Responsabilidad y aspectos legales de la protección de datos personales en los sistemas de información sanitarios

Luis Fernández Luque
José Manuel Sánchez Parrado
Natalia Almudevar Arnal
Anna García Martínez

PID_00193890

Tiempo mínimo previsto de lectura y comprensión: **4 horas**

UOC
Universitat Oberta de Catalunya

Índice

1. Régimen jurídico de la protección de datos 5
1.1. La protección de datos en el ámbito sanitario 5
1.2. Aspectos básicos de la protección de datos 6
1.2.1. Origen y evolución legislativa 6
1.2.2. La protección de datos. Definición 7
1.2.3. Ámbito de aplicación 7
1.3. LOPD: principales obligaciones de la normativa sobre protección de datos 8
1.3.1. Notificación de la creación, modificación o supresión de ficheros 8
1.3.2. Principios de la protección de datos 11
1.3.3. Derechos de los afectados 16
1.4. Reglamento de Medidas de Seguridad 18
1.4.1. Objeto y ámbito de aplicación 18
1.4.2. Niveles de seguridad 19
1.4.3. Medidas de seguridad 20
1.5. Régimen sancionador 22
1.5.1. Autoridades de control 22
1.5.2. Infracciones y sanciones 22

2. Introducción a los elementos técnicos de modelos de seguridad 25
2.1. Fundamentos de seguridad técnica 25
2.1.1. Niveles de seguridad 28
2.2. Firma electrónica y criptografía 32
2.2.1. Identificación y autenticación 32
2.2.2. Nociones básicas de criptografía 33
2.2.3. Validez legal y regulación de la firma electrónica 34
2.3. Plan director de seguridad 35

3. Aspectos legales en las aplicaciones móviles 39
3.1. Marco legal de las aplicaciones móviles 39
3.2. Aplicaciones de salud 40
3.2.1. Un caso práctico de certificación en España 42
3.3. Otras normativas internacionales 43
3.3.1. Normativa IEC 62304 43
3.3.2. UK MHRA 44
3.3.3. USA-FDA 44
3.4. Seguridad 45
3.4.1. Protección de datos 45
3.4.2. *Big data* 45
3.4.3. Transparencia 45

3.4.4. Casos de autorregulación 45

4. Anexos..... 47
4.1. Legislación 47
4.2. Otra documentación de interés 49
4.3. Recursos en Internet 49

1. Régimen jurídico de la protección de datos

1.1. La protección de datos en el ámbito sanitario

Los datos tratados en el ámbito sanitario son necesarios para prestar adecuadamente la atención sanitaria a la que los ciudadanos tienen derecho; si bien, más allá de esta esfera de prestación sanitaria, existe el ámbito de la intimidad de las personas, que requiere que los profesionales sanitarios, así como los gerentes de los centros sanitarios, observen los principios de la normativa sobre protección de datos personales y den cumplimiento a las obligaciones recogidas en ella.

La normativa sobre protección de datos personales y, en particular, la LOPD (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal), tiene como finalidad:

> "[...] garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."

Por lo tanto, y atendiendo a la definición que dicha norma establece de fichero, "[...] todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", queda patente que tanto la gestión de la historia clínica, como cualquier otro tratamiento de datos personales realizado por los centros sanitarios quedan sujetos a las obligaciones de la citada normativa.

La LOPD califica los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen especialmente riguroso para su obtención, tratamiento, custodia y posibles comunicaciones.

Con la aprobación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica y, en Cataluña, de la Ley 21/2000, de 29 de diciembre sobre los derechos de información concerniente a la salud y la autonomía del paciente y la documentación clínica, se regula por primera vez de forma específica la historia clínica y la protección de datos médicos.

1.2. Aspectos básicos de la protección de datos

1.2.1. Origen y evolución legislativa

La normativa sobre protección de datos personales surge como consecuencia de la preocupación del legislador ante los riesgos asociados al desarrollo de las nuevas tecnologías. El desarrollo de grandes computadoras se considera como una nueva amenaza potencial dadas las posibilidades que ofrecen para los tratamientos masivos de información.

Esto hace que el legislador considere necesario regular estos aspectos con la finalidad de proteger la intimidad de los ciudadanos, lo cual se lleva a cabo mediante el mandato al legislador recogido en la Constitución de 1978, que establece en su artículo 18.4 que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

No es hasta 1992 cuando dicho mandato es desarrollado con la aprobación de la LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal), la cual, y atendiendo a lo establecido en su articulado, tenía por objeto:

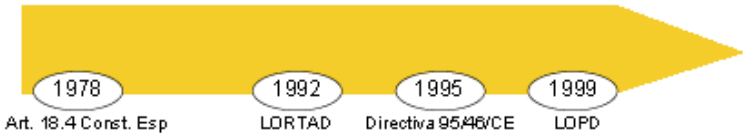
> "[...]limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos."

Debemos destacar que, dado que la preocupación era el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos, el ámbito de aplicación de la LORTAD venía limitado a los datos de carácter personal que figuraran en ficheros automatizados.

La aprobación, en 1995, de la Directiva 95/46/CE establece un marco común para todos los países miembros de la Unión Europea, ampliando el ámbito de aplicación:

> "Las disposiciones de la presente directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."
>
> 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.

Finalmente, en diciembre de 1999, se publica la LOPD, que tiene como principal novedad ampliar el ámbito de aplicación a todo tipo de ficheros, independientemente del soporte en el cual sean tratados. Asimismo, se adecua a lo establecido en la directiva. En la actualidad, es la norma básica vigente en materia de protección de datos personales.



Principales hitos legislativos en materia de protección de datos personales

1.2.2. La protección de datos. Definición

El derecho a la protección de datos es un derecho fundamental de todas las personas, que se traduce en la potestad de control sobre el uso que se realiza de sus datos personales.

Tras la aprobación de la LOPD, la Sentencia 292/2000 del Tribunal Constitucional viene a reconocer el derecho a la protección de datos como un derecho fundamental independiente del derecho al honor, intimidad e imagen, dotando a la protección de datos de carácter personal, de este modo, de identidad propia e independiente de cualquier otro derecho fundamental.

Por lo tanto, toda organización pública o privada que trate datos personales está obligada a cumplir los requerimientos establecidos en la LOPD, normativa de desarrollo y normativa sectorial aplicable.

Como premisa, deberíamos identificar qué se entiende por dato personal. Atendiendo a la definición establecida por la LOPD, un dato personal es "cualquier información concerniente a personas físicas identificadas o identificables". Esto supone que en el momento en que se recabe o trate información, como nombre y apellidos, DNI, dirección de correo electrónico, número de historia clínica, imagen, cualquier código de identificación personal, etc., estaremos ante un fichero objeto de la normativa.

1.2.3. Ámbito de aplicación

Desde la aprobación de la LOPD, la normativa vigente se aplica a los datos de carácter personal registrados en cualquier soporte que los haga susceptibles de tratamiento, así como a su uso posterior:

- Soporte informático: aplicaciones, bases de datos, etc.

- Soporte papel: ficheros manuales organizados que recojan toda la información clínica de un proceso asistencial a un paciente, el expediente de un trabajador, etc.

La normativa se aplica tanto a los ficheros públicos (titularidad de la Administración), como a ficheros privados (titularidad de empresas) en tanto que contengan datos personales.

La normativa no se aplica a:

- Ficheros que hayan sido sometidos a un procedimiento de disociación; es decir, que no sea posible asociar la información a una persona física identificada o identificable.

- Ficheros mantenidos por personas físicas en el ejercicio de sus actividades personales o domésticas.

- Ficheros relativos a materias clasificadas.

- Ficheros relativos a terrorismo o delincuencia organizada.

Existen una serie de supuestos en los que los ficheros se regirán por sus disposiciones específicas y por lo especialmente previsto en la LOPD, como es el caso de los ficheros estadísticos, entendiendo por fichero estadístico aquel que sirva a fines exclusivamente estadísticos y esté amparado por la legislación estatal o autonómica sobre la función estadística pública. Asimismo, están sujetos a régimen específico:

- Los ficheros regulados por la legislación de régimen electoral
- Los ficheros de las fuerzas armadas
- El Registro Civil y Registro de Penados y Rebeldes
- Videocámaras de cuerpos y fuerzas de seguridad

No son objeto de la normativa los datos relativos a las personas jurídicas.

1.3. LOPD: principales obligaciones de la normativa sobre protección de datos

1.3.1. Notificación de la creación, modificación o supresión de ficheros

Una de las principales obligaciones establecidas por la normativa es la de notificar a la autoridad de control correspondiente la creación de ficheros que contengan datos personales. En el caso de que ya existan, deberá notificarse a la autoridad de control correspondiente la modificación o supresión de los mismos.

Entidades privadas

El artículo 25 de la LOPD establece:

> "Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que esta ley establece para la protección de las personas".

Además, el artículo 26.1. LOPD establece:

> "Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos".

Previamente a la notificación de ficheros tratados, se deben identificar los tratamientos de datos realizados. Para ello, es necesario mantener entrevistas con las áreas que tratan los datos personales con el fin de identificar su origen, tipología, finalidades del tratamiento, tratamientos realizados, nivel de seguridad a aplicar, cesiones o comunicaciones de datos y transferencias internacionales de datos.

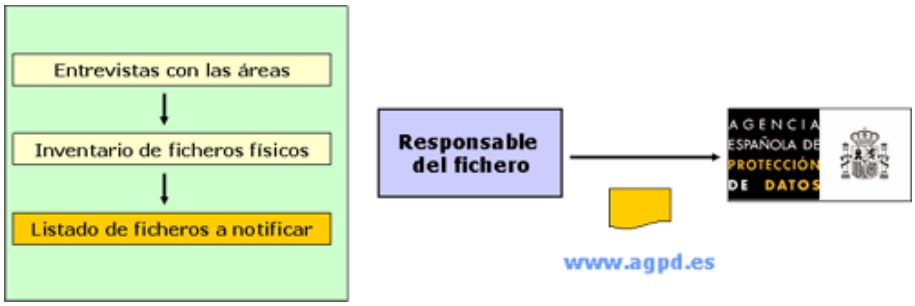
Una vez obtenida la relación de ficheros tratados por las distintas áreas, deben agruparse creando ficheros lógicos para notificar a la Agencia Española de Protección de Datos su creación o tratamiento.

