# PROTECCIÓN DE DATOS DE SALUD
# CRITERIOS Y PLAN DE SEGURIDAD

Pau López, Francesc Moya, Santiago Marimón,
Ignasi Planas

(Editores)

DIAZ DE SANTOS

# AUTORES Y COLABORADORES

Este libro es el resultado de un trabajo colectivo coordinado por un **Grupo de Trabajo** de responsables y técnicos de Sistemas de Información del Consorci Hospitalari de Catalunya (CHC) y de algunos de sus Centros sanitarios asociados. Grupo de Trabajo integrado por:

Oscar Barrabés Vilafranca, Hospital General de Vic.
Josep Mª Coll Riumbau, Hospital General de Manresa.
Guillem Herrera Fontanals, Consorci Sanitari de l'Alt Penedès.
Pau López García, Hospital de la Santa Creu i Sant Pau.
Francesc Llampallas Miró, Hospital de la Santa Creu i Sant Pau.
Santiago Marimón Suñol, Consorci Hospitalari de Catalunya.
Francesc Miquel Gavaldà, Pius Hospital de Valls.
Jordi Morell Vilanova, Hospital de la Santa Creu i Sant Pau.
Francesc Moya Olvera, Hospital General de Granollers.
Ignasi Planas Costa, Institut Municipal d'Assistència Sanitària.

Dentro del Grupo de Trabajo la principal **labor de integración**, revisión y adaptación de textos existentes, así como de confección de nuevos, la han realizado:

Pau López García.
Francesc Moya Olvera.

El Grupo de Trabajo ha contado también con la colaboración de la **Asesoría Jurídica** del Consorci Hospitalari de Catalunya (CHC) y aportaciones de su documento «*El deure de confidencialitat*», Informes jurídics. CHC. Junio 2000»:

Francesc José María Sánchez.
Iolanda Puiggròs Jiménez de Anta.

La División de Sistemas y Tecnologías de la Información y las Comunicaciones del CHC elaboró un modelo de «*Pla de Seguretat dels Accessos a Dades Automatitzades de Caràcter Personal en l'Hospital de...*», que fue analizado y revisado por Responsables de Sistemas de Información de Centros sanitarios del CHC y adaptado, entre otros, en hospitales a los que pertenecen los miembros del Grupo de Trabajo. A destacar, por su utilización en este libro, el trabajo de adaptación realizado en el Hospital General de Granollers y en el Hospital de la Santa Creu i Sant Pau. En su labor, el Grupo de Trabajo consideró estas adaptaciones e incorporó también, una vez adecuados según las características del libro, los documentos que se estaban desarrollando en el Hospital de la Santa Creu i Sant Pau —particularmente sobre Acceso a la Información Asistencial— y en el Institut Municipal d'Assistència Sanitària —particularmente sobre Política de Seguridad del Sistema de Información.

El Grupo de Trabajo ha contado también con algunas colaboraciones colectivas:

**Participantes del Hospital de la Santa Creu i Sant Pau, Barcelona:**

Xavier Borràs Pérez, Jefe de Ecocardiología.
Josep Corbella Duch, Asesoría Jurídica.
Pau López García. Departamento de Informática.
Francesc Llampallas Miró, Jefe de Sistemas, Departamento de Informática.
Jordi Morell Vilanova, Jefe del Departamento de Informática.
Mª Virtudes Pacheco Galvan, Jefe del Servicio de Atención al Usuario.
Juliana Ribera Catarina, Directora de Sistemas de Información para la Gestión.
Maria Rovira Barberà, Jefe del Servicio de Documentación Médica.
Montserrat Rue Monne, Servicio de Epidemiología.

**Participantes del Institut Municipal d'Assistència Sanitària, Barcelona:**

Mª Carmen Álvarez Abella, Departamento de Informática.
Marina Clarambo Semis, Servicio de Documentación Clínica.
Núria Martín Lafuente, Departamento de Informática.
Ignasi Planas Costa, Departamento de Informática.
Antonio Ramos Muñoz, Departamento de Informática.
Pilar Torre Lloveras, Servicio de Documentación Clínica.
Joan Viñas Trullenque, Servicio de Documentación Clínica.

