Informes SEIS

La seguridad y confidencialidad de la información clínica

3

Pamplona, 12 de Diciembre de 2000

La presente edición ha sido posible gracias a la financiación del Fondo de Investigaciones Sanitarias

Informes SEIS

Diseño de cubierta: Roberto Montoro

Primera edición, Marzo 2001

Fotocomposición: Negociado de Composición. Dirección General de Organización y Sistemas de Información.

http://www.seis.es

Secretaría Técnica: CEFIC
C/ Olimpo, 33 - 1.º C. 28043 - Madrid
Tel: 91 388 94 78 Fax: 91 388 94 79
cefic@cefic.com

Printed in Spain - Impreso en España

Depósito legal: NA-1075 / 2001

ISBN: 84-930487-2-0

Imprime: ONA Industria Gráfica
Polígono Agustinos, Calle F - 31013 Pamplona
Tel. 948 35 10 14

La seguridad y confidencialidad de la información clínica

Javier Carnicero Giménez de Azcárate
Sebastián Hualde Tapia
(Editores)

Autores:

Pilar Mazón Ramos
Javier Carnicero Giménez de Azcárate
Javier Gost Garde
José Luis Conde Olasagasti
Jokin Sanz Ureta
Sebastián Hualde Tapia
Juan Antonio Pérez-Campanero Atanasio
Jordi Buch i Tarrats
Francisco Jordán
Alberto Andérez González
Jesús Rubí Navarrete

Participantes en el III informe SEIS:

Albareda Albareda, Jorge. *FEA Traumatología y Cirugía Ortopédica. Hospital Clínico Universitario de Zaragoza.*

Amézqueta Goñi, Carlos. *Médico, Centro de Salud de Iturrama. Servicio Navarro de Salud.*

Andérez González, Alberto. *Director de Administración y Recursos Humanos. Asesor Jurídico del Gobierno de Navarra. Servicio Navarro de Salud.*

Bermejo Parra, Julia. *Directora del Servicio de Atención de Sistemas Sanitarios. Gobierno de Navarra.*

Buch i Tarrats, Jordi. *Director de servicios profesionales. Safelayer.*

Carnicero Giménez de Azcárate, Javier. *Servicio Navarro de Salud.*

Conde Olasagasti, José Luis. *Agencia de Evaluación de Tecnologías. Instituto de Salud Carlos III.*

Etxebarría Etxebarría, José Luis. *Subdirección de Informática y Sistemas de información. Osakidetza.*

Ferrer Ripollés, Carmen. *Jefa del Servicio de Coordinación de Sistemas de Información de la Red Sanitaria. Consejería de Sanidad de Valencia.*

Garbayo Sánchez, José Antonio. *Jefe de la Sección del Área Secundaria de Salud. Gobierno de Navarra.*

García Quintans, Antonio. *Subdirector de Atención Primaria. Servicio Galego de Saude.*

Gost Garde, Javier. *Jefe del Servicio de Medicina Preventiva. Hospital de Navarra.*

Hualde Tapia, Sebastián. *Director del Servicio de Organización y Sistemas de Información. Gobierno de Navarra.*

Jiménez Pérez, Carlos. *Subdirector de Gestión de Sistemas de Información. Hospital Gregorio Marañón.*

Laredo de la Iglesia, Jorge. *Consultor. INDRA.*

Mazón Ramos, Pilar. *FEA Cardiología. Hospital Universitario de Santiago de Compostela.*

Nieto Cervera, Jaime. *Subdirector de Sistemas de Información y Evaluación. Hospitales Universitarios Virgen del Rocío.*

Nogueira Fariña, Javier. *Servicio de Documentación. Servicio Hospitalario de Pontevedara.*

Oiza Casado, Maite. *Jefa de la Sección de Protección de Datos. Gobierno de Navarra.*

Pérez Campanero, Juan Antonio. *Jefe de Negocio Electrónico. Telefónica de España, S.A.U.*

Povés Saénz de Ibarra, Gorka. *Consultor. INDRA.*

Ratón Aspiumza, Ernesto. *Gerente Administración. INDRA.*

Rubí Navarrete, Jesús. *Adjunto al Director. Agencia de Protección de Datos.*

Sanz Ureta, Jokin. *Jefe de la Sección de Sistemas. Gobierno de Navarra.*

La reunión correspondiente al III informe SEIS ha sido posible gracias a la colaboración de INDRA y al apoyo del Departamento de Salud del Gobierno de Navarra.

P R Ó L O G O

La Sociedad Española de Informática de la Salud (SEIS) agradece a todo el grupo de expertos que ha participado en la elaboración de este III INFORME SEIS, su colaboración y dedicación para conseguir que este documento sea útil para orientar a todos los profesionales, en la tarea común de avanzar en la innovación del sistema sanitario.

Nuestra convicción de que, a través de estudios y puesta en común de los conocimientos y experiencias que se tienen en nuestras organizaciones, se obtienen valoraciones, análisis y líneas de actuación que aportan una excelente base de trabajo útil para todos, lleva a nuestra Sociedad a planificar anualmente los INFORMES SEIS.

Los INFORMES SEIS son una actividad estratégica de nuestra Sociedad, que materializa anualmente el grupo de la SEIS de la Comunidad Foral de Navarra, con la dirección del Delegado en esta Comunidad Foral y con la inestimable colaboración del Gobierno de Navarra siempre sensible a apoyar estas iniciativas.

Para la redacción del III INFORME SEIS, "La seguridad y confidencialidad de la información clínica", se han introducido varias innovaciones metodológicas con el fin de mejorar la elaboración del documento. Esperamos que los lectores acogerán favorablemente los cambios introducidos. Nuestro objetivo es prestar servicios de utilidad para los profesionales, las organizaciones sanitarias y las entidades de desarrollo tecnológico, agentes todos involucrados en la innovación tecnológica de nuestro sistema sanitario.

Confiamos en que esta pretensión se cumpla y ustedes así lo entiendan.

Marzo de 2001

Luciano Saéz Ayerra
Presidente
Sociedad Española de Informática de la Salud

"Así lo juro –respondió don Quijote–, y aun le echaré una losa encima para más seguridad, porque quiero que sepa vuestra merced, señor don Antonio –que ya sabía su nombre–, que está hablando con quien, aunque tiene oídos para oír, no tiene lengua para hablar; así que con seguridad puede vuestra merced trasladar lo que tiene en su pecho en el mío y hacer cuenta que lo ha arrojado en los abismos del silencio".

(Miguel de Cervantes. El ingenioso hidalgo don Quijote de la Mancha. II Cap. 62)

ÍNDICE

I N T R O D U C C I Ó N

Las Tecnologías de la Información y de las Comunicaciones (TIC) permiten la continua innovación y mejora de la asistencia sanitaria. El registro de información por medio de la historia clínica electrónica, y su disponibilidad para todos los profesionales implicados en la atención de un paciente de una forma ágil y fiable, comienza a ser una realidad en los hospitales y centros de atención primaria. La puesta a disposición de los profesionales del conocimiento científico, con mayor facilidad que nunca, a través de Internet y las bases de datos de publicaciones médicas, y los avances en tecnologías sanitarias basados precisamente en las TIC, son algunas de las innovaciones que se han producido en los últimos años. Otros aspectos menos desarrollados todavía en nuestro país, pero ya inminentes, son facilitar el acceso a los usuarios a la información y al sistema sanitario.

Todas estas ventajas deben redundar en una mejora de la calidad del servicio que el sistema sanitario presta a los ciudadanos. Como ha expresado el Primer Ministro Británico "El desafío para el NHS es aprovechar la revolución de la información y utilizarla en beneficio de los pacientes".

Justificación y objetivos del informe

La revolución de las TIC además de ventajas como las señaladas, tiene también sus inconvenientes, uno de ellos son los problemas de seguridad y confidencialidad de la información clínica. Esta cuestión fue puesta de manifiesto en el II Informe SEIS, que trató sobre "Las tecnologías de la información y las comunicaciones en el futuro de la atención primaria", en el que el aspecto más resaltado por los asistentes fue su preocupación por la seguridad y confidencialidad de la información clínica.

Por ello la SEIS decidió elaborar su III Informe SEIS sobre "La seguridad y confidencialidad de la información clínica".

El objetivo del informe es analizar desde diferentes puntos de vista los problemas de confidencialidad y seguridad que se plantean en la era de la información, ofreciendo un documento útil al sistema sanitario para que revise y actualice sus procedimientos de salvaguarda de la intimidad de los pacientes.

Contenido del informe

Para la elaboración del informe se encargó a varios expertos que redactasen un documento sobre los siguientes aspectos:

–La informatización de la documentación clínica: oportunidad de mejora de la práctica clínica y riesgos para la seguridad y confidencialidad.

–Gestión sanitaria y tecnologías de la información.

–El derecho a la intimidad y las necesidades de la investigación y la evaluación en el ámbito sanitario.

–Aspectos técnicos de la seguridad en la información sanitaria.

–Gestión de la seguridad de los sistemas de información y de las comunicaciones.

–La seguridad de las transacciones bancarias en Internet.

–Aspectos legales de la seguridad y confidencialidad en la información clínica.

–Funciones de la agencia de protección de datos. Tratamiento y confidencialidad de datos de salud.

El día 12 de Diciembre de 2000, se celebró en Pamplona la reunión a la que asistieron además de los redactores de las ponencias, médicos, gestores sanitarios, profesionales y gestores de sistemas de información. En la sesión los ponentes presentaron su trabajo, siguiendo después un coloquio con todos los presentes. Ese mismo día, todos los asistentes acordaron las conclusiones de la jornada que se incluyen al final del texto de las ponencias.

LA INFORMATIZACIÓN DE LA DOCUMENTACIÓN CLÍNICA: OPORTUNIDAD DE MEJORA DE LA PRÁCTICA CLÍNICA Y RIESGOS PARA LA SEGURIDAD Y CONFIDENCIALIDAD

Pilar Mazón Ramos
Hospital Universitario de Santiago

Javier Carnicero Giménez de Azcárate
Servicio Navarro de Salud

"Todo lo que haya visto u oído durante la cura o fuera de ella en la vida común, lo callaré y conservaré siempre como secreto, si no me es permitido decirlo". (Juramento hipocrático) [1]

INTRODUCCIÓN

El instrumento fundamental en la atención a un paciente es la historia clínica, que integra la información registrada por su médico y los profesionales sanitarios implicados en su asistencia, la de las exploraciones, pruebas complementarias y procedimientos médicos y quirúrgicos, con la identificación del paciente y sus datos administrativos.

Gracias a los avances de las tecnologías de la información y de las comunicaciones que se han producido en los últimos años la historia clínica se transforma. Primero asistimos a la informatización de la historia que unifica toda la información del paciente registrada en el centro sanitario, a continuación a la integración o no con la de otros niveles sanitarios y finalmente, por el momento, a la disponibilidad de la misma en cualquier centro sanitario en que sea atendido el paciente.

La relación médico paciente debe estar basada en la confianza y en el secreto profesional. Es una obligación de los profesionales guardar el debido secreto y de las organizaciones sanitarias, y de los propios profesionales, garantizar la seguridad de la información y su confidencialidad.

En el presente trabajo se revisan los elementos básicos de la historia clínica, las ventajas de su informatización, y la necesidad de garantizar su confidencialidad y seguridad.

HISTORIA CLÍNICA

Se puede considerar la Historia Clínica el elemento básico de información para el médico en su práctica diaria, con independencia de su ámbito de trabajo. Aunque pueda haber algunas variaciones, hay una serie de datos que pueden considerarse imprescindibles como son los siguientes[2]:

1.–Datos de identificación del paciente: nombre, apellidos, domicilio, fecha y lugar de nacimiento, sexo, estado civil, profesión y actividad, número de DNI o de

identificación del sistema sanitario, pariente más cercano o representante legal y forma de contacto con el mismo.

2.–Datos de identificación del centro.

3.–Datos clínicos: antecedentes personales y familiares de interés, anamnesis, exploración física, órdenes de exploración diagnóstica, diagnóstico de presunción.

4.–Consentimiento escrito del paciente o representante legal, tanto para el ingreso, como para la práctica de procedimientos quirúrgicos y exploraciones especiales y, en su caso, para la utilización con fines distintos al estrictamente asistencial de los datos contenidos en la historia.

5.–Procedimientos y datos diagnósticos y terapéuticos (análisis, radiografías, exploraciones y tratamientos médico y quirúrgico).

6.–Forma: las historias clínicas deben ser normalizadas en su estructura física y lógica con el fin de facilitar su uso por el personal sanitario y permitir obtener la información con fines administrativos, estadísticos y de evaluación de la calidad, escrita a máquina o con letra legible, evitando la utilización de símbolos o abreviaturas. Toda anotación deberá ser fechada y firmada de forma que permita la identificación del personal sanitario que la realice.

Informatización de la historia clínica

Aunque el concepto de historia clínica, en cuanto instrumento de registro de la información clínica, imprescindible para atender adecuadamente a un paciente, permanece inalterado, la historia clínica ha evolucionado en los últimos años. Clásicamente era un documento personal del médico en el que éste registraba la información de sus pacientes. En los hospitales jerarquizados la historia es un documento en el que se integra toda la información clínica de un paciente, con independencia de en qué servicio se produzca. El paso del archivo personal del médico o del servicio, al archivo general del hospital no se produjo sin discusiones, pero puede considerarse un hecho en nuestro país. Más tarde, la historia se informatiza y se incluye la información procedente de todos los servicios del centro sanitario y de los diferentes equipos de electromedicina, como los de diagnóstico por imagen y autoanalizadores. En esta fase se encuentran cada vez más hospitales de nuestro sistema sanitario.

En la actualidad la discusión se centra en si cada paciente debe disponer de una historia única con independencia de en qué centro es atendido, si la historia no es única pero la información clínica se comparte entre los diferentes niveles asistenciales y centros sanitarios, y en cómo se garantiza la confidencialidad y seguridad de la información.

Las tecnologías de la información y de las comunicaciones permiten una mayor disponibilidad y accesibilidad a la información clínica impensable sólo hace unos años, de forma que los médicos y el resto de profesionales sanitarios pueden acceder a la historia, informes y pruebas complementarias de un paciente, de cualquier centro sanitario en que éste haya sido atendido previamente y en el momento que se necesite. Sin embargo, la mayor accesibilidad y disponibilidad de la información hace pensar siempre en la necesidad de mayores precauciones para garantizar la seguridad y la confidencialidad.

A pesar de las evidentes ventajas de la historia informatizada, algunas de las cuales se enumeran más adelante, debemos resaltar que hay todavía un escaso desarrollo de la informática médica en la práctica diaria, no sólo por la falta de formación de los propios profesionales sanitarios en esa materia, sino también porque hay gran cantidad de programas informáticos en uso, lo que parece reflejar que ninguno responde por completo a las necesidades clínicas[3].

En nuestros hospitales es habitual que haya diferentes tipos de soporte informático, no sólo en el mismo centro sanitario, sino incluso dentro del mismo servicio médico, con lo que no se obtienen muchas de las ventajas esperadas. Esta situación se debe al retraso con que se ha informatizado la actividad clínica de nuestros centros sanitarios. Los hospitales comenzaron su informatización por la parte administrativa como la contabilidad, gestión de personal y almacenes, y médico-administrativa como la admisión. Sólo recientemente se informatiza, de forma ordenada, la historia clínica. Todo ello ha provocado que exista un retraso entre la situación real y la de las posibilidades que ofrecen las tecnologías de la información y de las comunicaciones, generando ansiedad en los profesionales que contemplan avances espectaculares en la informatización de cualquier actividad en nuestra sociedad sin que estos avances se hayan visto reflejados en su actividad clínica.

Por otra parte, en nuestro medio es muy frecuente que las firmas que comercializan equipos de electromedicina como autoanalizadores o de diagnóstico por imagen, o laboratorios farmacéuticos, ofrezcan el "programa" que necesita el médico para su quehacer diario y, como es lógico, ante la falta de perspectivas de la implantación de la solución técnica "oficial", este tipo de soluciones se extienden. Tampoco resulta excepcional que los propios médicos tomen la iniciativa y desarrollen sus propias aplicaciones para salir del paso. El caso más llamativo de esto último es el del Hospital de Tudela, perteneciente al Servicio Navarro de Salud, que se ha informatizado en su totalidad partiendo de la aplicación de historia clínica desarrollada por uno de sus médicos[4, 5], aunque en la actualidad el desa-

rrollo del sistema ya corresponde al llevado a cabo por el Departamento de Organización y Sistemas de Información del Gobierno de Navarra.

Además de las dificultades señaladas se deben añadir algunas inquietudes, la principal de ellas es la que nos ocupa en este trabajo: la seguridad y la confidencialidad de la información clínica.

Ventajas de la historia clínica informatizada

Las ventajas de la historia clínica informatizada son muchas, algunas de ellas pueden resumirse a continuación:

Las historias en papel suelen estar escritas a mano, con letra no siempre legible, pueden acabar siendo voluminosas y resultar difícil revisar la información necesaria para atender al paciente. Aquí se cumple la regla de que muchos datos no suponen necesariamente más información.

Los sobres, como ya se ha indicado, a veces muy voluminosos, deben ser almacenados en archivos cada vez de mayor tamaño, que ocupan un espacio precioso en los centros sanitarios y con mucha frecuencia acaban en naves situadas en polígonos industriales alejados de los centros hospitalarios. Además del problema de almacenamiento se añade entonces el del transporte, lo que hace que las historias no siempre están accesibles cuando son necesarias. En estas condiciones de archivo es habitual la pérdida de datos y resultados, la duplicidad de informes y a veces de pruebas, el retraso en conseguir la información, y también el deterioro físico e incluso la desaparición de historias completas.

Una dificultad que se añade cuando los archivos son de gran tamaño o quedan fuera de los centros sanitarios, es que cada vez son más las personas, muchas de ellas que no son profesionales sanitarios, las que tienen acceso a la documentación clínica.

La historia clínica informatizada permite, en condiciones normales, el acceso inmediato a una completa información sobre el paciente, su permanente actualización, su facilidad de lectura y el procesamiento y presentación de la información de una forma sencilla y eficaz. Simplifica el quehacer diario del personal sanitario, facilitando la labor de completar la historia clínica, pues hay muchos datos que no hay que repetir, muchos textos que no necesitan escribirse, se recurre a códigos, bases de datos previamente elaboradas, en definitiva se ahorra mucho tiempo, a la vez que se hace un mejor trabajo.

Una historia clínica informatizada supone además que el trabajo médico administrativo resulta más fácil: la confección de partes médicos de alta y baja, las recetas médicas, los informes, la documentación necesaria en admisión se automatiza. Resulta también mucho más sencilla la revisión de los datos necesaria para controles de calidad, estudios estadísticos y de investigación.

Además la historia clínica electrónica no plantea los problemas de espacio que se presentan con la documentación convencional. No se almacena en naves industriales lejos del hospital y no se transporta físicamente de un lugar a otro, por lo que es más "segura" en la conservación de los datos, y es más fácil evitar pérdidas de información.

La historia clínica en soporte informático permite diferenciar sus contenidos de forma que se pueda acceder a toda o a parte de la información, según los privilegios de acceso que tengan los empleados del centro. Esta diferenciación no es posible cuando se trata de papel y sobres.

Pero la mayor ventaja desde el punto de vista clínico es que la historia clínica informatizada puede ser única para cada paciente, recogiendo toda la información relativa al mismo, de todos los ámbitos en los que haya sido atendido: atención primaria, atención especializada, consultas de enfermería y urgencias. Con ello se puede conseguir una mayor comunicación entre todos los profesionales implicados en su atención sanitaria, alcanzando una mayor continuidad asistencial. Esta continuidad asistencial no queda restringida a su área "geográfica", sino que puede extenderse, gracias a las tecnologías de la información y de las comunicaciones a otros profesionales de centros alejados, utilizando los recursos que Internet pone a nuestro alcance, como consultas a distancia, videoconferencias y sesiones clínicas interactivas.

La historia clínica informatizada amplía la utilidad de la tarjeta sanitaria en un doble sentido. Por un lado, permite que el paciente lleve consigo información clínica relevante, con lo que la tarjeta se convierte en una *tarjeta clínica.* Por otro lado puede convertirse en la llave que autorice el acceso a su información, con lo que se convierte en un instrumento de seguridad.

PREVISIONES PARA LOS PRÓXIMOS AÑOS

Nos encontramos en pleno desarrollo de la Sociedad de la Información, que se supone alcanzará su plenitud en el Siglo XXI. Castells incluso ha introducido el concepto de *sociedad informacional*, "Organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes

fundamentales de la productividad y el poder debido a las nuevas condiciones tecnológicas que surgen en este periodo histórico"[6]. Esta revolución es similar en magnitud e intensidad a las que trajeron la máquina de vapor en el siglo XIX y la cadena montaje en el siglo XX[6, 7].

La actual revolución tecnológica sin precedentes en el ámbito de la información, abre amplios horizontes de progreso económico, de empleo y de calidad de vida. Estos últimos años, la Unión Europea ha mostrado una gran preocupación al respecto, creando numerosas comisiones que han elaborado propuestas relacionadas con la aplicación de las tecnologías de la información y de las comunicaciones en la sanidad.

Iniciativas de la Unión Europea

El informe Bangemann[8] titulado "Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo" de 1994, propone 12 aplicaciones para el futuro; la séptima consiste en la creación de redes sanitarias basadas en la tecnología informática y de telecomunicaciones; en Europa todos los profesionales y centros sanitarios estarán conectados por redes de comunicaciones de alta velocidad. Las historias clínicas, totalmente informatizadas, podrán circular de un hospital a otro de todo el continente y aparecer traducidas en la pantalla. Los datos de laboratorio y prescripciones terapéuticas se enviarán por correo electrónico a los consultorios y oficinas de farmacia. Las enfermeras de atención primaria actualizarán sus fichas de asistencia e informarán del curso de los pacientes a través de la red. En este contexto, los servicios telemáticos han avanzado más que los programas o aplicaciones.

En el Informe Final de la Conferencia de Helsinki[9] referente a las tecnologías en la Sociedad de la Información: IST 99, se insiste en la historia clínica electrónica como elemento indispensable en la evolución de las tecnologías de la información en la asistencia sanitaria, haciendo hincapié en el problema que se presenta con la posibilidad de transmisión de datos a otros centros y otros profesionales, pues surge la cuestión ¿quién es el propietario de la información? ¿quién puede ver qué, y cuándo?

Otro aspecto que se resalta es que cada vez hay más información médica disponible en Internet, lo que constituye para pacientes y familiares una fuente alternativa de información, incluso llegando a tener datos que el propio profesional desconoce, lo que puede suponer un cambio de mentalidad en la clase médica, al no ser los únicos que controlan la información.

En la Cumbre extraordinaria de Lisboa, de Marzo de 2000, se planteó el objetivo de explotar las oportunidades de Internet, creándose la llamada iniciativa *e*Europa[10], con tres grandes apartados, que tiene como propósitos:

Llevar a cada ciudadano, hogar, colegio, empresa y administración la era digital.

Crear una Europa de formación digital con una cultura empresarial innovadora.

Asegurar que el proceso sea socialmente integrador, afirme la confianza de los consumidores y refuerce la cohesión social.

Para alcanzar esos propósitos se plantea conseguir una red más barata, rápida y segura, invertir en personal y material, y estimular el uso de Internet en múltiples campos de la Sociedad, entre ellos la Sanidad. Además de las acciones propias de sanidad, se propone como uno de los objetivos el que antes de terminar el año 2002 ha de extenderse el uso de la tarjeta inteligente a las aplicaciones de elevado nivel de seguridad (datos médicos).

Para la sanidad se promueve la acción "La salud en línea" que tiene en cuenta consideraciones como las siguientes:

La prestación a todos los ciudadanos de servicios de salud de calidad es un reto para todos los gobiernos europeos.

Las nuevas tecnologías avanzan vertiginosamente y la población envejece progresivamente.

El reto es: mejorar la calidad y accesibilidad conteniendo los costes.

Las tecnologías digitales pueden mejorar la productividad y cobertura de la asistencia sanitaria.

Sólo el 1% del gasto sanitario se destina a las tecnologías de la información.

La iniciativa plantea los objetivos siguientes:

Todos los profesionales y directivos de salud deben estar conectados a una infraestructura telemática para la prevención, el diagnóstico y el tratamiento.

Identificar y promocionar la mejor práctica sanitaria electrónica en Europa, fijando criterios de cuota de mercado *(bench-marking)*.

Establecer criterios de calidad para las páginas web relacionadas con la Salud.

Crear redes sobre manejo de datos y tecnología sanitaria.

También existe el compromiso de publicar una comunicación titulada "Aspectos Legales de *e*Salud en 2001". El objetivo es revisar la legislación actual al respecto, aclarando la existente y conseguir una confianza de la industria para entrar en el mercado.

La iniciativa del National Health Service

El National Health Service ha publicado su estrategia de sistemas de información, Information for Health[11], que parte de la frase del Primer Ministro británico cuando afirma: "El desafío para el NHS es aprovechar la revolución de la información y utilizarla en beneficio de los pacientes"

En ese contexto se plantea el propósito de que durante los próximos años se disponga de los recursos, conocimientos y procesos necesarios para que:

Los clínicos y gestores tengan la información necesaria para cumplir con la misión del NHS, que se define como "Dar a los ciudadanos de este país el mejor sistema de salud del mundo"

Los pacientes y el público tengan una amplia información de calidad y fácilmente accesible acerca de la salud y de los servicios sanitarios.

Como necesidades de los clínicos en su práctica diaria el documento plantea las siguientes:

Información sobre sus pacientes fiable, completa y disponible en el momento.

Acceso a guías y bases del conocimiento para dar soporte a la toma de decisiones clínicas.

Acceso a la información que permita evaluar su efectividad y facilite la formación continuada.

Entre los objetivos que se plantea el plan está la extensión de la historia clínica electrónica, la cita previa amigable, la rapidez en la entrega de resultados diagnósticos, el NHS *direct* para información y consejo, la biblioteca nacional de salud digital y como claves en el plan, la telemedicina y teleasistencia. Todo ello teniendo en cuenta que una de las inquietudes de los pacientes es que la información sea fiable, completa y segura.

En resumen, los servicios sanitarios se encuentran inmersos en la sociedad de la información o *informacional* que abre unas importantes perspectivas de mejora de la eficiencia y en la calidad de la atención. Instituciones como el National Health Service y la Unión Europea[8-11], plantean acciones y objetivos concretos para aprovechar la oportunidad de mejorar la atención de los ciudadanos. En todos los documentos se observa la preocupación por que los más desfavorecidos no se vean aún más marginados, y por la seguridad y confidencialidad de la información clínica.

CONFIDENCIALIDAD Y SEGURIDAD

La Ley General de Sanidad[12] y la Ley de Protección de Datos[13] se ocupan de aspectos relacionados con la Seguridad y la Confidencialidad, pero el médico clínico tiene presente, desde que existe su profesión, el "Secreto Profesional".

El Código de ética y deontología de la profesión médica[14] dedica los artículos 14 a 16 del capítulo IV al secreto profesional del médico. En síntesis el código fija la cuestión en los siguientes términos:

El secreto del médico, inherente al ejercicio de la profesión es un derecho del paciente que obliga a cualquier médico en su ejercicio y que no se extingue por el fallecimiento del paciente.

Es un deber del médico exigir el mismo secreto a sus colaboradores.

El ejercicio de la medicina en equipo supone el deber de secreto para todos los implicados y sobre todo el secreto.

Cuando ello sea imprescindible y con carácter restrictivo, se puede revelar el secreto en los siguientes casos:

Por imperativo legal.

En las enfermedades de declaración obligatoria.

En las certificaciones de nacimiento y defunción.

Si el silencio diera lugar a un perjuicio del paciente, de otras personas o colectivo.

Cuando el médico se vea injustamente perjudicado por el secreto y el paciente permita la situación.

Cuando el médico se vea acusado ante el colegio o sea llamado a testificar en materia disciplinaria.

Cuando el paciente lo autorice, pero siempre con carácter restrictivo.

El código dedica además el artículo 17 a los sistemas de información estableciendo que estos deben garantizar el derecho del paciente a la intimidad. Además establece que:

En las instituciones sanitarias la documentación clínica y la administrativa deben separase.

Los bancos de datos extraídos de las historias clínicas estarán bajo la responsabilidad de un médico.

Se prohíbe la conexión de los bancos de datos médicos a una red informática no médica.

En los estudios de auditoría clínica, epidemiológica o de gestión la información no permitirá identificar a ningún paciente.

Algunas de las cuestiones que plantea el código deontólogico son de dificil ejecución o no se encuentra debidamente explicadas, como la separación de la documentación clínica y administrativa, la responsabilidad de un médico de los bancos de datos o la conexión de los bancos de datos médicos a una red informática no médica. Sin embargo, lo que interesa del código profesional es que refleja el derecho del paciente a su intimidad y el deber del médico al secreto profesional y a exigirlo a los que le rodean.

NORMAS DE UTILIZACIÓN DE LA INFORMACIÓN CLÍNICA

Como se ha expuesto anteriormente el médico se encuentra inmerso en una sociedad que se está transformando; las tecnologías de la información y de las comunicaciones irrumpen en su quehacer diario y las previsiones apuntan a que la historia clínica se va a transformar de un sobre repleto de papeles y radiografías, a un ente virtual que circulará por la red, accesible a otros profesionales y cuya llave de acceso estará en poder del paciente por medio de su tarjeta sanitaria. Con independencia o no de que estas previsiones se cumplan, lo cierto es que la historia clínica se informatiza y que el paciente tiene derecho a que su intimidad esté salvaguardada y a que la información clínica esté a disposición de quienes le atienden en el momento oportuno. El garantizar estas cuestiones no está sólo en manos del médico, pero sí que se precisa que él se implique en el proceso y se preocupe de respetar él mismo y quienes le rodean una serie de normas de utilización de la historia clínica dirigidas a salvaguardar la confidencialidad y seguridad de la información.

Las normas de utilización deben contemplar entre otras cuestiones las siguientes, que son independientes de que la historia sea en papel o electrónica:

1.–Quién puede acceder al sistema.

Los profesionales sanitarios (médicos, farmacéuticos y enfermeras) implicados en la atención del paciente, personal administrativo a las órdenes de los anteriores, los encargados de la gestión (admisión, facturación...), la dirección del centro y del sistema de Salud, los inspectores médicos y los responsables del control de calidad e investigadores autorizados.

2.–A qué información puede acceder.

Cada Profesional debe acceder únicamente a aquella información que le es necesaria para el ejercicio específico de su función. Cuando la historia está informatizada pueden establecerse claves que permitan sólo acceder a apartados concretos y específicos. En cambio, en la historia recogida en papel, el documento puede considerarse único y no es posible, o es muy difícil, establecer este control.

3.–Quién utiliza realmente el sistema.

Aunque sean los profesionales reseñados anteriormente los que deben tener acceso a la información clínica, existe la posibilidad de que ésta sea accesible a personas ajenas a la atención directa de los pacientes: encargados del almacenamiento y transporte de las historias clínicas en papel, celadores, personal administrativo, sanitarios de otros departamentos. Este personal debe estar instruido en la importancia del secreto profesional, en la falta en que incurre por acceder a una historia sin que ello sea necesario y por supuesto, en la gravedad de la falta que supone transgredir las normas. En los sistemas informáticos es imprescindible que se registre y quede constancia de quién y cuándo accede a la historia.

4.–Consentimiento informado del paciente al acceso a su información clínica.

Aunque en la práctica diaria no se solicita al paciente un consentimiento para que haya acceso a su historia clínica, se da por supuesto que confía en que su médico utilizará toda la información disponible con el único objetivo de proporcionarle la mejor asistencia sanitaria, compartiendo los datos obtenidos con otros profesionales y otros centros cuando sea necesario. El acceso a la historia con fines epidemiológicos, de evaluación y de investigación se trata en otra parte de esta publicación.

5.–Con qué garantías de seguridad tanto físicas como lógicas contamos.

Debemos garantizar que sólo las personas autorizadas acceden a la información clínica y quedan registradas cuando lo hacen. Como se ha comentado con anterioridad, el traslado de expedientes clínicos a través de largas distancias añade el peligro de pérdida de los mismos. En la historia clínica informatizada, con transmisión de datos por redes internas y externas, podría existir una “fuga” de datos, para lo que deben arbitrarse mecanismos de seguridad. Esta cuestión también es objeto de otra parte de esta publicación.

6.–Auditorías.

Todo sistema de seguridad que se precie debe contar con auditorías periódicas que comprueben la bondad del mismo y su nivel de cumplimiento. Los profesionales sanitarios y no sanitarios deben conocer esa posibilidad y colaborar en la práctica de las auditorías de seguridad.

RESUMEN Y CONCLUSIONES

La sociedad de la información y la revolución de las tecnologías de la información y de las comunicaciones también influyen en el ejercicio de la medicina y demás profesiones sanitarias, y en la transformación de la historia clínica. Existen iniciativas en la Unión Europea que respaldan estas transformaciones, que se dirigen a mejorar la calidad y la eficiencia de la atención sanitaria.

Uno de los más importantes derechos del paciente es la confidencialidad de la información que ha facilitado a su médico. Una de las obligaciones más importantes del médico y del resto de profesionales sanitarios o no, es garantizar ese secreto. Los servicios sanitarios deben arbitrar procedimientos que garanticen la seguridad y la confidencialidad de la información clínica.

Las tecnologías de la información y de las comunicaciones permiten la informatización de la documentación clínica y su accesibilidad a cualquier profesional que deba atender al paciente, mejorando la continuidad de la asistencia. A pesar de ello, todavía existe un escaso desarrollo de este proceso en los centros sanitarios de nuestro país.