Los ficheros lógicos

Los ficheros lógicos agrupan determinados ficheros físicos (o de menor nivel), que cumplen unos determinados requisitos que permiten su agrupación para poder notificar a la autoridad correspondiente datos como su finalidad, las características básicas de su tratamiento y su nivel de seguridad.

Un fichero lógico de personal podrá contener distintos ficheros, como por ejemplo, un archivo Excel para gestionar la formación, o una base de datos que contenga los turnos de los trabajadores.

Requisito imprescindible para la creación de nuevos ficheros de datos de carácter personal es la previa inscripción en el Registro de la Agencia Española de Protección de Datos.



Identificación y notificación de ficheros en entidades privadas

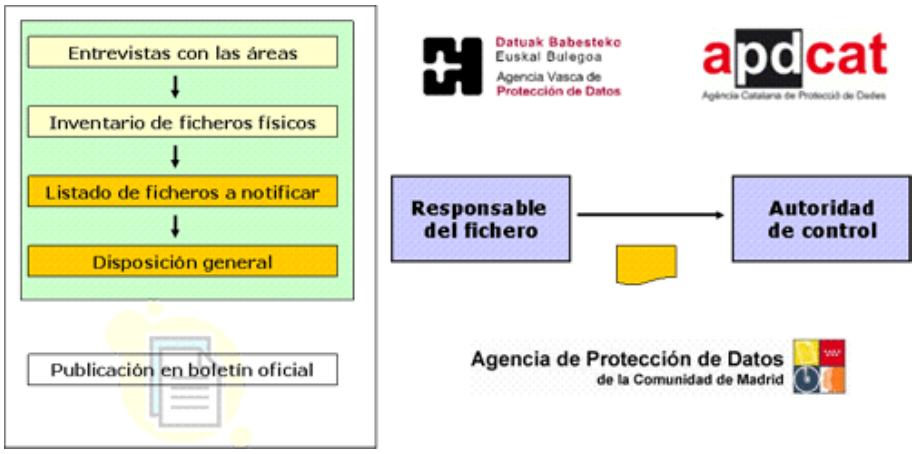
Entidades públicas

Tal como recoge el artículo 20.1 de la LOPD:

> "La creación, modificación o supresión de ficheros de las administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente".

Así, para la creación de un fichero de titularidad pública, el organismo competente debe aprobar una disposición, que habrá de ser publicada en el boletín oficial correspondiente. Una vez aprobada la disposición, será necesario notificar la creación del fichero a la autoridad de control competente.

Una vez más, es necesario realizar el proceso previo de identificación de los ficheros físicos tratados por la organización con la finalidad de agruparlos en ficheros lógicos. Este proceso de inventario de la información permitirá mantener actualizadas las notificaciones a la autoridad de control competente (modificaciones y supresiones).



Identificación y notificación de ficheros en entidades públicas

Ficheros tipo en una organización sanitaria

A modo de ejemplo, se ofrece una compilación de los posibles ficheros a notificar a la correspondiente autoridad de control por un hospital tipo:

Fichero a notificar (fichero lógico)	Ficheros físicos
Pacientes	Historias clínicas Laboratorio Urgencias Registro de consentimiento informado Resultados de pruebas diagnósticas Quirófano ...
Nóminas	Gestión de nóminas
Personal	Formación Control de turnos Gestión de beneficios sociales Peticiones y solicitudes del personal ...

Fichero a notificar (fichero lógico)	Ficheros físicos
Administración y contabilidad	Gestión de compras Gestión de proveedores Facturación Pedidos ...
Seguridad	Control de acceso Videovigilancia ...

1.3.2. Principios de la protección de datos

Todo responsable de fichero debe establecer los mecanismos o los procesos internos de su organización de forma que se cumplan los principios de la protección de datos recogidos en el título II de la LOPD y que trataremos seguidamente.

Calidad de los datos

La calidad de los datos se aborda en el artículo 4 de la LOPD y es un pilar fundamental de una buena gestión de la información, siendo especialmente importante en los sistemas de información sanitarios.

El principio de la calidad de los datos se concreta es los siguientes aspectos:

- Los datos personales deben adecuarse a la finalidad para la que fueron recabados; es decir, los datos sólo se podrán recoger para su tratamiento y sólo podrán someterse a dicho tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

- Los datos personales no podrán usarse para finalidades incompatibles con aquéllas para las que hubieran sido recogidos.

- Los datos deberán ser exactos y puestos al día (actualizados). Esto no significa que las organizaciones deban mantener exactos los datos cuando no tengan medios para conocer la exactitud de los mismos; pero, si tienen conocimiento de la inexactitud de un dato, deben actualizarlo.

- Los datos serán cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual fueron recabados o registrados; es decir, no deben mantenerse indefinidamente sin justificación, salvo que alguna obligación legal establezca la necesidad de conservar los datos una vez concluida la finalidad que motivó su recogida o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado. La organización podrá conservar los datos a través del bloqueo del mismo o previo proceso de disociación.

- Los datos deben haber sido recogidos de forma lícita.

Derecho de información en la recogida de datos

El artículo 5.1. de la LOPD establece la obligación previa de informar al titular de los datos en el momento de recabarlos, de forma que la persona pueda o no facilitar sus datos con pleno conocimiento del tratamiento que van a recibir.

> "Los interesados a los que se solicite datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
>
> **a)** De la existencia de un fichero o tratamiento 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 tratamiento o, en su caso, de su representante."

Los datos recabados mediante cuestionarios, formularios u otros impresos (en formato papel o electrónico), las menciones anteriores deberán figurar en los mismos de forma claramente legible y no será necesario informar del contenido de los apartados b), c) y d) si se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Por lo que se refiere a los **datos recabados de terceros**; es decir, principalmente, a los supuestos de cesiones de datos entre empresas o entre administraciones públicas, la LOPD establece en su artículo 5.4, que:

> "Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo."

Por ello, en el caso de obtener datos que no hayan sido directamente recabados de los interesados, es necesario asegurar que la organización que los facilita haya cumplido con el deber de información; en caso contrario, se deberá comunicar al interesado:

- Procedencia de los datos.
- El titular del fichero.
- Las finalidades del tratamiento.
- El carácter obligatorio/facultativo de las respuestas.
- Los derechos que le asisten y su posibilidad de ejercicio.
- La dirección y, en su caso, las condiciones para ejercitar tales derechos.

Las cláusulas de información deben detallar las finalidades con las que se recaba la información.

Modelo de cláusula de información

En cumplimiento de lo establecido por la normativa sobre protección de datos personales, les informamos que sus datos van a ser incorporados a un fichero titularidad de [NOMBRE DE LA ORGANIZACIÓN], con la finalidad de [INDICAR FINALIDAD]. Sus datos serán comunicados a [INDICAR DESTINATARIOS] con la finalidad de [INDICAR FINALIDAD]. Puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición dirigiéndose a: [NOMBRE Y DIRECCIÓN DE LA ORGANIZACIÓN].

El artículo 5.5. LOPD establece una serie de **excepciones a la obligación de informar** cuando los datos no procedan del interesado:

"No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. "

Consentimiento del afectado

El consentimiento es la manifestación de voluntad, libre, inequívoca, específica e informada por la que el interesado consiente el tratamiento de sus datos personales.

El artículo 6.1. LOPD dice:

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

La obtención del consentimiento se suele realizar a la hora de la recogida de los datos mediante la cláusula de información, dado que se considera que a partir de dicha información el afectado es consciente y toma conocimiento de la existencia del tratamiento que se va a realizar, las finalidades y los derechos que le asisten.

La ley dispone, para determinadas categorías de datos, un tipo especial de consentimiento. En este grupo se incluyen los **datos de salud**, que, como ya se ha indicado, gozan de un régimen especialmente riguroso, que requiere el consentimiento expreso para su tratamiento. Concretamente, el artículo 7.3. LOPD dice:

"Los datos de carácter personal 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."

En caso de tratamiento de esta tipología de datos, será necesario que la organización acredite que ha obtenido el consentimiento del interesado con todas las garantías establecidas por la ley; es decir, que el consentimiento sea libre, inequívoco, específico, informado, y prestado por escrito y de forma expresa.

Con la finalidad de conciliar las obligaciones de la normativa sobre protección de datos personales con otros bienes jurídicos que igualmente merecen protección, la LOPD establece en su artículo 6.2. una serie de **excepciones al consentimiento**. De acuerdo con este artículo, no será necesario el previo consentimiento del afectado para el tratamiento de sus datos personales en los siguientes casos:

- Datos recogidos para el ejercicio de las funciones propias de las administraciones públicas.
- Datos relativos a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa.
- Cuando el tratamiento de datos sea necesario para proteger un interés vital del interesado.
- Datos provenientes de fuentes accesibles al público.

Por lo que respecta a los datos relativos al origen racial, a la salud y a la vida sexual, aunque por norma requieren el consentimiento expreso del interesado, la norma también establece una serie de excepciones:

- Cuando el tratamiento de datos sea necesario para la prevención o diagnósticos médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.

- Siempre que el tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

- Cuando el tratamiento de datos sea necesario para salvaguardar el interés vital de un afectado o de otra persona, en caso de que el afectado esté físicamente o jurídicamente incapacitado para otorgar el consentimiento.

Comunicación de datos

Se considera cesión de datos toda revelación de datos realizada por persona distinta del interesado, entendiendo por cesión cualquier forma de acceso de un tercero a la información (entrega, comunicación, consulta, transferencia...).

Siguiendo lo establecido en el artículo 11 LOPD, en toda cesión de datos deben concurrir los siguientes requisitos:

- Que sólo será posible la cesión de los datos para el cumplimiento de fines directamente relacionados con las funciones de cedente y cesionario. Este

es el principal punto de interés, puesto que la ley pretende evitar que se realicen cesiones que tengan poco o nada que ver con el ámbito de las funciones, atribuciones o competencias de la organización cedente y la organización cesionaria.