**Participantes del Hospital General de Granollers:**

Francesc Moya Olvera - Departamento de Sistemas de Información.
Antoni Navinés Vera - Departamento de Sistemas de Información.
Victoria Nortes Muntades - Coordinadora de la Comisión de Ética Asistencial.
Albert Riera Clapés - Departamento de Sistemas de Información.

**Panel de Responsables y Técnicos de Sistemas de Información revisores del Plan de Medidas de Seguridad, modelo** (además de los miembros del Grupo de Trabajo) :

Domingo Barrabés Moreno, BCGEST.
Cèlia García González, Hospital de Puigcerdà.
Lluïsa Giménez Carola, Consorci Hospitalari de Catalunya.
Anna Gómez Gabarra, Institut d'Assistència Sanitària.
Josep Mª Lisbona Ginesta, Hospital de Palamós.
Xavier Martínez Fontes, Consorci Hospitalari de Catalunya.
Josep Parés Marimón, Fundació Sanitària d'Igualada.
Josepa Ribes Puig, Institut Català d'Oncologia.
Josep Mª Roca Salvatella, Institut d'Assistència Sanitària.
Alicia Romero Alonso, Hospital Municipal de Badalona.
Josep Soriano Barbau, SAGESSA.
Josep Manel Vicente Colomer, Pius Hospital de Valls.
Josep Mª Vidal Codina, Hospital de la Santa Creu, Vic.
Maria Vila Font, Consorci Sanitari de la Creu Roja a Catalunya.
Josep Vila Sans, Hospital de Palamós.

# ÍNDICE

**Autores y colaboradores** ..... VII

**Prólogo** ..... XVII

**Introducción** ..... XIX

**Primera Parte**
**POLÍTICA DE SEGURIDAD DE UN SISTEMA DE INFORMACIÓN HOSPITALARIO**

1. INTRODUCCIÓN ..... 3
2. CRITERIOS DE CONFIDENCIALIDAD ..... 4
   - 2.1. Derecho a la intimidad-deber de confidencialidad ..... 4
   - 2.2. Contenido del deber de confidencialidad ..... 5
     - *2.2.1. Excepciones al deber de confidencialidad* ..... 7
   - 2.3. Consecuencias de la vulneración del deber de confidencialidad .. 8
   - 2.4. Criterios para la recogida, tratamiento y comunicación de datos de salud en la Ley de Protección de Datos ..... 10
     - *2.4.1. Tratamiento* ..... 10
     - *2.4.2. Recogida* ..... 11
     - *2.4.3. Comunicación a terceros* ..... 12
     - *2.4.4. Conclusión* ..... 13
3. CRITERIOS LEGALES DE SEGURIDAD ..... 13
   - 3.1. Marco legal ..... 13
   - 3.2. Ámbito de aplicación y calidad de los datos ..... 14
   - 3.3. Recogida de los datos y consentimiento ..... 15
   - 3.4. Datos especialmente protegidos ..... 16
   - 3.5. Confidencialidad ..... 17
   - 3.6. Derechos de las personas ..... 18
   - 3.7. Transferencia internacional de datos ..... 19
   - 3.8. Criterios de aplicación ..... 19

4. CRITERIOS DE PARTICIPACIÓN (MOTIVACIÓN) ..... 21
5. CRITERIOS DE DIFUSIÓN ..... 22
5.1. Criterios de difusión al personal ..... 22
*5.1.1. Difusión inicial* ..... 22
*5.1.2. Información de mantenimiento* ..... 22
5.2. Criterios de difusión a pacientes ..... 22
5.3. Plan de difusión al personal ..... 23
*5.3.1. Difusión inicial. Puesta en marcha del Plan de Seguridad*.. 23
*5.3.2. Mantenimiento* ..... 23
5.4. Plan de difusión a pacientes ..... 24
5.5. Plan de difusión a terceros ..... 24