La documentación clínica informatizada no supone menos garantías de seguridad y confidencialidad que la documentación en papel, pero también exige establecer procedimientos y planes que garanticen esa confidencialidad y seguridad.

Todos los avances tecnológicos no deben hacernos olvidar que lo importante sigue siendo la práctica clínica, la relación médico paciente y el contenido de la historia clínica, con independencia de si está o no informatizada. Puede concluirse con la definición que hace Laín Entralgo[15] de la buena historia clínica, que a pesar de todos esos avances, sigue estando vigente:

"El atenimiento de una historia clínica a la realidad que debe describir –la enfermedad de un hombre– le concederá su idoneidad; la fidelidad de la narración a la estructura canónica del relato, la hará íntegra; por el cumplimiento de las dos intenciones narrativas y la buena observancia de las prescripciones retóricas, llegará a ser clara, precisa y elegante. Idoneidad, integridad, claridad, precisión, elegancia: he ahí el nombre de las virtudes que constantemente debe proponerse el patógrafo. Ellas son, por otra parte, la más firme garantía del progreso en el arte de ver, oír, entender y describir la enfermedad humana"

BIBLIOGRAFÍA

1. Juramento Hipocrático. En: Singer C., Underwood EA. Breve Historia de la Medicina. Guadarrama, Madrid 1966: 51.
2. Aulló Chaves, M. Pelayo Pardo, S. La Historia Clínica. Plan de Formación en Responsabilidad Legal Profesional. Asociación Española de Derecho Sanitario. 1997: 9-10.
3. Ferrer Salvans, P. Recursos informáticos en el ejercicio de la Medicina. En: Farreras-Rozman. Medicina Interna, 14.ª Ed. Harcourt, Madrid 2000.
4. Escolar F, Escolar JD, Sampériz AL, Alonso JL, Rubio MT, Martínez-Berganza MT. Informatización de la historia clínica en un servicio de medicina interna. Med. Clin (Barc) 1992; 99 (17-20).
5. Escolar F. Informatización de la historia clínica en el Hospital "Reina Sofía" de Tudela. Informática y Salud 1998; n.º 16; 808.
6. Castells M. La era de la información, economía, sociedad y cultura, Vol. 1, la sociedad red, Alianza Editorial, Madrid 2000: 47.
7. BSCH y Andersen Consulting. España on line, ideas para afrontar la nueva economía, http://www.bsn.es/: 6
8. Europa y la Sociedad Global de la Información. Informe Bangemann. Diario Oficial del Consejo Europeo, 222, 21 de Julio de 1994, pag. 39.
9. La Salud en la Sociedad de la Información. Informe Final de la Conferencia IST 99. Helsinki. Publicaciones de la Unión Europea. http://europa.eu.int
10. Iniciativa eEuropa 2002. Plan de Acción elaborado por la Comisión Europea para el Consejo de Europa en Feira, 19-20 de Junio de 2000. Publicaciones de la Unión Europea. http://europa.eu.int
11. Burns F. Information for Health. Department of Health Publications. 1998 http://www.imt4nhs.exec.nhs.uk/strategy/index.htm
12. Ley 14/1986, de 25 de abril, General de Sanidad. BOE 29-4-1986, núm. 102.
13. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal. BOE 14-12-1999, núm. 298.
14. Código de Ética y Deontología de la Organización Médica Colegial de España. Septiembre de 1999.
15. Laín Entralgo P. Historia clínica. Triacastela. Madrid, 1998: 763.

GESTIÓN SANITARIA Y TECNOLOGÍAS DE LA INFORMACIÓN

Javier Gost Garde

Servicio de M. Preventiva y Gestión de la Calidad. Hospital de Navarra

RESUMEN

Este artículo realiza una revisión no sistemática del estado del arte de las tecnologías de la información y su repercusión en los servicios de salud de los países industrializados. Se exponen principios y estrategias para desarrollar un sistema de información del Sistema Nacional de Salud. Se define la misión, visión y objetivos estratégicos. Se describen, desde el punto de vista de la gestión de los servicios de salud, las oportunidades y problemas ligados a las principales herramientas utilizadas: historia clínica informatizada e Internet. Se desarrollan los aspectos ligados a la seguridad y confidencialidad de los datos, así como a la calidad de la información y materiales disponibles en Internet.

Palabras clave:

Tecnologías de la información y comunicación. Historia clínica informatizada. Internet. Confidencialidad. Seguridad. Gestión de servicios de salud.

INTRODUCCIÓN

El rápido desarrollo de las tecnologías de la información, especialmente Internet, está suponiendo un notable cambio en la sociedad de los países industrializados. En España, se estima que son ya casi cuatro millones las personas con acceso a Internet. En el 2001 serán más de trescientos millones las que utilicen la red en todo el mundo. Las transacciones comerciales a través de Internet se incrementan asimismo en progresión geométrica. Las empresas han pasado a considerar la inversión en tecnologías de la información y comunicación (TIC) como uno de los elementos estratégicos (junto con las personas y procesos) para alcanzar la excelencia de la organización.

Este fenómeno también se produce en el entorno sanitario. Se estima que son más de 100.000 las páginas web que sobre este tema existen en la red[1]; a través de las cuales planificadores, gestores, pacientes y ciudadanos pueden acceder a una amplia gama de servicios: desde obtener información sobre la mejor evidencia disponible a realizar consultas o adquirir bienes o servicios. En la práctica, casi cualquier cosa que podamos imaginar será factible realizarla a corto plazo por Internet.

En la Unión Europea las iniciativas para implementar la utilización de las TIC en el campo de la salud se remontan a 1986[2]. En la actualidad está en fase de desarrollo el 5.º Programa[3].

En España ¿cuál es la situación en el Sistema Nacional de Salud? La única referencia cooperativa encontrada corresponde al Programa PISTA, promovido por la Secretaría General de Comunicaciones del Ministerio de Fomento. Dicho programa tiene como objetivo la implantación y explotación de una Intranet para cada una de las administraciones sanitarias participantes (Consejería de Sanidad de la Comunidad de Madrid, Servicio Vasco de Salud-Osakidetza, Servicio Navarro de Salud-Osasunbidea, Servei Catalá de la Salut)[4]. El Centro Nacional de Información Sanitaria (http://www.isciii/unidad/Sgecnsp/centros/cnis/cfunciones.html), creado mediante Real Decreto 1983/1966, ha coordinado el desarrollo del área de Salud Pública del citado programa, y concretamente aquellas aplicaciones relacionadas con los subsistemas de la Red Nacional de Vigilancia Epidemiológica, Agencia de Evaluación de Tecnologías Sanitarias, Laboratorios de Salud Pública y Servicios de Información y Comunicación de interés general. No ha podido localizarse ningún otro dato que permita inferir cual es la situación actual del programa.

Como primera reflexión surge la pertinencia y oportunidad de avanzar en la elaboración, desarrollo y seguimiento de un Plan Estratégico de Información del Sistema Nacional de Salud, máxime si tenemos en cuenta que al final de la actual legislatura está prevista la transferencia de la gestión del INSALUD a aquellas CCAA que todavía no han asumido dicha competencia y que tendremos en el conjunto del estado diecisiete servicios de salud autonómicos.

PRINCIPIOS DEL SISTEMA DE INFORMACIÓN DEL SISTEMA NACIONAL DE SALUD

Llegados a este punto es obligado mencionar los trabajos realizados por el National Health Service (NHS) del Reino Unido, toda vez que, por sus características, puede servir de referencia al sistema nacional de salud español. Sobre la base de la misión del NHS *"Proporcionar a la población de este país el mejor sistema de salud del mundo"*[5], se ha elaborado el documento "Information for Health"[6] que desarrolla tanto las estrategias generales como de implementación local a poner en marcha durante el periodo 1998-2005.

Vistas las recomendaciones y estrategias de los citados documentos y entendiendo que las mismas están lo suficientemente elaboradas como para constituir un importante elemento de estudio y debate, se explicitan, adaptadas a la realidad del

Sistema Nacional de Salud español, aquellos principios que, en nuestra opinión, debería reunir el **Sistema de información del Sistema Nacional de Salud.**

Misión:

Ayudar a que los ciudadanos reciban la mejor asistencia posible por parte de los servicios de salud existentes en el estado español.

Visión:

Disponer de las mejores herramientas y estrategias para garantizar la calidad y accesibilidad de la información. La información estará disponible en el lugar y tiempo adecuado (I want it now) para que las personas puedan adoptar las decisiones oportunas y alcanzar los resultados previstos.

Objetivos generales:

–Los profesionales, pacientes y ciudadanos dispondrán de la información precisa para tomar decisiones sobre sus cuidados de salud.

–Los gestores dispondrán de información para conseguir una gestión efectiva y eficiente de los recursos.

–Los planificadores dispondrán de la suficiente información sobre los problemas y necesidades de salud para establecer los programas y acciones adecuadas.

Estos objetivos se corresponden con los diferentes fines para los cuales registramos los diferentes datos sanitarios: prestación de cuidados (incluidos los preventivos), gestión de servicios de salud, análisis de necesidades y planificación, asignación de recursos, evaluación y seguimiento, investigación, epidemiología, etc.

Existe un debate previo: el ámbito en el que debiera aplicarse el sistema de información. El Sistema Nacional de Salud necesita disponer de una información que analice e integre la originada en los distintos servicios de salud de las CCAA. Si bien es coherente avanzar hacia un sistema de información del Sistema Nacional de Salud, ello plantea dificultades importantes y su viabilidad no parece alcanzable a corto plazo.

La implantación de los sistemas de información en los diferentes servicios de salud presenta desarrollos muy dispares (Plan Estratégico de Osakidetza –PESIS– ….). La equidad del sistema puede quebrarse, ya que la disponibilidad de un adecuado sistema de información favorece una atención de calidad.

Los Hospitales y los centros de salud presentan también un desarrollo irregular. Se plantean diferentes temas de debate: ¿Qué nivel de prioridad tiene –en el contexto actual– el desarrollo de los sistemas de información en los hospitales ya en funcionamiento? ¿Existen y son suficientes las partidas presupuestarias destinadas al efecto? ¿Puede compatibilizarse el desarrollo oportunístico de sistemas de información en los servicios con las necesidades de información de la institución? ¿Responden a los mismos objetivos?

Asimismo, y desde un punto de vista exclusivamente técnico, ¿Son compatibles los diferentes sistemas de información existentes? ¿Responden a los mismos estándares? ¿Es factible su integración?[7]

En definitiva, existen unos planteamientos clave tan importantes, que se hace imprescindible alcanzar un consenso entre todas las partes implicadas. En este sentido el Consejo Interterritorial pudiera ser el marco adecuado para su resolución. De hecho el acuerdo de la Subcomisión de Sanidad del Congreso de los Diputados de consolidación y modernización del Sistema Nacional de Salud hace referencia, en el apartado 12.d, a un modelo central de información, del que no se ha encontrado desarrollo posterior (en el momento de la redacción del presente informe sólo hemos encontrado una referencia relativa a un acuerdo del Consejo Interterritorial sobre el proyecto de creación de un sistema de información sobre Tarjeta Sanitaria[8] y que es varios años anterior al citado acuerdo de la Subcomisión ya que data de 1993).

Desde el punto de vista de la gestión de los servicios de salud, y de acuerdo con estos enunciados, vamos a analizar brevemente las diferentes herramientas y estrategias que nos proporcionan las TIC para alcanzar la excelencia en su misión y objetivos estratégicos.

La misión de cualquier hospital (y, en general, de todo servicio y/o centro de salud) debiera ser proporcionar a las personas de su comunidad la mejor atención posible; ello implica que el paciente sea el centro del proceso y que se debe potenciar las capacidades de su personal a través de una adecuada gestión del conocimiento. Se trata de un proceso global de transformación que también debe ser gestionado (gestión del cambio).

OBJETIVOS ESTRATÉGICOS DEL SISTEMA DE INFORMACIÓN

Tomando como base el documento elaborado por el NHS[9], las estrategias en la gestión de la información debieran responder fundamentalmente a:

–Garantizar el acceso de los profesionales a los datos clínicos relevantes de sus pacientes con el fin de facilitar su atención.

–Garantizar el acceso de los profesionales a aquellas fuentes que les permitan disponer de las mejores evidencias, así como evaluar la efectividad (cuanti y cualitativamente) y eficiencia de su trabajo mediante la comparación con los mejores.

–Garantizar la adopción de guías y estándares basados en la evidencia científica que disminuyan la variabilidad de la práctica clínica.

–Facilitar a los pacientes la realización on-line de las gestiones relacionadas con su servicio de salud.

–Facilitar a los pacientes el acceso, comprobación y validación de sus datos clínicos, así –como en su caso– de los datos correspondientes a sus valores relevantes (preferencias) que tengan repercusión en la prestación de cuidados.

–Posibilitar a los pacientes el acceso a fuentes de información que les faciliten el implicarse en el cuidado de su salud.

–Garantizar la calidad de los datos introducidos en el sistema.

–Disponer de cuadros de mando integrados que permitan conocer el cumplimiento de objetivos (coste-efectivos).

–Evaluar si las prácticas del centro responden a los criterios de la evidencia científica disponible.

–Garantizar que existe información disponible para la planificación de nuevos servicios y actividades.

–Garantizar el intercambio de información relevante entre niveles.

–Posibilitar el seguimiento telemático de determinados procesos.

–Posibilitar la hospitalización virtual en determinadas circunstancias.

–Comercio electrónico (E-comercio).

Para que las TIC se constituyan en elemento estratégico debieran estar fundamentadas en las siguientes premisas:

–Centradas en el paciente (la información asistencial es la base de la gestión del centro).

–Gestión del conocimiento.

–Accesibles para planificadores, gestores, profesionales, pacientes y ciudadanos.

–Respondan a criterios de seguridad, privacidad y confidencialidad.

–Permitan la obtención de sistemas integrados de gestión (cuadros de mando).

–Disponibles en el conjunto del hospital (o del área de salud…) en dependencia del acceso individual (privilegio) otorgado.

Entre las principales herramientas tecnológicas cabe citar:

–Historia clínica informatizada.

–Tarjeta individual sanitaria.

–Otros registros de actividad clínica (radiología: RIS, PACS[10], análisis clínicos, anatomía patológica… etc.)

–Otros subsistemas integrados de gestión (económico-financiero, personal…).

–Intranet (arquitectura de servicios de información que aplica tecnología Internet en un entorno corporativo).

–Internet.

Antes de comentar las oportunidades y problemas relacionados con alguna de las utilidades citadas, conviene revisar dos cuestiones clave en el proceso de gestión de los servicios de salud: El paciente como centro del proceso y la gestión del conocimiento.

El paciente como centro del proceso

Los datos provenientes de la actividad asistencial deben constituir la base de la gestión clínica y de la planificación del hospital (de manera similar a lo que preconiza la estrategia del NHS[11]). Los datos provenientes de los pacientes se integran con los de otros subsistemas (personal, económico-financiero... etc.), permitiendo disponer de información válida y segura en tiempo real, “cuadro de mando”, para la toma de decisiones, ya sean operativas, tácticas o estratégicas. La información está disponible para el conjunto del hospital (o del área, o del servicio autonómico de salud... etc.) con los problemas de seguridad, privacidad y confidencialidad que posteriormente se mencionarán en el apartado de ética. Por otra parte la movilidad de las personas cada vez es mayor, y un paciente –a lo largo de su vida– puede ser visto por diferentes profesionales. Tanto clínicos como pacientes reconocen la importancia de que la información clínica pueda estar disponible para así garantizar una mayor efectividad de los cuidados[12].

Gestión del conocimiento

El acceso a la información no puede ser un objetivo en sí mismo y no debe convertirse en un nuevo juguete al que sólo algunos privilegiados tienen acceso. La información tiene un objetivo prioritario y es ayudar a la toma de decisiones en un contexto de incertidumbre.

Como el hospital está obligado a prestar una asistencia de acuerdo con la mejor evidencia disponible, deberá facilitar a sus profesionales el acceso a las lecciones aprendidas por el centro (quién sabe qué y dónde se encuentra recogida dicha información) y a una actualización permanente de la mejor evidencia existente. Asimismo debiera facilitar a sus potenciales usuarios el acceso a fuentes de información cualificadas, ya sean propias del centro, del servicio de salud, de grupos de autoayuda, tanto específicas (para determinados procesos, conductas de riesgo... etc.) como generales, con el objetivo de promover el autocuidado y la responsabilización del individuo sobre su estado de salud.

Esta es una de las cuestiones clave a las que van a enfrentarse, quiéranlo o no, los gestores y los profesionales sanitarios. No cabe duda de que se está produciendo un cambio, cada vez más acelerado, en la relación hasta ahora existente, entre planificadores, gestores, médicos, pacientes y ciudadanos.

Queda aun por ver en qué grado esta mayor accesibilidad a la información va a modificar la demanda de servicios (el NHS podría colapsarse incluso si sólo un 1% de las personas que consultan Internet solicitaran ser visitadas por su médico para un problema que no precisa[10]). Asimismo puede incrementar las desigualdades existentes no sólo entre determinados colectivos sino también entre países desarrollados y en vías de desarrollo[13].

Pero no sólo el gestor de los servicios de salud está interesado en conocer qué procedimientos son efectivos, cuánto cuestan y cuáles son sus resultados. Los ciudadanos, con independencia de la existencia o no de un mercado sanitario (aunque mucho más evidente en éste último caso), cada vez están más interesados en conocer los resultados de los servicios (autonomía, sobre la base de una adecuada información, para decidir ir a un hospital o a otro) y su coste (bien directo, mediante aseguramiento o vía impuestos) por lo que parece imparable la tendencia a hacer accesible al público dichos resultados y establecer –pese a todos sus condicionantes– benchmarking entre servicios semejantes[14]. En Internet se encuentra ya accesible importante información al respecto.

En cualquier caso, es un hecho que los sistemas y tecnologías de la información han ampliado su campo de acción y ofrecen sus servicios a todos los ciuda-

danos. Entre los factores facilitadores de este cambio pueden citarse el deseo por parte de muchos ciudadanos de reducir el desequilibrio informativo existente con los médicos y el de asumir mayores responsabilidades en el cuidado de su salud[15].

PRINCIPALES HERRAMIENTAS

Historia clínica informatizada

La experiencia nos indica que los datos recogidos en soporte papel plantean graves dificultades para ser convertidos en información. En la década de los setenta comenzaron a desarrollarse en nuestro país las primeras aplicaciones informáticas en los establecimientos sanitarios con el objetivo de facilitar su administración (el Hospital de Navarra fue uno de los hospitales pioneros en España), aun cuando funcionaban en entornos muy poco "amigables" para los usuarios (HOST). Los diversos subsistemas (económico-financiero, personal, administración-gestión y clínico) se han desarrollado conforme a la evolución tecnológica, pero la implantación de la historia clínica informatizada (HCI) ha sido mucho más lenta de lo esperado y en una primera etapa se ha limitado a ser una reproducción de la historia tradicional en papel. Esta lenta implantación ha sido debida, entre otras circunstancias, a una falta de aceptación de la herramienta informática por parte de los médicos[16]. No se debe minusvalorar el hecho de que se precisa una preparación y entrenamiento para gestionar adecuadamente este cambio cultural[17], ya que va a requerir una nueva forma de gestionar sus procesos y ello –al menos en una primera fase– requiere esfuerzo y tiempo (en un reciente ensayo clínico aleatorizado se evidenció que el médico emplea 6 minutos más por paciente y día si prescribe los análisis y pruebas por ordenador[18]).

Entre las ventajas de la HCI cabe mencionar las siguientes:[19]

–Acceso remoto, en tiempo real (conectividad).

–Legibilidad.

–Incorporación e integración con otras fuentes de datos, tanto clínicas como de otro tipo.

–Facilidad de búsqueda.

–Actualización permanente.

–Facilidad de explotación para investigación clínica, epidemiológica o sobre servicios de salud.

–Facilidad para evaluar la calidad de los datos.

–Seguridad en el almacenamiento de datos (datawarehouse).

–Enlaces a los valores relevantes del sujeto.

–Enlaces automáticos a lecciones aprendidas en el centro (protocolos, vías clínicas… etc.)

–Enlaces automáticos a búsqueda de la evidencia para problemas específicos.

–Enlaces para facilitar información complementaria al paciente sobre sus cuidados de salud específicos.

Todo ello supone un profundo cambio cultural en la organización y, por consiguiente, la puesta en marcha de la HCI debe realizarse evaluando cuidadosamente sus estrategias de implantación. Aun cuando en una primera fase puedan coexistir tanto la historia en papel como en la HCI, no debe perderse de vista la necesidad de implementar la operatividad de la herramienta HIC, aprovechando todas las posibilidades que brindan las TIC, para convertirla en un instrumento de gestión del conocimiento, tanto para gestores, profesionales como pacientes.

No obstante, existen problemas importantes en su desarrollo, especialmente cuando se diseñan estrategias corporativas o supracorporativas. Tales problemas están en relación con la necesidad de un vocabulario clínico homogéneo (SNOMED en el contexto del NHS, UMLS coordinado por la National Library of Medicine) y una definición estandarizada de los datos recogidos, con el fin de que pueda realizarse su agrupación y explotación[20]. Si no se resuelve de manera adecuada como codificar datos complejos de tal manera que puedan ser interpretados por el ordenador, si no se posibilita como compartir información entre diferentes instituciones garantizando simultáneamente la confidencialidad de los datos y la participación activa de los pacientes, la potencialidad de la HCI quedará seriamente mermada[21].

Tarjeta de identificación sanitaria

Otra importante herramienta es la denominada tarjeta de identificación sanitaria, TIS, pero dotada con una funcionalidad muy diferente de la actual. A este respecto cabe señalar que la directiva de la Unión Europea sobre protección de datos (vigente desde 1998) requiere a todos los estados miembros para que establezcan las medidas legislativas necesarias que garanticen el acceso a los pacientes a sus historiales médicos. En una iniciativa más reciente, se determina que "para el 2003 todo ciudadano europeo deberá tener la posibilidad de acceder segura y confidencialmente mediante su tarjeta de salud –EUROCARD– a la red donde se encuentre su historial médico[22]". En línea con esta iniciativa, la tarjeta sanitaria, junto con los datos administrativos y demográficos (entre los que se encuentra el número de identificación) debiera incluir asimismo datos sobre sus antecedentes para facilitar

la atención en caso de urgencia, acceso para realizar gestiones en su servicio de salud, acceso a su historial clínico… etc. En definitiva, dotar a la tarjeta sanitaria con potencialidades similares a las que presentan otras tarjetas de empresas de servicios actualmente en uso[23].

Un aspecto importante, a juicio del que suscribe, es que se hace ineludible la existencia de un número de identificación personal único para el conjunto del Sistema Nacional de Salud (tal y como se viene utilizando en el Servicio Navarro de Salud-Osasunbidea[24, 25]), siendo –cuando menos– muy preocupante que hasta la fecha no se haya avanzado significativamente en su puesta en práctica. De dicho número debieran colgar, a la manera de un perchero, los eventuales registros electrónicos de sus procesos de enfermedad que este paciente haya tenido a lo largo de su vida, tanto en atención especializada como en primaria. La tarjeta de identificación sanitaria debiera facilitarse, con carácter sistemático y mediante la logística adecuada, lo más precozmente posible a todos los recién nacidos con el fin de que fueran generando su historial de salud bajo un identificador unívoco.

Internet

Internet se está convirtiendo en una herramienta decisiva ya que está posibilitando el acceso a fuentes de información sanitaria en un volumen y con una accesibilidad desconocidas hasta la fecha. Internet puede, de esta manera, beneficiar la toma de decisiones basadas en la evidencia, proveyendo un acceso más barato, rápido y eficiente a las últimas actualizaciones, proporcionando un conocimiento válido y relevante en el momento justo, en el lugar adecuado y en el formato y cantidad precisas. Asimismo, puede facilitar y potenciar la comunicación entre el profesional sanitario y el paciente[26, 27], facilitando la integración de las preferencias y valores de los pacientes con la evidencia científica, en el marco de la propia historia del paciente y de su entorno social.

Sin embargo, también ha motivado la aparición de nuevos problemas, especialmente los ligados a la privacidad y confidencialidad de los datos, a la cantidad de información disponible y a la evaluación de su calidad[28-30].

Si bien determinados aspectos (v.g. privacidad, adquisición de bienes y/o servicios, etc.) han podido ser objeto de legislación específica, en lo que hace referencia a la calidad de la información disponible en las webs de E-salud, la tendencia adoptada ha sido potenciar el establecimiento voluntario de códigos de conducta.

Cualquier usuario puede, teóricamente, acceder a la mejor evidencia disponible, la multiplicidad de fuentes de información unida a la variabilidad de las mismas hace pensar en la necesidad de adoptar diferentes estrategias para garantizar la pertinencia y eficiencia de la búsqueda realizada. Sin embargo, todavía ningún estudio ha mostrado que la calidad de Internet sea diferente de la de otros lugares o que ello implique la adopción de decisiones diferentes por parte del público[31]; así en tanto algunos abogan por un "principio de precaución" otros entienden que este tipo de medidas choca con el espíritu de libertad que impregna la red[32].

Mayoritariamente existe un consenso para exigir que las diferentes webs sanitarias adopten unos criterios éticos mínimos, cuando menos en relación a tres aspectos (información acerca de sus realizadores y patrocinadores, contenido y confidencialidad, así como sobre sus actividades comerciales en el caso de que las realicen). Por otra, los usuarios deben seleccionar aquellas fuentes que o bien se nutran de referencias que sistemáticamente son sometidas a un proceso de *peer-review* o dispongan de una certificación o acreditación por parte de organismos competentes.

Estos códigos no sólo hacen referencia a la calidad intrínseca de la información facilitada, sino que abordan otros aspectos igualmente importantes: su finalidad y objetivos explícitos, quién ha desarrollado la web, quién la patrocina, si existen conflictos de intereses (v.g. comerciales), cómo se garantiza la privacidad y confidencialidad, de dónde provienen sus contenidos, y como se evalúa y actualiza[33].

En los últimos 4 años diversos grupos o instituciones han desarrollado sus códigos de conducta en la Web.

El primer código "The Health on the Net (HON) apareció en Julio de 1996 (www.hon.ch/HONcode/Conduct.html) y es el más utilizado (lo emplean miles de webs, entre ellas algunas españolas).

En la Unión Europea y bajo sus auspicios, está en marcha un "Plan de Acción para una utilización más segura de Internet", que en el ámbito de salud tiene como objetivo ayudar a los profesionales y usuarios a identificar la información de alta calidad disponible en Internet. La estrategia de dicho programa, MedCERTAIN, se basa en determinar un núcleo de central de metadatos, denominado medPICS, que permita tanto una evaluación descriptiva como evaluativa. Propugnan la puesta en marcha de un proceso colaborativo para la evaluación de la información para la salud, la Colaboración Heidelberg, que desempeñaría un papel similar al que desarrolla la colaboración Cochrane en la evaluación de la evidencia científica[34].

En España existe, asimismo, la experiencia del Colegio Oficial de Médicos de Barcelona con 76 webs acreditadas a la fecha de la publicación de la referencia[35].

Los últimos códigos son muy recientes, ya que aparecen en el año 2000; la Guía de la Asociación Médica Americana (AMA)[36] en el mes de Marzo (www.ama-assn.org/Principles/index.asp); el Código Etico en E-salud, de la eHealth Ethics Iniciative (www.ihealthcoalition.org) y los Principios Eticos para ofrecer servicios de salud por Internet a los consumidores elaborado por la Health Internet Ethics (Hi-Ethics) (www.hiethics.org/Principles/index.asp) en Mayo de este año.

Sin entrar a reseñar las diferentes características y peculiaridades de cada código, la existencia de tantas iniciativas refleja por una parte la importancia del problema, y por otra la ausencia de un *gold* estándar (aun cuando todos ellos tienen muchos elementos en común), en parte debidos a los propios intereses de los promotores y al distinto contexto social en el que han sido desarrollados.

ASPECTOS ÉTICO - LEGALES DEL SISTEMA DE INFORMACIÓN SANITARIA

La proliferación de diferentes bases de datos que contienen datos personales (administrativos) y sobre la salud de los pacientes, aun cuando permiten mejorar la calidad en la atención prestada y facilitan la investigación sanitaria, presentan también efectos negativos en tres áreas muy relacionadas: la privacidad de los datos, su fiabilidad y la responsabilidad en su utilización.

Se trata de un tema complejo, dónde confluyen diferentes intereses (el ámbito normativo sanitario y el de protección de datos pueden no ser coincidentes) en un entorno que cambia rápidamente, dado que los avances tecnológicos son imparables. Ello conlleva que determinadas regulaciones legales puedan quedar obsoletas en breve tiempo, si no están sometidas a un proceso continuo de revisión (hecho infrecuente, máxime si la norma es de un rango elevado).

Aun cuando el tema legal es propio de un asesor jurídico experto en la materia y existen interesantes aportaciones al respecto[37-39], se exponen a continuación y como temas de debate, aquellos aspectos fundamentales en relación con la privacidad y confidencialidad de los datos y su repercusión en la utilización de la historia clínica y las TIC.

En España la legislación básica de aplicación es la prevenida en:

–La Ley 14/1986, de 23 de Abril, General de Sanidad, en sus artículos 10.11 y 61.

–La Ley Orgánica 5/1992, de 29 de Octubre, reguladora del tratamiento automatizado de los datos de carácter personal.

–Real Decreto 63/1995, de 20 de Enero, regulador de las prestaciones sanitarias del Sistema Nacional de Salud. Anexo I, apartado 5.

–La Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal (amplía el ámbito de actuación, ya que se refiere a cualquier soporte de datos y no sólo al tratamiento automatizado).

–Real Decreto Ley 14/1999, de 17 de Septiembre, que regula la firma electrónica.

Cuestiones clave:

–Informatización de la Historia Clínica: La Ley General de Sanidad en su artículo 10.11 dice expresamente "constancia por escrito"; ¿Puede sustituir la HCI a la HC en soporte papel. Si bien es cierto que la norma puede ser anacrónica, en cualquier caso no ha sido modificada hasta la fecha.

–Validez jurídica de los archivos electrónicos: ¿Qué ocurre con aquellos registros que no reúnan los requisitos establecidos en el Real Decreto Ley? ¿Tienen valor de prueba?

–Tratamiento de los datos: ¿El deber de guardar secreto se extiende sólo a profesionales sanitarios o también a otros colectivos?

–Consentimiento del paciente: ¿Es preceptivo su consentimiento para recoger datos en la HC? ¿Debe ser informado de la existencia de un fichero, de su tratamiento y del responsable del mismo? ¿En qué situaciones requiere la solicitud expresa de consentimiento para la utilización de dichos datos?

–Modificación y/o cancelación de datos: ¿El paciente puede exigir este derecho o la HC se considera exceptuada? ¿El paciente tiene derecho a hacer desaparecer datos clínicos?

–Confidencialidad y Seguridad: por su importancia se trata en un apartado diferenciado, aun cuando están muy ligadas a:

- Accesibilidad: ¿Cómo se conjuga el criterio de restricción al acceso con la HCI disponible en un puesto de trabajo multidisciplinario? ¿El establecimiento de diferentes niveles de acceso es garantía suficiente? ¿Es realista una solución que sólo permita el acceso a las historias activas? ¿Es factible restringir el acceso a información calificada cómo sensible? ¿Quién otorga dicha calificación?

- Migración de datos para constituir bases de datos con fines planificación, administración-gestión, epidemiología, investigación… etc. ¿Existe seguri-

dad de que se importan solamente aquellos datos que no permiten la identificación de pacientes? ¿Se rompen los enlaces que permiten la identificación individual? ¿Se importan los mínimos datos necesarios?

–Repercusiones civiles y penales.

Confidencialidad de la HCI

Es, junto con la seguridad, la cuestión más conflictiva. Son numerosas las referencias bibliográficas que, a título individual o institucional, han abordado el tema[40 - 48]. Sin que nadie ponga en duda el derecho de todo ciudadano a exigir la adecuada custodia y confidencialidad de sus datos personales que libremente ha facilitado, no cabe duda que el contexto social español es muy diferente del anglosajón y ello es evidente ya desde el propio proceso de información que se genera en la relación médico (profesional sanitario) y paciente. El principio de autonomía del paciente no está tan arraigado o se ve matizado por el entorno familiar que tiende a protegerlo de las malas noticias. Son suficientemente conocidas las dificultades que se presentan en la práctica clínica cuando un profesional debe informar sobre un importante problema de salud en un contexto socio-familiar determinado y, en ocasiones, de difícil valoración.

Este diferente contexto social y cultural puede generar serios problemas si simplemente nos dedicamos a copiar o a aplicar, con carácter mimético, regulaciones o normativas que han tenido su origen en otros ámbitos. A modo de ejemplo la Ley General de Sanidad, que ya en 1986 preveía que había que facilitar “información completa y por escrito”, produjo el efecto perverso de que, además de dilatarse en el tiempo la aplicabilidad de este precepto, el proceso de comunicación médico-paciente tuvo el serio riesgo de convertirse en un trámite administrativo más (la firma de un impreso, ininteligible por la profusión de terminología médica).