- El previo consentimiento informado del interesado; es decir, que antes de proceder a la cesión, la organización debe recabar el consentimiento informado del interesado para efectuar la cesión de sus datos, informándole de:
  - Identificación, actividad y dirección del cesionario.
  - Finalidad a la cual se destinarán los datos cedidos.

El mismo artículo establece supuestos tasados en los que no será preceptivo informar y recabar el consentimiento previo de los interesados para ceder los datos:

- Cuando la cesión esté autorizada por una ley. Así, encontramos supuestos en los que están permitidas las cesiones de datos como en la Ley General Tributaria y en la Ley de Enjuiciamiento Civil.

- Cuando se trate de datos recogidos de fuentes accesibles al público, siempre que el tratamiento de los datos sea necesario para la satisfacción del interés legítimo perseguido por el cedente o por el cesionario y se respeten los derechos de los interesados.

- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente 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.

- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

- Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos. Además, no se permiten por ley las cesiones de datos entre distintas administraciones públicas para el ejercicio de competencias diferentes o para fines distintos a los que motivaron la recogida de los datos.

- 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.

Deber de secreto

El deber de secreto, que se regula en el artículo 10 LOPD, afecta a todo el personal que tiene acceso a los datos personales, independientemente del tipo de relación que le vincule a la organización (es decir, afecta tanto a personal laboral, como a colaboradores externos, subcontratados, becarios, etc.), bien sea mediante el acceso a los sistemas de información o bien mediante el acceso a la información en papel.

La obligación del deber de secreto subsiste aún una vez finalizadas las relaciones con el responsable del fichero e implica que el personal no deberá ni podrá divulgar o comunicar a terceras personas la información o los datos que maneja o de los que tenga conocimiento en el desempeño de su cargo o funciones.

El personal debe firmar, bien sea en el momento de la contratación o bien el momento de incorporarse a la organización, cláusulas de confidencialidad y de deber de secreto.

1.3.3. Derechos de los afectados

La LOPD, en su título III, regula los derechos que asisten al titular de los datos y que éste puede ejercer directamente delante de la organización responsable del fichero. La organización debe establecer procedimientos internos para garantizar que se aporta respuesta en tiempo y forma a los ciudadanos que solicitan el ejercicio de derechos, dado que la no respuesta en los plazos tasados por la normativa puede suponer una reclamación ante la autoridad de control competente.

Las solicitudes de ejercicio de derechos deben ir acompañadas de una solicitud, dirigida a la organización responsable del fichero, junto con una fotocopia del DNI o mediante cualquier otro medio válido en derecho que acredite la identidad del interesado.

Los principales derechos del titular de los datos son los siguientes:

Derecho de acceso

El derecho de acceso es el derecho del titular de los datos a solicitar y obtener gratuitamente, de la organización responsable del fichero, información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevé hacer de los mismos.

La organización, por tanto, tiene obligación de informar gratuitamente al ciudadano que así lo solicite en relación con sus propios datos de lo siguiente:

- Datos personales que se almacenan (todos los datos base, así como los resultados de cualquier elaboración o proceso informático).
- Cómo se obtuvieron (si los datos proceden de fuentes diversas, deberán especificarse éstas, identificando la información que proviene de cada una de ellas).
- Ficheros en los que se encuentran.
- Finalidad y uso de esos datos.
- Si han sido o van a ser cedidos a terceros (con la indicación de los cesionarios de esos datos).

La organización tiene un mes desde la recepción de la solicitud para contestarla, la falta de contestación se entiende como desestimación y legitima para reclamar ante la autoridad de control competente.

Derecho de rectificación

El derecho de rectificación es el derecho del titular de los datos a solicitar a la organización responsable del fichero la rectificación de sus datos personales cuando éstos sean inexactos, incompletos, inadecuados o excesivos.

La organización tiene la obligación de corregir gratuitamente los datos incompletos o inexactos del ciudadano cuando éste así lo solicite.

La solicitud, además de acreditar la identidad del solicitante, como se ha citado anteriormente, deberá ir acompañada de la documentación que acredite la inexactitud o incorrección de los datos.

La organización deberá corregir los datos, si procede, en el plazo máximo de 10 días desde la recepción de la solicitud.

Derecho de cancelación

El derecho de cancelación es el derecho del titular de los datos a solicitar a la organización responsable del fichero la cancelación de sus datos personales cuando éstos son inexactos o incompletos, inadecuados o excesivos, así como cuando revoque el consentimiento prestado inicialmente para tratar los datos personales que le son propios.

Es necesario indicar que la cancelación no procederá cuando exista una obligación de conservar los datos.

En el caso de las historias clínicas, tal y como estable la Ley 41/2002, existe la obligación de que figure en ellas toda la información que se considera trascendental para el conocimiento veraz y adecuado del estado de salud del paciente, por lo que no se eliminarán datos relevantes de la historia.

Además, la citada norma establece que la documentación clínica deberá conservarse para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial.

En caso de proceder la cancelación, ésta se realizará en una plazo máximo de diez días desde la recepción de la solicitud.

1.4. Reglamento de Medidas de Seguridad

La norma que establece las medidas de carácter técnico y organizativo que deben ser adoptadas por todas las organizaciones, tanto públicas como privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal es el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad para los Ficheros automatizados de Datos de Carácter personal.

1.4.1. Objeto y ámbito de aplicación

El reglamento sobre medidas de seguridad tiene por objeto determinar las medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información que contenga datos personales, con la finalidad de preservarlos frente a su alteración, pérdida, tratamiento o acceso no autorizado. Dichas medidas deberán ser adoptadas e implantadas por la organización responsable del fichero y, en su caso, por la empresa que realice la gestión de los sistemas de información que traten los ficheros.

Las medidas técnicas y organizativas establecidas por el reglamento sobre medidas de seguridad deben aplicarse sobre:

- Los ficheros automatizados, entendidos como todo conjunto organizado de datos de carácter personal, cualquiera que fuere su forma o modalidad de creación, almacenamiento, organización y acceso.

- Los centros de tratamiento, entendidos como los lugares habilitados donde se encuentran los ordenadores, equipos y servidores que almacenan la información.

- Los locales, entendidos como aquellos lugares donde se encuentran físicamente ubicados los equipos y el personal que trata datos.

- Los equipos, entendidos como todo material en soporte físico que sirva para tratar y almacenar electrónicamente datos personales.

- Los sistemas y programas informáticos que tratan los datos de carácter personal.

- Las personas que acceden a los datos (personal laboral, personal subcontratado, becarios, personal en prácticas, etc.) que, de acuerdo con sus funciones y obligaciones, interviene en cualquiera de las fases del tratamiento de los datos.

Los ficheros en papel

En el momento de redactar este material, el reglamento en vigor, el Real Decreto 994/1999, no se aplica a los ficheros en papel, aunque se prevé la aprobación de un nuevo reglamento que los comprenda.

1.4.2. Niveles de seguridad

El reglamento sobre medidas de seguridad establece tres niveles de seguridad, que tienen la consideración de mínimos legales exigibles, por lo que cada organización podrá implantar las medidas de seguridad adicionales que considere adecuadas atendiendo al tipo de información tratada, así como a otros requerimientos a los que pueda estar sujeta.

Los niveles de seguridad establecidos son los que siguen:

- Nivel básico: aplicable a todos los ficheros que contengan datos de carácter personal.

- Nivel medio: aplicable a los siguientes tipos de datos:
  - Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales.
  - Ficheros que contengan datos sobre Hacienda Pública.
  - Ficheros que contengan datos sobre servicios financieros.
  - Ficheros que contengan datos sobre solvencia patrimonial y crédito.

– Ficheros que contengan un conjunto de datos suficientes que permitan elaborar un perfil del afectado.

- Nivel alto: aplicable a aquellos ficheros que contengan datos de ideología, religión, creencias, origen racial, salud, vida sexual.

Sobre los niveles de seguridad

El reglamento establece los niveles de seguridad de forma acumulativa; así, en caso de tratamiento de ficheros de nivel medio, deberán implantarse todas y cada una de las medidas de seguridad descritas para el nivel básico y las del medio. Igualmente sucederá con los ficheros de nivel alto, que deberán implantar las medidas descritas para el nivel básico, el medio y el alto.

1.4.3. Medidas de seguridad

	Nivel básico	Nivel medio	Nivel alto
Documento de seguridad / Ámbito de aplicación	• Medidas, normas, procedimientos reglas y estándares de seguridad. • Funciones y obligaciones del personal. • Estructura y descripción de ficheros y sistemas de información. • Procedimiento de notificación, gestión y respuesta ante incidencias. • Procedimiento de realización de copias de respaldo y recuperación de datos.	• Identificación del responsable de seguridad. • Control periódico del cumplimiento del documento. • Medidas a adoptar en caso de reutilización o desecho de soportes.	
Personal	• Funciones y obligaciones claramente definidas y documentadas. • Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
Incidencias	• Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados.	• Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. • Autorización por escrito del responsable del fichero para su recuperación.	
Identificación y autenticación	• Relación actualizada de usuarios y accesos autorizados. • Procedimientos de identificación y autenticación. • Criterios de accesos. • Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. • Almacenamiento ininteligible de contraseñas activas.	• Se establecerá el mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. • Límite de intentos reiterados de acceso no autorizado.	

	Nivel básico	Nivel medio	Nivel alto
Control de acceso	• Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. • Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. • Concesión de permisos de acceso sólo por personal autorizado.	• Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	
Gestión de soportes	• Identificar el tipo de información que contienen. • Inventario. • Almacenamiento con acceso restringido. • Salida de soportes autorizada por el responsable del fichero.	• Registro de entrada y salida de soportes. • Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. • Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.	• Cifrado de datos en la distribución de soportes.
Copias de respaldo	• Verificar la definición y aplicación de los procedimientos de copias y recuperación. • Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. • Copia de respaldo, al menos semanal.		• Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
Responsable		• Uno o varios nombrados por el responsable del fichero. • Encargado de coordinar y controlar las medidas del documento. • No supone delegación de responsabilidad del responsable del fichero.	
Pruebas		• Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado.	
Auditoría		• Al menos cada dos años, interna o externa. • Adecuación de las medidas y controles. • Deficiencias y propuestas correctoras. • Análisis del responsable de seguridad y conclusiones al responsable del fichero. • Adopción de las medidas correctoras adecuadas.	