**Segunda Parte**
**REGLAMENTO DE ACCESO A LA INFORMACIÓN ASISTENCIAL**

1. INTRODUCCIÓN ..... 29
2. ANTECEDENTES Y EVOLUCIÓN HISTÓRICA ..... 30
3. OBJETIVO ..... 31
4. NORMAS DE ACCESO A LA INFORMACIÓN CLÍNICA ..... 31
4.1. Criterios de la Ley Catalana ..... 31
4.2. Criterios de acceso a los datos personales ..... 32
*4.2.1. Criterio de motivo de consulta de los datos* ..... 32
*4.2.2. Criterio de tipos de datos* ..... 33
*4.2.3. Criterio de ámbito de trabajo* ..... 34
*4.2.4. Criterio de perfil funcional* ..... 35
*4.2.5. Criterio de autorización de acceso* ..... 36
*4.2.6. Criterio de grupos de pacientes* ..... 36
4.3. Accesibilidad a los datos en función de los criterios ..... 36
*4.3.1. Acceso a los datos identificativos* ..... 37
*4.3.2. Acceso a los datos médicos* ..... 37
*4.3.3. Acceso a los datos médicos especialmente sensibles* ..... 38
5. RECOMENDACIONES, DERECHOS Y OBLIGACIONES DEL PERSONAL ..... 38
6. NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS ..... 41
ANEXOS:
Anexo 1. Normas de acceso a la información con finalidades de investigación ..... 45
Anexo 2. Tablas de estructura de los accesos a los datos ..... 46
Anexo 3. Información interna sobre la Normativa de protección de datos relacionados con la salud ..... 49
Anexo 4. Manual para personal de primer contacto ..... 52

## Tercera Parte
## PLAN DE MEDIDAS DE SEGURIDAD

**I. PRESENTACIÓN** ..... 57

**II. PLAN DE MEDIDAS DE SEGURIDAD (MODELO)** ..... 59

1. Objeto, estructura y evolución del plan de seguridad ..... 59
   1.1. Estructura de coordinación del plan de seguridad ..... 60
   1.2. Evolución del plan de seguridad ..... 62
   1.3. Niveles de seguridad definidos ..... 62
   1.4. Clasificación de los ficheros según contenido y niveles de seguridad ..... 63
2. Ámbito de aplicación ..... 64
3. Medidas, normas y procedimientos ..... 65
   3.1. Procedimientos de identificación y autenticación ..... 65
   3.2. Procedimientos de asignación, comunicación y archivo de las palabras de paso ..... 65
   3.3. Procedimientos y medidas organizativas y técnicas para preservar física y electrónicamente los recursos y soportes informáticos ... 66
   3.4. Normas específicas del fichero ..... 66
   3.5. Soportes informáticos ..... 66
      *3.5.1. Inventario* ..... 66
      *3.5.2. Ubicaciones y personal autorizado* ..... 67
      *3.5.3. Registro de salidas* ..... 67
      *3.5.4. Reciclaje/Obsolescencia de los soportes* ..... 69
4. Funciones y obligaciones para la Seguridad de los datos de carácter personal ..... 69
   4.1. Funciones y obligaciones del personal específicas según función ..... 69
      *4.1.1. Dirección General* ..... 69
      *4.1.2. Coordinador del Plan de Seguridad* ..... 69
      *4.1.3. Responsable interno del fichero* ..... 71
      *4.1.4. Responsable de aplicación* ..... 72
      *4.1.5. Responsable de seguridad* ..... 72
      *4.1.6. Personal de administración del sistema o personal informático* ..... 73
      *4.1.7. Responsable del Registro de Incidencias* ..... 74
      *4.1.8. Responsable del Libro de Calidad* ..... 74
      *4.1.9. Responsabilidades del personal con acceso a Datos Protegidos* ..... 74
      *4.1.10. Personal de mantenimiento y limpieza* ..... 75
   4.2. Funciones y obligaciones generales del personal ..... 75

*4.2.1. Cláusulas especiales para el personal contratado* ..... 75
*4.2.2. Cláusulas especiales para las empresas prestadoras de servicios* ..... 76
*4.2.3. Cesión de información* ..... 76
*4.2.4. Funciones y obligaciones hacia la confidencialidad* ..... 77
*4.2.5. Funciones y obligaciones hacia las palabras de paso* ... 77
*4.2.6. Funciones y obligaciones hacia las incidencias* ..... 78
*4.2.7. Funciones y obligaciones hacia los soportes de información* ..... 78
*4.2.8. Funciones y obligaciones hacia los ficheros temporales* 79
*4.2.9. Funciones y obligaciones hacia las conexiones externas o remotas* ..... 79
*4.2.10. Funciones y obligaciones hacia los ficheros de uso propio* ..... 80
*4.2.11. Funciones y obligaciones hacia los pacientes.* ..... 80
4.3. Descripción de los accesos ..... 80
*4.3.1. Sistemas informáticos* ..... 80
*4.3.2. Monitorización o fiscalización* ..... 81
4.4. Descripción de las funciones y responsabilidades del personal de informática propio y ajeno ..... 81
5. Estructura de ficheros ..... 82
6. Procedimientos sobre Incidencias: notificación, gestión y respuesta.. 82
6.1. Registro de incidencias ..... 82
6.2. Circuito de notificación ..... 84
7. Procedimientos de realización de copias de seguridad, restauración de los datos, parada y puesta en funcionamiento ..... 84
8. Calendario de adaptación a las normas del plan de seguridad ..... 85