Otro ejemplo bien conocido es el cambio legislativo introducido en el estado de Minnesota que no permite, a partir del 1 de Enero de 1997, la utilización de los registros clínicos con fines investigadores salvo que se cuente con un consentimiento expreso del paciente. El legislador, aun en ausencia de una norma o recomendación estatal consensuada, primó el principio de autonomía del paciente sobre su historial clínico, a la vez que pretendía evitar la eventual mala utilización que pudieran realizar los centros (y aseguradoras) y los profesionales sanitarios. Ello supuso importantes problemas para instituciones tan prestigiosas como la Clínica Mayo con una dilatada experiencia en la investigación aplicada[49]. En este mismo sentido, cabe citar la problemática generada en el Reino Unido con la Ley de Protección de Datos que ha entrado en vigor en Marzo del presente año[48].

Como ya se ha mencionado la generación de bases de datos a partir de los registros clínicos de los pacientes trae como consecuencia una colisión entre dos principios: el derecho de cada ciudadano a que sus datos sean secretos frente al beneficio potencial que para la sociedad tiene el análisis de datos agregados[42, 48, 50, 51]. Con el fin de garantizar que aquella información que permita identificar al paciente sólo se transferirá cuando sea imprescindible y únicamente el mínimo de información necesaria, el Caldicoot Committee ha elaborado unas conclusiones y recomendaciones dignas de estudio[52].

Aun cuando la defensa del derecho a la privacidad tiene un indudable atractivo para los políticos, coincidimos con la opinión de Donna Shalala cuando dice "Recomendamos que el hospital utilice la información contenida en la historia clínica de sus pacientes para enseñar, aprender, investigar, prestar asistencia y garantizar la calidad. Pero, por otra parte, aquellos empleados que utilicen la información sanitaria, no pueden utilizarla para ningún otro propósito que no esté relacionada con la salud"[53]. De otro modo, las lecciones aprendidas por el hospital, la gestión del conocimiento, no podrá ser llevada a cabo y la excelencia del centro (proveer de los mejores cuidados a sus pacientes con una eficiente utilización de sus recursos) será, simplemente, una mera declaración de intenciones.

Seguridad de la HCI

El acceso a los registros informáticos puede ser vulnerado tanto por usuarios que carecen de la necesaria autorización (hacking) como por usuarios autorizados que hacen una utilización inapropiada de su privilegio. Las razones pueden ser muy variadas, y entre ellas no cabe duda que puede haber importantes razones económicas. El hecho de que los registros clínicos del paciente se encuentren disponibles en una red corporativa (Intranet) o en Internet genera problemas adicionales de seguridad en la custodia de la historia clínica, ya que los datos son muy fáciles de inspeccionar, copiar y transmitir, a pesar de los trazadores que puedan introducirse[42] . Si el profesional sanitario no tiene confianza en que los datos que introduce sobre su paciente no vayan a ser manipulados, o simplemente revisados, por personas ajenas, sus reticencias para el uso de la HCI se verán incrementadas. Por ello es preciso que el diseño del sistema informático responda desde el comienzo a esta problemática.

Independientemente del sistema de actualización, copia y almacenaje de datos que garanticen la integridad de los mismos, frente a determinadas incidencias (accidentales o voluntarias), las medidas que podrían adoptarse para hacer frente a

los problemas de seguridad y confidencialidad, sobre la base de las citadas en estudios recientes[54-56], podrían resumirse en:

Problema	Descripción	Solución
Identificar al usuario (autentificación)	¿Cómo conoce el sistema que el usuario puede acceder?	La clave y password (de ordenador y de programa) pueden no ser suficientes. Si el acceso al programa se realiza mediante tarjeta se introduce una nueva dificultad adicional. Se sugiere certificación y firma digital.
Nivel de acceso	A que partes de la HCI tiene acceso	Establecer niveles de acceso (privilegios) tanto para lectura, introducción y/o explotación de datos.
Aseguramiento de la correcta utilización por parte del personal autorizado	¿Cómo minimizar el riesgo de una mala utilización?	Trazador de acceso y auditoría aleatoria o específica.
Aseguramiento de la fuente de datos	¿Cómo sabemos que hemos entrado al programa y que este no ha sido manipulado?	Autentificación de la fuente: feed-back sistema-usuario.
Proteger entrada Intranet	¿Cómo evitar a los *hacker*?	Instalación de *Firewall*

Sin perjuicio de las medidas anteriormente citadas, el componente más importante es el de la responsabilidad personal, ya que la implementación de medidas tecnológicas no evita su uso incorrecto o irresponsable. Así, si se quiebra la privacidad de las claves de acceso cualquier persona no autorizada podrá entrar en el programa haciéndose pasar por otra. De nuevo, un ejemplo de la diferente actitud que puede darse en la práctica diaria entre las precauciones individuales que se adoptan, por ejemplo, con las tarjetas bancarias versus otras claves de acceso como pueden ser las de HCI.

CONCLUSIÓN

Aun cuando las implicaciones de Internet sobre el estado de salud de los usuarios (comportamientos, resultados… etc.) están todavía en fase discusión[22], es evidente que las tecnologías de la información constituyen una estrategia fundamental para el desarrollo de las políticas de salud de los países desarrollados.

En este sentido, el Sistema Nacional de Salud y los actuales y futuros servicios de salud de las CCAA, se encuentran ante la obligación de dar una respuesta coordinada y satisfactoria al respecto.

La tercera gran revolución[57] de la humanidad está poniendo de manifiesto las contradicciones de muchos de nuestros valores. Como gestores debemos responder ante los pacientes del cumplimiento de sus cinco derechos fundamentales[58]: "a través de unos datos clínicos correctos, disponibles en tiempo y forma, adoptaremos –conjuntamente con el paciente[59]– las decisiones pertinentes que, mediante un proceso adecuadamente desarrollado, posibilitarán la obtención de los mejores resultados". En esta responsabilidad, las tecnologías de la información y comunicación se han convertido en una parte muy importante de nuestra estrategia pero plantean también repercusiones importantes para los pacientes. Podrán perdonársenos muchos errores pero nunca que vivamos de espaldas a un futuro que ya es presente.

BIBLIOGRAFÍA

1. Eysenbach G, Sa ER, Diepgen TL. Shopping around the Internet today and tomorrow: towards the millenium of cybermedicine. BMJ 1999; 319: 1294.
2. Carpentier M. The use of telematics for healthcare european Union actions. http://www.hon.ch/Library/papers/carpentier.html (revisado 05/10/2000).
3. 5th Framework Programme (1998-2002). http://www.ehto.org/ht_projects/infosoc.html (revisado 05/10/2000).
4. Programa PISTA. http://www.labein.es/pista/pistasan/general/generfr.htm (revisado 02/11/2000).
5. The new NHS: Modern/Dependable. Cm 3807, December 1997.
6. Information for Health. http://www.nhsia.nhs.uk (revisado 05/10/2000).
7. De Moor GJE. The role of CENT/TC251 and its international relationships. http://www.hon.ch/Library/papers/demoor.html (revisado 05/10/2000).
8. Acuerdos del Consejo Interterritorial de Salud (1987-1998). http://www.msc.es/consejo/acuerdos/home.htm (revisado 30/10/2000).
9. Information for health. 1. An information strategy for the modern NHS. http://www.nhsia.nhs.uk/ strategy/full/1.htm (revisado 09/10/2000).
10. Ratib O. From PACS to the world wide web. http://www.hon.ch/Library/papers/ratib.html (revisado 05/10/2000).
11. Wyatt J, Keen J. The NHS's new information strategy. BMJ Oct 1998; 317: 900.

12. Neame R. Creating an infraestructure for the productive sharing of clinical information. Top Health Inf Manage 2000; 20(3): 85-91.

13. Godlee F, Horton R, Smith R. Global information flow: Publishers should provide information free to resource poor countries. BMJ Sept 2000; 321: 776-7.

14. US health research and policy developments. http://www.ehto/journal/issue3/us.html (revisado 05/10/2000).

15. Eysenbach G. Consumers health informatics. BMJ June 2000; 320: 1713-6.

16. Dansky KH, Gamm LD, Vasey JJ, Barsukiewicz CK. Electronic medical records: are physicians ready? J Healthc Manag Nov-Dec 1999; 44(6): 440-54.

17. Kelly G. Electronics, clinicians and the NHS. BMJ Oct 2000; 321: 875-6.

18. Tierney WM, Miller MF, Overhage JM, McDonald CJ. Physicians under writing on microcomputer workstation. JAMA 1999; 269: 579-88.

19. Powsner SM, Wyatt JC, Wright P, Opportunities for and challenge of computerization. The Lancet 1998; 352: 1617-22.

20. NHS Information Authority. Annual Report 1999-2000. Part Four. Information for personal health. Snomed Clinical Terms. Data Standars. http://www.nhsia.nhs.uk/annual_rep/part4.htm (revisado 06/10/2000).

21. Szolovits P. A revolution in electronic medicalrecords systems via the world wide web. http://www.hon.ch/Library/papers/psz.html (revisado 05/10/2000).

22. *e*Europe: an information society for all. Comunication on a commission iniciative for the special Council of Lisbon, 20-21 March 2000. http://www.europe.eu.int/comm/information-society/eeurope/pdf/com081299-en.pdf.

23. Neame R. Smart cards: the key to trustworthy health information systems. BMJ 1997; 314: 573-7.

24. Carnicero J, Lezaun MJ, Corella JM, Maiza C. Respuestas de la población al envío masivo de tarjetas sanitarias en la Comunidad Foral de Navarra. Todo Hospital 1993; 95: 55-9.

25. Carnicero J, Lezaun MJ, Vázquez JM. La base de datos de la tarjeta sanitaria de Navarra. Informática y salud 2000; n.º 25: 1254-60.

26. Jadad AR, Haynes RB, Hunt D, Browman GP. The internet and evidence-based decision-making: a needed synergy for efficient knowledge management in health care. CMAJ 2000; 162(3): 362-5.

27. Jadad AR. The internet and evidence-based healthcare. He@lth Information on the Internet. June 1998; 6-8.

28. Eysenbach G, Diepgen TL. Towards quality management of medical information on the internet: evaluation, labelling and filtering of information. BMJ Nov 1998; 317: 496-502.

29. Jadad AR, Gagliardi A, Rating health information on the Internet: navigating to knowledge or to Babel. JAMA 1998; 279: 611-4.

30. Gottlieb S. Health information on internet is often unreliable. BMJ July 2000; 321: 136.

31. Eysenbach G. A framework for evaluating e-health: Systematic review os studies assessing the quality of health information and services for patients on the internet. J Med Internet Res 2000; 2 (Iss1 Suppl 2). Proceedings of MedCERTAIN Workshop.

32. Coiera E. Information epidemics, economics, and inmunity on the internet: We still know so little about the effect of information on public healt. BMJ, Nov 1998; 317: 1469-70.

33. Baur C, Deering MJ. Proposed Frameworks to improve the quality of healtl web sites: Review. http://www.medscape.com/Medscape/GeneralMedicine/journal/2000/v02.n05/pnt-mgm0926.baur.htm (Revisado 03/10/2000).

34. Eysenbach G, Yihune G, Lampe K, Cross P, Brickley D. Quality mangement, certification and rating of heath information on the Net with MedCERTAIN: Using a medPICS/RDF/XML metadata structure for implementing eHealth ethics and creating trust globally. J Med Internet Res 2000; Vol 1 (Iss1); Suppl 2. Proceedings of Med CERTAIN workshop.

35. Sarrias R, Mayer MA, Latorre M. Acredited Medical Web: an experience in Spain. J Med Internet Res 2000; Vol 2 (iss1); Suppl 2.

36. Winker MA, Flanagin A, Chi-Lum B, White J, Andrews K, Kennet RL, DeAngelis CD, Musacchio RA. Guidelines for medical and health information sites on the Internet: principles governing AMA web sites. JAMA, Mar 2000; 283(12): 1600-6.

37. Andérez A. Historia clínica e informática: aspectos legales (I). Informática y salud 1998; n.º 18: 896-9.

38. Andérez A. Historia clínica e informática: aspectos legales (II). Informática y salud 1999; n.º 19: 968-9.

39. Andérez A. Historia clínica e informática: aspectos legales (III). Informática y salud 1999; n.º 20: 1022-26.

40. Electronics Health Records options: a discussion paper. http://www.doh.gov.uk/nhsexipu/whatnew/ehrdis.htm (revisado 06/10/2000).

41. Neame R, Kluge EH. Computerisation and health care: some worrries behind the promises. BMJ nov 1999; 319: 1295.

42. Kelly G. Patient data, confidenciality, and electronics. BMJ March 1998; 316: 718-9.

43. Gostin L. Health care information and the protection of personal privacy: ethical and legal considerations. Annals of Internal Medicine Oct 1997; 127: 683-90.

44. The EU data protection directive. http://www.ehto.org/ehto/journal/issue4/eu_dataprotection.html (revisado 05/10/2000).

45. Vanderbroucke JP. Maintaining privacy and the health of the public. BMJ, May 1998; 316: 1331-2.

46. Gostin LO, Lazzarini Z, Neslund VS, Osterholm MT. The public health information infraestructure. A national review of the law on health information privacy. Jama Jun 1996; 275(24): 1921-7.

47. Hodge JG Jr, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. JAMA, Oct 1999; 282(15): 1466-71.

48 Al-Shahi R, Warlow Ch. Using patient-identifiable data for observational research and audit. BMJ Oct 2000; 321: 1031-2.

49. Melton LJ 3rd. The threat to medical records research. N Engl J Med 1997; 337: 1466-70.

50. Davidoff F. Databases in the next millenium. Annals of Internal Medicine Oct 1997; 127: 770-4.

51. Strobl J, Cave E, Walley T. Data protection legislation: interpretation and barriers to research. BMJ Oct 2000; 321: 890-2.

52. The Caldicott Committe: report on the review of patient-identifiable information. December 1997. http://www.doh.gov.uk/confiden/app12.htm; http://www.doh.gov.uk/confiden/recs.htm (revisados 24/10/2000).

53. HHS Secretary outlines principles that will guide department's recomendations to Congress on privacy of medical records. Epidemiology Monitor 1997; 18(8): 6-7.

54. Anderson JC. Security in clinical information systems. London BMA 1996.

55. Denley I, Weston Smith S. Privacy in clinical information systems in secondary care. BMJ May 1999; 318: 1328-31.

56. Chadwick DW, Crook PJ, Young AJ, McDowell DM, Dornan TL, New JP. Using the internet access confidential pacient records: a case study. BMJ Sept 2000; 321: 612-5.

57. Fuller S. To "E" or not to "E": HIM and the dawn of E-Health. Journal of AHIMA. April 2000.

58. Kremsdorf R The five rigths of effective patient care http://www.informatics-review.com/thoughts/5rights.html (revisado 31/10/2000).

59. Eysenbach G. Rating information on the internet can empower users to make informed decisions. BMJ 1999; 319: 385.

EL DERECHO A LA INTIMIDAD Y LAS NECESIDADES DE LA INVESTIGACIÓN Y LA EVALUACIÓN EN EL ÁMBITO SANITARIO

José Luis Conde Olasagasti

Agencia de Evaluación de Tecnologías.
Instituto de Salud Carlos III

INTRODUCCIÓN

El respeto a la vida privada y el derecho a que los elementos que la constituyen no sean objeto público de información general está reconocido en todas las Constituciones y marcos legales de los países avanzados y democráticos.

Simultáneamente al reconocimiento de ese derecho, se ha ido produciendo en esos mismos países una creciente necesidad y uso de datos personales por parte de las Administraciones y las organizaciones públicas o privadas prestadoras o vendedoras de bienes y servicios. Hoy día, son muy pocas las relaciones y transacciones entre individuos y organizaciones que permanecen en el anonimato. Si a ello se une la enorme capacidad de almacenamiento y recuperación de información que proporcionan las tecnologías informáticas, se comprenderá la preocupación existente por preservar la intimidad mediante normas y procedimientos que garanticen la protección de aquellos datos de carácter personal que en principio no deben ser usados para otros fines que aquellos para los que su titular o "propietario" los proporcionó. Tal preocupación ha motivado la promulgación de leyes que en el caso de España, tienen su máxima expresión en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LORPD) de 11 de Diciembre[1] y el Real Decreto 994/1999 de 11 de Junio[2] por el que se aprueba el Reglamento de medidas de seguridad de ficheros automatizados que contengan datos de carácter personal.

Un ámbito donde la protección de la intimidad tuvo siempre una especial relevancia es el que corresponde al ejercicio de la práctica médica y la relación medico-paciente. Recuérdese el principio del secreto profesional ya presente en el juramento hipocrático. Sin duda alguna, la gran cantidad de información que genera la práctica médica y su carácter sensible hace que ésta se constituya como un conjunto de archivos que debe ser particularmente protegido, ya que el uso de datos pertenecientes a áreas tan personales como las que afectan a la salud para fines distintos de aquellos para los que se suministraron es particularmente rechazable. Así lo reconoce la LORPD en su artículo 7[3].

Siendo cierto cuanto hasta ahora se ha dicho, no lo es menos que la propia naturaleza del ejercicio de los cuidados de salud en lo individual y en lo colectivo ha convertido esta proclamada inviolabilidad de la intimidad en una declaración de principios que muchas veces tiene escasa traducción práctica. La salud de las personas suele ser uno de los secretos peor guardados.

Son dos los niveles o campos en los que la inviolabilidad del dato clínico personal se vulnera sistemáticamente en orden a poder aplicarse a los cuidados de salud.

El primero de ellos es el que corresponde a la necesaria transmisión de datos entre profesionales e incluso entre centros sanitarios. El proceso asistencial actual complejo y multidisciplinar exige que la información obtenida por un médico y contenida en la historia clínica del paciente (o cualquier otro registro rutinario) sea transmitida y conocida por otros médicos o profesionales sanitarios. Esta transmisión no plantea en principio problemas de orden ético o legal por cuanto los datos se utilizan para el fin para el que fueron proporcionados. Sin embargo ello supone en la práctica, que cualquier profesional puede tener (y de hecho tiene) acceso libre a información relativa a pacientes sean estos suyos o no.

El segundo nivel es el que afecta al ámbito del interés público, o con mayor precisión al de la salud pública. El descubrimiento de un problema de salud individual que puede afectar a otros (enfermedades transmisibles, intoxicaciones) obliga a poner en conocimiento de los eventuales individuos en riesgo y de la autoridad sanitaria la existencia de ese problema. Tal ruptura del secreto profesional no solo está admitida sino que en muchos casos es además obligatoria. Ello no obstante no quiere decir que la intimidad personal no deba ser protegida hasta donde sea posible manteniendo la identidad de la persona tan oculta como lo permita la plena operatividad de las medidas de protección general.

Las dos excepciones a la regla general mencionadas están ampliamente reconocidas, aceptadas y contempladas en el marco legal español vigente[4] por cuanto en el primer caso la ruptura del secreto es coherente con el fin para el que el afectado proporcionó sus datos, y en el segundo el interés general prevalece sobre el derecho individual a la intimidad.

Queda un tercer nivel o ámbito, hasta ahora no mencionado, en el que el dato clínico individual tiene un enorme interés y su uso puede colisionar con el derecho a la intimidad; este no es otro que el área de la investigación y de la evaluación, a cuyo análisis se dedica cuanto sigue en este trabajo.

EL DATO CLÍNICO PERSONAL Y SU USO EN EVALUACIÓN E INVESTIGACIÓN

Cuando un paciente acude a un servicio de salud, sabe y admite tácitamente que los datos que proporciona o que de él se obtienen, van a ser utilizados en el proceso asistencial que se le aplicará. No es tan claro que sepa o admita que esa misma información pueda ser utilizada con fines investigadores o evaluadores por perso-

nas muchas veces ajenas a su proceso asistencial individual (no nos referimos aquí a eventuales experimentos o ensayos específicos en los que está participando de manera voluntaria). Sin embargo, y pese al relativo desconocimiento que el paciente pueda tener acerca de este tipo de usos, éstos son prácticas consagradas por la costumbre y en alguna medida reconocidos por la ley[5].

Pese a todo lo hasta ahora expuesto acerca del reconocimiento social y legal del uso de datos personales con finalidad investigadora o evaluadora, existe una notable confusión respecto del alcance de la normativa legal vigente en las materias citadas.

Con el fin de contribuir a aclarar en alguna medida el panorama existente, se exponen a continuación algunas propuestas de definición y sus relaciones con los textos legales.

Entenderemos por investigación relacionada con el uso de datos de carácter personal, cualquier actividad que persiga aumentar o mejorar el conocimiento existente a partir del análisis de datos clínicos o biológicos contenidos en registros de información habituales (historias clínicas, registros clínico-administrativos rutinarios) o realizados esporádicamente con alguna finalidad determinada. A estos efectos podrá entenderse que el fin investigador está contemplado en la LORPD que en su texto aparecen términos tales como “fines científicos” o “estadísticos”[6], o realización de “estudios epidemiológicos”[7].

Por lo que se refiere al concepto evaluación, éste implica una dimensión de medida, estimación, o valoración de funcionamiento y resultado orientada en algún sentido predefinido como pueda ser la auditoría de calidad o la mera inspección sanitaria o de servicios. En sí misma comporta un cierto nivel de investigación al que se añade un componente de análisis. El fin evaluador estará contemplado en la ley no solo cuando se utilizan los términos a los que más arriba se ha aludido, sino también cuando se menciona “gestión de servicios sanitarios”[8].

ADECUACIÓN DE LA LEY A LAS NECESIDADES DE INVESTIGACIÓN Y EVALUACIÓN

Existe una considerable inquietud entre la comunidad investigadora y evaluadora respecto de las restricciones que la legislación protectora del derecho a la intimidad pueda imponer a la realización de su tarea.

Hay que decir sin embargo que una lectura detenida de la ley junto a una interpretación amplia de su espíritu, conduce a pensar que tal inquietud no está justificada.

Aunque son muchos los aspectos que pudieran ser considerados, centraremos el análisis en cuatro de particular relevancia.

Uso de datos con finalidad distinta a aquella para lo que fueron recabados

Con arreglo a lo expuesto en el articulo 7, apartado 2, la LORPD admite que el uso científico o estadístico de datos se constituye en excepción al principio general de prohibición de uso de datos con finalidad distinta a aquella para lo que fueron recabados. Datos clínicos recogidos con fines asistenciales, son por tanto utilizables con fin investigador o estadístico.

Obligatoriedad de información a los interesados

El artículo 5 de la LORDP establece con carácter general que los interesados a los que se soliciten datos habrán de ser informados de varios aspectos relacionados con el registro de datos incluyendo ciertas reservas respecto de datos no recabados directamente del interesado.

Quedan excluidos de estas limitaciones y reservas, de nuevo el fin científico o estadístico[9].

Consentimiento del afectado

En el mismo sentido los artículos 6 y 7 de la LORDP, eximen de la obligatoriedad de requerir consentimiento del afectado para hacer uso de sus datos a las Administraciones públicas en el ejercicio de sus funciones en el ámbito de sus competencias[10] y más específicamente las que correspondan a la prevención y asistencia sanitaria así como la gestión de servicios sanitarios[11]. En este aspecto cabe invocar o asumir que dichas tareas incluyen labores investigadoras y sobre todo evaluadoras.

Comunicación de datos

El artículo 11 establece que el consentimiento del interesado para ceder sus datos a terceros no es necesario para la realización de estudios epidemiológicos en los términos establecidos en la legislación sanitaria estatal o autonómica.

Por otra parte el artículo 8 específicamente referido a datos relativos a la salud, hace una excepción a la obligatoriedad de requerir el consentimiento del interesado

para ceder sus datos, a los centros y profesionales sanitarios en el ejercicio de la atención de pacientes que a ellos acudan.

Parecería pues que el marco legal vigente en materia de protección de datos ofrece en términos generales un considerable margen de actuación a la investigación y evaluación en materia de salud y servicios sanitarios, permitiendo la utilización del notable y rico volumen de información que rutinaria o finalistamente se recoge y almacena en la práctica diaria de la asistencia sanitaria.

PROBLEMAS PENDIENTES

No obstante lo hasta ahora dicho existen considerables lagunas o espacios legales y normativos vacíos que motivan diferencias interpretativas e indefensiones que con frecuencia impiden o dificultan el ejercicio de la función investigadora/evaluadora. De todas las existentes hay tres que merecen especial atención.

a) Protección de la identidad de los individuos cuyos datos se manejan: Con independencia de todas las excepcionalidades mencionadas, sigue no obstante prevaleciendo el principio de protección a la intimidad, que no permite que la identidad del afectado sea conocida por quien está haciendo uso de sus datos a menos que ello sea imprescindible para el desarrollo de la función para la que el dato fue recogido.

Tal principio puede respetarse en la inmensa mayoría de los estudios de carácter observacional o epidemiológico, particularmente aquellos que manejan datos agregados o parciales para estudios de prevalencia o incidencia que no precisan del conocimiento de la identidad del afectado. Sin embargo hay circunstancias en las que la identificación precisa del afectado a lo largo del tiempo es necesaria para conocer por ejemplo la evolución de una enfermedad o la respuesta a un tratamiento.

En estos casos la investigación es posible respetando el anonimato, si se aplica el procedimiento de disociación que la ley define[12], asignando un código al paciente objeto de seguimiento cuya asociación con la identidad del mismo es solo conocida por el profesional responsable de su asistencia.

b) Autorización y acreditación de usuarios de archivos y bases de datos: Una cuestión de importancia mayor es el establecimiento del procedimiento de autorización y acreditación de acceso a datos de posibles investigadores o evaluadores, ya que parece obvio que no basta la mera manifestación de la voluntad investigadora o evaluadora para autorizar el acceso a cualquiera que lo plantee.

A primera vista parece que aquellos funcionarios o servidores públicos pertenecientes a centros o asignados a funciones específicamente investigadoras o evaluadoras/inspectoras debieran tener reconocido de oficio el derecho de acceso a la información necesaria para el desarrollo de sus tareas.

Otro caso sería el de investigadores ocasionales, públicos o privados para los que la autorización debiera producirse en cada caso con arreglo a procedimiento explícito y conocido, hasta ahora sólo desarrollado parcialmente[13].

c) Ausencia de un manual o reglamento específico para el ámbito sanitario: Una de las realidades más constatadas es la ignorancia o desconocimiento existente acerca del alcance de la normativa vigente en materia de protección de datos entre investigadores, evaluadores, y gestores sanitarios lo que permite actuaciones al margen de la ley al tiempo que otras veces, y por interpretaciones restrictivas o sesgadas de la misma se impide, frena o dificulta la realización de trabajos perfectamente posibles en el marco legal vigente.

CONCLUSIONES Y PROPUESTAS PRÁCTICAS FINALES

A lo largo del presente trabajo hemos ido viendo como, pese a lo temido, los principios generales de la LORPD permiten la realización de evaluación y la investigación de carácter observacional tan necesaria y relevante hoy día[14 - 17].

Pese a ello se constata la existencia de escaso desarrollo normativo de la LORDP de manera que permita su aplicación en un abanico amplio de casuística. Por otra parte es reseñable la notable ignorancia que sobre tales cuestiones existe entre los profesionales.

Es por todo ello que se propone una actuación en dos fases.

Preparación de un manual de procedimientos

Una recopilación ordenada y comentada de los elementos pertinentes más relevantes que existen en la legislación actualmente en vigor, ayudaría mucho a quienes quieren y deben hacer uso de los datos clínicos y epidemiológicos.

Debería plantearse de modo práctico respondiendo a preguntas que ya se hayan planteado en la casuística, relativas a bases de datos en registros disponibles.

Esta misma tarea de recopilación y estructuración sería un paso previo y necesario para acometer la segunda fase.

Redacción de una norma legal específica

La ley y el reglamento existentes son de carácter general y no alcanzan a ofrecer soluciones y respuestas a las variadas cuestiones que en la casuística sanitaria puedan plantearse. Debería por tanto prepararse una disposición (probablemente un Real Decreto) que al tiempo de compendiar lo disponible, desarrolle con detalle el marco legal específico del uso del dato de carácter personal con finalidad asistencial, gestora, evaluadora e investigadora en el ámbito de la salud y sus cuidados.

REFERENCIAS

1. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298, de 14 de Diciembre de 1999, pag. 43088-43099.
2. Real Decreto 994/1999 de 11 de Junio por el que se aprueba el Reglamento de medidas de seguridad de ficheros automatizados que contengan datos de carácter personal BOE n.º 151, de 25 de Junio de 1999, pags. 24241-24245.
3. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 7, aptdo. 3, pag. 43090.
4. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Arts. 7, aptdo. 6 y 11, aptdo. 2 f), y Art. 8, pag. 43090.
5. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Arts. 7, aptdo. 6 y 11, aptdo. 2 f), pag. 43090.
6. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 11, aptdo. 2 c), pag. 43090.
7. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 11, aptdo. 2 f), pag. 43090.
8. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 7, aptdo. 6.
9. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 5, aptdos. 1, 4 y 5, pag. 43089.
10. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 6, aptdo. 2, pag. 43089.
11. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 7, aptdo. 6, pag. 43090.

12. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de 11 de Diciembre BOE n.º 298. Art. 3 f), pag. 43088.

13. Real Decreto 994/1999 de 11 de Junio por el que se aprueba el Reglamento de medidas de seguridad de ficheros automatizados que contengan datos de carácter personal BOE n.º 151, de 25 de Junio de 1999, pags. 24241-24245.

14. Jack P. Whisnant. Effectiveness versus efficacy of treatment of hypertension for stroke prevention. Neurology 1996; 46: 301-307.

15. Jaume Marrugat y Joan Sala Registros de morbimortalidad en cardiología: metodología. Rev. Esp. Cardiol. 1997; 50: 48-57.

16. TU JV, Pashos cl, Naylor CD, et al. Use of cardiac procedures and outcomes in elderly patients with myocardial infarction in United States and Canada. N. Engl. J. Med. 1997; 336: 1500-5.

17. Kjell Benson, B.A., and Arthur J. Hartz, Md., Ph.D. A comparison of observational studies and radomized, controlled trials. N. Engl. J. Med. 2000; 342: 1878-86.

ASPECTOS TÉCNICOS DE LA SEGURIDAD EN LA INFORMACIÓN SANITARIA

Jokin Sanz Ureta
Jefe de la Sección de Sistemas
Gobierno de Navarra

Sebastián Hualde Tapia
Director de Servicio de Organización y Planificación de la Información
Gobierno de Navarra

INTRODUCCIÓN

Nunca, hasta ahora, la tecnología había influido tan positivamente sobre los sistemas de información, ya que consigue la mecanización casi total de todos los procesos del entorno sanitario, ampliando, además, a través de la red sanitaria, el uso de mejores herramientas a todos los usuarios de la misma. Hay que destacar claramente este efecto beneficioso, pero contrastándolo con el riesgo de que nunca la información ha recorrido tantas vías ni ha estado tan fácilmente accesible para tantas personas.

Por supuesto nos estamos refiriendo a la Tecnología de la Información y de las Comunicaciones (TIC). Hasta ahora otras tecnologías habían conseguido no sólo salvaguardar la información sino también proteger suficientemente la misma, pero con una reducida población usuaria y con unos sistemas complicados y no inmediatos en el acceso a la información. En definitiva sistemas fuertes en la protección física, pero muy débiles en el traslado y difusión de la información.

El grupo de TIC dedicadas a la seguridad (TIC_S) no viene a sustituir a otras tecnologías, sino a, junto con ellas, completar los sistemas de seguridad, permitiendo la difusión de la información y del conocimiento a todos los usuarios en función de su perfil de acceso.

Al hablar de las, en parte novedosas TIC_S, surgen una serie de interrogantes en el plano *no técnico* que hay que tratar de responder: ¿Qué se les pide? ¿Qué no dan todavía? ¿Qué valor añadido tienen? ¿Son sólo un coste obligado? ¿Basta sólo con la tecnología? ¿Cómo ayuda y obliga la Administración? ¿Están normalizadas? ¿Cómo inciden sobre la Sociedad de la Información?

La gran capacidad de proceso de los ordenadores y la alta velocidad de las comunicaciones, que se está consiguiendo y mejorando constantemente, y además a precios asequibles, está facilitando el auge y uso de las TIC_S. Estas tecnologías son utilizadas en los procesos sanitarios con un alto rendimiento y sin penalizar gravemente el tiempo de respuesta, que es prácticamente imperceptible por el usuario.

Por otra parte, se va consiguiendo minimizar con éxito la acción destructiva de las tecnologías de *contra seguridad,* a pesar de que el delincuente dispone de la misma

capacidad de proceso y de comunicación. Por supuesto, para ello ha sido necesario incrementar el nivel tecnológico y por lo tanto, el coste dedicado a la seguridad.

De todos modos, se puede afirmar que las TIC_S ayudan a conformar un sistema mucho más seguro y utilizado por muchos más usuarios desde cualquier punto de la red mundial. Pero esto no evita ni las políticas de seguridad, ni la normativa, ni las auditorías, ni el resto de procedimientos y cautelas que se han de adoptar para garantizar unos niveles de seguridad válidos para los centros sanitarios.

Las TIC_S dificultan, previenen e impiden en la mayor parte de los casos el delito, mejoran la seguridad preventiva, y almacenan además la información propia sobre los accesos a la información sanitaria. Este almacenamiento añadido, permite detectar en casi todos los casos, si hay colaboración por parte de las autoridades mundiales, las herramientas, puestos y vías que se han utilizado y las personas que han intervenido.

A pesar de los grandes logros de las TIC_S, ha de quedar bien claro, que en el campo de la seguridad es más importante avanzar en la cultura de las personas que en la propia tecnología.

Por supuesto es evidente que no hay tecnología que pueda contra la falta de cultura. Para poder hacer un buen uso de la tecnología en seguridad hay que adquirir una cultura y concienciarse de la importancia de la seguridad en los procesos de los centros sanitarios.