	Nivel básico	Nivel medio	Nivel alto
Registro de accesos			• Registrar usuario, hora, fichero, tipo acceso y registro accedido. • Control del responsable de seguridad. Informe mensual. • Conservación 2 años.
Telecomunicaciones			• Transmisión de datos cifrada.

1.5. Régimen sancionador

1.5.1. Autoridades de control

Las autoridades de control, o agencias de protección de datos, se constituyen como el garante de la aplicación de los principios recogidos en la normativa. En el Estado español se establecen dos ámbitos de actuación:

- Agencia Española de Protección de Datos: tiene potestad sobre los ficheros privados en todo el estado español.

- Agencias autonómicas: su ámbito competencial se circunscribe a los ficheros creados o gestionados por las administraciones públicas de su ámbito territorial:
  - Agencia Catalana de Protección de Datos.
  - Datuak Babesteko Euskal Bulegoa (Agencia Vasca de Protección de Datos).
  - Agencia de Protección de Datos de la Comunidad de Madrid.

Con carácter general, las principales funciones de los órganos de control son las siguientes:

- Velar por el cumplimiento de la legislación vigente sobre protección de datos personales.
- Proporcionar información sobre los derechos de las personas en materia de tratamientos de datos personales.
- Atender las peticiones y las reclamaciones formuladas por las personas afectadas.
- Dictar las instrucciones necesarias para adecuar los tratamientos a los principios de la legislación.
- Ejercer la potestad de inspección y ejercer la potestad sancionadora.

1.5.2. Infracciones y sanciones

Las infracciones y sanciones se abordan en el título VII de la Ley. En concreto, el artículo 44 nos dice lo siguiente:

"**1)** Las infracciones se calificarán como leves, graves o muy graves.

2) Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta ley, salvo que constituya infracción grave.

3) Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el director de la Agencia Española de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4) Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del director de la Agencia Española de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero."

Por lo que respecta a las sanciones, cabe comentar que el régimen sancionador de la LOPD es de los más severos del entorno europeo. Así, en su artículo 45, la LOPD establece lo siguiente:

"**1)** Las infracciones leves serán sancionadas con multa de 601 a 60.101 euros.

2) Las infracciones graves serán sancionadas con multa de 60.101 a 300.506 euros.

3) Las infracciones muy graves serán sancionadas con multa de 300.506 a 601.012 euros."

El artículo 46 de la ley hace especial mención de las infracciones cometidas en ficheros de los que sean responsables las administraciones públicas.

"**1)** Cuando las infracciones a las que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las administraciones públicas, el director de la Agencia Española de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera.

2) El director de la agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3) Se deberán comunicar a la agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores."

Es decir, en el caso de las administraciones públicas, las infracciones no llevan aparejada ninguna sanción económica.

2. Introducción a los elementos técnicos de modelos de seguridad

2.1. Fundamentos de seguridad técnica

Se dice que algo es seguro cuando no es susceptible de fallar en cualquiera de los sentidos o alusiones hacia ese objeto o afirmación. La seguridad es un concepto que trasciende a la mayor parte de las actividades humanas.

En este sentido, hemos de tener en cuenta dos aspectos:

- Siempre que exista un bien a proteger, se dedicará tiempo y recursos a neutralizar las posibles amenazas que pueda sufrir por medio de lo que llamamos mecanismos de seguridad.

- La tecnología asociada al proceso de datos se ha convertido en elemento esencial en nuestras vidas. La informática ha pasado a ser algo sin lo cual es imposible concebir ciertos aspectos de la actualidad, tanto científica como civil.

La combinación de los dos aspectos anteriores nos indica ya la importancia que tiene la seguridad informática en nuestras vidas. Cada vez con más frecuencia se delega en los equipos informáticos la responsabilidad de la gestión de productos, personas, votos, información en general. Debido a esto, cada vez será mayor la posibilidad de que se produzcan errores en la gestión de la información:

- Aumentará la gravedad de los errores en la gestión.
- Aumentará el beneficio extraíble de los errores.
- Aumentará el número de personas interesadas en que se produzcan errores.

Aparte de lo escrito anteriormente, existen otros factores que hacen de la seguridad informática una disciplina particularmente difícil:

- Pueden ocasionarse muchos daños a distancia, con un riesgo mínimo para quien los provoca.

- El equipo necesario para ejercer la delincuencia informática tiene un coste relativamente bajo.

- Es posible, aunque difícil, borrar toda huella del delito.

- No existe una formación sólida sobre los sistemas a administrar, debido a la complejidad y el rápido avance de los mismos.

- La legislación no va a la par con los avances informáticos y existen dificultades para aplicar las leyes existentes.

- Los delitos no siempre son denunciados por parte de las organizaciones debido a la publicidad adversa que se puede generar.

Un agravante

Por si esto fuera poco, cada vez con mayor frecuencia, los medios de comunicación, especializados o no, dan a conocer casos de fraude, espionaje, destrucción de la propiedad intelectual, sabotaje, intrusión, robo, plagio o competencia desleal, relacionados con el mundo de la informática.

Estos sucesos pueden ocasionarlos un empleado vengativo, un administrador ineficaz, un intruso informático, un usuario irresponsable, software mal desarrollado o una catástrofe natural. Sus blancos pueden estar perfectamente seleccionados o ser totalmente aleatorios, de consecuencias inmediatas o solamente visibles con el paso del tiempo, pero todos ellos se traducen en pérdidas de tiempo y dinero para las empresas que los sufren.

Hasta la aparición de la informática, la valoración de los activos de una empresa se hacía según los objetos físicos útiles, las producciones propias, las infraestructuras, la tesorería y el capital humano. Desde su aparición, la información ha cobrado un valor como capital. No es que antes no existiera información en las empresas, el espionaje industrial es tan antiguo como la revolución industrial, pero se mantenía con el sistema de papel y archivadores y formaba parte de los activos de la oficina. Hoy en día, se maneja una cantidad ingente de información de procedencias muy diversas. El valor añadido de una empresa puede ser la información que maneja.

En consecuencia, cada vez es más importante mantener la seguridad de la información, pero también es más difícil porque los riesgos son mayores.

Podemos identificar tres tipos de riesgos, atendiendo a su origen:

- Errores involuntarios de personas y/o máquinas
- Desastres naturales
- Ataques voluntarios

Los errores involuntarios son las amenazas más comunes: sobre el 80 % de los casos. Los problemas creados por éstos se pueden clasificar en dos familias:

- Denegación de servicio: no disponibilidad de los recursos.

- Observación no autorizada (ataque a la confidencialidad): acceso a la información y su modificación ya sea borrando, añadiendo o sustituyendo datos.

La protección de la información es más difícil desde la aparición de las redes telemáticas. Estas redes, y especialmente Internet, hacen que la información sea un problema global y no aislado a las máquinas internas de la empresa. Las tecnologías aplicadas a la seguridad en redes están en su fase de desarrollo inicial, especialmente por dos motivos:

- La mayoría de los sistemas operativos están pensados para arquitecturas mainframe/terminal y no para arquitecturas cliente/servidor o Internet/intranet que se utilizan actualmente.

- No existen estándares ni organizaciones mundiales aceptadas por todas las empresas proveedoras de seguridad.

Al diseñar un sistema de seguridad para una empresa se debe tener en cuenta que **no** existe un sistema completamente seguro. Entre los informáticos se suele comentar lo siguiente: "Un ordenador seguro es aquel que está desconectado de la red, enterrado en un bunker de hormigón, varios metros bajo tierra, con un guardia de seguridad en la puerta..., y aun así no es posible garantizar que esté completamente seguro".

En general, para proteger la información se utilizan los siguientes servicios de seguridad:

- Autenticación. Autenticar a un usuario es comprobar que es quien declara ser. La autentificación se puede realizar actualmente con diferentes métodos. El más común es el de *login* y *password*, pero también existen los *tokens*, las *smart cards*, sistemas biométricos, los certificados digitales, etc.

- Control de accesos. El control de accesos consiste en proteger la información contra accesos no deseados, tanto físicos como lógicos.

- Confidencialidad. La confidencialidad es la capacidad de mantener en secreto el contenido de un documento.

- Integridad. La integridad consiste en garantizar que el contenido de un documento no ha sido alterado o modificado.

- No repudio. El no repudio evita que una persona pueda negar que ha realizado una acción cuando la ha realizado.

- Disponibilidad. La disponibilidad consiste en asegurar el funcionamiento de todos los recursos.

2.1.1. Niveles de seguridad

Podemos identificar tres niveles de seguridad, que desarrollaremos en los siguientes apartados:

Seguridad física

Por seguridad física podemos entender todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema.

Ejemplos de recursos a proteger

Entendemos por recursos a proteger desde un simple teclado hasta una cinta de *backup* con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

En muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o denegaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema.

Esto motiva que, en determinadas situaciones, un atacante se incline por aprovechar vulnerabilidades físicas, ya que puede resultarle más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él a través de fallos en el software.

El nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos que hay que proteger.

A continuación enumeraremos diferentes peligros que afectan a la seguridad física:

- **Desastres naturales**. Los desastres naturales no son demasiado frecuentes, pero cuando se dan, acostumbran a acarrear gravísimas consecuencias, debido, sobre todo, a la falta de prevención.
  - Las tormentas con aparato eléctrico, especialmente frecuentes en verano (cuando mucho personal se encuentra de vacaciones, lo que las hace más peligrosas) generan súbitas subidas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica. Si cae un rayo sobre la estructura metálica del edificio donde están situados los equipos, es casi seguro que habrá que comprar otros nuevos. Sin llegar a ser tan dramáticos, la caída de un rayo en los alrededores de un edificio con material informático puede inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados.