**III. GUÍA PRÁCTICA DE APLICACIÓN DEL PLAN DE MEDIDAS DE SEGURIDAD** ..... 87

1. INTRODUCCIÓN ..... 87
2. ¿CÓMO DECLARAR LOS FICHEROS A LA APD? ..... 87
3. ¿CÓMO RELLENAR LOS ANEXOS? ..... 89
4. ¿QUÉ FICHEROS DECLARAMOS? ¿QUÉ FICHEROS LÓGICOS NOS PODEMOS ENCONTRAR? ..... 92

**IV. ANEXOS DEL PLAN DE MEDIDAS DE SEGURIDAD** ..... 97

**A.** Inventario Ficheros Lógicos: descripción y relaciones ..... 97
**B.** Inventario general de Hardware ..... 100

**C.** Relación de Software ..... 101
**D.** Procedimientos de identificación y autenticación..... 102
**E.** Procedimientos de asignación, comunicación y archivo de palabras de paso ..... 103
**F.** Procedimientos y medidas organizativas y técnicas para preservar física y electrónicamente los recursos y los soportes informáticos ..... 104
**G.** Normas específicas fichero ..... 105
**H.** Registro de la evolución de los ficheros y sus soportes informáticos: inventario, ubicaciones y personal autorizado, registro de salidas, reciclaje y obsolescencia ..... 106
**I.** Inventario de soportes: creación, recepción y bajas ..... 107
**J.** Autorización de salida de soporte ..... 108
**K.** Descripción accesos ..... 109
**L.** Descripción de las funciones y responsabilidades del personal de informática propio y ajeno ..... 110
**M.** Relación de ficheros declarados según formulario APD ..... 111
**N.** Estructura de ficheros ..... 112
**O.** Formularios Registro Incidencias ..... 113
**P.** Procedimientos de realización de copias de seguridad, restauración de los datos, parada y puesta en marcha ..... 116
**Q**. Plazos de implantación de las medidas de seguridad ..... 117
**R**. Modelos para ejercer los derechos de acceso, cancelación y rectificación ..... 131

**Índice analítico**..... 139

**Versión CD-Rom** ..... 141

cular que «*únicamente tratará los datos conforme a las instrucciones del responsable*», «*que no los aplicará o utilizará con fin distinto al que figure en dicho contrato*» y que «*ni los comunicará (...) a otras personas*» (art. 12.2).

### *2.4.4. Conclusión*

La nueva regulación de la protección de datos de carácter personal ha introducido una serie de limitaciones al derecho de la información en la recogida de datos y de excepciones a la regla general del consentimiento del afectado por el tratamiento y la comunicación de sus datos personales relativos a la salud, que hace innecesaria la elaboración de un documento de consentimiento específico del paciente autorizando a la institución sanitaria el tratamiento de sus datos de salud o su comunicación a terceros cuando resulten necesarios para la prevención o para el diagnóstico médico, para la prestación de la asistencia sanitaria o tratamientos médicos, para la gestión de servicios sanitarios o para la realización de estudios epidemiológicos, estadísticos o científicos.

Será necesaria una información al paciente en la recogida de los datos en los términos que hemos expresado en este trabajo y, sobre todo, deben adoptarse las medidas de seguridad de índole técnica y organizativa más adecuadas para garantizar que no podrán acceder a los datos de salud de los pacientes personas no autorizadas que, en definitiva, es la mejor forma de garantizar su derecho a la intimidad y a la confidencialidad de toda la información relacionada con su proceso y su estancia en el hospital, que la Ley General de Sanidad les otorga.