Otro aspecto relevante a considerar es la fuerte incidencia que las TIC_S están teniendo en el Empleo, dado que se precisan nuevos puestos de trabajo de diferentes perfiles, que requieren un alto grado de capacitación y de renovación.

Se da el triste caso, de que las Universidades no están proporcionando esta formación, siendo por tanto necesario, por parte de las empresas, invertir mucho tiempo y dinero en la misma. Con el consiguiente riesgo de que una vez formados la alta demanda del mercado en estos nuevos puestos, provoque una falta de estabilidad y continuidad en la implantación de los sistemas de seguridad y en su mantenimiento. Lo que está provocando, y es práctica habitual, que los gerentes opten por subcontratar la seguridad a empresas externas especializadas en la misma. Lo cual plantea ciertas alarmas y paradojas en la ciudadanía.

En definitiva, las TIC_S introducen otras tareas y puestos de trabajo que son difíciles de acometer por falta de personal preparado, lo que conlleva no sacar el máximo aprovechamiento de las mismas, con la consiguiente duda en los gestores de asumir o no el nivel de riesgo de extender su sistema de información a la Red.

Finalmente resumamos cómo el auge y desarrollo de las TIC_S ha afectado a diferentes sectores y actores de las Sociedad de muy diversa e intensa manera:

En la Justicia y Policía: Se ha desarrollado un nueva Norma, caracterizada por la innovación, el riesgo que asume y los plazos de difícil cumplimiento que impone. Se han desarrollado potentes sistemas de análisis de intrusión y se facilita la persecución del delito tanto a priori como a posteriori.

Los Gestores se ven obligados a invertir más en seguridad, decidiendo aparte de la obligada cumplimentación de la Norma, qué riesgos quieren asumir y qué planes de contingencia se han de activar.

Los Clínicos se ven animados a capturar, tratar e imprimir la información con sistemas informáticos seguros, garantizándoles su responsabilidad en la información producida y aportando calidad a la información y conocimientos consultados.

Los Administradores y Gestores de la Seguridad cuentan ya con las máximas oportunidades para proteger los sistemas, siempre que al aplicar las políticas y planes de seguridad, ejecuten una serie de procedimientos e implanten las TIC_S de forma adecuada y con los profesionales necesarios.

Los Ciudadanos se pueden sentir ya realmente propietarios de su historia clínica y pueden optar, los más autónomos, por tomar decisiones sobre su propia salud.

Los Desarrolladores de programas informáticos mejoran la calidad de sus productos contando con bases de datos de pruebas más completas, al generar las mismas mediante técnicas de seguridad a partir de las bases de datos reales.

Las áreas de Formación y Docencia, así como la de Investigación cuentan, a partir de la historia clínica limitada en el acceso identificativo, con más información y con la tranquilidad del uso adecuado de la misma.

Los Auditores cuentan con mejores sistemas, tanto para los propios sistemas de seguridad como para el resto de procesos de los centros sanitarios.

Las TIC en Seguridad, en definitiva, permiten al clínico, gestor, ciudadano y a otros actores y sectores una mayor responsabilidad, calidad en el acceso a los datos, y mejores servicios tanto clínicos como administrativos.

Pero no hay que olvidar que el delincuente está cada vez más preparado, que actúa más desde el interior de la propia empresa que desde fuera. Y que las noticias sobre sistemas inseguros surgen en su mayor parte cuando interviene gente que busca notoriedad, pero que la mayor parte de los delitos no se conocen y si se detectan no salen en los periódicos, sobre todo si ocurren en el sector privado.

Hay que recalcar que si todo se ha hecho bien, gracias a las TIC_S y con el apoyo de la Norma adecuada, se puede conseguir dar un salto cualitativo en el uso y tratamiento de la información sanitaria. Y además con la garantía, de que se consigue autenticar al usuario, sin que sea admisible el repudio de la responsabilidad adquirida.

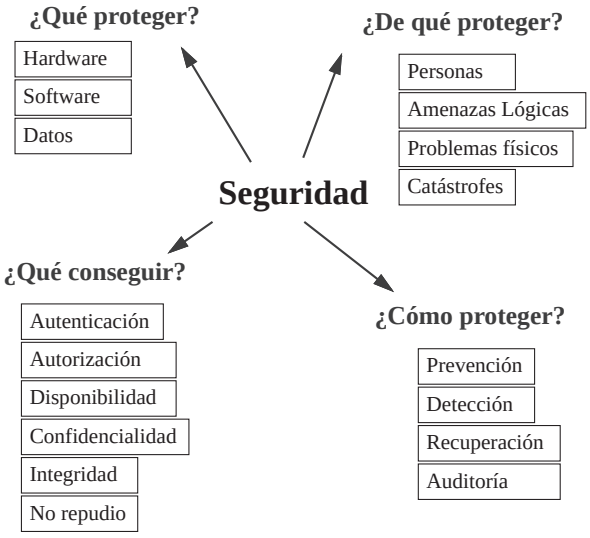
En este trabajo vamos a detallar las tecnologías que integran las TIC_S, haciendo más hincapié en aquellas que han surgido para dar respuesta a los sistemas distribuidos tanto por la red privada como por la red pública.

El esquema seguido parte de *que hay que proteger y de quién nos hemos de proteger,* expresando las necesidades de *que queremos conseguir,* e indicando *cómo hemos de protegernos.*

Por otra parte desarrollamos los elementos significativos de la *Criptología, y sus principales usos,* desarrollando a continuación la infraestructura de clave publica PKI (Public Key Infraestructure).

DEFINICIÓN

Seguridad es una característica de un sistema (sea informático ó no) por la cual podemos decir que el sistema está libre de peligro, daño o riesgo y que es, de alguna manera, *infalible.* Centrado en el ámbito informático, podemos decir que seguridad sería la característica de un sistema que lo hace ser capaz de proteger sus datos frente a la destrucción, interceptación ó modificación no deseadas.



¿QUÉ PROTEGER?

Dentro de un sistema informático los 3 elementos que debemos proteger son el hardware, el software y los datos. Por *hardware* entendemos los elementos físicos que conforman el sistema como el procesador, los discos, las cintas, los cableados, los elementos de comunicaciones, etc. Por *software* entendemos el conjunto de programas lógicos que hacen funcionar el hardware, tanto sistemas operativos como aplicaciones. Y como *datos* entendemos el conjunto de información lógica que manejan el hardware y el software, como por ejemplo las entradas que se encuentran en una base de datos, o los paquetes que viajan por una red.

Habitualmente lo que debemos proteger son los datos, ya que tanto el hardware como el software son fácilmente recuperables. De todos modos debemos proteger estos dos últimos elementos ya que son el camino para atacar los datos.

¿DE QUÉ PROTEGERNOS?

a) Personas

La mayoría de amenazas provienen de personas en última instancia, y además se suele afirmar con toda razón que los elementos más débiles de nuestros sistemas informáticos son las personas. Sus actuaciones pueden ser tanto *intencionadas* como *no intencionadas.* Habrá que arbitrar las medidas necesarias para protegerse de estos tipos de personas: personal, ex-empleados, hackers, crackers, phreakers.... Conviene no olvidar que la mayor amenaza para nuestros sistemas proviene del personal que trabaja ó ha trabajado con ellos.

b) Amenazas lógicas

Programas que pueden dañar nuestros sistemas, de nuevo pueden haber sido creados para ello, o por error. Habría que distinguir entre: software incorrecto (*bugs*, y *exploits* los programas que se aprovechan de ellos), puertas traseras, herramientas de seguridad, bombas lógicas, virus (gusanos, caballos de troya...), bacterias, técnicas salami, etc.

c) Problemas físicos

En este apartado debemos encargarnos de proteger el hardware. Aquí debemos atender diversos aspectos:

–Sobrecargas eléctricas e interrupciones de alimentación: solucionados normalmente con redundancia en elementos críticos como las fuentes de alimentación, las líneas que proporcionan la corriente eléctrica... con SAI’s y grupos electrógenos.

–Temperaturas extremas, humedad, polvo...: solucionados en las salas de equipos críticos (servidores, armarios de red...) con elementos como climatizadores, deshumidificadores, extractores... que controlen las condiciones medioambientales

–Accesos físicos no autorizados, robo de hardware, uso no autorizado de bocas de red...: se soluciona con medidas de uso racional de las instalaciones (cerrar puertas, deshabilitar bocas de red de lugares aislados...) con sistemas de control de acceso físico, contraseñas de acceso al hardware, deshabilitar unidades de CD-ROM y disquete....

–Fallos en elementos físicos, especialmente en discos y en cintas, tratados con soluciones de redundancia física (RAID, RAIT...)

–Fallos en CPU's: solucionados con sistemas tipo *cluster*, sistemas que tienen duplicados (ó n-plicados) los servidores y ante la caída de uno de ellos, otro u otros asumen sus funciones.

–Fallos de memorias: solucionados con elementos redundantes, sistemas de paridad, memorias auto-correctivas...

–Destrucción física de datos y borrados accidentales de información: se soluciona con políticas de copias de seguridad de los datos, almacenamiento de cintas de respaldo *rojas* en lugares protegidos (bunker de bancos).

d) Catástrofes

Habrá que buscar el asegurarse razonablemente de ellas, buscando un equilibrio entre la protección ante ellas y el coste que conlleva dicha protección. Podemos destacar los incendios, inundaciones, terremotos, humo, atentados...

¿QUÉ CONSEGUIR?

a) Autentificación

Es el proceso de identificar un usuario, máquina u organización de modo preciso. Existen muchas tecnologías que se pueden usar para autenticar:

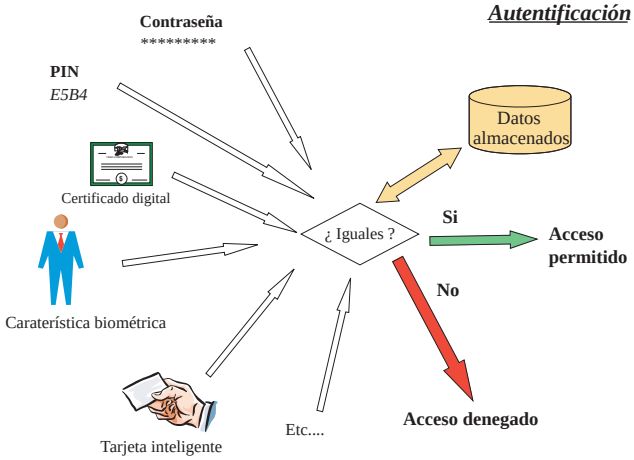
–Contraseñas

–Certificados

–Tarjetas Inteligentes (Smart card)

–Biometría. (voz, escritura, huellas, patrones oculares, mano...)

–Firma digital...



La autentificación tradicional (UNIX, NT...) garantiza que las contraseñas se mantienen en secreto, pero utilizan sistemas de encriptación muy simples.

Una tecnología consolidada y en auge es Kerberos, un protocolo de autentificación distribuida con cualidades de identificación única (Single Sign-On) que permite establecer privacidad e integridad de los datos, utilizando mecanismos de clave pública, mucho más seguros que la autentificación tradicional. Sistemas operativos avanzados, como Windows 2000 ó algunos UNIX, emplean este sistema..

b) Autorización

Es el proceso de determinar lo que un elemento autenticado puede hacer. Ejemplos son las listas de control de acceso ó la seguridad del sistema de archivos (NTFS, por ejemplo), que asocian los usuarios autenticados a perfiles de acceso a aplicaciones, ficheros, equipos, etc. Mediante este proceso se determinan los privilegios de un usuario (u otro elemento autenticado) en un sistema.

c) Disponibilidad

Consiste en proteger los sistemas para mantenerlos en funcionamiento el mayor tiempo posible. Ya hemos hablado de la protección física. Existen sistemas que nos permiten aumentar la disponibilidad del software con sistemas de particionado lógico de máquinas físicas, tecnologías cluster, tanto de discos como de red...

d) Confidencialidad

Consiste en asegurar que la información es accedida tan solo por los usuarios (u otras entidades) autorizados. Para garantizar la confidencialidad utilizaremos mecanismos de *encriptación,* fundamentalmente.

e) Integridad de la información

Consiste en asegurar que la información no se ha transformado durante su procesamiento, transporte ó almacenamiento. Además de todos los mecanismos que garantizan la integridad de las señales transmitidas y de los datos físicos almacenados, también recurriremos a la *encriptación.*

f) No repudio

Consiste en asegurar que ninguna de las partes implicadas en una comunicación (ya autenticadas) puede negar haber participado en una determinada transacción. De nuevo nos apoyaremos en la *encriptación* y mecanismos asociados a ella como la tecnología de clave pública y la firma electrónica.

¿CÓMO PROTEGERNOS?

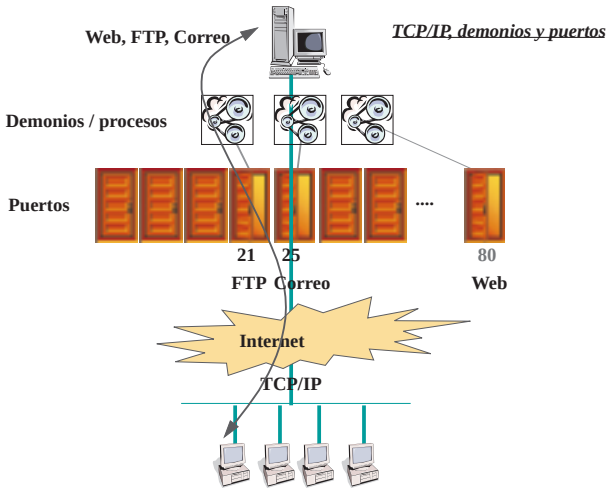
Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia. Partiendo de este análisis diseñaremos una política de seguridad que incluya responsabilidades y reglas para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. Para ello estableceremos una serie de mecanismos de seguridad que se dividen en 4 grandes grupos, mecanismos de prevención, de detección, de recuperación y de auditoría.

a) Mecanismos de prevención

Garantizan la seguridad del sistema durante su uso habitual. Podemos destacar los mecanismos ya mencionados en autentificación, autorización, confidencialidad, integridad de la información, no repudio y disponibilidad.

Los disquetes, CD-ROM's, y otros medios *removibles* que entran y salen de nuestro sistema deberán ser tenidos en cuenta, así como los medios no electrónicos como impresos, faxes, teletipos, pantallas,... con que las personas tratan la información. Para todos ellos las soluciones serán fundamentalmente organizativas.

Hoy la inmensa mayoría de los ordenadores está conectado a una red, y de éstos, la inmensa mayoría utiliza *TCP/IP* como lenguaje de comunicación. TCP/IP



es el conjunto de protocolos de comunicación estándar de internet, por lo que todo ordenador conectado a internet entiende TCP/IP. Mediante este protocolo, una máquina puede establecer múltiples conexiones simultáneas por lo que se denominan *puertos*, un concepto similar a los canales del televisor, los cuales vienen en un único cable. Existen puertos dedicados a tareas específicas, como por ejemplo, el puerto 80, dedicado a dar servicio de páginas Web. Para atender las peticiones a estos puertos existen diversos programas, llamados *demonios*, que se encargan de responder a esas peticiones. Los demonios son programas, por lo que no son perfectos. Es posible enviar peticiones extrañas a un demonio asociado a un puerto y conseguir efectos como la parada del equipo, tomar el control del equipo, conseguir contraseñas, etc. Esta suele ser la labor de los **hacker.**

Un hacker es un concepto amplio que abarca a cualquiera que se dedica a infiltrarse en sistemas informáticos. Protegerse totalmente de un grupo de hackers es prácticamente imposible pero se pueden establecer medidas de seguridad razonables, como vigilar los registros de intentos de acceso, limitar el número de demonios a lo exclusivamente necesario, cambiar habitualmente las contraseñas, no colocar más información de la necesaria en los servidores expuestos, actualizar el software permanentemente, colocar cortafuegos y software de detección de intrusos...

Un elemento especialmente interesante que nos permite delimitar claramente quien entra y qué hace es el **cortafuegos** *(firewall).* Este elemento se utiliza para controlar el acceso desde unas redes a otras. Se basa, fundamentalmente, en el filtrado de paquetes IP. Este sistema está, generalmente, implementado como una

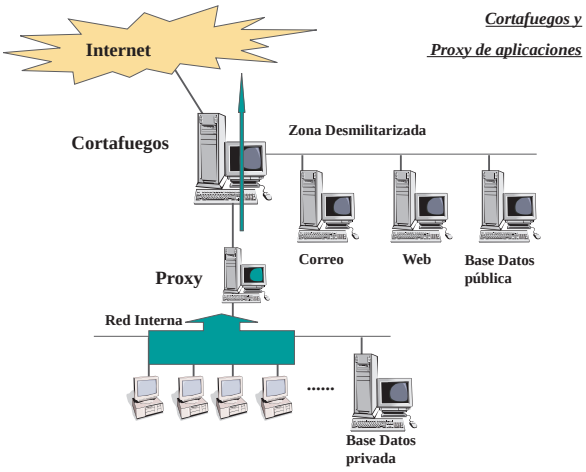


tabla de condiciones y acciones, reglas que efectúan un filtrado de paquetes basándose en el origen y destino del paquete, así como el servicio TCP/IP que utiliza (Web, correo...).

Un cortafuegos moderno, además del filtrado de paquetes implementa toda una serie de mecanismos adicionales de seguridad que nos defienden de ataques de denegación de servicio, de ataques *spoofing* (cuando alguien modifica sus paquetes IP para simular que se encuentra en una zona diferente a la real),...

Otro elemento que aporta un alto grado de seguridad es el denominado **proxy** de aplicaciones. Su funcionamiento también es muy simple. Consiste en una especie de embudo por la que hacemos pasar los servicios TCP/IP de todo un grupo de máquinas para limitarlos. Obtenemos una serie de ventajas como que el exterior tan solo ve una máquina trabajando fuera (con la consiguiente simplificación de nuestras reglas de cortafuegos) y que podemos limitar los servicios según nuestras necesidades (por ejemplo permitir FTP en descarga pero no en envío).

A la vez se pueden añadir técnicas de NAT (Traducción de direcciones de red) que nos permiten ocultar al exterior las verdaderas direcciones de nuestras máquinas. Un ejemplo muy habitual es transformar la dirección de nuestro proxy.

b) Mecanismos de detección

Un grupo de tecnologías se encargan de detectar intentos de ataques ó ataques propiamente dichos. Aportan unas ciertas medidas de monitorización y detección de actividad sospechosa, que pueden ser más o menos “inteligente”. Desde el sim-

ple registro de los paquetes que llegan al sistema, pasando por los que analizan las franjas horarias, las direcciones que nos "scanean", ..., hasta aquellos que simulan servicios que no existen para tentar a los atacantes y así descubrirlos. Los propios cortafuegos implementan muchas de estas técnicas.

Otro tipo de tecnologías son las de análisis de riesgos. Estas se encargan de detectar problemas de seguridad en nuestros sistemas. Los hay de muchos tipos:

–Herramientas que realizan un barrido en nuestros sistemas comprobando agujeros de seguridad conocidos en el sistema. Son los analizadores de vulnerabilidades.

–Herramientas que se encargan de advertir de todos los servicios que nuestra sistema está ofertando a la red ya que en muchas ocasiones son más de los necesarios. Los *scanner de puertos.*

–Herramientas que hacen una "foto" del sistema en su origen, y que permiten comprobar que todo sigue igual con el paso del tiempo, y no se han producido modificaciones al software básico. Estas "fotos" se basan en algoritmos *hash* sobre los archivos clave del sistema.

–Herramientas que actúan sobre las contraseñas del sistema. Se encargan de detectar la vulnerabilidad de estas contraseñas.

Otro tipo de tecnologías se encarga de los fallos hardware, la monitorización, las alertas, acciones ante fallos, etc. Todo un abanico de herramientas de gestión de infraestructuras que permiten detectar fallos, en muchas ocasiones, antes de que produzcan daños al sistema. Y no solo fallos, también se encargan de detectar los niveles de saturación de los elementos críticos antes de que se produzcan problemas en el servicio.

Por último un elemento imprescindible de detección en una red es el *antivirus.* Programa, o conjunto de programas, encargados de mantener un ordenador y/o una red libres de virus. Se deberán colocar antivirus en todos los puntos de entrada/salida de información de nuestro sistema.

c) De recuperación

Nos permiten recuperar el estado habitual del sistema tras un fallo ó ataque. Fundamentalmente son herramientas basadas en las copias de seguridad.

d) De auditoría

Nos permiten determinar las causas de los problemas antes, durante y después de que suceda. Fundamentalmente son registros de los sucesos que se van produciendo en el sistema: usuarios que entran, acciones que realizan, tiempos en los que se hacen las cosas...

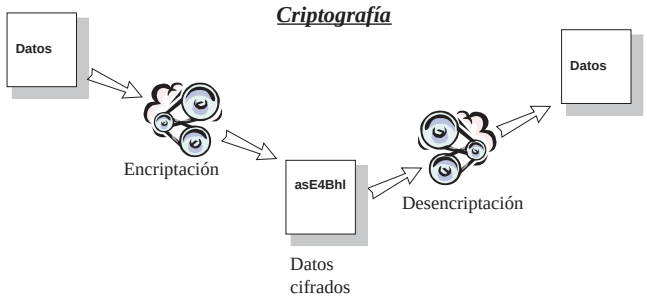
CRIPTOGRAFÍA

"Es el conjunto de técnicas que permiten transformar un trozo de información, de tal forma que quienes deseen recuperarlo sin estar en posesión de otra pieza de información (clave), se enfrentarán a un problema intratable. Conviene recordar que "intratable" no significa lo mismo que "insoluble"; puesto que el número de posibles claves ha de ser finito, la fuerza bruta siempre nos permitirá recuperar el mensaje original, al margen de que seamos luego incapaces de reconocerlo. En cualquier caso, desde un punto de vista práctico la casualidad deberá ser descartada, ya que las probabilidades de que se descifre por la fuerza bruta un mensaje en tiempo razonable es inferior a la de que le caiga a usted en este preciso instante un meteorito sobre la cabeza.

Pero, ¿qué es exactamente un problema intratable? Sencillamente aquel que para ser resuelto de forma satisfactoria requiere una cantidad de recursos computacionales (tiempo y memoria) más allá de las posibilidades del atacante. De hecho, si tuviéramos claves de 256 bits y la Física actual no se equivoca, no hay suficiente materia ni energía en el Universo para construir una computadora que recorra todas las posibles combinaciones.

Sin embargo, existe un último e inquietante detalle para tener en cuenta: la definición anterior necesita para ser operativa que el contrincante carezca de "atajos" para resolver nuestro problema en teoría intratable. Por desgracia, y para satisfacción de muchos paranoicos, prácticamente para ninguno de los problemas que plantean los algoritmos criptográficos actuales se ha demostrado que no pueda existir algún atajo..."*

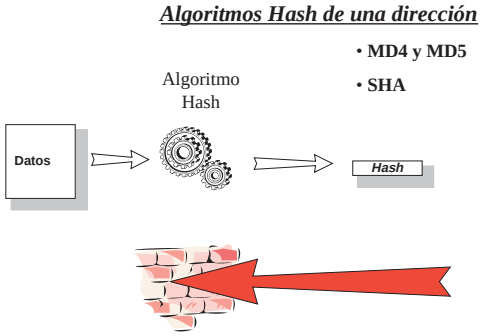
Vamos a describir los principales tipos de tecnologías empleados para cifrar información y sus diversas implementaciones.



* Lucena López M. Números primos y criptografía. Kriptópolis 8 Julio 2000. htpp://www.kriptopolis.com/luc/20000708.html

a) Algoritmos hash de una dirección

Un algoritmo *hash de una dirección* funciona de este modo: se introduce un documento en el algoritmo y se genera un *hash* que es un pequeño trozo de información que representa al mensaje original.



La característica fundamental de estos algoritmos es que tan solo funcionan en una dirección, es decir, no se puede obtener el documento original a partir del *hash.* Y un determinado *hash* tan sólo se puede obtener de un determinado documento origen.

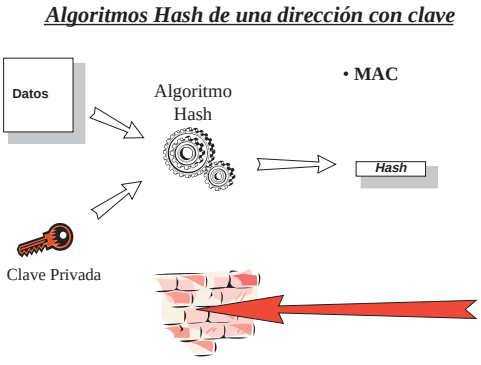
Ejemplos de algoritmos:

–MD4 y MD5 (Message Digest) 128 bits.

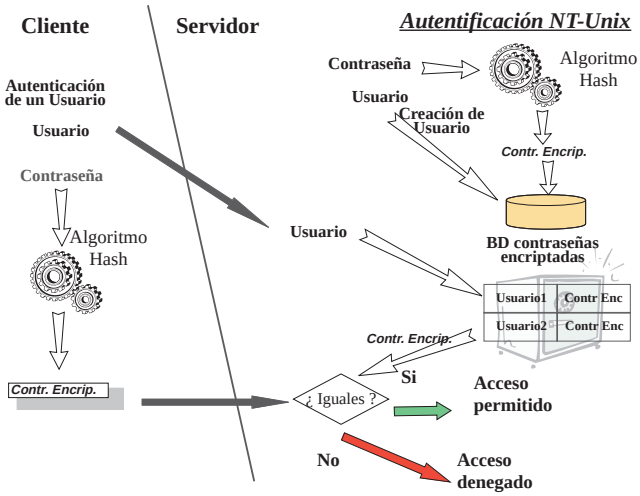
–SHA (Secure Hash Algorithm) 160 bits.

Un subconjunto de estos algoritmos es el que utiliza una clave (conjunto de bits) como parte de la función. Un ejemplo de algoritmo de este tipo es:

–MAC (Message Authentication Code).

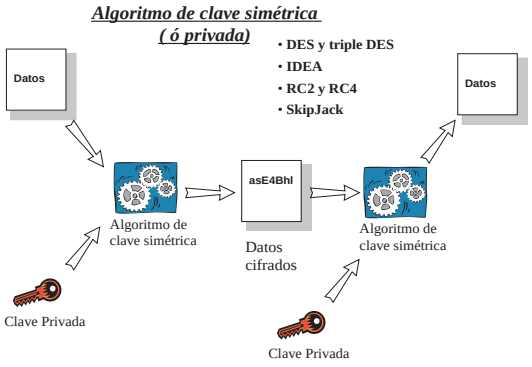


A modo de ejemplo describimos en esta imagen el proceso de Autentificación en un entorno NT ó UNIX tradicionales. La línea negra determina lo que viaja por la red. Claramente se observa que no viaja nunca la información de la contraseña. Además, el servidor no conoce la contraseña.



b) Algoritmos de clave privada (simétricos)

Un algoritmo de *clave privada* funciona de este modo: el emisor introduce un documento en el algoritmo así como la clave privada (trozo de información conocido sólo por el emisor y el receptor), se obtiene el mismo documento pero cifrado, es decir, ininteligible. El receptor recoge el documento cifrado y lo introduce de nuevo en el algoritmo así como la clave privada obteniendo el documento origen.



Ejemplos de algoritmos:

–DES y triple DES. –RC2 y RC4.

–IDEA. –SkipJack.

La característica principal de este algoritmo es que existe *una única clave* que solo conocen los interlocutores, y que sirve tanto para cifrar como para descifrar. Es muy rápido.

c) Algoritmos de clave pública (asimétricos)

Un algoritmo de *clave asimétrica* se basa en la existencia de una pareja de claves: la **clave privada,** conocida solo por el propietario de la pareja, y la **clave pública,** que el emisor reparte a quienes él desee. Ambas claves se generan en un mismo proceso y forman una pareja que depende una de la otra.

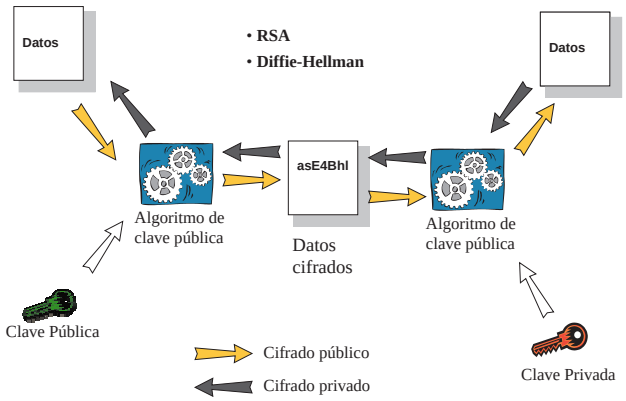
Funciona de este modo: el emisor introduce un documento en el algoritmo así como su clave privada, se obtiene el mismo documento pero cifrado, es decir, ininteligible. El receptor recoge el documento cifrado y lo introduce de nuevo en el algoritmo así como la clave pública del emisor, obteniendo el documento origen. Del mismo modo el algoritmo funciona de forma inversa. Es decir, lo cifrado por el receptor con la clave pública del emisor, sólo puede ser descifrado por éste, con su clave privada.

Ejemplos de algoritmos:

–RSA (Rivest-Shamir-Adleman).

–Diffie - Hellman.

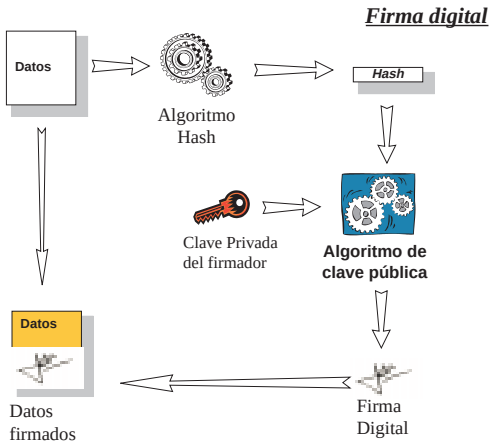
Algoritmo de clave asimétrica (ó pública)



USOS DE LAS TECNOLOGÍAS DE ENCRIPTACIÓN

Estas tecnologías tienen múltiples utilidades entre las que destacaremos las siguientes.

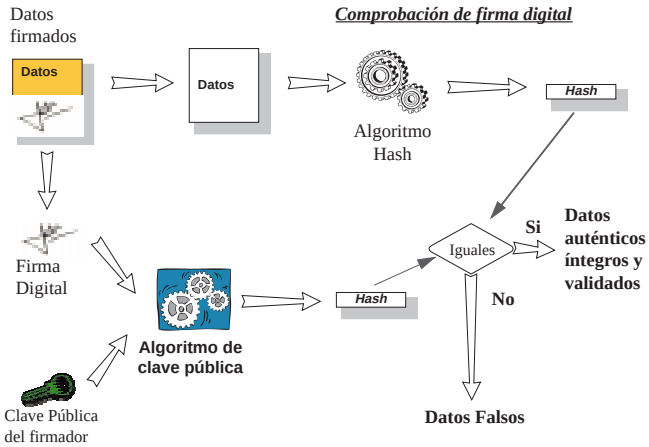
a) Firma digital



Para garantizar la integridad de un documento así como validar su autor utilizamos el mecanismo de firma digital, que utiliza tecnología de clave pública.

Para **firmar** debemos introducir el documento en un algoritmo hash de modo que obtenemos el resumen cifrado (hash) del documento. Este resumen lo introducimos a su vez en un algoritmo de clave pública junto con la clave privada del emisor obteniendo el hash cifrado. Ese hash se adjunta al documento garantizando la integridad del documento y su propietario.

Cuando el documento firmado llega a alguien que pretende **validarlo** debe realizar este proceso. Introduce la firma del documento así como la clave pública del emisor en el algoritmo de clave pública para obtener el hash del documento. Por otro lado introduce los datos del documento en el algoritmo hash para obtener el resumen (hash) que deberá ser igual en ambos casos para garantizar la validez del documento.



b) Certificados

Para realizar intercambios de información seguros es preciso que, además de cifrar la información mediante mecanismos de clave pública, algo ó alguien nos garantice que las claves públicas de nuestros interlocutores sean verdaderas. Para esto utilizamos los llamados certificados digitales, algo así como el DNI digital.

Un certificado digital contiene, fundamentalmente, los datos de un usuario (o entidad) y su clave pública (ligada a su clave privada). Esta información viene avalada por una entidad tercera que garantiza la validez de su contenido: es la *entidad certificadora.* Ésta valida el contenido firmando digitalmente todo el certificado, de modo que cualquiera que quiera validar su contenido solo deberá comprobar la firma del certificado.

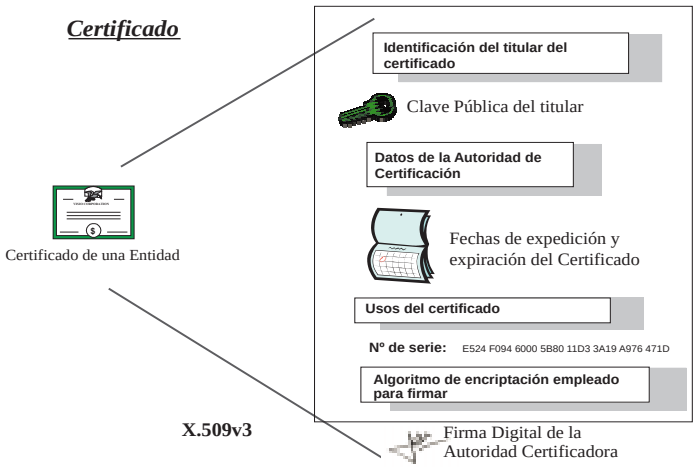
Tipos de certificados y su utilidad:

–Personales:

Firma digital
Cifrado de correo electrónico (S/MIME)
Firma de formularios
SSL
Soluciones de Single-Sign-On (identificación única)
...