  - Las inundaciones. En muchas empresas el centro de proceso de datos se encuentra en el sótano, ya que éste es un lugar poco accesible por no disponer de ventanas por las que puedan entrar los posibles ladrones. Pero los sótanos son especialmente vulnerables ante las inundaciones. Dado que la ubicación de los equipos ya suele estar decidida cuando se piensa en las medidas de seguridad, habrá que utilizar medidas de detección, como por ejemplo detectores de agua en los suelos o falsos

suelos de las salas de operaciones que provoquen el apagado de los equipos en caso de que se activen.

- **Desastres del entorno**. Entre los más frecuentes podemos destacar las subidas o bajadas de tensión, la corriente estática, incendios, accesos físicos no autorizados o robos de datos.
  - Cambios de tensión. La forma más efectiva de proteger equipos contra los cambios de tensión es utilizar un SAI (servicio de alimentación ininterrumpido).

  - Corriente estática. Es este un fenómeno extraño que la mayoría de gente piensa que no afecta a los equipos, sólo a otras personas. Nada más lejos de la realidad: simplemente tocar con la mano la parte metálica de teclado o un conductor de una placa puede destruir completamente un equipo. Contra el problema de la corriente estática existen muchas soluciones y muy baratas: spray antiestático, ionizadores antiestáticos, etc.

  - Incendios. Los incendios suelen estar muy relacionados con la electricidad (la causa del fuego puede ser también, evidentemente, un desastre natural): la sobrecarga de la red debido al gran número de aparatos conectados al tendido, un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio.

  - Acceso físico no autorizado. Debemos tener en cuenta que, aunque una parte de los equipos suele estar bien protegida ante accesos físicos no autorizados, como los servidores, muchos equipos estarán en lugares semipúblicos a los que es fácil acceder (y discreto) y desde los que es también fácil lanzar un ataque completo sobre la red. Se debe extremar la protección de todos los equipos ante estos accesos no autorizados.

  - Robo de datos. La seguridad física también implica una protección de la información de nuestro sistema, tanto de la que está almacenada en él como de la que se transmite entre diferentes equipos. De todas maneras, hay ciertos aspectos que se deben tener en cuenta al diseñar una política de seguridad física que afectan principalmente, aparte de a los elementos físicos, a los datos de una organización: algunos ataques tienen como objetivo no destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en él.
    Un error muy habitual es almacenar los dispositivos de *backup* en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala. Esto, que en principio puede parecer correcto (y cómodo si se necesitan restaurar unos archivos) puede convertirse en un problema: un mismo ataque podría hacer que se perdiesen tanto los equipos como los datos (los de los propios equipos y los del *backup*). Es recomenda-

ble guardar las copias de seguridad en una zona alejada de la sala de operaciones, aunque ello implique doblar los sistemas de seguridad.

Seguridad al nivel de enlace-red-transporte

La seguridad de una red depende en gran medida de los niveles OSI enlace, red y transporte.

Para introducirse en las redes, los atacantes suelen aprovechar problemas en el diseño de la topología de las redes y en los protocolos de direccionado entre los distintos elementos. Por lo tanto, éstos son los puntos sobre los que un administrador de sistemas debe prestar especial atención.

- Seguridad en dispositivos de red. Los dispositivos de red (*switches*, direccionadores, *hubs*, balanceadores de carga, etc.) son los puntos débiles de cualquier red, son los responsables de la topología de red resultante y, por tanto, una variación en su configuración puede afectar a toda la red.

Vulnerabilidad de los dispositivos de red

Estos dispositivos tienen diferentes modos de administración, pero básicamente su administración remota se basa en un protocolo algo desfasado en cuanto a seguridad como es el SNMP.

- Vulnerabilidades en la pila TCP/IP. En la época en la que se diseñó el protocolo TCP/IP, se tuvo más en cuenta la estabilidad y su rendimiento que la seguridad, cuestión que carecía de importancia en su diseño preliminar. Hoy en día es uno de los protocolos de red más utilizados y el responsable de la red Internet.

Identificación de equipos

En un servidor podemos tener varios puertos o servicios escuchando. La manera más simple de representar esta situación es la dirección IP del equipo seguido del número identificador del puerto. Por ejemplo, 172.16.1.123:80 es el servicio web del equipo con IP 172.16.1.123.

- Direccionadores y técnicas de direccionamiento. Se entiende por direccionamiento o enrutamiento la función que hace llegar paquetes de información de una máquina a otra, sin tener en cuenta ni el medio físico ni la calidad de los datos que se transmiten. Para que esto se lleve a cabo, el sistema emisor debe saber qué otros sistemas están en su misma red y a dónde debe enviar los datos en caso de que la máquina no pertenezca a su entorno directo.

- *Proxies*. Un *proxy* es un sistema software de intermediario entre dos redes, que permite regular el tráfico de salida y entrada entre ellas a través de un único *host*, gestionándose de esta manera tanto el tráfico como el contenido de las comunicaciones entre los dos entornos. Generalmente, un *proxy* de sesión permite a equipos de una red local conectarse a otra red, por ejemplo a equipos de Internet, a través de un único equipo y de una única conexión a Internet.

- *Firewall* o cortafuegos, es un sistema, ya sea hardware o software, que se encarga de filtrar tráfico TCP/IP generalmente entre redes; por ejemplo entre Internet y una red local de una oficina. Por tanto, el cortafuegos filtrará el tráfico entrante desde Internet (una red no fiable) hacia la LAN (nuestra red), y permitirá el tráfico saliente desde la LAN hacia Internet. A un nivel muy sencillo, un cortafuegos de red puede evitar e incluso bloquear la extensión de un ataque.

- *Sniffers*. Son dispositivos que capturan paquetes de la red. Su uso legítimo es analizar el tráfico de red e identificar las áreas más preocupantes en potencia. Por ejemplo, si un segmento de la red tiene un bajo rendimiento se usará un *sniffer* para determinar la causa de forma precisa.
  Los *sniffers* son peligrosos porque pueden capturar *passwords*, información confidencial o propietaria, y pueden ser usados para traspasar la seguridad de redes interconectadas o para ganar privilegios. De hecho, la existencia de un *sniffer* no autorizado en la red indicará que la seguridad está realmente comprometida.

- *Tunneling*. La necesidad de seguridad hace que cada vez sea más común el uso de VPN (redes virtuales privadas). Estas redes se implementan por medio de un protocolo llamado PPTP (*point to point tunneling protocol*) que asegura tráfico encriptado entre puntos de enlace corporativos basándose en una red de trabajo vía TCP/IP. Esto elimina la necesidad de líneas propias o alquiladas y también el peligro del *sniffing*.

Seguridad al nivel de aplicación

- Código maligno-virus. En general podemos decir que un virus informático es un pequeño programa diseñado para alterar el funcionamiento de un ordenador.
  Un concepto más completo de virus informático sería el de un pequeño programa capaz de autorreproducirse. Lo calificamos de maligno porque está diseñado para dañar sistemas informáticos, alterando su forma de trabajar o dañando información almacenada en el disco duro, sin el conocimiento o permiso del afectado. En términos más técnicos, un virus se define como una porción de código de programación cuyo objetivo es implementarse a sí mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro. Además, los virus están diseñados para realizar una acción concreta en los sistemas informáticos. Esta acción puede ir desde la simple aparición de un mensaje en la pantalla, hasta la destrucción de toda la información contenida en el sistema.
  Los virus poseen rutinas de destrucción de datos que se activarán cuando se den ciertas condiciones. Algunos virus se activan en una fecha determinada.
  La fase de descubrimiento no tiene por qué producirse después de la activación, pero usualmente sucede así. Esto se produce cuando alguien da la noticia de un nuevo virus. Generalmente pasa a manos de la National

Computer Security Association (NCSA) que se documenta y luego se distribuye a los diseñadores de antivirus.

- Vulnerabilidades de código. A la hora de asegurar un sistema, no se debe olvidar el código que ejecuta para realizar sus funciones asignadas. Siempre existe determinado grado de divergencia entre el diseño de los programas y su implementación, estas pequeñas diferencias pueden hacer que un determinado software sea inseguro, o que herramientas específicas de seguridad no cumplan su función como deberían.
  Aunque estas vulnerabilidades dependen del uso que se haga del lenguaje de programación, cada lenguaje es susceptible frente a determinados fallos, es necesario conocerlos y evitarlos. Para localizar estos errores, se recurre a la ingeniería inversa, esta técnica consiste en descompilar el código y observar qué vulnerabilidades son explotables por el atacante. A un determinado programa de ataque, para un determinado programa objetivo y sobre un sistema operativo concreto, se le denomina *exploit*. Y a la respuesta a este *exploit* (para neutralizarlo), por parte de la compañía propietaria del software atacado, se la denomina *patch*, o parche.

2.2. Firma electrónica y criptografía

2.2.1. Identificación y autenticación

Ya hemos explicado en qué consiste la autenticación. Y sabemos que es imprescindible para poder relacionarnos por medios electrónicos: primero hemos de identificar con quién nos relacionamos, y probablemente dotar de algún elemento de seguridad esta identificación (una contraseña, una tarjeta o un certificado) para ser capaces de comprobar su identidad cada vez que deseemos establecer una nueva transacción.

En general, cada usuario tendrá su propio identificador que debería ser único, no se permite que varios usuarios compartan un identificador. Todo identificador de un sistema tendrá su propietario, el cual será responsable de las acciones que se realicen con él.

Hasta la fecha se han venido empleando, y se siguen empleando, nombres de usuario y contraseñas, aunque se aprecia un avance de los sistemas basados en firma electrónica y certificados reconocidos, especialmente debido a la sensibilidad del sector sanitario por tratar datos con exigencia de seguridad de nivel alto y a la nueva regulación administrativa de la firma electrónica.

Un certificado electrónico es, sencillamente, un documento electrónico firmado, que garantiza a las terceras personas que lo reciben o que lo utilizan una serie de manifestaciones contenidas en el mismo que pueden referirse a la identidad de una persona, a la titularidad o posesión de una clave pública (y de la correspondiente clave privada) de sus privilegios (en forma de roles o perfiles) o a su capacidad de representar a otra persona física o jurídica.