## 3. CRITERIOS LEGALES DE SEGURIDAD

Se definen con el objetivo de establecer la política general de la institución y así garantizar la seguridad de los datos.

### 3.1. Marco legal

• La Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPDCP), tiene por objeto garantizar y proteger los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar. Modifica la anterior Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD).

• Directiva 95/46CE 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 los datos personales y a la libre circulación de éstos.

• El Real Decreto 1332/94 de 20 de junio por el que se desarrollan algunos preceptos de la LORTAD para dictar las disposiciones necesarias para la aplicación y desarrollo de la referida Ley. Regula determinados aspectos, en su mayoría de orden procedimental, referentes al ejercicio de los derechos de acceso, rectificación y cancelación.

• 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.

• En Cataluña: Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica (DOGC n.º 3303, de 11 de enero de 2001).

En los siguientes apartados se citan, casi textualmente, los párrafos más significativos de los artículos más relevantes en seguridad de datos de salud de la Ley de Protección de Datos (LOPDCP).

### 3.2. Ámbito de aplicación y calidad de los datos

*Artículo 2*. Ámbito de Aplicación:

• Será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

*Artículo 4*. Calidad de los datos**:**

• Los datos de carácter personal sólo se podrán recoger cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido.

• No podrán usarse para finalidades distintas de aquellas para las que fueron recogidos.

• Deberán ser exactos y puestos al día.

• Si no son exactos o están incompletos deben ser cancelados o sustituidos por los correctos.

• Serán cancelados cuando dejen de ser necesarios. No podrán ser conservados (salvo en el caso en que se decida su mantenimiento por valores históricos) una vez que dejen de ser útiles para la función prevista.

• Se almacenarán de forma tal que permitan el ejercicio del derecho de acceso a los mismos del afectado.

• Prohibición de recogida de datos por medios fraudulentos, desleales o ilícitos.

### 3.3. Recogida de los datos y consentimento

*Articulo 5*. Derecho de información en la recogida de datos:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

   *a)* De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

   *b)* Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

   *c)* De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

   *d)* De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

   *e)* De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos de forma claramente legible las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, (…).
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea (…).

*Artículo 6*. Consentimiento del afectado:

1. El tratamiento de los datos de carácter personal requerirá del consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, cuando se refieran a las partes de un contrato o precontrato de una relación negocial o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6,…
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado, y siempre que una ley no disponga lo contrario, el afectado podrá oponerse al tratamiento de sus datos.

### 3.4. Datos especialmente protegidos

*Artículo 7*. Datos especialmente protegidos:

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.
3. Los datos que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
6. No obstante podrán ser objeto del tratamiento los datos de carácter personal a los que se refiere el apartado 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos o la gestión de servicios sanitarios.

*Artículo 8*. Datos relativos a la salud:

Sin perjuicio de lo que se dispone en el artículo 11 respecto a la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos.

### 3.5. Confidencialidad

*Artículo 9*. Seguridad de los datos:

El responsable del fichero, y en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal.

*Artículo 10*. Deber de secreto:

El responsable de fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos.

*Artículo 11*. Comunicación de datos:

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:

   *a)* Cuando la cesión está autorizada en una ley.

   (…)

   *c)* Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

   (...)

   *f)* Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

*Artículo 12*. Acceso a los datos por cuenta de terceros.

### 3.6. Derechos de las personas

*Artículo 13*. Impugnación de valoraciones:

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

*Artículo 14*. Derecho de consulta al Registro General de Protección de Datos.

*Artículo 15*. Derecho de acceso

*Artículo 16*. Derecho de rectificación y cancelación:

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

   …

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan notificado.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

*Artículo 17*. Procedimiento de oposición, acceso, rectificación o cancelación.

*Artículo 18*. Tutela de derechos:

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

*Artículo 19*. Derecho a indemnización:

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

### 3.7. Transferencia internacional de datos

*Artículo 33*. Norma general:

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

*Artículo 34*. Excepciones:

*a)* Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

*b)* Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

*c)* Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

(...)

### 3.8. Criterios de aplicación

El Real Decreto 994/1999 de 11 de junio establece tres niveles de seguridad:

- básico, para ficheros con datos personales;
- medio, para ficheros con datos económicos, hacienda, infracciones, etc;
- alto, para ficheros con datos de salud, ideología, origen racial, cuando permitan la identificación ideológica, etc.