–De servidor

SSL
Time stamp
VPN's
...



–Autoridad de certificación
Firma digital de certificados
Firma digital de CRL's

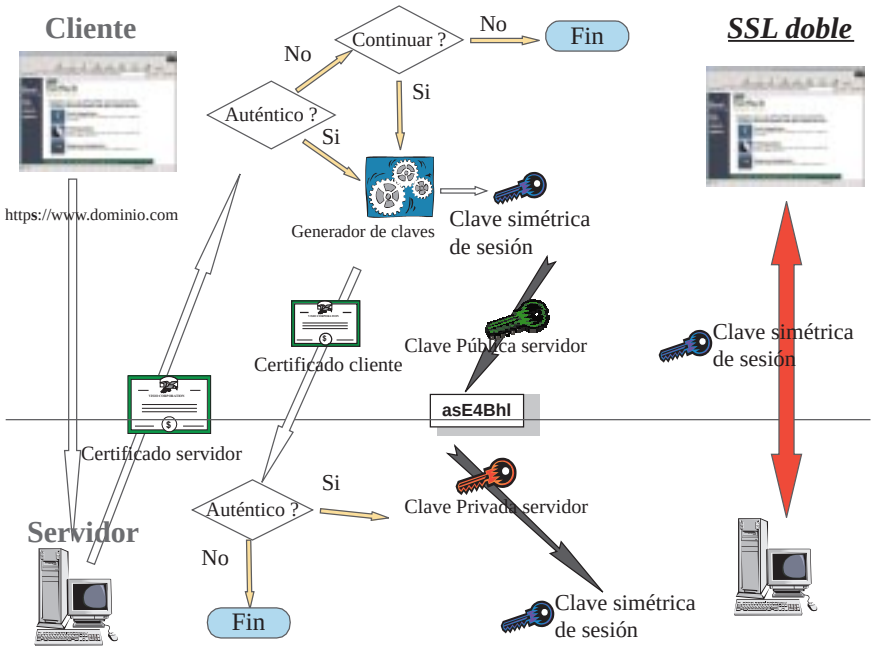
–Firma de código
Autenticidad del software

c) Comunicación segura con un servidor

SSL (Secure Sockets Layer) creado por Netscape, y **TLS** (Transport Layer Security) abierto y basado en SSL, son dos protocolos que aportan una capa de seguridad para garantizar la autenticidad, integridad y confidencialidad en una comunicación.

SSL es el protocolo que utilizamos con el navegador cuando nos conectamos a los llamados **sitios seguros.**

Mediante SSL es posible autenticar al servidor y al cliente. Si solo interesa autenticar al servidor, éste entregará su certificado al cliente. Si además es preciso autenticar al cliente, el servidor solicitará un certificado al cliente.



d) Comunicación segura en sistemas financieros

SET, Secure Electronic Transaction, es un standard abierto creado por VISA y Mastercard para facilitar las transacciones comerciales y los pagos sobre Internet. El protocolo SET utiliza criptografía basada en certificados. El sistema es similar a SSL pero con la ventaja de disponer de una encriptación mucho más fuerte, además de exigir la certificación de todas las entidades que intervienen en una transacción comercial: el titular de la tarjeta de crédito, el comercio, la pasarela de pagos y las entidades financieras emisora y adquiriente.

SGC, Server Gated Crypto, es una extensión de SSL también para el entorno financiero muy similar a SET.

e) Cifrado de correo y ficheros

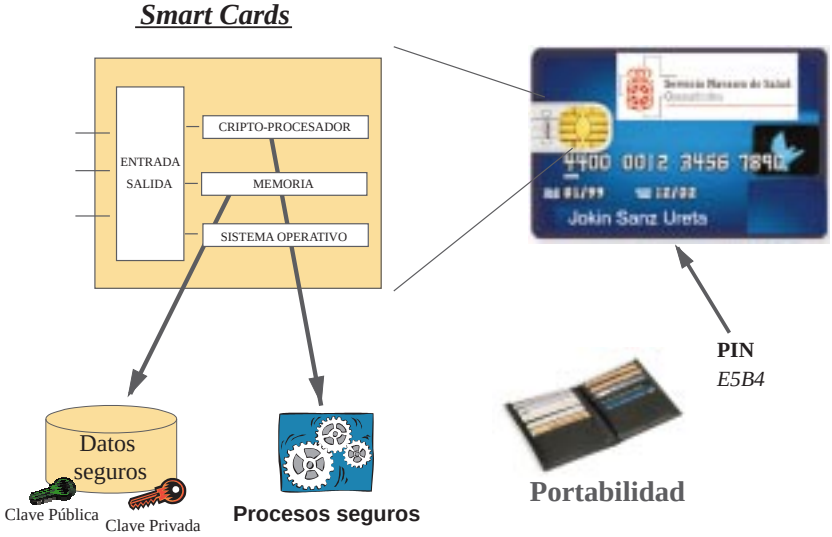
Dos entes especialmente sensibles son los ficheros y los correos electrónicos. Ambos son documentos con información que de algún modo debemos proteger.

PGP (Pretty Good Privacy) es un sistema de clave pública para encriptar correo, ficheros y hasta tráfico TCP/IP desarrollado a principio de los 90 por Phill Zimmerman. Su uso se ha extendido ampliamente debido a su facilidad para gestionar las claves públicas y privadas.

S/MIME es otro sistema más moderno de securizar mediante tecnología de clave pública el formato de correo MIME (Multipurpose Internet Mail Extensions).

f) Smart Cards (Tarjetas inteligentes)

Las llamadas tarjetas inteligentes son un dispositivo de seguridad del tamaño de una tarjeta de crédito que ofrece funciones de almacenamiento y procesamien-



to seguro de información. La diferencia con las tarjetas normales estriba en que éstas tienen una banda magnética en la que existe cierta información, mientras que las tarjetas inteligentes disponen de un chip empotrado en la propia tarjeta.

Las tarjetas aportan las siguientes características de seguridad:

–Almacenamiento resistente a ataques para claves privadas y otra información sensible.

–Aislamiento de los procesos de autentificación, firmado digital e intercambio de claves de otros elementos del sistema que no tienen porqué conocerlos.

–Portabilidad de las credenciales digitales y otras informaciones.

–Doble seguridad: algo poseído (la tarjeta) y algo conocido (el PIN de identificación).

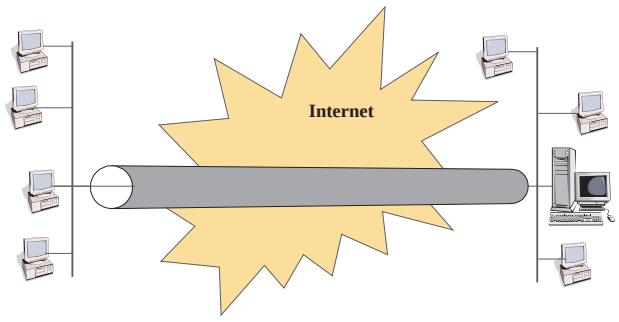
Su funcionalidad es la misma que aportan los certificados digitales, teniendo en cuenta que puede almacenar también la clave privada.

g) Redes privadas virtuales (VPN's)

Para proteger la información que viaja a través de redes públicas ó poco seguras se emplea la tecnología de *Redes Privadas Virtuales.* Existen diferentes aproximaciones tecnológicas para solucionar este problema pero todas ellas consisten en crear un 'túnel' entre dos extremos que se comunican. El túnel se crea encriptando la información en el origen y desencriptándola en el destino. Existe un gran número de protocolos empleados para crear túneles, vamos a mencionar las tecnologías más utilizadas:

–**PPTP:** (Point to Point Tunneling Protocol) diseñado para autenticar y encriptar (además de comprimir) una comunicación entre dos extremos, en base a un identificador y una contraseña.

VPN (Red Privada Virtual)



–**L2F:** (Layer 2 Fordwarding). Ofrece la misma funcionalidad que PPTP.

–**L2TP:** (Layer 2 Transfer Protocol) es una combinación de PPTP y L2F que mejora sus funcionalidades.

–**IPSec:** Añade a los anteriores la capacidad de garantizar la integridad de los paquetes enviados por la red. Limitado a tráfico IP.

PKI

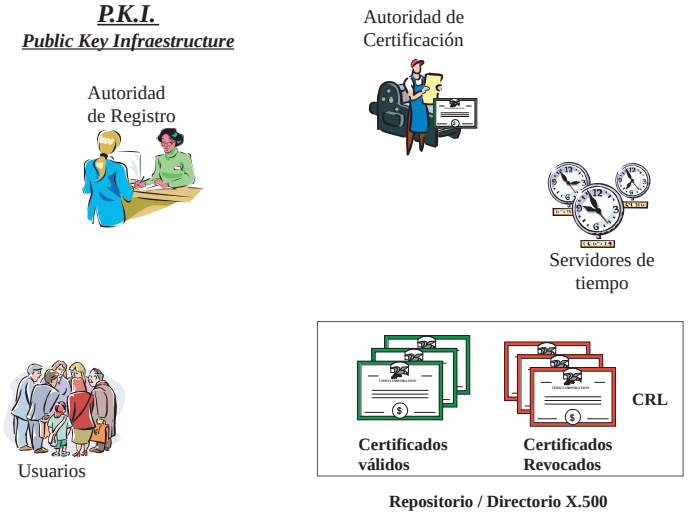
PKI (Public Key Infraestructure) es un conjunto de tecnologías que se aprovechan de los algoritmos de encriptación de clave pública, de clave privada y hash.

Nace de la necesidad que surge en una comunicación entre dos extremos de garantizar, la autenticidad, integridad y confidencialidad de los comunicantes y del contenido de la transmisión. Esto se realiza mediante la intervención de un tercero confiado por ambos.

Una PKI está compuesta por una serie de entidades: Usuarios, Autoridad de Registro, Autoridad de certificación, Servidores de tiempo y Repositorio de la información.

a) Autoridad de registro

La *Autoridad de Registro (RA)* es una entidad autorizada por la *Autoridad de Certificación (CA)* para auxiliarla en el proceso de asegurar que los usuarios satis-



facen todos los requisitos para que se le expida un certificado, es decir, se encarga de *dar fe* ante la CA de la validez de los datos que le envía. Estas son sus funciones:

–Recibe solicitudes de certificación y mantiene una base de datos con ellas. Las solicitudes pueden ser de dos tipos:

1.–De firma de certificado *(CSR, Certificate Signing Request).* En este caso el solicitante ha creado, con un software, la pareja de claves privada-pública y, junto a sus datos identificativos, entrega a la RA su clave pública para ser firmada.

2.–De creación de certificado completo. El solicitante solo entrega sus datos identificativos y recibirá el certificado y su clave privada asociada.

–Recibe solicitudes de revocación de certificados previas a la expiración de éstos.

–Recibe solicitudes de renovación de certificados ante su expiración. La RA debe advertir a sus clientes de la necesidad de renovación de sus certificados antes de que se creen situaciones de denegación de servicio.

–Debe decidir la validación o deniego de todas estas solicitudes.

–Debe mantener una base de datos con todas las solicitudes.

–Generalmente es parte de su responsabilidad la publicación en el repositorio correspondiente de los certificados y de las listas de certificados revocados.

b) Autoridad de certificación

La *Autoridad de Certificación (CA)* es una entidad de prestigio y confianza que *da fe* de que una clave pública pertenece realmente a la entidad que consta en el certificado. Éstas son sus funciones:

–Recibe las peticiones de la RA y genera los certificados. En función del tipo de solicitud realiza esto de dos formas:

1.–Si el solicitante entrega la clave pública, junto con los datos asociados, tan solo los firma digitalmente con su clave privada.

2.–Si el solicitante solo entrega los datos identificativos, la CA crea la pareja de claves pública-privada y después firma la pública junto con el resto de datos.

–Entrega los certificados y, en su caso, las claves privadas a la RA.

–Genera las *Listas de Certificados Revocados (CRL)* para que se publiquen en el repositorio. En la CRL están los números de serie de los certificados revocados, todos ellos firmados por la CA para garantizar su validez.

–Debe mantener una base de datos con todos los certificados y claves emitidas.

–Son las encargadas de definir las *Políticas de Certificación (CPS, certification practice statements),* que son las reglas que definen los procedimientos a seguir en los procesos de certificación.

Al conjunto de CA's que se rigen por una misma CPS se denomina *Dominio de Certificación.* Dentro de un dominio todos los usuarios de certificados se pueden validar unos a otros, pero fuera de él no. Para evitar esto los CA's se certifican unas a otras en base a dos modelos diferentes:

a. El modelo *jerárquico,* en el que existen dos tipos de CA's. Las *CA raíz* que generan sus propios certificados y se encuentran en el punto más alto de la jerarquía, y las *CA subordinadas,* que obtienen sus certificados de sus CA padres.

b. El modelo de *certificación cruzada* de CA's, en el que las CA's se certifican unas a otras de forma bilateral.

c) Repositorio de información pública

El *repositorio* es un servicio de red que permite el almacenamiento y la distribución de los certificados (y CRL's) de una PKI. Es un servicio público, es decir, debe estar accesible por todo el mundo de modo que cualquiera pueda validar los certificados de la CA. El estándar de facto que se utiliza como repositorio es un directorio (X.500) compatible LDAP que almacena la información en forma de árbol. Este tipo de repositorio tiene numerosas ventajas:

–Las aplicaciones pueden acceder a los certificados y CRL's de forma transparente al usuario utilizando el estándar LDAP.

–Esta tecnología es escalable en cuanto a número de certificados que pueden almacenar (millones), tiempos de respuesta en accesos, búsquedas eficaces, distribución del directorio...

–Como valor añadido los directorios pueden almacenar numerosa información de la organización además de los certificados: direcciones de correo de los usuarios, teléfonos...

d) Servidores de tiempo

Son servicios de red generados por una tercera parte confiable que permiten asociar a los procesos digitales una fecha y hora. Los servidores de tiempo son claves en todos los procesos en los que el momento de realización de la transacción es de vital importancia como periodos de validez, caducidad, garantías...

e) Entidades de certificación

Españolas:

–El proyecto *CERES* (CERtificación ESpañola) liderado por la FNMT (Fábrica Nacional de Moneda y Timbre) ha creado una Entidad Pública de Certificación con el principal objetivo de asegurar las comunicaciones electrónicas de los ciudadanos con la Administración.

–*ACE* (Agencia de Certificación Española), se constituyó en 1997 con socios como Telefónica, Sistema 4B, SERMEPA y CECA. Proporciona certificación bajo SET y X.509v3.

–*FESTE* (Fundación para el Estudio de la Seguridad en las Telecomunicaciones) integrado por los Notarios, los corredores de comercio y la Universidad de Zaragoza. Aunque su vocación es realizar estudios y proyectos, también actúa como servicio de certificación.

–*CAMERFIRMA* está basado en las Cámaras de Comercio de toda Europa. Proporciona certificación bajo X.509v3.

Internacionales:

–VeriSign

–SecureNet

–Entrust

–.....

CONCLUSIONES

Parece evidente concluir que la seguridad no es un pequeño apartado más dentro de las tecnologías de la información, sino que debe abarcarlas en su totalidad. Un buen plan de seguridad debe ser integral o dejará de ser un plan de seguridad. Debe contar con todos los recursos: organizativos, humanos, instalaciones, hardware, software... además de partir de los niveles altos en la jerarquía de la organización.

En toda organización debe existir un equipo de expertos con sus herramientas preventivas y de detección, así como con sus mecanismos de recuperación y de auditoría. El mundo de la seguridad es algo vivo que debe ser continuamente evaluado y actualizado.

También parece algo ya probado que caminamos hacia sistemas que implementen de un modo u otro sistemas de clave pública en sus diversas formas. Desde los sistemas operativos hasta los sistemas de autentificación, pasando por las

comunicaciones, el correo, los ficheros, etc. No todo el mundo precisa de una tarjeta inteligente para realizar sus operaciones (aunque el precio actual de esta tecnología la ha puesto al alcance de cualquier organización), bastaría con un sistema software que almacene las claves pública y privada.

Pero más importante que el sistema que se implemente es tener una buena cultura de seguridad en la que se encuentren implicados todos los estamentos de la organización. De nada sirve tener sistemas protegidos por contraseñas, encriptaciones pesadas o cualquier otro sistema, si un usuario deja su equipo encendido durante toda la noche.

RECURSOS Y BIBLIOGRAFÍA

1. Los estándares en la tecnología de clave pública los publica PKCS (Public Key Cryptography Standars) creados por RSA laboratories en colaboración con Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom., Novell y Sun.

   http://www.rsasecurity.com/rsalabs/pkcs/"

   -PKCS#1: algoritmo RSA.

   -PKCS#3: algoritmo Diffie-Hellman.

   -PKCS#5: algoritmos basados en contraseña.

   -PKCS#6: certificado extendido X.509v3.

   -PKCS#9: atributos de los certificados extendidos.

   -PKCS#7: mensajes firmados digitalmente (respuesta con certificado).

   -PKCS#8: información de clave privada.

   -PKCS#10: petición de certificado.

   -PKCS#11: API (Cryptoki) de interface de acceso a dispositivos físicos que almacenan información criptográfica y realizan funciones criptográficas (smart cards ó PCMCIA).

   -PKCS#12: formato para guardar o transportar claves privadas, certificados u otros secretos.

2. La revista Kriptopolis publica en esta página algunos libros muy interesantes:

   http://www.Kriptopolis.com/pubs.html

3. INDRA dispone en la web de varios números de su Boletín Interno Tecnológico en los que aparecen interesantes aportaciones sobre el tema de la seguridad.

   http://www.indra.es/webindra/castellano/noticias/bit.htm

LA GESTIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y DE LAS COMUNICACIONES

Juan Antonio Pérez-Campanero Atanasio

Jefe de Negocio Electrónico. Telefónica de España, S.A.U.

INTRODUCCIÓN

Con los últimos planes respecto a las Tecnologías de la Información y las Comunicaciones, plasmados en la Iniciativa INFOXXI de la Administración, el crecimiento del parque informático y de soluciones basadas en las comunicaciones crecerá exponencialmente en los próximos años. Uno de los ámbitos de la sociedad que más se está viendo afectado es el entorno sanitario donde se esperan, y ya se están produciendo, importantes inversiones en estas tecnologías.

Pero la proliferación de estas tecnologías, además de ofrecer infinitas posibilidades para la Sanidad en todos sus aspectos, conforma un ambiente perfecto para la actuación de desaprensivos que, basados en el anonimato, intentan acceder a la información existente en estos sistemas, casi siempre con fines delictivos o destructivos...

Son muchas las violaciones que se pueden producir en los sistemas informáticos por usuarios que, sin tener acceso permitido, logran entrar en los mismos para obtener información confidencial, pudiendo incluso manipularla en su beneficio o destruirla, o utilizarla contra terceros. Sin duda la información clínica es altamente sensible y así lo ha reconocido el Reglamento de Junio de 1999 que desarrolla la LORTAD, que considera que debe ser protegida con el más alto grado de seguridad.

Entendemos por **seguridad informática** el conjunto de actividades y medidas orientadas a la protección de la información contenida en los sistemas e instalaciones informáticas frente a su posible destrucción, modificación, utilización y difusión indebidas.

Ahora bien, los procedimientos de seguridad no sólo deben prever posibles transgresiones de usuarios desaprensivos, sino que deben tener en cuenta los posibles errores producidos por un incorrecto funcionamiento del hardware, o bien prevenirse contra acciones involuntarias que pudieran atentar contra el buen estado de la información contenida en el sistema, o aquellos que pudieran deberse a causas de fuerza mayor, como pudieran ser inundaciones, incendios...

Otro problema de la seguridad de los sistemas de información son los virus. Consisten en un pequeño código, normalmente destructivo, que puede ser "contagiado" de un sistema a otro con el único fin de que al activarse destruya la información contenida en la memoria del ordenador y en los discos, ya sea total o parcialmente.

Aunque siempre son noticia los casos espectaculares de penetración en grandes sistemas, han sido contadas ocasiones en las que un intruso ha conseguido penetrar en un sistema que sea realmente seguro, planificado de una manera adecuada; pero la mayoría de las veces bien por falta de presupuesto, bien por desconocimiento, o bien por una mala planificación del sistema, no se tiene en cuenta las necesidades de seguridad del sistema escatimando recursos que a la larga resultan ser más costosos que si se hubiesen previsto desde el principio.

Indudablemente, todos los mecanismos se complementan entre sí, persiguiendo el objetivo de que si un individuo logra saltarse algunas de las protecciones de un tipo, se encontrará con otras nuevas, haciendo el camino lo más difícil posible a todos aquellos transgresores que intenten penetrar ilegalmente en el sistema.

Los riesgos comunes para la seguridad de los sistemas de la información y de las comunicaciones son:

1. *Acceso no autorizado:* una persona consigue acceder al sistema de información (lo que se suele conocer como "penetración"), o bien teniendo permiso para utilizar el sistema con un propósito determinado, lo utiliza con otro distinto.

2. *Caballo de Troya:* cuando una persona deja dentro del sistema algún mecanismo para facilitar futuros ataques.

3. *Monitorización de las comunicaciones:* para obtener información confidencial sin necesidad de acceder al sistema, es decir, interceptar la comunicación entre dos personas.

4. *Simulación:* para engañar al verdadero usuario de manera que se obtiene su contraseña para posteriormente poder entrar en el sistema.

5. *Denegación de acceso:* cuando un usuario legítimo, al intentar acceder a información a la que está autorizado, el sistema le deniega el acceso.

6. *Repudio:* cuando una persona u organización envía a otra cierta información, y posteriormente niega haberla enviado.

7. *Rastreo:* Se presenta cuando un usuario recorre el sistema intentando encontrar un punto débil del sistema y obtener información que no debía.

8. *Prueba y error:* En los sistemas en que el acceso al sistema esté basado en una contraseña, un usuario puede intentar el acceso constantemente probando diferentes combinaciones hasta encontrar la que es correcta. Esta tarea parece bastante difícil pero puede ser realizada fácilmente teniendo en cuenta que muchas de las contraseñas suelen referirse a datos personales del usuario que la posee, por lo que

son relativamente sencillas de descubrir. Así mismo, también puede ser buscada por medio de un ordenador que se conecta al principal, y por medio de un programa buscar continuamente la contraseña hasta lograr encontrarla.

9. *Obtención de contraseña:* Un usuario deja ejecutándose un proceso sobre una pantalla idéntica a la que muestra el sistema para pedir los datos de autentificación del usuario, de manera que cuando éste los escribe son capturados por el proceso almacenándolos en un fichero, acabando su ejecución y terminando la sesión del usuario. Posteriormente el propietario del programa espía podrá leer los datos de identificación del usuario para utilizarlos y poder acceder a sus datos.

10. *Abortar programas:* Muchos sistemas permiten al usuario abortar un programa por medio de teclas de control como, por ejemplo, <control>-C, de manera que una vez abortado un programa, el usuario queda con los privilegios y características del propietario del programa que se estaba ejecutando, pudiendo acceder a sus datos, e incluso al sistema.

11. *Gusanos y Bombas lógicas:* Normalmente se pueden introducir este tipo de programas por medio de las líneas de comunicaciones existentes entre ordenadores.

Todos los problemas relativos a la seguridad de los sistemas informáticos podemos resumirlos agrupándolos bajo cuatro grandes aspectos, atendiendo a la manera en que deben ser tratados:

1. *Violación de la privacidad de la información:* Se produce cuando un usuario hace uso ilegal de una información a la que tiene acceso o bien cuando un individuo que no tiene acceso a la misma consigue obtenerla y robarla. Se puede lograr a través de diversos mecanismos, como los Caballos de Troya, u objetos descargables a través de Internet (Actives, Applet Java, scripts...), ejecución de programas para acceso a determinados ficheros.

2. *Destrucción o modificación de la información:* Este es el caso de la pérdida de información en el sistema ya sea por errores en el funcionamiento del sistema o por acciones de sabotaje. Se puede llevar a cabo por medio de programas destructores como puedan ser los virus, o por acciones específicas para destruir información concreta...

3. *Hacer uso de los servicios sin autorización:* Cuando un usuario intenta "engañar" al sistema con el fin de utilizar servicios que en condiciones normales no podría utilizar. Se lograría a través de los mecanismos ya recogidos en los dos puntos anteriores, así como a través del uso de direcciones “ilegales” o permitidas por el sistema, insuficiente prot4ección o privilegios por parte del Sistema Operativo...

4. *Controlar el sistema:* bloqueando o inutilizando alguno de los servicios del sistema para que no puedan ser utilizados por otros usuarios, o tomando el control absoluto del sistema o, incluso, desviar el acceso de los usuarios hacia un servicio controlado por el transgresor.

El FBI y el CSI (Computer Security Institute), en el año 2000 han realizado un informe en el que se recogen las formas habituales de ataques a los sistemas de información (Figura 3) y el incremento respecto al año anterior, observando que en general es de un 29% respecto al año 1999.

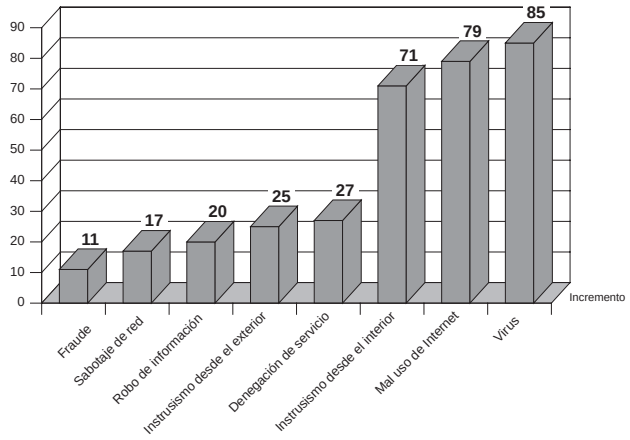


Figura 1. Ataques a un sistema de información (Fuente FBI/CSI)

En cuanto a los puntos críticos en un sistema, referente a la seguridad del mismo, podemos resumirlos en dos:

6. *Sistema Operativo y aplicaciones:* la forma de identificación de usuarios, normalmente basado en nombre y contraseña, pero con débil protección real, errores en la configuración y en su funcionamiento, que pueden abrir brechas en el sistema y permitir accesos indeseados y, por supuesto, los virus que es la principal plaga en cuanto a trasgresión de las defensas del sistema se refiere.

7. *Redes de comunicaciones:* Ataques a través de las líneas de comunicación aprovechando las facilidades o servicios, y la sencillez en cuanto a seguridad se refiere de muchos de los protocolos de comunicaciones, como pudiera ser el TCP/IP profusamente empleado en Internet, así como el acceso a servidores FTP que permiten en muchos casos entrar en el propio servidor y trabajar dentro de él.

REQUISITOS DE SEGURIDAD

El entorno donde se instalará el sistema de información deberá reunir ciertas características con el fin de asegurar que, bien el acceso de personas no autorizadas, bien el mal estado del propio sistema, o bien la destrucción de la información por fuerzas de causa mayor como pueden ser incendios, inundaciones, etcétera, causen los menores daños posibles, intentando que estos lleguen a ser nulos.

Pero en necesario que la institución donde se intenta implantar las medidas de seguridad tenga una política de seguridad impulsada por la propia Dirección, pues cualquier decisión tomada a nivel de servicio estará abocada al fracaso si no tiene el apoyo explícito de la Dirección.

En cuanto a la puesta en marcha de un sistema de seguridad podemos basarnos en las directrices definidas por diferentes organismos de normalización, cuyo principal exponente es la Organización Internacional de Normalización (OSI) que dicta normas referentes a las líneas generales sobre seguridad (control de acceso, autentificaciones, confidencialidad, integridad, rechazos y auditoría), arquitectura y mantenimiento, así como a la infraestructura de los sistemas de información.

El modelo definido por OSI se basa en el de referencia de siete niveles para la interconexión de sistemas abiertos. Dentro de los procesos de autentificación se trata el control de accesos a directorios, el servicio de autentificación general, y los servicios y protocolos para establecer dicha seguridad.

En cuanto a la arquitectura se tienen en cuenta los aspectos de administración de los sistemas de autentificación, control de accesos y auditoría, incluyendo la gestión de conexiones, la gestión de protocolos y la gestión de claves de cifrado. No obstante no cubren aspectos de seguridad importantes como son los sistemas de comunicaciones, tratamientos de eventos de seguridad y su recuperación en el caso de que se produzcan, la seguridad en las bases de datos, en los sistemas operativos, etcétera, por lo que cada instalación tendrá soluciones diferentes.

En el momento de instalar un sistema y haber decidido invertir en el establecimiento de unos mecanismos de seguridad, una cuestión que deberíamos plantearnos es: ¿cuál debe ser el nivel de seguridad de nuestra instalación? La contestación dependerá de la importancia que tenga la información y los recursos que compongan el sistema y que, por tanto, haya que asegurar ya que no será lo mismo un sistema informático bancario, que los que contengan información que afecte a la seguridad del estado, o que aquellos destinados al desarrollo de aplicaciones informáticas comerciales, o al uso doméstico.

Es necesario diseñar un **Plan de Seguridad Informática** que nos permita establecer los mecanismos de protección adecuados, así como los procedimientos a

realizar en caso de que se produzca la trasgresión. Se deberían cubrir al menos los siguientes aspectos:

–Seguridad externa o física.

–Seguridad interna o lógica.

–Seguridad funcional.

Una vez implantados y definidos los planes, habrá que realizar un seguimiento de los mismos con objeto de comprobar si funcionan adecuadamente o hay que modificarlos o completarlos. Es decir, llevar a cabo una **auditoría** de la seguridad del sistema.

Este seguimiento se deberá basar en mediciones cuantitativas que proporcionen datos estadísticos suficientes para poder fijar aquellos valores a partir de los cuales se pueda asegurar que se ha producido un intento de violación del sistema. Por otro lado, estos datos siempre podrán ser estudiados con el fin de mejorar y adecuar el sistema a las necesidades de los usuarios.

La auditoría consistirá en acciones para comprobar que los mecanismos de seguridad implantados están correctamente planificados, realmente puestos en marcha y actualizados de acuerdo con las necesidades cambiantes de la instalación y de los usuarios. Estas auditorías se deberán realizar periódicamente, de manera que los métodos y formas de las mismas deberán estar clara y completamente recogidos en el plan de seguridad del sistema.

SEGURIDAD EXTERNA

La seguridad externa hace referencia a todos aquellos mecanismos dirigidos a asegurar la inviolabilidad del sistema informático en cuanto a las posibles intrusiones que pudieran producirse sin intervención del sistema, o fallos o errores que, debiéndose al sistema, no pueden ser controlados por el mismo. Para ello dividiremos su estudio en dos apartados, que no son independientes entre sí: *Seguridad física y seguridad de personal.*

Seguridad física

Tiene por objeto la protección contra los desastres y se lleva a cabo por medio de mecanismos de detección contra incendios, humos; o protecciones eléctricas contra sobretensiones, grupos electrógenos o baterías para prevenir fallos de tensión ineducados...

Otro aspecto importante serían las condiciones del medio ambiente, como pueden ser la temperatura, la limpieza, la pureza y humedad del aire, la electricidad estática, etcétera. Para adecuarlo lo mejor posible se instalan falsos suelos, aire acondicionado, ventilación, control de la humedad y otras medidas de limpieza y acceso que impidan que dichas condiciones se modifiquen peligrosamente.

Normalmente todos estos mecanismos son costosos y en muchos casos ignorados al suponer que difícilmente se pueden presentar dichos problemas, pero con que se presenten una sola vez, el daño puede ser enorme, superando con mucho el ahorro que hemos obtenido al escatimar en dichos sistemas.

Seguridad de personal

Se deben prever los mecanismos con que dotar a las instalaciones informáticas con el fin de impedir o, al menos, entorpecer el acceso físico de las personas a las instalaciones. Esto se suele llevar a cabo mediante puertas con llaves especiales, mecanismos electrónicos de apertura por clave secreta, huellas digitales, voz, etcétera, incluso hay experiencias de control de acceso a través del reconocimiento del iris, pero en la mayoría de las instalaciones del entorno sanitario no sería necesario llegar a estos extremos de seguridad.

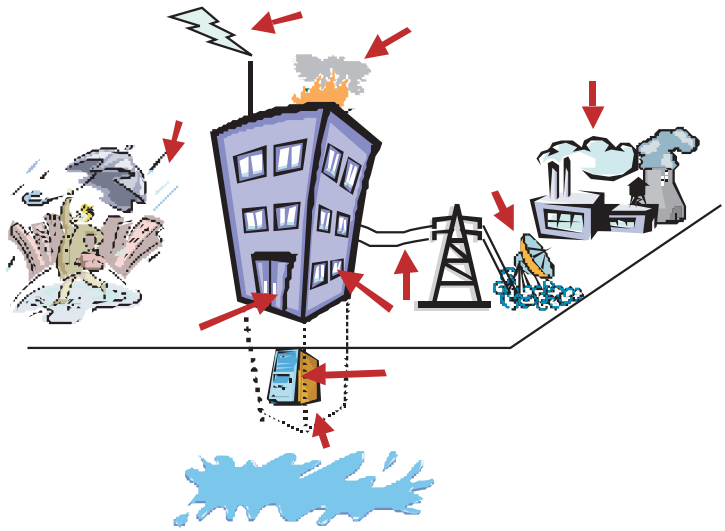


Figura 2. Seguridad externa

SEGURIDAD INTERNA

Suponiendo que los mecanismos de seguridad externa establecidos en la instalación informática sean suficientes para evitar que cualquier extraño pueda tener acceso al sistema, el resto de mecanismos relacionados con la seguridad deberán estar encaminados a asegurar que los usuarios del sistema, o incluso que los pocos individuos que hayan logrado transgredir las barreras impuestas por los mecanismos de seguridad externa, no puedan manipular la información contenida en el mismo para la cual no estén autorizados.