Ejemplo de certificado electrónico

El ejemplo más claro de certificado electrónico es el certificado reconocido de clave pública para la identificación y la firma de las personas físicas y jurídicas.

2.2.2. Nociones básicas de criptografía

La criptografía es la técnica que permite convertir un texto inteligible (*plaintext*), en otro, llamado criptograma (*ciphertext*), cuyo contenido de información es igual al anterior pero sólo pueden entenderlo las personas autorizadas.

El proceso que se aplica a los datos para que sean incomprensibles se denomina *cifrado* o *encriptado*. Dado que la función inversa (la que permitiría recuperar el texto inteligible) únicamente la conocen las personas autorizadas, el cifrado permite asegurar la confidencialidad de los datos.

El certificado digital, compuesto de una clave pública y una clave privada, es uno de los métodos que permiten cifrar un documento. Para ello es necesario que tanto el emisor como el receptor dispongan de dicho certificado.

La certificación digital funciona mediante criptografía asimétrica; es decir, lo que se ha codificado con una clave privada necesita su correspondiente clave pública para ser descodificado, y al revés.

Funcionamiento de los sistemas de clave pública

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo las de los números primos.

Una función de un solo sentido es aquélla cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos.

Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primarios y conocemos uno de los factores, es fácil computar el segundo.

Infraestructura de clave pública

La infraestructura de clave pública o PKI (*public key infrastructure*) es el sistema técnico, jurídico, de seguridad y de organización de los servicios de certificación y de firma electrónica.

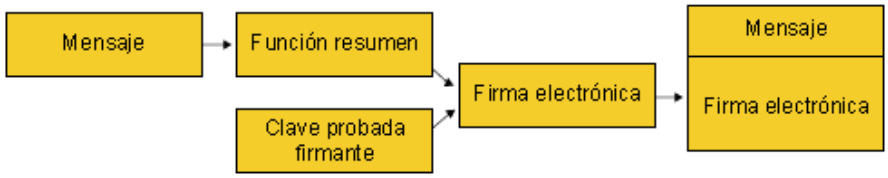
La infraestructura se llama de clave pública porque las operaciones de firma y cifrado requieren como elemento fundamental la publicación y distribución de las claves públicas de los usuarios de los servicios, en forma de certificados electrónicos de clave pública.

La comunicación encriptada requiere que el documento se cifre mediante la clave pública de la persona que se desea que pueda leerlo. Este documento solo podrá ser descifrado por la persona que posee la clave privada complementaria.

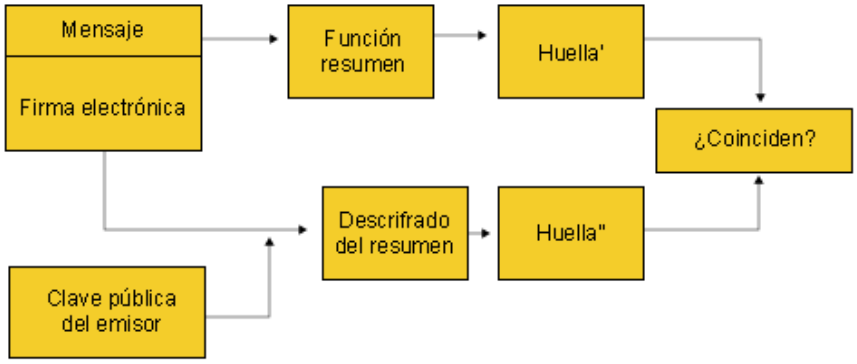
- La clave privada es secreta y sólo la tiene el usuario. Con ella puede firmar documentos electrónicos.

- La clave pública está a disposición de cualquier usuario. Permite validar una firma digital generada con la clave privada complementaria.

Para generar una firma digital, es necesario aplicar una función *hash*, mediante la cual se obtiene la "huella digital" de quien quiere firmar el mensaje. Después, la clave privada del usuario cifra esta huella y da como resultado la firma digital del documento o mensaje.



Quien necesite validar la firma del mensaje o documento podrá comprobar que éste no ha sido modificado aplicando la función de resumen para generar la huella, y comparándola con la que ha recibido.



2.2.3. Validez legal y regulación de la firma electrónica

La legislación sobre firma electrónica determina en su artículo 3.4 que bajo el cumplimiento de determinados requisitos, "la firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel."

Debe realizarse la distinción entre los distintos tipos de firma electrónica que distingue la normativa:

- Firma electrónica, respecto de la cual se establece que no se le negarán efectos jurídicos, ni será excluida como prueba en juicio.

- Firma electrónica avanzada, a la que no se le otorga un reconocimiento específico aunque, evidentemente, debe tener un valor mucho más alto que la anterior puesto que, en virtud de los mecanismos criptográficos empleados, dota a los documentos de autenticidad e integridad.

- Firma electrónica reconocida que, al estar basada en un certificado reconocido y haber sido generada con un dispositivo seguro de creación de firma, debería equiparse a la firma manuscrita. Los certificados reconocidos son aquellos certificados expedidos por un prestador de servicios de certificación, que cumple una serie de requisitos establecidos en la ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación.

Cabe destacar que el hecho de que la firma reconocida sea equiparable a la firma manuscrita implica que la capacidad probatoria de la firma electrónica reconocida es mayor que la de las otras dos modalidades, pero sin que éstas pierdan dicha capacidad.

2.3. Plan director de seguridad

El funcionamiento interno y la imagen ante los clientes de una empresa, o ante los ciudadanos en el caso de la administración, dependen en gran medida del funcionamiento continuado de sus sistemas de información entre los que podemos destacar:

- El correo y las agendas electrónicas, así como el archivo de documentos
- Las web y los procedimientos de tramitación

Debemos tener en cuenta que muchas empresas e instituciones disponen de sistemas de información que tratan datos sensibles y que, además, requieren de medidas de seguridad importantes, ya que son datos que necesitan de un nivel de seguridad alto.

El objetivo de un análisis de riesgos es identificar todos los datos y procesos de una determinada organización cuya sensibilidad/criticidad es importante para el desarrollo de sus funciones.

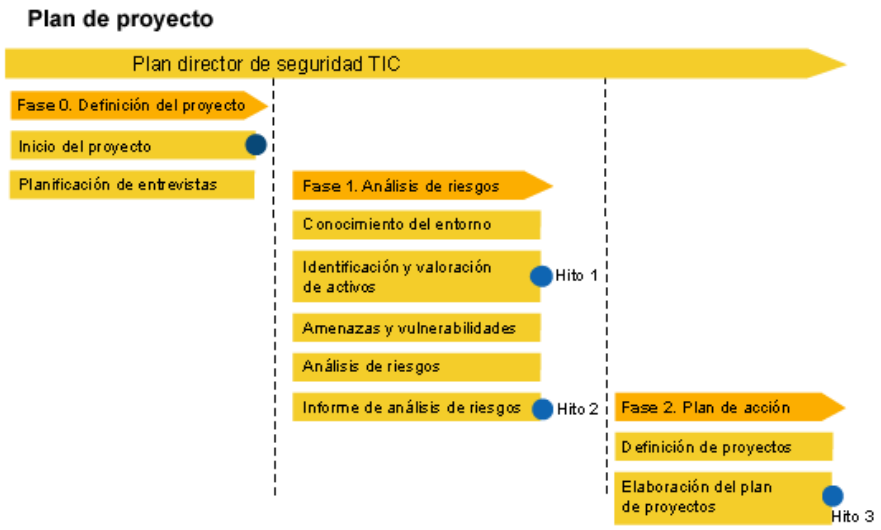
Normalmente, la información necesaria para llevar a cabo un análisis de riesgos se recoge mediante entrevistas con los responsables de la entidad, y el enfoque es de autoevaluación asistida.

El análisis de riesgos y la clasificación de los datos y los procesos puede realizarse con diferente nivel de detalle. Es de utilidad concretar un primer nivel y enfocar el estudio a la identificación de los riesgos más significativos. Por tanto, se puede realizar la valoración del cumplimiento de los controles recogidos en la norma de prácticas de seguridad (ISO17799).

La gestión del riesgo consiste en equilibrar el coste de la protección con el coste de exposición (vulnerabilidades), de forma que se minimice el riesgo.

Las fases de un análisis de riesgos son las siguientes:

- Conocimiento del sistema actual
- Identificación y valoración de activos
- Amenazas y vulnerabilidades
- Análisis de riesgos
- Informe del proyecto



Fases de un plan director de seguridad

Todo análisis de riesgos empieza por la **descripción de la organización**, de los procesos que se tratan y de los sistemas de información que han desarrollado.

A continuación se realiza el **inventario de activos**[1] y sus requisitos de seguridad. Es útil representar los activos a través de una jerarquía o **árbol de activos**, donde se identifican las dependencias de los distintos elementos que comprende un activo de información. En el árbol de activos se representan las aplicaciones, los elementos de red o los edificios donde se encuentran los centros de procesos de datos.

Ejemplo de dimensiones de seguridad

Las dimensiones de seguridad más utilizadas son la confidencialidad, la integridad y la disponibilidad.

(1)Entendemos por *activo de información* aquella información o conjunto de informaciones significativas y necesarias para el desarrollo de los diferentes procesos de negocio.

Un activo de información es independiente de los diferentes elementos de tratamiento o almacenamiento; es decir, de las aplicaciones, base de datos, soportes, edificios donde se ubiquen los sistemas, las redes de comunicaciones, etc.

Seguidamente, se lleva a cabo el **análisis de amenazas y vulnerabilidades** de los activos de información. Para la clasificación de las vulnerabilidades se puede seguir la norma UNE ISO/IEC 17799:2005:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y medioambiental
- Gestión de las telecomunicaciones y operaciones
- Control de accesos a los datos
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de Incidencias
- Gestión de la continuidad de las operaciones de la empresa
- Conformidad

En los análisis de riesgos se pueden incluir tests de intrusión (acceso a la información explotando las vulnerabilidades encontradas para probar de forma fehaciente que un atacante las podría utilizar) para preservar la confidencialidad de la información, con el objetivo de identificar los riesgos siguientes:

- Indisponibilidad del sistema
- Acceso no autorizado
- Incumplimiento del Reglamento de Medidas de Seguridad LOPD

Nota

El análisis de riesgos puede o no cubrir los requisitos de la auditoría bianual que marca la normativa de seguridad y puede comportar, o no, pruebas de auditoría.

