413
      2.4.1. Roles y responsabilidades 413
      2.4.2. Copias de seguridad 414

2.4.3. Gestión de incidencias 415
3. Uso de los medios en la entrada y la salida de los datos a través de la red ... 416
4. Controles periódicos de verificación del cumplimiento 417
   Check-list para verificación del control periódico interno. 418
5. El tratamiento de la información 420
   5.1. Capacidad legal para tratar información de terceros 420
      5.1.1. Legalización de los ficheros 420
         5.1.1.1. Notificación para la inscripción de ficheros 421
         5.1.1.2. Inscripción de los ficheros 421
         5.1.1.3. Modificación y cancelación de la inscripción 422
      5.1.2. Legitimación de los datos para poder ser tratados por nuestros procedimientos 422
         5.1.2.1. Requisitos previos para proceder al tratamiento 422
         5.1.2.2. Requisitos para la obtención del consentimiento de los afectados. Información del interesado 423
      5.1.3. Régimen de tratamiento de la información con acceso a terceros 425
   5.2. La entrada de información en la base de datos 426
      5.2.1. El archivo documental de accesos 426
      5.2.2. El archivo documental transitorio 427
   5.3. Tratamiento y mantenimiento de los datos 428
      5.3.1. Forma de tratamiento 428
      5.3.2. El acceso a la base de datos general de administración del servicio .. 428
      5.3.3. Ubicuidad, adecuación y longitud 428
      5.3.4. Calidad 429
      5.3.5. Conservación 429
      5.3.6. Destrucción 429
   5.4. La cesión de información 429
      5.4.1. El contrato perimetral 430

III. NORMAS DE CONDUCTA OBLIGATORIA COMÚN PARA TODO EL PERSONAL SANITARIO EN EL TRATAMIENTO DE LA INFORMACIÓN SOBRE PERSONAS FÍSICAS 431

1. Requisitos legales para el tratamiento de la información 431
   1.1. Condiciones que se han de dar para poder iniciar la recogida de datos de personas 431
      1.1.1. Calidad de los datos 431
      1.1.2. Finalidad concreta antes de proceder a la recogida 432
      1.1.3. Exactitud de la información contenida en los datos 432
      1.1.4. Sustitución directa en caso de inexactitud 432
      1.1.5. Cancelación cuando se haya terminado el objeto que hizo precisa su recogida 432
      1.1.6. Conservación 432
   1.2. Derecho de información del afectado en la recogida de datos 433

1.2.1. Modo en que hay que informar cuando los datos sean solicitados al afectado 433
1.2.2. Información obligatoria que hay que darle al afectado antes de pedirle los datos 433
1.2.3. Cuando los datos de carácter personal no hayan sido recabados del interesado 434
1.3. Obligación de solicitar el consentimiento al afectado 434
1.4. La comunicación de datos 435
1.5. Acceso a los datos por cuenta de terceros 436
1.6. La seguridad de los datos 437
1.7. Los derechos de acceso, rectificación y cancelación 437
1.8. Tratamientos con fines de publicidad y de prospección comercial. El censo promocional 438
1.9. Tipos de infracciones 439
1.9.1. Son infracciones leves 439
1.9.2. Son infracciones graves 439
1.9.3. Infracciones muy graves 440
1.10. Niveles de seguridad 441
1.10.1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto 441
1.10.2. Aplicación de los niveles de seguridad [¿H?] 441
2. Normas obligatorias para los usuarios de los dominios, red, soportes y medios de telecomunicación, así como de tratamiento audiovisual de la información 442
2.1. Obligaciones de todo el personal del servicio 442
2.1.1. Números de identificación y claves de acceso 442
2.1.2. Confidencialidad de la información 444
2.1.3. Uso del correo electrónico 445
2.1.4. Acceso a internet 445
2.1.5. Propiedad intelectual e industrial 446
2.1.6. Incidencias 446
2.1.7. Protección de datos 446
2.2. Funciones específicas de los responsables y encargados del fichero y del tratamiento de la información y de los datos 447
2.2.1. Funciones específicas del responsable del fichero 447
2.2.2. Funciones específicas del responsable de seguridad 447
2.2.3. Funciones del jefe de personal-encargado del subfichero de personal 448

GLOSARIO TERMINOLÓGICO 449