Administración de usuarios

Los mecanismos para llevar a cabo este nivel de seguridad se basan en la *autorización* de acceso al sistema. El acceso se reduce a los intentos que se pudieran realizar desde un terminal del sistema, o bien desde otro sistema a través de una red de comunicaciones a la cual estén conectados los dos.

Este tipo de problemas no sólo exige que el sistema esté dotado con mecanismos de detección de posibles intrusos, sino que además será necesario que el administrador compruebe constantemente si ha habido intentos de penetrar en el sistema o no, así como si ha tenido éxito o no en caso de que los hubiera habido.

El sistema dota al Administrador de facilidades para gestionar el movimiento y contabilidad de los usuarios de manera que, al darlos de alta, les asignará a cada uno un **nombre** y una **contraseña** que irán asociados entre sí. Mientras que el nombre puede ser público, la contraseña no, siendo el verdadero mecanismo de seguridad.

Esta contraseña o *password* la asigna el Administrador del sistema, junto con el nombre y toda aquella información necesaria para llevar a cabo la contabilidad y gestión de dichos usuarios dentro del sistema. También asignará al usuario los derechos y privilegios de acceso a los distintos recursos del sistema.

En el caso de permitir el uso de cierta información contenida en nuestro sistema de información, se pueden utilizar contraseñas-de-un-solo-uso (one-time-password), que una vez utilizadas quedan inservibles y no se pueden volver a utilizar.

El sistema registrará todos aquellos intentos de acceso indebidos o infructuosos, con el fin de que el Administrador del sistema pueda estudiarlos posteriormente.

La contraseña se suele almacenar en el sistema de manera que no sea legible directamente por los distintos usuarios, e incluso, en algunos sistemas, ni siquiera por el administrador, que sólo podrá borrarla y asignar una nueva. Es decir, la contraseña suele *codificarse* o *encriptarse*.

Hay sistemas con necesidades más fuertes de seguridad que exige dos contraseñas asociadas a un nombre para permitir el acceso, y además los servicios del sistema permiten que cada usuario cambie su contraseña cuando así lo desee. En otros, se obliga a que la contraseña sea cambiada con una determinada periodicidad, por ejemplo mensualmente, con el fin de que si alguien ha logrado descubrir la contraseña de un usuario, no pueda seguir accediendo al mismo.

También hay algunos sistemas que, en vez de preguntar por el nombre del usuario y una palabra que franquee el paso al sistema, establecen un **diálogo** con el usuario durante el cual éste debe contestar a varias preguntas antes de que se le conceda el acceso al sistema. Estas preguntas pueden ser nombre, fecha de nacimiento, número de D.N.I., número de Seguridad Social, etcétera.

Existen otros muchos métodos de controlar el acceso de los usuarios como por ejemplo llaves que bloqueen el terminal, acceso a través de tarjetas de banda magnética que tienen asociada una clave específica (como las tarjetas de crédito o débito), y actualmente a través del reconocimiento de la voz del usuario, o de la huella digital, o de la firma, pero estos últimos son muy costosos de poner en práctica y además pueden considerarse como mecanismos de seguridad externa. Un nuevo sistema de control de acceso, y que será el que seguramente se termine imponiendo en el futuro es la tarjeta inteligente en la que además de los datos del usuario, se encuentra el certificado y lleva un procesador criptográfico para cifrar dicha clave, y permitir establecer comunicaciones seguras.

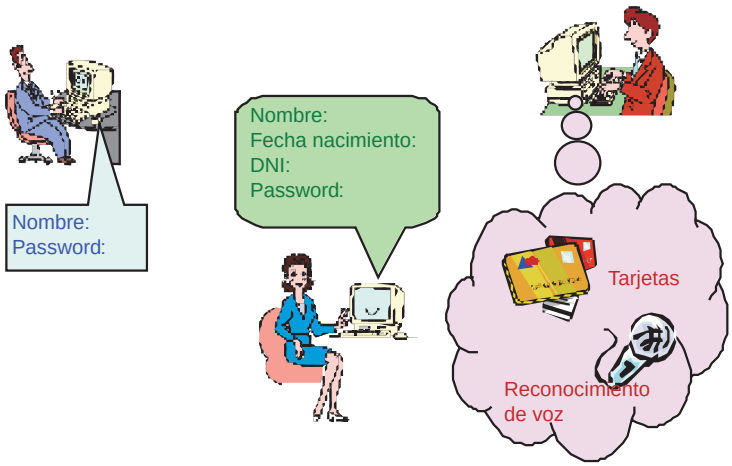


Figura 3. Tipos de protección de acceso de los usuarios

Seguridad en los ficheros

La finalidad última de los ordenadores es el tratamiento de la información que se almacena permanentemente en los ficheros. La pérdida o alteración indeseada de dicha información causaría trastornos que podrían ser irresolubles en algunos casos.

Pensemos en un ordenador en cuyos ficheros se halla almacenada la información operativa de un hospital (historias clínicas, proveedores, contabilidad, nóminas, etcétera). Si por cualquier razón, accidental o provocada, se destruyese dicho equipo, sería fácil reponer el hardware (bastaría con comprar otro) aunque resulte oneroso, pero sería imposible recuperar la información contenida en sus ficheros (la más importante de la entidad) si previamente no se han tomado las medidas adecuadas.

La seguridad de los ficheros, es decir, de su contenido, se debe enfocar bajo tres aspectos:

8. **Disponibilidad** de la información, es decir, los ficheros tienen la información prevista y se puede acceder a ella.

9. **Privacidad** de la información, o control de acceso a dichos ficheros.

10. **Integridad,** es decir, la información debe ser consistente, fiable y que no pueda ser manipulada.

Por lo tanto, los derechos de los usuarios o de sus procesos debe ser restringido en cuanto al acceso a los ficheros. Sin embargo, los ficheros son un medio indispensable de compartir información entre los usuarios, si así lo desean, por lo que dichas restricciones deberían ser selectivas.

Disponibilidad de los ficheros

El objetivo fundamental es lograr que los usuarios dispongan de la información que han almacenado en el sistema cuando la necesiten.

La técnica básica consiste en obtener, periódicamente, copias del contenido de los ficheros de forma que si se destruyeran éstos, podría recuperarse la información correspondiente a partir de dichas copias. La operación de realizar esta *copia de seguridad* o *back-up* se suele realizar mediante programas de utilidad del sistema que permiten así mismo la recuperación de la información contenida en tales copias.

La fiabilidad de la información contenida en las copias dependerá de la periodicidad con que se realicen éstas en relación con el ritmo al que se actualicen los ficheros, y que debe definir el Administrador del Sistema.

Estas copias se suelen realizar en cintas magnéticas que se guardan en lugares alejados del sistema o incluso en otras dependencias o salas y, normalmente, en armarios preparados especialmente contra incendios que puedan soportar altas temperaturas sin que se destruya el contenido de los mismos. De esta forma, si en alguna ocasión, la información del sistema quedase destruida, sería fácil reponer la información original a partir de estas copias.

En algunos casos, la importancia y continua utilización de algunos ficheros obliga a mantener copias en disco de los mismos de tal forma que, en realidad, estarán duplicados. Lógicamente, estas copias deberán estar almacenadas en discos distintos por si se destruyera el disco original poder utilizar las copias existentes en el disco donde se almacenen las copias.

Privacidad de los ficheros

El contenido de los ficheros se debe proteger de posibles accesos ineducados. Entre el peligro de permitir a todos los usuarios acceder a cualquier fichero, y la rigidez de permitir a cada uno acceder sólo a los suyos, el sistema de protección debe permitir los accesos de forma controlada, según unas reglas predefinidas.

En cualquier sistema informático siempre existirán *sujetos* o entidades que desean acceder a *objetos*, es decir, información y recursos. En el caso real, los sujetos siempre serán los usuarios o procesos y los objetos serán los distintos recursos y los ficheros que contengan la información deseada por dichos sujetos. El *modo de acceso* de los sujetos sobre los objetos será determinante y por tanto una característica importante a tener en cuenta.

Normalmente cada recurso tendrá unos modos de acceso definidos por el hardware y por su propia operación. En cambio, los modos de acceso que se pueden realizar sobre los ficheros pueden ser muy diferentes de un sistema a otro ya que son definibles y dependen extraordinariamente del diseño y finalidad de dicho sistema. Los modos de acceso más comúnmente definidos son los siguientes:

Derecho de acceso	Modo de acceso
Read (r)	Leer u obtener información del fichero.
Write (w)	Escribir por primera vez o modificar la información en el fichero.
Execute (x)	El fichero es la imagen de un programa y puede ser ejecutado. Este modo es diferente al de lectura ya que en este modo, el fichero sólo puede ser leído para su ejecución, pero nunca podrá ser copiado si no se tiene además el derecho de lectura.
Delete (d)	Borrar el fichero.

SEGURIDAD FUNCIONAL

Bajo este epígrafe se tratan las cuestiones relacionadas con la propia funcionalidad de los sistemas de información y que, no siendo ni aspectos de seguridad interna ni externa, están relacionados con ambos. Es decir, hablaremos de los problemas de seguridad que suscitan las líneas de comunicaciones, y el funcionamiento anormal del propio sistema debido a fallos y caídas.

Seguridad en la transmisión de datos

Cuando se envían datos por las líneas de comunicaciones, existen diversos problemas de seguridad debido a la relativamente fácil violabilidad de dichas líneas que se escapan a nuestro control directo. Por ello, para enviar datos entre ordenadores se utilizan diversas técnicas encaminadas a dotar de la mayor seguridad posible a los mensajes transmitidos.

Los programas de comunicaciones normalmente ofrecen facilidades básicas de seguridad, cuya finalidad es asegurar que los bits que salen de un ordenador llegan intactos al otro. Como ejemplo podemos citar algunas de las técnicas más utilizadas:

1. *Bit de Paridad:* Es un bit que se añade a cada octeto o palabra que se envía por la línea de comunicaciones de manera que será un 1 si el número total de bits a 1 del octeto o palabra es par, y 0 si es impar. Esta política se conoce como *paridad par,* siendo paridad impar en el caso contrario. Cualquier palabra u octeto con error en uno de sus bits presentará una paridad incorrecta, pudiendo ser detectada. El único problema es que si se dieran dos errores en la misma palabra, no se detectarán ya que la paridad obtenida será la misma que en el octeto o palabra original, pero la probabilidad de que esto ocurra es bastante baja.

2. *Distancia de Hamming:* Si la probabilidad de que se produzcan errores dobles en cada octeto o palabra es alta, deberemos pensar en un mecanismo que nos permita evitarlo. Para ello añadiremos más bits de seguridad a esta unidad básica de información de manera que, no sólo puedan ser detectados los errores, sino además corregidos.

El cubo de la Figura 4 fue usado por R.W. Hamming para ilustrar este concepto. Se define la distancia de Hamming como el número de posiciones de los dígitos que hacen que dos estados difieran entre sí.

Por ejemplo, si se transmitieran tres bits, la distancia de Hamming mínima permitida será 1, permitiéndose en este caso, los ocho posibles códigos definidos por los tres bits, es decir podría ser cualquier vértice del cubo de la figura 4.

Lógicamente esta solución hace que cualquier código recibido sea correcto y por lo tanto no se podría detectar ningún error. El extremo opuesto sería utilizar sólo los códigos 000 y 111 como válidos de manera que el resto de códigos indicasen error. En este caso para llegar del vértice 000 al 111 del cubo es necesario pasar por dos esquinas, por lo que la distancia de Hamming sería 3.

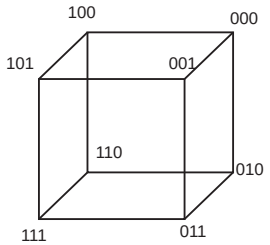


Figura 4. Cubo de Hamming

3. *Código de Redundancia Cíclica (CRC):* En el caso de que los daños esperados no sean en un bit de una unidad de información (octeto o palabra), sino en una secuencia es estos, de tal manera que invalidaría el mensaje completo, se utiliza un contador que recoge la suma de los resultados de aplicar un determinado algoritmo a cada octeto, conociéndose dicha suma como *Suma de Chequeo* o *Checksum.* Al recibir el mensaje se trata con el mismo algoritmo, y si el resultado es el mismo que el de la suma recibida, el mensaje se considera válido.

4. *Control dos entre tres:* Si deseamos transmitir una información concreta, por ejemplo, una A, ésta se transmitirá repetida tres veces de manera que en el receptor se supondrá como correcta la que se haya repetido más veces de las tres recibidas

5. *Códigos autodetectores del tipo p de n:* Corresponden a una codificación con *n* bits sabiendo que se está obligado a no utilizar más que los códigos para los que sólo *p* bits de ellos tienen el valor 1. Tiene el inconveniente de no detectar los errores dobles.

Desde el punto de vista de accesos indeseados, el sistema se puede ver amenazado por diversos tipos de ataques a la seguridad del mismo y de la información que contiene. Podemos resumir los distintos tipo de ataques en cuatro:

a) *Destrucción de la línea,* debido a un corte físico en la misma, a la destrucción del ordenador receptor, o del emisor...

b) *Escucha de la línea:* "pinchando" la misma un usuario no autorizado y obteniendo una copia de la información transferida. Es difícil de detectar, y la única forma de combatirlo es por medio del cifrado de los mensajes.

c) *Modificación de los mensajes:* cuando una entidad no autorizada recibe la información, la manipula y la retransmite modificada con el fin de engañar al receptor

d) *Generación de mensajes* por usuarios desaprensivos y no autorizados que envían información a un ordenador simulando que la ha enviado otro del que dicho receptor espera recibir datos.

Los servicios de seguridad que los sistemas de información actuales ofrecen para combatir los accesos indeseados anteriormente descritos los podemos resumir en:

a. ***Autentificación:*** identificándose el origen del mensaje y así pueda asegurar el destino que el mensaje es de quien está esperando. Actualmente se suele basar en sistemas de *firma digital.*

b. ***Integridad:*** asegura que el mensaje es totalmente correcto, de manera que sólo pueda ser manipulado por usuarios autorizados. Se basa en las técnicas anteriores de bit de paridad...

c. ***Control de acceso:*** que requerirá la autentificación del usuario que desea acceder al sistema y fijar permisos y privilegios para que sólo pueda acceder a la información prevista.

d. ***Confidencialidad:*** que asegura que a la información sólo acceden aquellos que lo tengan permitido. Va ligado a los permisos y privilegios mencionados en el control de acceso.

e. ***Certificación:*** de los mensajes enviados y recibidos, para que el origen así reconocido no pueda negar nunca que envió un determinado mensaje. Es una actividad similar a la que ejecuta un Notario en la vida real.

La mayoría de ellos necesitan utilizar técnicas criptográficas y de cifrado para alcanzar el objetivo fijado. La criptografía, por su importancia actual, la tratamos en un apartado posterior.

Sistemas tolerantes a fallos

Estos sistemas, ante un mal funcionamiento, consiguen recuperarse y continuar operando correctamente, sin perjuicio para la información tratada y almacenada por ellos. Este tipo de sistemas también se conocen como **Sistemas Redundantes.**

En general, en estos sistemas es transparente para los usuarios la recuperación del sistema ante la presencia de un fallo o mal funcionamiento ya que tendrán la

impresión de que ha estado funcionando continuamente sin la existencia de interferencias. Este tipo de sistemas se basan en ordenadores multiprocesador.

El grado de redundancia puede ser tan elevado como se desee, pero se deberá estudiar si realmente es necesario y práctico para la instalación y el tipo de información que se va a almacenar. Se deberá obtener información clara de las partes del sistema que pueden presentar problemas con el fin de reforzaras. Podemos resumir como más frecuentes los siguientes fallos:

–Problemas en los discos magnéticos.

–Errores de instalación de los discos.

–Errores de paridad en la memoria.

–Errores en el procesador: es raro que se presente, aunque con los actuales sistemas multiprocesador, este problema está resuelto.

Para resolver el problema de los discos se suele utilizar un sistema de discos en espejo, donde los datos se copian a una unidad adicional que queda oculta a los usuarios. En el caso de un funcionamiento incorrecto del disco principal, la unidad de disco de reserva tomaría automáticamente el control pudiendo hacerlo sin traumas al contener actualizada toda la información existente en el disco principal.

En cuanto al mal funcionamiento de la memoria se trataría de una forma similar a la de los discos espejo, pero ahora instalando dos memorias iguales, una principal y otra de reserva.

Criptografía

Cifrado es la transformación que se puede aplicar a los datos para ocultar su contenido. Intenta asegurar que nadie pueda leer los datos si no es el destinatario de la información. Se conoce como *texto claro* a la información antes de ser cifrada, es decir, que puede ser leída directamente sin ningún procesado previo. Así mismo, se conoce con el nombre de *texto cifrado* aquel que ha sido sometido a algún tipo de procesado y por tanto no puede ser leído directamente necesitándose algoritmos especiales para su descifrado y su posterior lectura.

Normalmente un algoritmo de cifrado suele tener asociado un algoritmo de descifrado para obtener la información original, por ejemplo, se podrían rotar todas los caracteres ASCII que componen un mensaje sustituyéndolos por los correspondientes a 10 caracteres más adelante, es decir, cada 'c' se sustituiría por una 'm' y así sucesivamente. Lógicamente este tipo de cifrado es demasiado sencillo por lo que se suelen emplear algoritmos más sofisticados.

Dicho de otro modo, el texto claro o mensaje a enviar M se procesa con una clave de cifrado Ko, para obtener el mensaje cifrado C, que es el que se envía y recibe en el destinatario, el cual procesa dicho mensaje con una clave de descifrado Kr para obtener el mensaje original M (ver figura 5)

Figura 5. Proceso de cifrado y descifrado

Si la clave Ko = Kr, se dice que es un sistema de **cifrado simétrico,** mientras que si no son iguales, será de **cifrado asimétrico.** El problema del cifrado simétrico es que la clave debe ser conocida tanto por el receptor como por el remitente, por lo que debe haber sido transmitida antes por un canal secreto, y que sin duda puede tener los mismos problemas que cualquier mensaje, además de los retardos que introduce necesariamente en el procesado de los mensajes, al necesitar dicha comunicación previa y secreta.

Debido al coste y retardos introducidos por la clave secreta, la Universidad de Stanford (1976) introdujo el concepto de clave pública, donde se utilizan partes de clave complementarias para separar los procesos de cifrado y descifrado. La clave, pues, tiene dos partes, una privada y secreta, y otra pública, de forma que aún conociendo la parte pública es imposible deducir la privada.

La mayoría de los sistemas que utilizan algoritmos de cifrado, exigen que el texto cifrado se pueda convertir en texto claro. Para ello existen diversas técnicas entra las que cabe destacar:

6. El **“or-exclusivo”** obtiene el texto cifrado al aplicar a cada octeto que compone la información la operación “or exclusivo” con una “clave” cuya longitud debe ser al menos tan larga como el mensaje. El algoritmo de descifrado es idéntico al de cifrado y utiliza la misma clave, la cual deberá cambiarse periódicamente ya que en caso contrario, cuanto más tiempo esté siendo utilizada, más fácil será de descubrir. Ya que el creador y el receptor del texto cifrado deben conocer la clave, ésta también debe ser transmitida, por lo que se crea un verdadero problema de seguridad al tener que diseñar algoritmos que cambien la clave constantemente sin seguir una pauta que sea fácil de adivinar.

7. El **Estándar de Encriptado de Datos** (DES - Data Encryption Standard) que fue desarrollado por la Oficina Nacional de Estándares de Estados Unidos, y es uno de los más utilizados actualmente. El algoritmo se suele suministrar en un chip especialmente construido para este fin, aunque también podría ser diseñado por software perdiendo una gran eficiencia en su ejecución, pero abaratando su utilización. Trabaja con bloques de datos de 64 bits y se basa en claves de 56 bits de longitud, habiendo suficientes posibilidades para elegir claves irrepetibles y difíciles de descubrir, aunque pueden darse casos de claves débiles o semidébiles que diesen cifrados fáciles de deshacer. Según las últimas investigaciones realizadas se piensa que con claves de unos 100 bits sería suficiente para asegurar que no existan claves débiles o, al menos, reducir sensiblemente el riesgo de ellas. En este caso la misma clave se utiliza para cifrar y descifrar al igual que en el método anterior.

El proceso de cifrado ejecuta una permutación inicial al texto en claro, y aplica 16 veces una función que depende de la clave. El algoritmo se basa en permutaciones, sustituciones y sumas en módulo 2. El algoritmo es el mismo para cifrar y descifrar.

Con el método DES, la clave de ambas partes es la misma y conocida (clave pública), pero esta situación compromete la seguridad de la misma.

8. **IDEA (International Data Encrypton Algortihm)** es un sistema de cifrado convencional más seguro que el DES. Es un algoritmo de bloques de 64 bits que utiliza una clave de 128 bits. Es un sistema, igual que el DES, de clave pública y simétrico.

9. El **método RSA** conocido con este nombre por sus inventores (Rivest, Shamir y Adelman), consiste en que cada estación tenga dos claves, una para el cifrado y otra para el descifrado, de manera que una es pública y la otra privada. Por ejemplo, si un usuario desea enviar un mensaje privado a otro, se busca la clave pública del destinatario y se cifra el mensaje con dicha clave pero el descifrado del mensaje sólo podrá ser realizado por el usuario receptor utilizando su clave privada

El algoritmo de RSA está muy extendido pero presenta problemas de lentitud si se aplica a mensajes de texto, estando más orientado a cifrar una clave DES que irá al principio del mensaje y que será con la que se habrá cifrado el resto del mensaje., lo que permite cambiar la clave con cada mensaje que se envía alcanzando una mayor seguridad en las transmisiones. Este es el caso del **PGP** (Pret Good Privacy) utilizado en Internet y que se basa en el algoritmo IDEA para transmitir el mensaje y la clave la envía cifrada con RSA.

De forma similar trabaja el **PEM** (Privacy Enhanced Mail) de Internet y con valor legal que no tiene el PGP, y que se utiliza para dotar de seguridad a las apli-

caciones de correo electrónico. En el PEM se pueden utilizar diversos algoritmos criptográficos, por lo que los mensajes deben enviar la identificación del algoritmo usado. Para proporcionar integridad, se añade un código aleatorio o hash calculado en Message Digest 2 (MD2) o MD5. en el caso de que se utilice RSA, el código hash sería la firma digital.

El algoritmo RSA es de cifrado asimétrico y son claves basadas en números primos y cuya longitud puede ser de 512, 1024 o 2048 bits.

10. **LUC** es otro sistema de cifrado de clave pública similar al RSA.

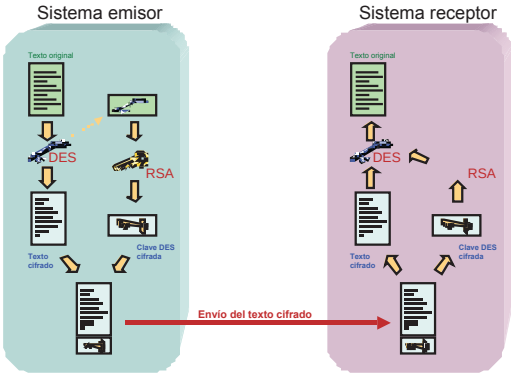


Figura 6. Algoritmo RSA de encriptación

PKI (Public Key Infraestructure)

PKI es la combinación de software, tecnologías de cifrado y servicios, que permiten proteger los mensajes transmitidos a través de las líneas de comunicación con el fin de que sean seguros, y que las transacciones comerciales a través de Internet sean seguras.

Los PKI integran certificados digitales, algoritmos de criptografía de clave pública y autoridades de certificación en una arquitectura de seguridad de redes de telecomunicación. La necesidad de utilizar PKI se basa en los siguientes puntos:

11. ***Autentificar la identidad del remitente,*** lo que se consigue a través de los certificados digitales que permiten a los usuarios individuales y organizaciones validar la identidad de cada una de las partes involucradas en una transacción.

12. Verificar la integridad de la información, y que el mensajes no se ha modificado o "corrompido" durante su transmisión.

13. Asegurar privacidad, evitando la interceptación de los mensajes.

14. Autorización de acceso, evitando tener que recordar las contraseñas, gracias a los certificados digitales.

15. Autorizar transacciones controlando los privilegios de acceso para transacciones específicas.

16. ***Asegurar el no repudio,*** al validar a los usuarios gracias al certificado digital, de manera que más tarde no puedan negar que enviaron tal mensaje o información.

Certificados digitales

Los Certificados Digitales son ficheros electrónicos que actúan como lo haría un pasaporte: son emitidos por una tercera parte autorizada (TTP), conocida como Autoridad de Certificación (CA), que verifica la identidad del poseedor del certificado.

Los certificados digitales tienen dos misiones:

1. Asegurar que sus poseedores son los que dicen que son.

2. Proteger la información transferida a través de redes de telecomunicación de robo o manipulación.

Hay dos tipos de certificados digitales:

6. Certificados de servidor: permiten a los visitantes de un sitio Internet (Web) intercambiar información personal, tales como números de tarjeta de crédito, asegurando que no son robadas, interceptadas o manipuladas. Por lo tanto, son imprescindibles cuando se trata de construir un sitio de comercio electrónico en la Red Internet.

7. Certificados personales: permiten autentificar a los visitantes y restringir el acceso a determinados contenidos de información. De igual forma pueden servir para enviar correo electrónico seguro.

El certificado es un conjunto de datos a los cuales se añade la firma digital. Así, por ejemplo, el certificado digital de VeriSign contiene:

1. El nombre del propietario y otra información que facilite la identificación, como por ejemplo la dirección de correo electrónico, ...

2. Una clave pública, que puede usarse para verificar la firma digital del remitente de un mensaje previamente cifrado con una clave privada única.

3. El nombre de la Autoridad de Certificación.

4. El periodo de validez del certificado.

Toda esta información se cifra y sella por la CA y puede ser verificado por el receptor. Así, cada vez que alguien envía un mensaje electrónico, se le adjunta el certificado digital y se cifra todo. El receptor, al recibir el mensaje, primero usa su propio certificado para comprobar que la clave pública usada por el autor es válida, y luego utiliza la clave pública para verificar el mensaje en sí mismo. El proceso completo se puede ver en la figura 7.

El formato de certificado de clave pública más extendido es el definido en el estándar X.509 de la UIT.

Autoridad de certificación

Las Autoridades de Certificación son equivalentes a lo que en la vida real son las Oficinas de Pasaportes de la Policía. Emiten los certificados digitales y validan la identidad de su poseedor, de forma que añaden una clave pública del individuo o de la organización al certificado digital de forma que al ser cifrada está resguardada de posibles manipulaciones. A la autoridad de Certificación también se la conoce como Tercera Parte Confiable (Trusted Third Party).

Además de la Autoridad de Certificación, puede existir también la Autoridad de Registro (RA) o entidad encargada de identificar de manera inequívoca a los usuarios, recibiendo las peticiones de los mismos, y gestionando la obtención del Certificado Digital correspondiente con la Autoridad de Certificación.

La autoridad de certificación basa su funcionamiento en directorios que suelen seguir o bien la norma X.500 o LDAP, de manera que recoge de forma distribuida todos los certificados expedidos, y gracias a los directorios es fácil de encontrar el certificado para su validación, siendo especialmente útil en organizaciones grandes.

En España hay varias Autoridades de Certificación, siendo las más importantes CERES y ACE, que actúan en libre competencia.

Estándares de seguridad

Son varios los protocolos de seguridad que se han definido para Internet y que están en uso, que podemos resumir de la siguiente forma:

6. SSL (Secure Sockets Layer): desarrollado por Netscape Communications Corporation es el estándar para autentificación e intercambio seguro de datos. Todos los navegadores están preparados para utilizar el método SSL de encriptación.

7. S-HTTP (Secure HTTP): es similar al SSL, pero diseñado específicamente como una extensión de seguridad para HTTP.

8. S/MIME (Secure Multipurpose Internet Mail Extensions Protocol): es el estándar para correo electrónico seguro y EDI. Utiliza el formato X.509.

9. SET (Secure Electronic Transactions Protocol): para hacer pagos seguros. Este estándar permite autentificar la identidad de los participantes en las compras realizadas con tarjetas de crédito. Utiliza Certificados Digitales para asociar al titular de la tarjeta y al comercio con las entidades financieras que intervengan y entidades de medios de pago.

Una vez que el titular de la tarjeta acepta la compra-venta, envía una orden de pago al vendedor a través de la red. El vendedor se comunica con la institución financiera correspondiente a través de una pasarela, reenviando la orden de pago para que sea autorizada, quedando desde ese momento el vendedor al margen, y entrando directamente en la transacción dicha entidad financiera. De esta manera el comerciante no tiene acceso a la información del Certificado SET y se mantiene la privacidad del proceso, evitando que posteriormente pueda hacer uso del número de tarjeta sin autorización de su titular.

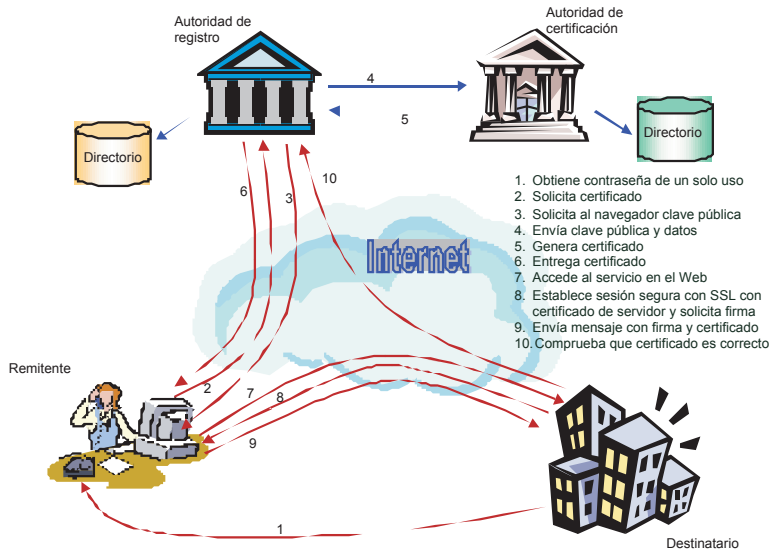


Figura 7. Proceso de transferencia de mensajes con PKI

Cortafuegos

El **cortafuegos** o **firewall** es un conjunto de componentes software y hardware destinados a establecer unos controles de seguridad en el punto de entrada de Internet a la red corporativa de la organización. Normalmente se sitúa en un servidor o en un encaminador o "router". Esto permite aislar el interior del exterior, siendo más fácil detectar los problemas de seguridad que surjan y así poder atajarlos.

Un cortafuegos actúa en los niveles de red y transporte (niveles 3 y 4 ISO de OSI) y en el de aplicación (nivel 7), con las siguientes funciones:

I. Llevar la contabilidad de las transacciones realizadas con la red.

II. Filtrar los accesos que se realicen y no estén autorizados.

III. Avisar ante intentos de penetración en el sistema, detectando posibles ataques, y ofreciendo medios de defensa contra ellos.

IV. Adicionalmente, también pueden realizar servicios de cifrado, inspección del contenido y de Redes Privadas Virtuales (VPN).

Podemos resumir el funcionamiento de los cortafuegos en torno a tres tipos diferentes:

a. ***Filtro de paquetes*** (packet filter): se establece una lista de filtros por interfaz que se aplicará a cada paquete IP independientemente de los anteriores. Estos filtros se ejecutan secuencialmente y sólo dejan pasar determinado tipo de tráfico, pero no distingue si el paquete lleva algún tipo de virus, caballo de Troya... (no actúan a nivel de aplicación)

Actúa en los niveles de Red y Transporte, con reglas basadas en el protocolo y en las direcciones de origen y destino.

b. ***Pasarelas a nivel de circuito o Filtro de paquetes Stateful:*** también se conocen como filtro de paquetes Stateful y se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red: por un lado reciben las peticiones de conexión a un puerto TCP, y por otro establecen la conexión con el destinatario deseado. Utiliza puntos conocidos y seguros para los canales de control, y puertos TCP/IP de asignación dinámica para la transferencia de datos. Es el mejor sistema, y servicios como FTP, Telnet o el correo electrónico deberán tratarse con este tipo de cortafuegos.

c. ***Pasarela a nivel de aplicación o Proxy:*** en lugar de realizar un filtrado del flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado para cada uno. El control es a nivel de aplicación y, por lo tanto, no es transparen-

te al usuario, ya que es la responsable de su identificación. Requieren un sistema operativo de propósito general, y actúan de intermediarias entre el cliente y el servicio remoto.

Suelen ser servidores de acreditación o servidores proxy, de manera que si la acreditación es positiva se establece la conexión.

Virus

Existe literatura especializada para tratar este tipo de problemas que afectan de forma importante a la seguridad de los sistemas, por ello sólo veremos someramente dicho fenómeno con el fin de llamar la atención sobre este tipo de programas que son de constante actualidad y quizás, de los más dañinos y difíciles de detectar, prevenir y corregir.