Las medidas exigidas para el nivel básico han de cumplirse el 26 de marzo de 2000, las de nivel medio, el 26 de junio de 2000; y las de nivel alto, el 26 de junio de 2001*.

* Estos plazos se aplican para los sistemas de información en funcionamiento el 26 de junio de 1999. Los nuevos sistemas de información deben cumplir ya con las medidas de los niveles que les corresponda.

Los tipos de datos de carácter personal incluidos dentro de estos niveles de seguridad son los siguientes:

| **NIVELES DE SEGURIDAD** | |
|---|---|
| *Nivel Básico*. Incluyendo algunos de los siguientes tipos de datos, cuando no constituyan un perfil de la persona:<br>Identificativos.<br>Características personales.<br>Circunstancias sociales<br>Académicos y profesionales.<br>Empleo y carrera administrativa.<br>Información comercial.<br>Económico-financieros.<br>Transacciones. | Medidas de seguridad de nivel básico. |
| *Nivel Medio*. Incluyendo datos del nivel básico que sí conformen un perfil de la persona:<br>Hacienda Pública.<br>Servicios financieros.<br>Solvencia patrimonial y crédito.<br>Infracciones penales y administrativas nivel medio. | Medidas de seguridad de nivel medio. |
| *Nivel Alto*. Cuando los datos se recaben para fines policiales y datos especialmente protegidos:<br>Ideología.<br>Creencias.<br>Religión.<br>Origen racial.<br>Salud.<br>Vida sexual. | Medidas de seguridad de nivel alto. |

El Real Decreto establece la necesidad de disponer de un *registro de incidencias* que permita a los usuarios internos y externos del centro dejar constancia de los problemas detectados en los ficheros de datos con los que trabaja el hospital y de las actuaciones derivadas de los mismos. Este registro es obligatorio por Ley.

Una incidencia es *cualquier evento* que pueda producirse esporádicamente y que pueda suponer un *peligro para la seguridad de los datos protegidos*, entendida bajo las tres vertientes de confidencialidad, integridad y disponibilidad de los datos:

- *Confidencialidad*. Los datos deben ser de fácil acceso sólo para los usuarios autorizados. La información debe estar protegida respecto a la consulta, modificación o destrucción por personas no autorizadas para evitar alteraciones y un uso incorrecto.
- *Integridad*. Una vez introducido un dato, éste debe mantenerse correctamente y ser actualizado adecuadamente cuando corresponda. El acceso a una información o dato debe ser suficientemente completa para no distorsionar el contenido de la misma.
- *Disponibilidad*. Los datos están disponibles para la persona que los necesita, en el momento que los necesita y en donde esté ubicada, siempre y cuando sea una disponibilidad autorizada (persona y ubicación).

El mantenimiento de un registro de incidencias que comprometen la seguridad de los datos personales es un instrumento imprescindible para la prevención de posibles ataques a esta seguridad y para la persecución de los responsables de los mismos.

## 4. CRITERIOS DE PARTICIPACIÓN (MOTIVACIÓN)

La motivación de los diferentes profesionales y, consecuentemente, la participación activa de la totalidad de los agentes del sistema se considerará un elemento básico para conseguir los objetivos del Plan de Seguridad y para mantener posteriormente, los niveles exigibles.

La participación de los diferentes profesionales implicados, tanto en el desarrollo inicial como en el seguimiento del Plan de Seguridad, se articula mediante el *Coordinador o Comité de Seguimiento* del Plan de Seguridad que coordinará y trabajará con los representantes de los diferentes estamentos de la institución con impacto en el sistema de información. (La caracterización del Plan de Seguridad es objeto de la tercera parte del libro).

Este *Coordinador o Comité de Seguimiento*, tal y como se describe en el apartado siguiente sobre «Criterios de difusión al personal», tiene la responsabilidad de diseñar las acciones informativas adecuadas para poder dar a conocer la existencia del Plan a la totalidad del personal canalizándolas a través de los responsables de ficheros y aplicaciones.

Una vez implementado el Plan de Seguridad, este Comité deberá mantener actualizada la información relativa a posibles modificaciones del mismo para adaptarlo a los cambios legislativos.

*El registro de incidencias* es un instrumento importante de participación, en la medida en que permite tanto a trabajadores de la institución como a usuarios