El análisis de vulnerabilidades ante ataques del exterior puede comprender:

- Las conexiones a Internet, las conexiones inalámbricas y las webs.
- Los componentes y sus posibles vulnerabilidades significativas.
- La configuración de los puntos de acceso inalámbrico.
- La infraestructura (direccionadores, *firewalls*, servidores web, servidores de aplicativos, etc.).
- Las aplicaciones.
- El personal técnico y los usuarios: ataques de ingeniería social

Siguiendo las directrices marcadas por los resultados del análisis de riesgos y teniendo en cuenta las recomendaciones asociadas a cada vulnerabilidad, se define el **plan de proyectos**.

Los proyectos sin un conjunto de recomendaciones identificadas en el análisis de riesgos y agrupadas para facilitar su ejecución.

Para la ejecución de los proyectos identificados, se establece una priorización, conforme a las dependencias que puedan existir entre ellos, y se propone un plan de acción de acuerdo con las necesidades y requisitos del organismo.

Para cada proyecto se analiza la disminución del riesgo que su realización comporta y también se puede mostrar la evolución en el cumplimiento de la norma ISO 17799 que significa. Es imprescindible describir de forma detallada las actividades de cada proyecto así como la duración y los costes del mismo.

3. Aspectos legales en las aplicaciones móviles

La llegada de los *smartphones* y sus tiendas de aplicaciones asociadas ha supuesto un cambio notable en la manera de crear y vender el software. Ya no es necesario, por ejemplo, que haya un distribuidor que se encargue de repartir el software en un soporte físico. Además, la manera de actualizar y/o crear nuevas versiones de software se simplifica, ya que el usuario final recibe en su teléfono una notificación para que se instale los nuevos cambios de la aplicación adquirida. Gracias a esto se consigue que la distribución de aplicaciones pueda llegar al público de una manera mucho más rápida. Hay otros aspectos, sin embargo, que no van a la misma velocidad, como son las cuestiones legales del software. Y este es un tema con el que se debe tener especial cuidado puesto que constantemente aparecen nuevos elementos a tener en cuenta, como puede ser, por ejemplo, la política de publicación de la propia tienda de aplicaciones.

Si se trata de crear una aplicación en el entorno de la salud, a estos aspectos legales hay que sumarle los relacionados con los dispositivos médicos, con las regulaciones a distintos niveles nacionales e internacionales y con la seguridad y protección de datos. Además, hay que tener en cuenta que los *smartphones* se pueden conectar cada vez a más dispositivos (gafas, relojes, pulseras, sensores corporales, etc.) que, si tienen alguna función médica, pueden añadir un nivel más de complicación.

3.1. Marco legal de las aplicaciones móviles

Antes de tratar de las aplicaciones orientadas al ámbito de la salud, es necesario comenzar con una base un poco más genérica en el entorno de las aplicaciones móviles.

Todas las aplicaciones móviles deben cumplir los siguientes requisitos:

- **Derechos y licencias**:
  - Se deben acoger a las normativas que regulan los derechos de los usuarios, como son la Ley orgánica de protección de datos (LOPD) y la Ley de servicios de la sociedad de información (LSSI).
  - Derechos propios y de terceros de los desarrolladores de la solución móvil: se debe proteger el contenido propio y contar con las respectivas licencias de uso de recursos de terceros que se usen en la aplicación.
  - Licencia y condiciones de uso. Es importante tenerlo desarrollado para evitar posibles reclamaciones.

Lectura recomendada

Audea. Seguridad de la información (2013). «Privacidad y seguridad en las aplicaciones móviles».

  - Informar al usuario. El usuario debe poder tener acceso a los textos de las condiciones legales, así como contar con información acerca de quiénes son los creadores y los responsables de las aplicaciones.

- **Tiendas de *apps***:
  - *Markets*. Las tiendas de aplicaciones de las diferentes plataformas móviles tienen sus propias condiciones que deben cumplir las aplicaciones que se ofrecen en ellas.

  - Información y permisos. El usuario debe estar informado de los permisos que facilita a la aplicación que se está instalando.

- **Funcionalidades y público objetivo**:
  - Funcionalidades. La aplicación deberá usar medios lícitos para lograr la funcionalidad que tiene como objetivo.

  - Menores. Los menores de catorce años están especialmente protegidos en la legislación de consumidores y usuarios.

  - Publicidad. En caso de llevar publicidad, la aplicación deberá mostrarla siempre identificada.

3.2. Aplicaciones de salud

Las aplicaciones diseñadas para su uso en el ámbito de la salud deben cumplir además otros requisitos y controles de calidad, aunque estos dependen de las funcionalidades que tenga cada aplicación. Por eso, lo primero que hay que determinar es si la solución tecnológica es considerada como **producto sanitario** basándose en la Directiva 93/42/CEE del Consejo de las Comunidades Europeas, modificada en 2007 por la Directiva 2007/47/CE del Parlamento Europeo y del Consejo, que lo define como:

> «Cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos destinados por su fabricante a finalidades específicas de diagnóstico y/o terapia y que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de:
>
> - diagnóstico, prevención, control, tratamiento o alivio de una enfermedad,
> - diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia,
> - investigación, sustitución o modificación de la anatomía o de un proceso fisiológico,
> - regulación de la concepción,
>
> y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios.»
>
> Directiva 93/42/CEE. Artículo 1, apartado 2.

En caso de que no se corresponda con esta definición y que, por lo tanto, no sea considerada como producto sanitario, la aplicación móvil solo debería ajustarse a las consideraciones previas junto con los aspectos de calidad y accesibilidad.

En cambio, las que sí se identifiquen como producto sanitario deben ajustarse al proceso establecido en la normativa europea. Estas soluciones tecnológicas deberán llevar el marchamo CE y clasificarse, en función del posible riesgo que presenten, en clase I, IIa, IIb o III. La normativa incluye en su anexo IX las dieciocho reglas que permiten evaluar el producto sanitario según su inocuidad o posible riesgo para la salud de las personas, y otorgarle la clasificación correspondiente.

Igualmente, el producto sanitario debe cumplir con unos requisitos generales y otros relativos al diseño y la fabricación. Los requisitos generales incluyen aspectos relativos a la seguridad y la reducción de riesgos para el paciente, así como la necesidad de adaptación de la solución tecnológica a los conocimientos y experiencias del usuario potencial.

Los requisitos que afectan al diseño y fabricación abarcan los siguientes puntos:

- Propiedades químicas, físicas y biológicas.
- Infección y contaminación microbiana.
- Propiedades relativas a la fabricación y al medio ambiente.
- Productos con función de medición.
- Protección contra las radiaciones.
- Infección y contaminación microbiana.
- Propiedades relativas a la fabricación y al medio ambiente.
- Productos con función de medición.
- Protección contra las radiaciones.
- Requisitos para los productos sanitarios conectados a una fuente de energía o equipados con una fuente de energía.
- Datos proporcionados por el fabricante. Información sobre el responsable y características del producto, así como las instrucciones de utilización.

Por último, las aplicaciones deben cumplir con otros procesos incluidos en la normativa relativos a controles, evaluaciones y disposiciones administrativas, recogidos en los anexos II («Sistema completo de garantía de calidad») y V («Garantía de calidad de la producción»).

Independientemente del tipo de producto sanitario de que se trate, es necesario que tenga un sistema de gestión de la calidad de acuerdo con estos anexos. Para el cumplimiento de estos requisitos de calidad se puede seguir la norma ISO 13485, que es una norma específica de calidad para productos sanitarios.

Ejemplos

A continuación se muestran como ejemplo un par de aplicaciones, una que sí se puede considerar como producto sanitario y otra que, por contra, no tiene porqué ser tratada como tal, aunque a primera vista lo pueda parecer:

- **Diabetes Companion**: Según su descripción, es un gestor para la diabetes que analiza los datos que el usuario introduce a diario para ajustar el tratamiento de la enfermedad. Si se realiza un análisis de los datos, se puede considerar como un producto sanitario y así está certificado dado que tiene tanto el distintivo CE como registro en la FDA.

- **Diario de Migrañas**: Según su descripción, es una aplicación para llevar un control de los dolores de cabeza en función de la fecha y las características propias del dolor, así como del tratamiento utilizado. Esta aplicación no entraría dentro de la definición de producto sanitario ya que lo único que realiza es un registro de síntomas (dolor de cabeza), por lo que no necesita ser tratada como producto sanitario.

Ilustración 1. A la izquierda, interfaz de la aplicación Companion, y a la derecha, la de Diario de Migrañas.

3.2.1. Un caso práctico de certificación en España

Una empresa dedicada a la investigación, desarrollo e implantación de las nuevas tecnologías en el sector sociosanitario tiene una aplicación que puede ser considerada como producto sanitario. Se trata de una solución móvil diseñada para la gestión de pacientes crónicos.

Una vez que han constatado que se trata de un producto sanitario y determinado qué clasificación tendría su producto, elaboran la documentación técnica para presentarlo al Organismo Notificado, que es el encargado de auditarlo y, en caso de considerar que cumple los requisitos, conceder el marchamo CE. Mientras tanto, han solicitado a la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) una licencia de fabricante, así como una declaración de actividades para ventas y distribución.

Una vez la empresa tenga el marchamo CE, la licencia de fabricante y la declaración de actividades para ventas y distribución, el producto estará listo para su comercialización como producto sanitario.

En total, todo este proceso puede llevar como mínimo un año:

- Tres meses para la obtención de la licencia de fabricante.
- Entre tres y cuatro meses para la preparación de documentación.
- Seis meses para el proceso de revisión de documentación y auditoría del marchamo CE.

3.3. Otras normativas internacionales

España ha incorporado la normativa europea a su ordenamiento, lo que queda recogido en el Real decreto 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios. En otros países se han puesto en marcha otras normativas para regular el desarrollo de aplicaciones móviles en el ámbito sanitario. A continuación veremos las más importantes.