Un **virus** es un programa que lleva a cabo acciones que resultan nocivas para el sistema informático en el que actúa. Presenta las siguientes características:

1. Es capaz de generar copias de sí mismo totalmente o por partes en los medios de almacenamiento secundario, bien como fichero independiente, bien ocupando de forma oculta un bloque, sector o pista del medio en el que se almacene. Es decir, tiene la facultad de *contagiarse.*

2. Modifica los programas ejecutables en los que se encuentra, consiguiendo así una *ejecución parasitaria.* Por ello, normalmente, será ejecutado de forma involuntaria e inconsciente por el usuario.

3. Sólo puede llevar a cabo su acción si, y sólo si, su código tiene oportunidad de ejecutarse.

Las acciones que puede llevar a cabo un virus son variadas, pudiendo ir desde un mensaje constante en la pantalla, o modificaciones de las características de funcionamiento del sistema, hasta la destrucción total de la información. Hay unos virus que podrían considerarse benignos siendo su única finalidad la diversión del programador que lo diseña, y otros malignos, pudiendo ser considerados como acciones verdaderamente delictivas. En cualquier caso, teniendo en cuenta que la misión de todos ellos es perturbar el correcto funcionamiento del sistema, consideraremos a todos ellos como verdaderos atentados contra la seguridad del sistema y, por lo tanto, malignos.

Los mecanismos por los cuales un virus se introduce en un sistema informático son variados pero, normalmente, irá disfrazado dentro de algún paquete software que se copie o se reciba regalado. No obstante, en sistemas interconectados a

través de redes de comunicaciones, es frecuente el contagio de dichos virus a través de las mismas, como se puede observar por los muchos mensajes que llegan a través del correo y de los medios de comunicación de nuevos virus, cada vez más dañinos.

Existen otro tipo de programas destinados a atacar los mecanismos de seguridad del sistema que, no siendo virus propiamente dichos, se confunden con ellos y pueden tener comportamientos similares. Estos programas son:

- **Gusano:** es un programa que se desplaza por la memoria del ordenador con identidad propia. Se diferencia de los virus en cuanto a que éstos se adosan a otros programas, y los gusanos, no. Este tipo de programas buscan espacio libre en la memoria donde realiza copias sucesivas de sí mismo hasta desbordar la memoria.

El medio de difusión de estos programas es a través de las redes de comunicaciones, utilizando, normalmente, el correo electrónico.

- **Caballo de Troya:** es un programa legítimo que en su interior lleva camuflado una sección de código que hace que el paquete software verdadero se comporte de manera diferente a como debería hacerlo. Este tipo de programas no tiene funciones de autocopiado y, por lo tanto, no se puede "contagiar" a diferencia del comportamiento de los virus.

Se ha utilizado para el redondeo de cuentas bancarias y su actualización, o para la destrucción de toda la información existente en el sistema.

- **Bomba lógica** es un programa que se ejecuta al producirse un evento determinado. La condición de activación es variables y puede ser una fecha, secuencias especiales de teclas, etcétera. Normalmente su misión es destructiva.

Las técnicas empleadas en este tipo de programas también ha sido utilizada en el desarrollo de los virus, siendo ésta la razón de que se confundan entre sí. Pero, como diferencia fundamental, podemos decir que un virus siempre tiene la virtud del contagio en medio magnético, característica de la que no gozan los otros programas.

GESTIÓN DE LA SEGURIDAD

La gestión de la seguridad involucra a tres ámbitos de la institución: la organización, el entorno físico y el entorno lógico o software y de las telecomunicaciones (estos dos ya los hemos visto en la exposición anterior)

Organización

La organización general

Un Plan de Seguridad limitado a los sistemas de información y procedente de los servicios de informática no garantizará la seguridad. La informática, al constituirse en sistema de información de la institución, formará parte de su infraestructura y penetran en sus funciones, modificando las formas de trabajar y las relaciones, constituyéndose en una parte de alto riesgo dentro de dicha institución.

Por ello, la Dirección General debe desempeñar un papel de motor y de animación en materia de seguridad, aplicando el **plan estratégico de seguridad,** que dé lugar a reglamentos de régimen interior en materia de seguridad, plan de contingencia y plan de seguridad informática. Todo esto requerirá, por supuesto, la implicación de todo el personal, debiendo dedicar una especial atención a la *información,* a la *formación* y a los *ejercicios tácticos.*

Las responsabilidades deberán estar claramente definidas, así como la coordinación entre los responsables. Así, debería existir un servicio o sección de seguridad vinculado a una dirección general independiente. También deberá disponer de una responsable especialista en seguridad general y otro de seguridad informática, éste último ligado también al servicio de informática.

El control

Los controles pueden ser de dos tipos: control visual que permiten eliminar muchos riesgos de forma sencilla, y los controles de validez que se basan en ratios y estadísticas que nos indiquen o avisen de posibles riesgos inminentes, y así poder prevenirlos.

Estos controles sólo podrán realizarse si existen reglas definidas, recogidas normalmente en forma de reglamentos de régimen interior que deberán estar mantenidos diariamente y debidamente actualizados. Estas normas deben estructurarse por función, por operación, por tipo de información y por sección o importancia del riesgo.

La auditoría

En el ámbito sanitario, los hospitales de cierto tamaño deberían tener definida la función de Auditoría Interna con la misión de efectuar periódicamente revisiones para comprobar el grado de cumplimiento de la normativa interna, participando activamente en la definición de los nuevos sistemas de información para dotar-

les de las medidas de seguridad necesarias y de los elementos que faciliten su auditabilidad.

En aquellas instituciones que por su reducido tamaño no sea aconsejable tener esta función, será conveniente contratar periódicamente una empresa que realice la Auditoría para supervisar el estado de la seguridad informática, y además para que mantenga los planes de seguridad actualizados convenientemente.

El entorno físico

El edificio

Es necesario conocer el entorno circundante del edificio para así poder prevenir los riesgos de seguridad. Así, no es lo mismo un pequeño edificio rodeado de bosques, que uno situado sobre acantilados, ya que está claro que será más accesible a efectos delictivos el primero que el segundo. De igual forma, no tendrá las mismas necesidades de sistemas de seguridad un edificio situado en zona de aluvión, o con posibles inundaciones, que un edificio situado en medio de una llanura castellana, o en zonas de tormentas seísmos, humedad, viento...

Se deben implantar controles de acceso, sistemas antiparásitos en las redes eléctricas, sistemas de detección de incendios, sistemas de vigilancia y observación.

Las salas de ordenadores

Según el equipo a proteger requerirá unas medidas de seguridad u otras. Está claro que si el equipo es un ordenador personal dedicado a escribir cartas o citas a pacientes, no requerirá las mismas medidas de seguridad que los que alberguen las historias clínicas de los pacientes. Es decir, todo dependerá de lo crítico de la información y de su sensibilidad a ser utilizada de forma delictiva.

Lo ideal es que los grandes ordenadores estén aislados lo más posible de las personas y del entorno, debiendo dedicarles salas cerradas y exclusivas para ellos. Los materiales que sean altamente ignífugos deberían separarse del ordenador, y se debería dotar a estas salas de sistemas antiincendios, sistemas de aire acondicionado y detectores de humedad.

También será necesario asegurar la continuidad de servicio, por lo que será necesario dotar al ordenador de sistemas de alimentación ininterrumpida (SAI o UPS).

En cuanto al material magnético de almacenamiento y copias de seguridad se deberán almacenar en armarios antiincendio y en salas separadas del ordenador.

El plan informático

El plan informático general

No sólo debe recoger la evolución esperada del parque informático, sino que debe basarse en una metodología que lleve a un plan exhaustivo, recogiendo:

1. Parque instalado
2. Análisis de necesidades y restricciones
3. Plan de sistemas de información: software, hardware, personal...
4. Presupuesto

El control

Deben definirse medios para garantizar la calidad y seguridad de los servicios, y crear y mantener actualizados permanentemente los procedimientos internos de seguridad y de controlarlos.

El plan de seguridad

Debe recoger las normas de seguridad, los procedimientos de revisión, los medios de emergencia, los medios de controles programados, la seguridad general de los locales de las instalaciones de los sistemas de información y telecomunicaciones, consignas para la lucha antiincendio... Debe recoger:

I. Identificación y evaluación de los riesgos.

II. Definición de los riesgos intolerables y jerarquización de las necesidades.

III. Medios de tratamiento de los riesgos, tanto de prevención, como de evitación y resolución en caso de que aparezcan.

IV. Estudio de las vulnerabilidades de la organización y del entorno, y medidas para corregirlas.

V. Valoración del presupuesto necesario.

VI. Organización y responsabilidades.

A continuación se recoge una relación de los fallos más comunes que pueden dar lugar a falta de seguridad y que, por lo tanto, deberían cuidarse con especial atención en el momento de diseñar el plan de seguridad:

a. *Cifrado:* Posiblemente las claves utilizadas para el cifrado de la información del sistema no son todo lo secretas que sería deseable, o son de fácil deducción.

b. *Sistema de seguridad:* Los procedimientos de seguridad del sistema están bien pensados y definidos pero no han sido correctamente puestos en práctica.

c. *Confianza:* Se piensa que el sistema funcionará siempre bien y no se llevan a cabo ciertas verificaciones necesarias para la prevención de problemas. Además, podemos pensar que la información que tenemos no es de interés para terceros, o que nunca vamos a tener ataques, y descuidamos las medidas de seguridad y prevención.

d. *Desconexión de línea:* Muchos sistemas toleran una desconexión de una línea sin dar por finalizada la sesión del usuario que está conectado de manera que, al restablecerse la conexión, podría otro usuario continuar con la sesión accediendo a la información del que realmente está dado de alta. Esta situación se debería evitar dando por finalizada la sesión del usuario, el cual podrá comenzarla de nuevo cuando se recupere la conexión.

e. *Sistema de contraseñas:* Las contraseñas son fáciles de obtener o deducir. Sería preferible, sobre todo en los sistemas actuales basados en la transmisión de datos, utilizar certificados seguros para identificar a los usuarios.

f. *Trampas indebidas:* Muchos sistemas ofrecen diversas trampas con el fin de atraer a los intrusos inexpertos y así conducirles hacia puntos en que no pueden hacer nada. Si dichas trampas no funcionan correctamente pueden ser una buena forma de transgredir la seguridad del sistema que es precisamente lo que tratan de evitar.

g. *Privilegios:* Hay sistemas que admiten gran cantidad de privilegios para los usuarios y programas, si existe algún programa con muchos de estos privilegios puede representar una futura penetración al sistema. A los programas sólo se les deberán conceder los privilegios que sean realmente imprescindibles.

h. *Caballo de Troya, gusano o bomba lógica (virus en general):* Incorrecta detección de estos programas, o indebidos mecanismos para evitarlos y destruirlos.

i. *Prohibiciones:* Se impide a los usuarios el acceso a determinadas zonas o recursos del sistema, pero los mecanismos dispuestos no son perfectos, o no se han implantado y los usuarios pueden acceder fácilmente a los mismos.

j. *Basura:* Lo que puede parecer impensable en la mayoría de los casos es la principal fuente de información para los intrusos. Debemos tener en cuenta que los residuos y papeles depositados en una papelera pueden ofrecer mucha información a posibles usuarios desalmados.

k. *Intentos de acceso:* El sistema deberá tener una cuenta del número de intentos de entrada fallidos que realiza un usuario, y a partir de una cierta cantidad de ellos, dicho usuario deberá ser bloqueado impidiéndole el establecimiento de cual-

quier sesión. Este mecanismo es similar al que utilizan los cajeros automáticos con las tarjetas de crédito para evitar actos fraudulentos con las mismas.

l. *Software regalado:* En muchas empresas se admite software regalado que con objetivos aparentes de marketing de nuevos programas o de diversos sistemas o, incluso, de divulgación, pueden transportar virus, gusanos, bombas lógicas o Caballos de Troya.

Plan de migración

Debe recoger los procedimientos a aplicar en el caso de que sea necesario trasladar de lugar cualesquiera de los componentes de los sistemas de información. El plan debe prever la necesaria "cobertura" durante la fase de traslado, con el fin de que la institución no se vea paralizada durante un tiempo excesivo, ni se resientan los pacientes o proveedores. Esta cobertura debe ser tanto física y material como de personal.

Plan de contingencia

Con el objeto de tener previstas todas las acciones a desarrollar en caso de que los mecanismos de seguridad puestos en marcha fueran transgredidos produciéndose una penetración en el sistema, será preciso prever de antemano todas las actividades a realizar en dicho caso, teniendo presente como se deberán encadenar y cuáles serán los recursos necesarios para llevarlas a cabo. Para ello se elaborarán ***planes de contingencia*** que recojan el conjunto de operaciones a realizar para solucionar las diversas adversidades que se puedan presentar.

TENDENCIAS ACTUALES

Las tendencias en seguridad informática está siguiendo dos caminos diferentes pero que tienden a converger en el futuro debido a la generalización de la informática y de la enorme potencia de los actuales sistemas. Las dos vías de estudio se dedican, por un lado a la prohibición del acceso sin autorización a determinada información (control de acceso, criptografía, seguridad en las comunicaciones...), y por otro lado al importante fenómeno y, en la mayoría de los casos, de extrema gravedad que representan los virus informáticos.

En el primer caso son muchas las investigaciones que se realizan en cuanto a criptografía y los algoritmos para tratarla, aunque los que se utilizan con mayor profusión son los algoritmos DES y RSA.

En cuanto a los virus presentan enormes dificultades puesto que constantemente surgen nuevos ejemplares que son inmunes a los tratamientos existentes por lo que la mejor solución será evitar la copia o acceso a cualquier aplicación o programa sospechoso.

Otro aspecto importante es el de la firma electrónica, que aunque incipiente está siendo fuertemente respaldado a nivel gubernamental y legislativo, y cada vez son más las organizaciones que ofrecen sus accesos seguros basados en firma electrónica y certificados digitales.

Hoy día, la nueva forma de trabajo entre empresas y de los empleados de las mismas, que fuerza al uso intensivo de las comunicaciones, y fundamentalmente de Internet, obliga a establecer fuertes medidas de seguridad en los sistemas de información y en las comunicaciones. Así, es habitual constituir a nivel corporativo una **Intranet** para el uso de los empleados de la empresa, una **Extranet** para las relaciones entre las diferentes empresas relacionadas o que colaboren habitualmente, y el uso de **Internet** como una forma de ofrecer los productos a clientes finales.

Las redes de comunicaciones son la base de los sistemas de información y uno de los elementos más críticos del entorno institucional y empresarial corporativo. La gestión de las comunicaciones es de máxima importancia actualmente en estos ámbitos, donde Internet y las transacciones comerciales a través de la red serán fundamentales en el desarrollo y competitividad de las empresas en el futuro. Pero las Redes de comunicaciones no dejan de ser una puerta abierta hacia el exterior, y por tanto, una forma de brindar la entrada a posibles intrusos, constituyendo por ello una posible brecha en la seguridad de los sistemas de información.

La gestión de estas redes debe permitir la definición de alarmas que actúen en respuesta a eventos específicos (caídas de nodos, trasgresión de la seguridad...). Estas alarmas facilitarán en gran medida el trabajo del administrador de la red al permitir la rápida detección y resolución de las incidencias.

El teletrabajo, los acuerdos comerciales con suministradores, la externalización de servicios, y la distribución geográfica, requiere permitir el acceso a los servicios corporativos, tanto desde el interior como desde el exterior, lo que afecta a la seguridad de la red corporativa. El sistema de seguridad a implantar será complejo, debiendo establecer reglas (relaciones lógicas entre usuarios, redes y servicios) para validar los datos de entrada y salida, impidiendo el acceso no autorizado.

Además, la generalización y globalización de la Red Internet como medio de comunicación entre empresas y para realizar transacciones comerciales, permite que los ataques proliferen, y donde antes el intruso debía ser un especialista con una profunda formación en estas técnicas y por ello eran contados dichos ataques, hoy estos son muchos y por personas que necesitan cada vez menos formación, al ser más fácil el acceso. Sin duda las comunicaciones presentan hoy el mayor peligro para la seguridad de los sistemas de información corporativos, y donde haya información muy sensible, como pueden ser, precisamente, las historias clínicas en Hospitales y Centros de Atención Primaria. Por todo ello, hoy es más importante que nunca, definir una Política de Seguridad que implique a todos los participantes, y que defina las líneas estratégicas de seguridad en la empresa, y fundamentalmente para los sistemas de información.

Basados en el Plan Estratégico de Seguridad de la organización, y de acuerdo con los Planes de Sistemas y de Seguridad, se deberán desarrollar **Proyectos de Seguridad** que, analizando las necesidades y vulnerabilidades del sistemas, implanten sistemas basados en hardware y software para detección y comprobación de la seguridad, y que permitan detectar continuamente nuevas formas de ataques. Para ello se seguirán los siguiente pasos:

7. *Análisis de necesidades:* que consistirá principalmente en estudiar quién puede ser el enemigo, y las situaciones de riesgo que se pueden presentar y contra las que habrá que defenderse, evaluando el coste del daño posible y su solución, comparándolo con el de evitarlo a través de medidas de seguridad. Todo ello se debe basar en proteger el sistema de información contra dichos ataques, pero sin menoscabar la conectividad universal de los distintos usuarios remotos que se deban conectar a la Red para llevar a cabo su trabajo cotidiano.

8. *Implantación:* Debiendo analizar la topología de la red y equipos involucrados (encaminadores, puentes, ordenadores, servidores...), así como la estructura del direccionamiento. A la luz de este análisis deberá decidirse qué, cómo y dónde se protege, y cuál debe ser el equipamiento a implantar.

9. *Comprobación periódica:* del funcionamiento de la Red y de los mecanismos de seguridad, en cuanto a los resultados obtenidos. De esta forma se podrán detectar las vulnerabilidades y las nuevas formas de ataques que surjan, pudiendo dar adecuada respuesta ante ellos.

La constitución de la Intranet da lugar a las VPN o Redes Privadas Virtuales, aplicadas en organizaciones geográficamente dispersas, donde es necesario conectar las distintas sedes a través de redes públicas de datos, con usuarios remotos

tanto a través de conexiones con móviles como de internet. Esto obliga a adoptar fuertes medidas de seguridad para evitar penetraciones indeseadas en el sistema, dotando al sistema de un férreo control de usuarios, hoy sería aconsejable identificarles a través de Certificados Digitales, y utilizar técnicas de encriptación que permitan establecer "túneles" para acceder a los sistemas corporativos. Un ejemplo de estos servicios se puede ver en la figura 8.

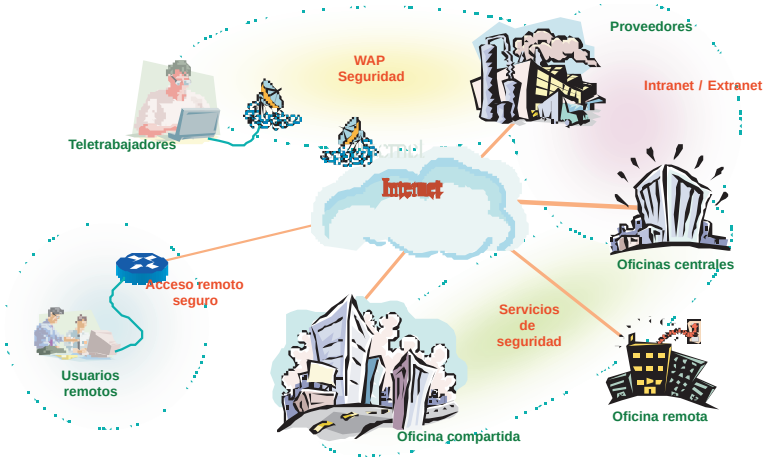


Figura 8. Servicios de "túnel"

Dentro de este escenario actual, las organizaciones se encuentran con distintos tipos de usuarios, como son los propios empleados que trabajan dentro de la sede de la empresa, o profesionales propios o de otras organizaciones que deben conectarse de forma remota a los sistemas, bien a través de móviles o de conexión a la red. Además, normalmente se dará acceso a usuarios o clientes finales a los que se ofrecen los productos o servicios de la organización.

Esto dará lugar a cierta diversidad de tipos de acceso, que irán desde la Red de Área Local (LAN), conexión a través de módem, ADSL, Cable, WAP..., con la finalidad de utilizar diversas aplicaciones como pudieran ser de teleformación, teletrabajo, trabajo en Red, servicios Web, B2B o compras por la red entre empresas y gestión de bienes y suministros, gestión de redes, gestión remota de seguridad en caso de que se externalizase esta función, o mantenimiento remoto de los sistemas, etcétera. En la figura 9 se puede observar de forma reducida las clases de usuarios y soluciones a adoptar.

Figura 9. Problemática de la situación actual

Esto obliga a dotar a nuestras instalaciones actuales y futuras de cortafuegos, programas de detección de virus o antivirus, establecimiento de importantes políticas de seguridad en la organización, si cabe más exigente que en un entorno cerrado en la empresa, y técnicas y mecanismos de cifrado. Igualmente, debe dotarse al sistema de medidas de seguridad no tradicionales en cuanto a la autentificación de los usuarios que intenten acceder al sistema, que se basarán fundamentalmente en certificados digitales y, por lo tanto, firma digital, expedida por una Autoridad de Certificación, y que permita establecer túneles de acceso a las distintas aplicaciones. En la figura 10 se puede observar un ejemplo de infraestructura de conectividad donde se recogen estas ideas.

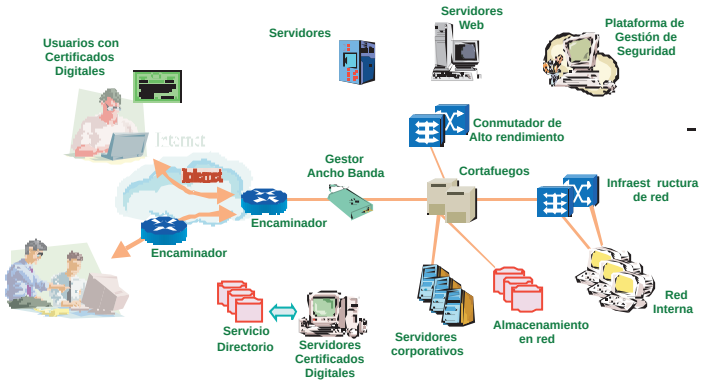


Figura 10. Infraestructura de conectividad

BIBLIOGRAFÍA

1. Anónimo. Máxima Seguridad en Internet. Anaya Multimedia. Madrid, 1998.
2. Diversos autores. Revista Novática. Monografía de Seguridad Informática. Número 116, Julio-Agosto, 1995.
3. Milan Milenkovic. Sistemas Operativos, 2.ª Ed. McGraw Hill, 1994
4. J.M. Lamere. La Seguridad Informática, Metodología. Ediciones Arcadia, S.A. (Colección: Informática Profesional). 1987
5. Para el uso avanzado de contraseñas se puede consultar el web "http://www.tis.com".
6. A.J. Thomas/I.J. Douglas. Auditoría Informática. Ed. Paraninfo. Madrid, 1988
7. Jesús Sánchez Allende, Joaquín López. [Redes]. Ed. McGraw Hill Interamericana. Madrid, 2000.
8. Microsoft. Fundamentos de Redes Plus. Curso Oficial de Certificación. 2000

LA SEGURIDAD DE LAS TRANSACCIONES BANCARIAS EN INTERNET

Jordi Buch i Tarrats
Director de servicios profesionales de Safelayer

Francisco Jordán
Director de Investigación y Desarrollo de Safelayer

"Las nuevas tecnologías basadas en infraestructuras de clave pública (PKI) y en los protocolos SSL (Secure Sockets Layer) y SET (Secure Electronic Transaction) son las únicas que permiten cubrir las carencias de seguridad de la red Internet."

INTRODUCCIÓN

Las transacciones bancarias se realizan en su mayor parte sobre redes de conmutación de paquetes X.25. Este tipo de redes se consideran suficientemente seguras por estar controladas por operadores autorizados y no por presentar medidas de seguridad basadas en técnicas criptográficas, autentificación segura o integridad de la información. La red Internet es una red pública, por lo que el riesgo de que las amenazas contra la autenticidad, integridad, confidencialidad y el no repudio de las transacciones que sobre ella se realicen será mayor.

Las nuevas tecnologías en el terreno de la seguridad en sistemas de información basadas en infraestructuras de clave pública (PKI) y en los protocolos SSL ("Secure Sockets Layer") y SET ("Secure Electronic Transaction") son las únicas que permiten cubrir las carencias de seguridad de la red Internet que afectan a la protección de la información que fluye a través de la red de redes.

La tecnología PKI también se aplica a los sistemas de banca virtual sobre Internet garantizando la seguridad de las operaciones bancarias tradicionales como órdenes de compra/venda de valores, órdenes de transacciones interbancarias, gestión de cuentas, etc.

DEFINICIONES

Certificado digital: Es la certificación electrónica generada por una autoridad de certificación, que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado tiene una validez determinada y un uso concreto.

Firma electrónica avanzada: Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que la detección de cualquier modificación ulterior de éstos.

Autoridad de Certificación (CA): Un servicio que genera un certificado digital después de verificar la identidad de la persona o entidad que se identificará mediante el uso de éste. La autoridad de certificación también genera las listas de revocación. Aunque existen varios estándares que definen el formato de los certificados digitales y las listas de revocación, el X509v3 para certificados y CRLv2 son los que están reconocidos por la mayoría de proveedores de tecnología.

Lista de revocación (CRL): La lista de revocación está firmada electrónicamente por la autoridad de certificación e indica los certificados que han sido revocados antes de que estos expiren.

Criptografía de clave pública: El conjunto de técnicas y estándares que permiten la identificación electrónica de una entidad, firmar electrónicamente y cifrar datos. Implica el uso de dos claves; una de privada y una de pública. La segunda, se pública en los certificados digitales.

Infraestructura de clave pública (PKI): Los estándares y servicios que facilitan el uso de la criptografía y los certificados en un entorno de red.

"Secure Sockets Layer" (SSL): Es un protocolo que permite la autentificación mutua de un usuario y un servidor con el propósito de establecer una conexión cifrada. "Secure Electronic Transaction" (SET): Protocolo que asegura la confidencialidad y la integridad de los pagos basados en tarjeta hechos por Internet, con independencia de quien sea el comprador y el vendedor del producto. El protocolo garantiza la autenticidad de las partes.

LA SEGURIDAD EN LA RED INTERNET

En el diseño de Internet, parte de la seguridad en Internet fue delegada en el mutuo respeto y honor de los usuarios, así como el conocimiento de un código de conducta considerado "apropiado" en la red. Una mínima seguridad se basa en una protección "blanda", consistente en una identificación del usuario mediante un identificador y una clave secreta que sólo éste conoce (login y password).

La red Internet tiene problemas de autenticidad, integridad, confidencialidad y repudio afectando a los requerimientos de las transacciones electrónicas u operaciones de banca virtual de la siguiente forma:

–Robo de información: El robo de información mediante escuchas de red, permite obtener información del usuario como números de cuentas o de tarjetas de crédito, balances de cuentas o información de facturación. Estos ataques, también

permiten el robo de servicios normalmente limitados a suscriptores. Por el hecho de conocer la realización de una transacción roza la invasión de la privacidad.

–Suplantación de identidad: La suplantación de identidad permite al atacante realizar operaciones en nombre de otro. Una situación de este tipo permitiría a un poseedor de miles de números de tarjetas de crédito la realización de numerosas pequeñas operaciones que representen en su totalidad una cantidad significativa. También puede interesar al atacante la suplantación de identidad del usuario de banca virtual.

–"Sniffers": Los "sniffers" son herramientas informáticas que permiten la obtención la lectura de la información que se transmite por la red (claves de paso o información de operaciones). Los "sniffers" permitirán la consumación de un ataque de suplantación de identidad y/o robo de información.

–Modificación de información: La modificación de datos permite alterar el contenido de ciertas transacciones como el pago, la cantidad o incluso la propia orden de compra.

–Repudio: El rechazo o negación de una operación por una de las partes puede causar problemas a los sistemas de pago. Si una parte rechaza un previo acuerdo con la respectiva, ésta deberá soportar unos costos adicionales de facturación.

–Denegación del servicio: Un ataque de denegación de servicio inhabilita al sistema para que éste pueda operar en su normalidad, por lo tanto imposibilita a las partes la posibilidad de realización de operaciones transaccionales. Éstos son de extrema sencillez y la identificación del atacante puede llegar a ser imposible. Las soluciones pueden no son únicas y no se tratarán en adelante.

PKI COMO SOLUCIÓN DEFINITIVA

El establecimiento de una infraestructura de clave pública permite garantizar los anteriores requerimientos. La confidencialidad se garantiza cifrando los datos que viajarán por la red. Mediante el uso de firmas digitales, se garantiza la autenticidad, la integridad y el no repudio de los datos. Sin embargo, la estructura no se puede desplegar sin la existencia del servicio de los componentes necesarios que aporten la confianza en el uso de las claves públicas mediante la generación de los certificados, su gestión y revocación cuando sea necesario.

Para el despliegue de la infraestructura se precisan los siguientes componentes:

–Autoridad de Certificación (CA). La CA emite certificados para las partes que intervienen, en definitiva, da fe de quien nos presenta una clave pública es quien

dice ser. La CA también mantiene las listas de revocación de certificados para resolver los casos de robo, pérdida o suspensión de claves privadas. La seguridad de la CA es crítica; un problema de seguridad que afecte a la CA puede afectar a toda la infraestructura existente.

–Directorio. El directorio es la base de datos donde se publican los certificados. De esta forma, los certificados están disponibles todas las entidades. En el directorio, además se guardan otros datos las listas de revocación.

–Sistema de revocación de certificados: Aunque sea un servicio asociado a la autoridad de certificación, éste se puede suministrarse por otra entidad.

–Actualización, históricos y copias de claves: Son los componentes que permiten la renovación del certificado, y el uso de claves antiguas. En los sistemas donde interviene datos cifrados hay que suministrar el servicio de recuperación de claves.

–Soporte para el no repudio: La protección de las claves privadas puede ser crítica para el no repudio de las firmas digitales realizadas. Los sistemas basados en tarjetas criptográficas son los que ofrecen las mayores garantías. Estos componentes deben existir y pueden estar gestionados por la propia entidad bancaria (por ejemplo Banco de Sabadell), un consorcio (por ejemplo, Iberion) o otra entidad externa.

BANCA VIRTUAL

En banca virtual, los clientes realizan las operaciones bancarias de forma remota. El sistema se implanta sobre redes TCP/IP (Internet), WAP (comunicaciones móviles) o propietaria (por ejemplo, cajeros automáticos). En el segundo, también interviene la red Internet.

El sistema de banca virtual distingue entre:

–Autentificación de usuario.

–Autorización de transacciones.

El sistema debe disponer de un servicio de acreditación fuerte para accesos a servicios (los basados en web son especialmente cómodos de implantar, aunque pueden complementarse con soluciones de mensajería segura) y ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos. Es importante resaltar que los sistemas actuales implantan mejoras en el sistema de autentificación, que aunque es más segura, sigue basándose en identificadores de usuario y contraseñas.

Para la acreditación fuerte se recomienda el protocolo SSL (o TLS) de forma que el usuario que dispone de un certificado digital de operación bancaria puede acreditarse al sistema, mientras que éste se acredita al usuario con su respectivo certificado de servidor. El mismo protocolo garantizará la confidencialidad y integridad de los datos. Si el usuario opera con un teléfono móvil, se usará el protocolo WTLS.

El sistema bancario virtual deberá guardar las órdenes de transacciones generadas por los usuarios, para los que éstos deberán firmarlas digitalmente con su clave de firma digital. Los estándares usados son el PKCS#7 definido por RSA y S/MIME si el sistema de basa en mensajería segura.

Procedimientos

La autentificación consiste en que el usuario entrega al servidor un desafío-respuesta (un paquete de datos aleatorios) firmado digitalmente con su clave privada. El servidor verificará que la el certificado se ha emitido por una Autoridad Reconocida (la propia del Banco u otra que reconozca), que el certificado no haya expirado ni revocado y que se ha usado el apropiado. En este momento, el sistema ya ha asociado el identificador o alias presente en el certificado a un contrato de banca virtual de un cliente.

En el procedimiento de autorización de transacciones, el usuario devuelve la orden firmada digitalmente y el servidor, una vez validada mediante el mismo procedimiento anterior la guardará para asegurarse el no repudio de ésta. La orden de transferencia no se procesará hasta que se hayan realizado los pasos anteriores.

TRANSACCIONES BASADAS EN SET

Con la ayuda de los grandes fabricantes de la industria de ordenadores y programas, Visa y MasterCard han desarrollado el que se está erigiendo en el protocolo de pago por excelencia para la práctica del Comercio Electrónico minorista (es decir, venta entre comerciante y usuario final). SET (Secure Electronic Transaction) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito[1].

1. Inicialmente sólo se pensó en tarjetas de crédito dada la naturaleza de sus patrocinadores, sin embargo posteriormente también se ha introducido el uso de tarjeta de débito con uso de PIN por Internet.

Arquitectura SET

Como método de pago basado en tarjeta, la solución SET (ver figura) conlleva la presencia de 3 nuevas entidades electrónicas a parte de los sistemas tradicionales ya utilizados en la actualidad. Los nuevos componentes son:

–Entidad “Merchant” SET o Comerciante SET es la entidad encargada de gestionar el pago del bien o servicio iniciado por un comprador. El pago siempre lleva asociado una transacción con un aceptador (“acquirer”) para la autorización del importe a pagar por el comprador. Habitualmente a esta entidad se le denomina POS (“Point Of Sale”) o TPV (Terminal Punto de Venta) virtual ya que su comportamiento, entre otras funciones, simula el de los sistema tradicionales.