3.3.1. Normativa IEC 62304

Para el software que es de por sí un producto sanitario o forma parte de un dispositivo o sistema que sí está declarado como producto sanitario, se ha desarrollado la normativa IEC 62304. Es una norma internacional conjunta entre Estados Unidos y la Unión Europea que especifica los requisitos para los procesos del ciclo de vida.

La IEC 62304 indica que el propio fabricante debe clasificar su software en función de los efectos negativos que pueda provocar.

- Clase A: no es posible lesión o daño para la salud.
- Clase B: es posible una lesión no seria.
- Clase C: es posible una lesión seria o la muerte.

En función de dicha clasificación, los procesos de vida del software tendrán unas exigencias acordes con la clase.

3.3.2. UK MHRA

En el Reino Unido, la Medicines & Healthcare Products Regulatory Agency (MHRA) tiene una sección dedicada a regular las aplicaciones. Siguen las directivas comunitarias de la Unión Europea y en la guía *Medical device stand-alone software including apps* indican que las aplicaciones que tengan asociado alguno de los siguientes términos pueden ser consideradas como producto sanitario: amplificar, análisis, interpretar, alarmar, calcular, controlar, convertir, detectar, diagnosticar, medir y monitorear.

3.3.3. USA-FDA

En Estados Unidos, la Food and Drug Administration (FDA) es la encargada de la regulación de este tipo de aplicaciones, y con ese objetivo tiene un espacio en su portal web denominado «Mobile Medical Applications». La FDA aplica el enfoque basado en el riesgo para garantizar la seguridad y la eficacia de los dispositivos médicos. El documento de orientación ofrece ejemplos de cómo la FDA podría regular las aplicaciones móviles en caso de que haya un riesgo moderado (clase II) o un riesgo alto (clase III). La guía también proporciona ejemplos de aplicaciones móviles que no son dispositivos médicos, aplicaciones móviles para las que la FDA podría de ejercer su potestad de cumplimiento de regulación pudiendo considerarlas como dispositivo médico, y aplicaciones médicas móviles que la FDA sí considera como dispositivo médico.

Las tres clases que establece son:

- Clase III. Estas aplicaciones móviles cumplen la definición de producto sanitario en la Ley de FD & C y su funcionalidad representa un riesgo para la seguridad del paciente si la aplicación móvil llegara a no funcionar según lo previsto.

- Clase II. Estas aplicaciones móviles cumplen con la definición de producto sanitario pero representan un riesgo bajo para la población y, por ahora, no estarán sujetas a los requisitos reglamentarios.

- Clase I. Estas aplicaciones móviles no son consideradas como un producto sanitario.

3.4. Seguridad

La seguridad y la protección de datos personales son aspectos esenciales en cualquier tipo de aplicación, más aún si está destinada al ámbito sanitario. La Comisión Europea ha publicado el «Green Paper on mobile Health (mHealth)», en el que se marcan unos retos entre los que destacan la protección y la recolección de datos. Cabe señalar que un problema en la seguridad con el manejo de este tipo de datos puede traer consecuencias nefastas a la imagen de la empresa o institución responsable de la custodia de estos datos, además de consecuencias legales.

Referencia bibliográfica

Comisión Europea (2014). «Green Paper on mobile Health (mHealth)».

3.4.1. Protección de datos

Dada la naturaleza de los datos personales relacionados con la salud, las aplicaciones de este ámbito deben contener garantías apropiadas y específicas de seguridad, como la encriptación de los datos del paciente y los mecanismos de autenticación de pacientes apropiados para mitigar los riesgos de seguridad.

3.4.2. *Big data*

Las aplicaciones móviles en el entorno de la salud pueden proporcionar grandes cantidades de información, como puede ser información de los sensores para alguna medida, imágenes, descripciones de síntomas, etc., de manera que se pueda hacer una minería de datos con la información proporcionada que permita, por ejemplo, mejorar tratamientos epidemiológicos.

Este tipo de procesos deben hacerse de conformidad con los requisitos legales, entre ellos la protección de los datos personales, y podrán dar lugar a cuestiones éticas, en particular en relación con el respeto del principio de consentimiento informado y explícito, cuando ello sea pertinente; por ejemplo, si el paciente no permite expresamente la cesión de sus datos personales para que sean utilizados con fines de investigación.

3.4.3. Transparencia

Se debe hacer especial hincapié en la transparencia de la información que el usuario va a consumir, dado que esa transparencia le dará al usuario una mayor seguridad a la hora de utilizar la aplicación.

3.4.4. Casos de autorregulación

Cuando hablamos de autorregulación, nos referimos a aquellos casos en los que no hay una legislación (o existe pero no es clara) y surgen entidades o asociaciones que deciden crear un marco que sirva de referencia para cumplir

una serie de criterios o normas a seguir para tener algún tipo de certificación o distintivo que indique que las aplicaciones cumplen con las expectativas fijadas. Entre las iniciativas actuales destacan:

Distintivo AppSaludable

A la hora de realizar el desarrollo de una aplicación móvil destinada a la salud, esté dirigida a pacientes o a profesionales sanitarios, se debería seguir una serie de pautas que contribuyan a la mejora de los servicios y no al perjuicio de los usuarios. La Agencia de Calidad Sanitaria de Andalucía, por ejemplo, ofrece un listado de treinta y una recomendaciones para el diseño, uso y evaluación de aplicaciones de salud.

Una vez que esta Agencia evalúa las aplicaciones que lo solicitan y comprueba que cumplan con los requisitos establecidos, dichas aplicaciones pasan a tener el distintivo AppSaludable, que es una concesión que reconoce la calidad y seguridad de la aplicación en el entorno de la salud. Además, la aplicación pasa a constar en un directorio de aplicaciones destacadas por su calidad y seguridad.

Farmaindustria: código de buenas prácticas

La Asociación Nacional Empresarial de la Industria Farmacéutica publicó un documento de buenas prácticas destinado a la promoción de medicamentos de prescripción, a la interrelación con profesionales sanitarios y con organizaciones sanitarias, así como a la interrelación con las organizaciones de pacientes.

Referencia bibliográfica

Farmaindustria (2014). «Código de buenas prácticas de la industria farmacéutica».

Dentro de dicho código se aborda la promoción de medicamentos en el entorno digital y se sugiere una serie de pautas a seguir en cuanto al contexto en el que se presenta dicha promoción. Igualmente, incluye algunas advertencias que deberá tener la publicación para indicar que está estrictamente dirigido a profesionales sanitarios facultados para la prescripción de medicamentos, por lo que se requiere una formación especial para su interpretación.

4. Anexos

4.1. Legislación

- Europea
  - 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

- Estatal
  - Constitución española de 1978
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
  - Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
  - Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos
  - Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos
  - Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica
  - 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
  - Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios
  - Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación
  - Ley 59/2003, de 19 de diciembre, de Firma Electrónica

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos

- Autonómica
  - Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid
  - Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos
  - Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos

- Sanitaria
  - Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica
  - Ley 14/1986, de 25 de abril, General de Sanidad
  - Ley 16/2003, de 28 de marzo, de Cohesión y Calidad del Sistema Nacional de Salud
  - Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias
  - Ley 25/1990, de 20 de diciembre, del Medicamento
  - Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida
  - Ley 45/2003, de 21 de noviembre, por la que se modifica la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida
  - Ley 21/2000, de 29 de diciembre, sobre los Derechos de Información Concernientes a la Salud y la Autonomía del Paciente, y la Documentación Clínica (Cataluña)
  - Ley 15/1998, de 9 de julio, de Ordenación Sanitaria de Cataluña

4.2. Otra documentación de interés

- Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME) - Grupo de trabajo sobre protección de datos del artículo 29

- Convenio del Consejo de Europa sobre el respeto a los derechos humanos y la biomedicina 1997

- Recomendación 2/2004, de la Agencia de Datos de la Comunidad de Madrid sobre la custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas

4.3. Recursos en Internet

- Autoridades de control
  - Agencia Española de Protección de Datos
    <www.agpd.es>

  - Agencia Catalana de Protección de Datos
    <www.apdcat.net>

  - Agencia Vasca de Protección de Datos
    <www.avpd.euskadi.net>

  - Agencia de Protección de Datos de la Comunidad de Madrid
    <https://www.agpd.es/portalwebAGPD/ficheros_inscritos/
    titularidad_publica/indice_organismos/index-ides-idphp.php?
    organismo=QUdFTkNJQSBERSBQUk9URUNDSU9OIERFIERBVE9
    TIERFIExBIENPTVVOSURBRCBERSBNQURSSUQ=&tipo_admin=
    QURNT04uIFkgT1JHQU5JU01PUyBQ2kJMSUNPUyBERSBDLiBBVVRPT
    k9NQVM=&comunidad=Q09NVU5JREFEIERFIE1BRFJJRA==>

  - Comisión Nacional de Informática y Libertades - Francia
    <www.cnil.fr/index.php?id=5>

  - Information Comissioner's Office ICO - Reino Unido
    <www.ico.gov.uk/>

- Organismos europeos
  - Comisión Europea
    <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>

  - Art.29 Data Protection Working Party

<http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>

  - Unión Europea
    <http://europa.eu/index_es.htm>

  - Consejo de Europa
    <http://hub.coe.int/>

- Universidades y docencia
  - Universidad Católica de Lovaina Centro Interdisciplinar de Informática y Derecho
    <http://www.law.kuleuven.be/icri/>

  - Universidad de Bolonia Informática y Derecho
    <http://www.cirsfid.unibo.it/cirsfid/index.html>

  - Institute for Legal Informatics Universidad de Hannover
    <http://www.iri.uni-hannover.de/>

  - Instituto de Informática Jurídica de la Universidad de Comillas
    <http://www.upcomillas.es>

- Publicaciones electrónicas
  - Revista *Datos personales* (APD Comunidad de Madrid)
    <http://www.datospersonales.org/>

- Otros
  - Taller de criptografía de la Universidad de Granada
    <http://www.cripto.es/>

  - Asociación Española de Derecho Sanitario
    <http://www.aeds.org/>