–Entidad “Cardholder” SET o Titular SET es la encargada de actuar en nombre del titular de la tarjeta virtual para realizar el pago. Habitualmente a esta entidad se le conoce como Wallet o Cartera ya que su funcionalidad es muy similar a una cartera en la cual se almacenan las tarjetas.

–Entidad “Gateway” SET o Pasarela SET cuya función es la de hacer de puente entre el sistema aceptador SET y el sistema financiero propietario ya existente. Esta entidad es muy importante en cuanto supone la conexión de los sistemas y redes de autorización privados existentes con el mundo de Internet.

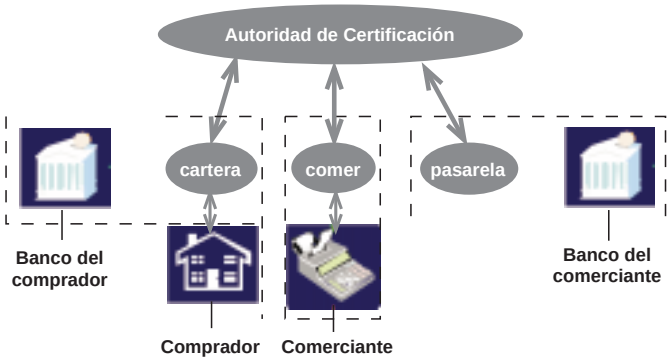


Figura 1. Componentes de SET

En el sistema SET la seguridad en las transacciones se ha cuidado hasta el último detalle. El sistema utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet.

Todas las entidades implicadas en el SET deben estar en posesión de un certificado válido para poder intervenir en una transacción de pago. Esto quiere decir que

tanto titulares, comerciantes y pasarelas SET deben de ser identificadas previamente y proveerles de un certificado para que puedan funcionar dentro del sistema.

Las entidades que generan los certificados para las entidades SET participantes se denominan CA SET o Autoridades de Certificación SET y generalmente son operadas por instituciones financieras capaces de emitir tarjetas (emisores) o instituciones asociadas, como bancos, que solicitan la emisión de tarjetas.

Las Autoridades de Certificación siempre están asociadas a una Marca de tarjeta particular. Esto quiere decir que los certificados de todas las entidades sólo son válidos para una Marca determinada siendo imposible utilizarlo en otro ámbito (al igual que en los sistemas tradicionales, es imposible utilizar una tarjeta Visa como si se tratase de una MasterCard). De lo que se desprende que una entidad deberá estar en posesión de tantos certificados como Marcas diferentes utilice (de ahí la acepción cartera para referirse a la entidad SET de titulares). Esto por otra parte hace muy flexible el sistema lo que, como se verá a continuación, nos permitirá utilizarlo dentro del ámbito de Marcas privadas.

Por último mencionar que existen varios tipos de Autoridades de Certificación SET dependiendo de su función y a quien certifiquen.

Protocolo de Pago SET

El protocolo de pago SET define los mensajes e interacciones entre las entidades SET (comprador, comerciante y pasarela de pago) para llevar a cabo una transacción de pago desde que el comprador acepta pagar hasta que dicho pago se realiza mediante un abono en la cuenta del comerciante desde la cuenta del comprador. La siguiente figura muestra un esquema en el que aparecen los mensajes e interacciones típicas de un pago (existen varias combinaciones de mensajes y este es el que obedece al esquema implantado en España).

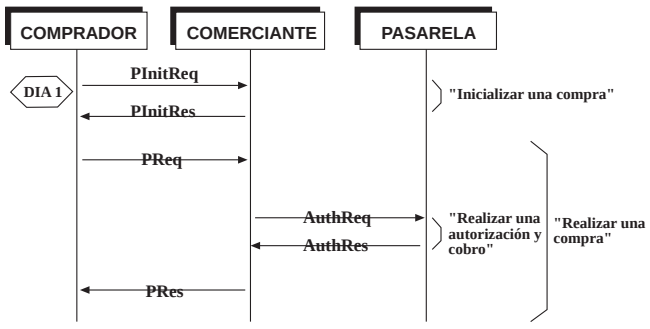


Figura 2. Protocolo de pago SET

Como se observa existen 3 fases:

1.–Fase de Inicialización: que corresponde al mensaje *PInit* y en la que el comprador contacta con el comerciante. El comprador informa de la marca de tarjeta que va a utilizar en el pago y el comerciante responde con un mensaje firmado que contiene el certificado de cifrado de la pasarela de pago asociada.

2.–Fase de Pago: que corresponde al mensaje *P* y en la que el comprador, si acepta el pago después de verificar la identidad del comerciante y las condiciones, realizara la orden de pago. La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago proveniente de la autorización.

3.–Fase de Autorización: que corresponde al mensaje *Auth* y en el que el comerciante solicita a la pasarela de pago (que a su vez solicitará al sistema financiero tradicional) si el comprador puede hacerse cargo de dicho pago (tiene crédito o saldo, la tarjeta no está revocada, etc.). La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago. En este esquema se ha optado realizar la captura o cobro del pago en la misma fase de autorización.

Mencionar que SET implementa el sistema de *firma dual* en el que el comprador en el mensaje *PReq* incluye datos protegidos para el comerciante y para la pasarela de forma que, el comerciante sólo puede ver los datos de la compra (pedido, modo de pago, cantidad, etc.) y la pasarela sólo puede ver los datos de pago (número de tarjeta, modo de pago, cantidad, etc.) que se enviarán en el mensaje *AuthReq*. De esta forma el comerciante nunca tendrá el número de tarjeta del comprador y la entidad financiera (a través de la pasarela) nunca tendrá los datos de la compra.

Como se puede observar del esquema presentado la fase de autorización ocurre durante la fase de pago. A esta modalidad se le conoce como pago en línea inmediato y es la más utilizada, aunque SET admite diferentes modalidades siendo un sistema que se adapta a los sistemas existentes en diferentes países.

Además de las fases y mensajes vistos, SET proporciona también servicios para retrocesos o cambios de autorizaciones realizadas y administración de “batchs”.

Problemas de implantación

En la actualidad existen varias implantaciones SET en el mercado (ver la lista de fabricantes en la web de SETCo-www.setco.org) pero hasta llegar a este punto se han encontrado con diferentes problemas. En el presente todavía persisten ciertos problemas que hacen que SET no se esté utilizando de forma masiva sin embar-

go dichos problemas se están paliando con la modificación de ciertos aspectos del sistema. A continuación se enumeran algunas de las barreras que se han encontrado en el desarrollo de SET:

–Debido a su gran contenido de funcionalidad y sus altos grados de seguridad, SET es un sistema complejo y ha hecho que los fabricantes tardaran mucho en tener un sistema completo y estable en el mercado. La misma causa ha hecho que los distintos desarrollos comerciales se encontraran ciertos aspectos de incompatibilidad a nivel de protocolo y funcionalidad.

–Las grandes inversiones de los fabricantes de sistemas SET en el desarrollo han hecho que los precios de los productos sean elevados frenando de este modo su adquisición masiva. Además, coyunturalmente tampoco parece que el comercio electrónico (minorista en este caso) haya despegado masivamente así que las inversiones en infraestructura no suponen una de las prioridades inmediatas y se hacen a un ritmo lento.

–Existe algún problema de aceptación en el usuario final (sobre todo del comprador). Debido también a la complejidad del sistema, en la mayoría de los casos el producto final resulta complejo de instalar y administrar.

TRANSACCIONES BASADAS EN SSL

Quizás por las dificultades de implantación del protocolo SET, la mayor parte de los sistemas transaccionales se basan en la actualidad en soluciones basadas en SSL y no en el protocolo SET, relajando las medidas de seguridad. A estos sistemas se les conoce de forma genérica como punto de venta virtual (TPV virtual).

La principal carencia de los pagos SSL es la imposibilidad de firmar digitalmente la orden de transacción que emite el comprador eliminando de esta forma el requisito que éste posea un certificado digital. Finalmente, se soluciona la problemática que supone el hecho de que el comerciante tenga acceso al número de tarjeta de crédito del comprador situando el TPV virtual en la pasarela de pagos (que se encuentra en la entidad financiera), y solicitando éste la autentificación al comerciante (en contra a la solución SET que es el comerciante quien traslada la orden que de compra a la pasarela).

Para reducir el riesgo que supone la imposibilidad de realizar una autentificación fuerte al comprador (basta conque el número de tarjeta tenga saldo para poder realizar una transacción), se han creado las denominadas tarjetas virtuales caracterizadas por disponer de un saldo fijo que se agota, siendo necesaria su recarga posterior.

Pagos SSL

Las pasarelas de pago SSL se activan en el momento que un comprador desea realizar el pago después de haber seleccionado los artículos deseados.

1.–El comercio informa a la pasarela que desea cargar un importe a un número de tarjeta de crédito o débito de un comprador. Para esto envía el importe a cargar, una referencia al TPV virtual. La operación implica un proceso de autentificación fuerte del comercio al TPV virtual (mediante un canal SSL y con un certificado generado por la CA de la pasarela).

2.–El comprador es redireccionado al TPV virtual, quien informa al comprador del importe, los datos del comercio y la referencia de la compra. La conexión entre el comprador y TPV virtual se realiza con el protocolo SSL, pero solo autenticando al servidor, garantizando al comprador que va a enviar datos al servidor correcto.

3.–El comprador introduce el número de tarjeta.

4.–El TPV virtual obtiene de la pasarela de pagos el resultado de la transacción presentándose ésta al cliente y informando al comerciante.

5.–El TPV virtual redirecciona el comprador al comercio.

Finalmente, el comercio puede gestionar el TPV virtual de forma remota mediante la correspondiente acreditación. Las operaciones que podrá realizar son las de operaciones “batch”, descarga de operaciones y consultas en general. Una operación adicional que permiten algunos TPV virtuales es la realización de operaciones manuales, actuando como un terminal punto de venda clásico.

Migración a SET

La mayor parte de las soluciones de TPV virtual permiten también la operación en SET y se deja en manos del comprador la posibilidad de realizar el pago SET o SSL. Se trata de una solución SET en donde el componente POS reside en el TPV virtual (confundiéndose con el componente pasarela) y no en el sitio del comerciante.

Actualmente la cartera SET del comprador sigue esta misma tendencia, situándose ésta en la propia entidad emisora de tarjetas. La solución se conoce como “server wallet” y esta apoyada por VISA y MASTERCARD.

CONCLUSIONES

La implantación de seguridad en las transacciones realizadas sobre la red Internet implica la disponibilidad de una infraestructura de clave pública (PKI) y el uso de protocolos seguros como SET o SSL. El componente CA de dicha infraestructura es crítico y debe gozar del suficiente grado de confianza por todas las partes. La CA puede gestionaste por un banco, un consorcio de bancos o alguna otra entidad externa.

SET es el protocolo que aporta el mayor grado de seguridad a al vez que es extremadamente complejo. Esta circunstancia ha imposibilitado el despliegue definitivo de los sistemas de pago basados en el protocolo definido por VISA y MasterCard. Se espera que el nuevo concepto de "server wallet", que se fundamenta en que los certificados digitales SET no residen en el cliente, sino en un servidor gestionado por las entidades de pago, suponga el despliegue definitivo. El "server wallet" supone una mayor facilidad de uso para el usuario aportando además un alto grado de movilidad a la vez que provoca una disminución del nivel de seguridad.

Las soluciones de pago basadas en SSL ofrecen una solución alternativa, mucho menos segura pero gozan de fuerte implantación. Se prevé que dichas soluciones migren a una solución final de SET basada en "server wallet" y pasando por una solución mixta en donde el TPV virtual se ofrezcan como servicio del banco.

La firma digital aplicada a los sistemas de banca virtual aporta la propiedad del no repudio a las órdenes de transacción emitidas por los clientes. Aunque en la actualidad el sistema no esta implantado en la mayoría de las soluciones de banca electrónica, la rápida consolidación de la tecnología PKI y el reconocimiento legal del sistema fuerce la implantación masiva a corto plazo.

REFERENCIAS

1. Sistema de Certificación Global <http://www.verisign.com>
2. Criptografía <http://www.rsa.com>
3. Protocolo SET <http://www.setco.org>
4. SSL, Firma de formularios, firma de código <http://www.netscape.com>
5. Microsoft Windows 2000 PKI <http://www.microsoft.com>
6. Demos de SET y SSL <http://www.safelayer.com>

PKI CASO PRÁCTICO: BANCO SABADELL

"Banco Sabadell, PRIMER banco en España que ofrece a sus clientes la tecnología PKI en tarjeta-chip para asegurar las operaciones de Banca Internet"

RESUMEN

Tras una introducción de las características de la PKI y diferentes aspectos a considerar, se explica como se implantó la solución de banca electrónica en el Banco de Sabadell. El modelo se fundamenta en una Autoridad de Certificación que emite lotes de certificados de autentificación y firma digital en tarjetas con sistema operativo TIBC.

Los certificados emitidos no están asociados a ningún cliente en particular, dicha asociación se realiza a posteriori. Esta característica permite que los clientes obtengan todo lo necesario para "Home Banking" de una sola vez y no deban volver a completar el procedimiento tal y como es habitual en otros sistemas PKI.

La emisión de este tipo de certificados se basa en el suministro de una clave privada y un certificado de firma digital y autentificación. Su fortaleza y viabilidad presenta tres pilares tecnológicos:

–Tamaño de llaves de 1024 bits

–Soporte de tarjetas inteligentes TIBC

–Integración con la tecnología existente usando un plug-in de acceso a la tarjeta inteligente para Netscape Communicator y Microsoft Internet Explorer

PKI COMO SOLUCIÓN DEFINITIVA

La implantación de una solución de infraestructura de clave pública –en adelante PKI– en una corporación tiene como finalidad la securización total de las comunicaciones, dando la mejor solución a los problemas de integridad, confidencialidad y acreditación. En una estructura PKI, los clientes –en adelante usuarios– y servidores disponen de un par de claves asimétricas, guardando la privada preferiblemente en una tarjeta inteligente y distribuyendo la pública en un certificado

emitido por un centro certificador –en adelante CA–. La CA garantiza la autenticidad de los datos que figuran en el certificado (nombre, clave pública, etc.) durante un período de validez también indicado en el propio certificado, definido por la CA. El certificado también indica los usos de su clave privada (ejemplo: firma digital, acreditación en servidores, sellos de tiempo, cifrado, etc.).

Los problemas más inmediatos que soluciona una estructura PKI son:

–Control de acceso: Acreditación de usuarios en servidores.

–No repudio: La firma digital, que tiene asociadas las propiedades de autentificación y integridad, posibilita que el firmante no pueda repudiar su acción.

–Confidencialidad: Cifrado de datos usando la clave pública de los destinatarios.

Aunque a también se extiende a soluciones de "single sign-on", VPNs, firma de código, firma de datos, "secure desktop", etc.

Problemas a resolver

El sistema de acreditación tradicional o basado en identificador de usuario y contraseña tiene tres importantes carencias:

–Copia/interceptación fácil y de difícil detección: La acreditación del usuario se basa en una/unas contraseña/s ("password") que se puede/n copiar sin que el propietario disponga de los mecanismos necesarios para la detección de copia y por lo tanto pueda iniciar un proceso de revocación.

–En ocasiones, el usuario dispone de diferentes contraseñas o incluso diferentes identificadores de usuario, lo que provoca que éstas acaben apuntadas en un papel.

–No se guarda constancia firmada por el usuario de las transacciones autorizadas.

Los dos primeros problemas no se dan con la PKI, y si se usan tarjetas inteligentes, son prácticamente inexistentes. Por otra parte, la PKI afronta directamente el tercer problema.

Características de la PKI

La solución PKI es el único esquema que no presenta las anteriores carencias. En definitiva, el sistema permite:

–Establecer un servicio de acreditación fuerte para accesos a servicios. Los basados en web son especialmente cómodos de implantar, pero la solución se extiende a sistemas de "single sign on".

–Ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos.

–Ofrecer la plataforma tecnológica para que los usuarios puedan ejecutar programas en su navegador de forma segura (firma de código).

–Ofrecer la tecnología para que los usuarios dispongan de correo seguro (S/MIME) y puedan securizar sus archivos (PKCS#7) de la forma más estándar.

–Ofrecer la plataforma para que los servidores puedan ser certificados y garantizar de esta forma su autenticidad.

–Total integración en cualquier solución futura basada el PKI (redes privadas virtuales, accesos a servidores, etc.).

Características de los certificados emitidos

Los certificados emitidos se deben ajustar a las especificaciones X509v3 y soportar las extensiones de Netscape. Esta característica permite la generación de certificados sin tener que conocer qué software va a usar el cliente, requisito importante en entornos donde no existe una política clara de soporte a un único proveedor.

Se generan diferentes tipos de certificados:

–Certificados de cliente para acreditarse en servidores seguros y firmar datos.

–Certificados para servidores.

–Certificados para programadores. Permiten firmar código ejecutable para garantizar a los usuarios la autenticidad del programa. Es la forma más segura de acabar con los virus y caballos de troya.

Es importante destacar que no se precisa de modo alguno de la clave de cifrado ya que las comunicaciones entre el cliente y la entidad se realiza sobre una conexión cifrada mediante el uso del protocolo SSL.

ESCENARIOS DE USO

En PKI existen diferentes escenarios para la implantación del modelo de certificación. La solución adoptada es un compromiso entre los procedimientos de registro, la facilidad de uso del cliente u la seguridad del sistema.

Modelos de Certificación: El problema del registro de los usuarios

Se contemplaron dos modelos de certificación de usuarios:

–Modelo tradicional: Los clientes generan su par de claves para solicitar la certificación a la CA, a partir de un formulario dispuesto para tal fin. Este es el esquema usado, por ejemplo por Verisign < hyperlink “http://www.verisign.com” http://www.verisign.com>.

–Un modelo donde la CA genera los pares de claves y los certificados por lotes, a partir de los datos suministrados por la entidad de registro (lista de clientes, personal en plantilla, etc.). Los certificados junto con las claves privadas se entregan en soporte de tarjeta inteligente (“smartcard”) o bien en fichero (PKCS#12).

El segundo modelo presenta importantes ventajas diferenciales sobre el primero, para el entorno objetivo del proyecto:

–En el primer modelo, el proceso de aprobación de peticiones se debe realizar una a una. Este proceso se caracteriza por ser necesaria la comprobación de los datos del solicitante mediante la solicitud del DNI, o cualquier documento acreditativo. Es el modelo válido en centros certificadores globales, pero puede llegar a ser redundante en corporaciones, empresas, etc. que ya disponen de los datos de los posibles solicitantes a priori, y que ya cuentan con medios seguros de comunicación con éstos. El segundo modelo, en cambio, admite como entrada peticiones ya validadas, para generar directamente los certificados y claves privadas en lotes, y reduciendo de forma considerable la carga administrativa.

–En el primer modelo, el usuario debe contactar con el centro certificador primero y esperar a que se le apruebe su solicitud, mientras que en el segundo, el usuario o cliente obtiene directamente el certificado. Para el usuario es más simple el segundo.

–El primer modelo precisa la necesaria formación del personal de las oficinas bancarias para que actúen de aprobadores de solicitudes de certificación.

–El servicio de certificación del segundo modelo no tiene que estar conectado en red, permitiendo de esta forma un mayor nivel de seguridad de forma inmediata.

–Finalmente, en el segundo modelo, no necesariamente se deben conocer los datos de los clientes, siendo posible el uso de “alias” que posteriormente se asociarán a éstos.

Modelos de firma y navegación

En los modelos de seguridad de PKI se distinguen tres modelos:

–"Modelo de seguridad web": Usa los mecanismos de seguridad de que disponen los navegadores más populares (Netscape y Internet Explorer). Tiene carencias de seguridad posiblemente no asumibles por la política de certificación corporativa (por ejemplo, en esta solución de "Home Banking").

–"Modelo de seguridad PROXY", donde se desconfía de la seguridad de los navegadores y se controla ésta mediante programas independientes (que interpretan la política de seguridad corporativa) y

–"Modelo de seguridad mixto" que pretende suplir las carencias de seguridad de los navegadores añadiéndoles módulos o "plug-ins". Este modelo soluciona las carencias de los anteriores garantizando que la ni la clave privada ni el PIN de la tarjeta del usuario van a estar en el ordenador del cliente[1] simplemente facilitando la interfaz PKCS#11/CSP con una tarjeta chip para integrarse de forma cómoda y eficiente en el programa.

Los tres basan su solución en el modelo PKI. La solución mixta es la que permite garantizar el nivel máximo posible de seguridad en un entorno como el requerido, solucionando las carencias del "modelo de seguridad web", manteniendo el nivel óptimo de libertad de los usuarios en la elección de su plataforma de trabajo y evitando en la medida de lo posible los posteriores problemas de dimensionado de carga de una "hot line"

SOLUCIÓN IMPLANTADA

El Banco de Sabadell se planteó el problema de cómo suministrar 10.000 certificados (en una primera fase) sin que tuviesen que pasar todos los clientes dos veces "por ventanilla".

La Autoridad de Certificación se creó con el propósito de que generase todos los certificados a partir de una lista de identificadores únicos que entrega la propia entidad –que por lo tanto, actúa de Autoridad de Registro–. Los identificadores únicos se incluyen en el atributo nombre ("CN") del campo sujeto del certificado X509. Dicho atributo se considera como un alias para asignarlo posteriormente a un contrato de "Home Banking" de un cliente de la entidad.

1. Usando un lector de tarjetas con teclado numérico y procesador o una tarjeta con procesador.

Este modelo además presenta otras importantes ventajas:

–La seguridad de la Autoridad de Certificación es extremadamente alta: Se trata de una autoridad que está desconectada de la red. Sólo se pone en marcha cuando es necesaria la generación de un lote de certificados.

–Calidad en la generación de las claves privadas: Es la CA quien genera las claves privadas de los usuarios, con lo que se garantiza una calidad óptima de éstas.

–Facilidad de administración: El número de personal de administración se reduce a dos operadores de un grupo superior a dos que tienen autorización para procesar un lote. No se precisan de administradores de registro.

Procedimiento de entrega de claves

Las tarjetas inteligentes generadas se distribuyen de forma estratégica en las oficinas de la entidad, junto con los PINs de acceso a éstas.

Cuando el cliente desea darse de alta al servicio de "Home Banking", éste deberá firmar el contrato de Banca Virtual en el que se le asocia un identificador único a su cuenta corriente (dicho identificador incluido en el certificado, también figura en la tarjeta para su comprobación visual). La aceptación de dicho contrato implica una alta en el sistema entregándosele un PIN, un lector y un plug-in de acceso al lector no siendo necesario ningún paso adicional por parte del cliente.

Sistema de "Home Banking"

El sistema se apoya en un servidor web seguro que garantiza la confidencialidad de la comunicación mediante el protocolo SSL usando claves de cifrado de 128 bits.

El sistema de "Home Banking" distingue entre autentificación de usuario y autorización de transacciones.

La autentificación consiste en que en usuario entrega al servidor un desafio-respuesta firmado digitalmente con su clave privada. El servidor verificará que la el certificado se ha emitido por una Autoridad Reconocida (actualmente la propia del Banco de Sabadell), que el certificado no haya expirado ni revocado y que se ha usado el apropiado. En momento, el sistema ya ha asociado el identificador o alias presente en el certificado a un contrato de "Home Banking" de un cliente.

En el procedimiento de autorización de transacciones, el usuario devuelve la orden firmada digitalmente y el servidor una vez validada mediante el mismo procedimiento anterior la guardará para asegurarse el no repudio de ésta. La orden de transferencia no se procesará hasta que se hayan realizado los pasos anteriores.

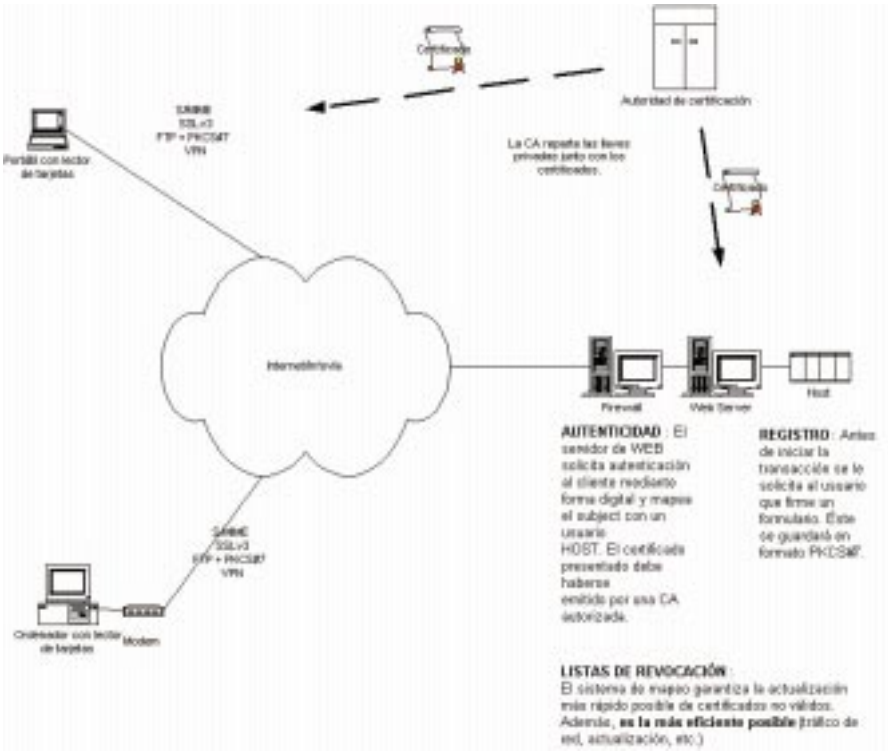


Figura 1. Sistema de “Home Banking”

Extensión del sistema y CRLs

En las operaciones de autentificación y autorización de transacción, debe existir un contrato de “Home Banking” asociado a los datos que presenta el cliente. Cuando el cliente solicita una revocación, se procede a una cancelación de contrato, existiendo un método de consulta de revocación análogo al que se usa en el protocolo SET y manteniendo a la vez, la posibilidad de que la entidad disponga de mecanismos de consulta de certificados revocados según el estándar CRL, OCSP o el mecanismo netscape-url-revocation. Dicha posibilidad permite posibles cambios en la política de certificación orientados a la ampliación de uso de los certificados en el contexto del Banco y para otras aplicaciones diferentes a la de “Home Banking”

Especificaciones funcionales

El modelo permite dar los servicios de correo electrónico seguro (S/MIME), control de acceso en entornos web (acreditación de clientes mediante presentación de certificado en protocolo SSLv3), firma/cifrado de ficheros en formato PKCS#7 y firma de código.

Integración en tarjeta monedero TIBC (Tarjeta Inteligente para Bancos y Cajas) utilizada en España. Soporte para los proveedores de lectores de tarjetas inteligentes que cumplen la norma PC/SC.

Módulo PKCS#11 y CSP (Crypto Service Provider) que permite el uso de cualquier lector en plataformas Windows 95, 98 y NT para aplicaciones Netscape Communicator y Microsoft Internet Explorer.

ASPECTOS LEGALES DE LA SEGURIDAD Y CONFIDENCIALIDAD EN LA INFORMACIÓN CLÍNICA

Alberto Andérez González

Director de Administración y Recursos Humanos del Servicio Navarro de Salud-Osasunbidea
Asesor Jurídico del Gobierno de Navarra
Letrado de la Administración de la Seguridad Social

INTRODUCCIÓN

Cuando el profesional del Derecho se enfrenta al estudio de la problemática que suscitan los sistemas de información en el ámbito sanitario (fundamentalmente en relación con la historia clínica), no puede sustraerse a una sensación, en cierto modo contradictoria, de inquietud intelectual, por un lado, y de insatisfacción e inseguridad, por otro. La complejidad propia de este sector del ordenamiento jurídico, que es el Derecho sanitario, se acentúa al entrar en conjunción la utilización en este ámbito de las nuevas tecnologías de la información que, amén de las cuestiones de índole estrictamente técnica, presenta una problemática jurídica peculiar derivada de la aparición de un nuevo cuerpo normativo cuyo objeto es regular el tratamiento de la información con la finalidad de garantizar la protección de los derechos de la persona.

En este marco son muchas las dudas y conflictos de naturaleza jurídica que ocupan la atención de los juristas que abordan esta materia, si bien son a su vez bastantes las ocasiones en que, para desesperación de los profesionales ajenos al mundo del Derecho que viven a diario esta problemática, no existe consenso respecto de la solución que la norma establece para cada uno de aquéllos.

Sin que pretenda servir de justificación a la situación descrita, sí pueden señalarse diversos factores que contribuyen a perfilar el panorama actual:

a) La complejidad del Derecho sanitario proviene en gran medida de la implicación, en muchas de las situaciones que regula, de derechos básicos de la persona (vida, integridad física, libertad individual, intimidad personal) que plantean dificultad para su articulación normativa y suscitan al mismo tiempo importantes conflictos no solo legales, sino también éticos a los que no son ajenos las distintas soluciones propugnadas.

b) El dinamismo que caracteriza el desarrollo tecnológico en la nueva sociedad de la información, amén de su contenido eminentemente técnico, encuentra difícil acomodo en un campo, como el del Derecho, con vocación de estabilidad y permanencia, y pone por ello mismo de manifiesto el anacronismo de algunas de las previsiones legales y la necesidad de su modificación, conclusión que es per-

fectamente predicable de una norma básica en el ámbito sanitario como es la Ley General de Sanidad de 25 de abril de 1986.

c) En este contexto, la aparición (con la Ley Orgánica 5/1992 y posteriormente con la Ley Orgánica 15/1999) de un marco legal ciertamente riguroso regulador de la protección de datos de carácter personal contribuye, en ocasiones, a clarificar ciertos debates, provoca en otros supuestos dudas razonables respecto de la solución ajustada a Derecho, y genera en todo caso una sensación de vértigo ante el alto nivel de exigencia que comporta la adaptación a los requerimientos legalmente establecidos.

d) La existencia de un severo régimen sancionador, tanto penal como administrativo, con el que se cierra el sistema de garantías diseñado por el legislador, contribuye a extender igualmente un temor generalizado, y muchas veces no del todo racional, entre los profesionales del ámbito sanitario, que deja en segundo plano en ocasiones las exigencias deontológicas que de modo ineludible deben estar presentes en toda buena práctica clínica y de gestión.

Estas consideraciones se hacen patentes de manera especial en el tratamiento de los aspectos de confidencialidad y seguridad relacionados con los sistemas de información clínica, cuyo estudio en este breve trabajo se estructura en tres partes que analizan, respectivamente, el ámbito de la regulación en materia de protección de datos, las cuestiones relativas al acceso y comunicación de los datos incluidos en sistemas de información clínica, y, por último, las notas principales de la regulación contenida en el Real Decreto 994/1999.

NORMATIVA SOBRE PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

La primera cuestión que debe suscitarse al abordar la problemática afectante a los aspectos de seguridad y confidencialidad de los sistemas de información es la que plantea el ámbito de protección dispensado por el nuevo marco legal regulador del tratamiento de datos de carácter personal, cuestión ésta de alcance no solamente teórico, sino también con especial trascendencia en cuanto a las repercusiones prácticas que pueden deducirse en relación con el régimen sancionador asociado al incumplimiento de la norma.

En esta materia concreta, la dificultad deriva en gran medida de la necesidad de poner en relación el fundamento o razón última que subyace al tratamiento legal de la protección de datos de carácter personal con el sentido o interpretación que se dé a determinados conceptos que la Ley utiliza y, en ocasiones, define, aun

cuando esta labor de definición no termine de despejar todas las dudas que puedan plantearse.

El artículo 18.4 de la Constitución y la llamada "libertad informática"

El punto de partida en cuanto al tratamiento legal de los datos de carácter personal se sitúa en el art. 18.4 de la Constitución, cuando señala 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".

Esta declaración constitucional ha dado lugar a un profundo debate en torno a si el precepto citado configura un derecho fundamental distinto al propio derecho a la intimidad personal y familiar (consagrado en el apartado 1 del mismo artículo), o por el contrario dicho precepto se limita a la afirmación de un derecho de carácter instrumental o accesorio respecto del derecho a la intimidad y demás derechos fundamentales, derecho que vendría delimitado por el propio legislador ordinario (se trataría así de un derecho de configuración legal) a través del establecimiento de los límites impuestos a la utilización de la informática como modo de contribuir a la garantía de aquellos derechos fundamentales.

Aún cuando puede considerarse mayoritaria la opinión doctrinal contraria a la afirmación de un derecho fundamental nuevo o autónomo a partir de lo preceptuado en el art. 18.4 de la Constitución, lo cierto es que una conclusión en gran medida distinta puede extraerse de los escasos pero interesantes pronunciamientos recaídos en esta materia hasta el momento, especialmente aquellos dictados por el Tribunal Constitucional en su función de intérprete máximo de la Carta Magna.

A raíz de la muy comentada sentencia 254/1993, de 20 de julio, ha venido conformándose un cuerpo de doctrina conforme al cual se entiende que la previsión del art. 18.4 citado no se ciñe a un mero mandato dirigido al legislador que no otorgaría derechos al ciudadano en tanto aquél no cumpla su función de desarrollo, sino que, acudiendo al fundamento y sentido de los textos internacionales ratificados por el Estado Español, la Constitución habría incorporado una nueva garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona". Dicha sentencia, con una posición un tanto ecléctica, afirma que nos encontramos "ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".

Moviéndose entre las dudas sobre su configuración o no como derecho autónomo, el Tribunal Constitucional señala que la garantía del derecho a la intimidad adopta actualmente un "contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona", dando así lugar a la llamada "libertad informática" como "derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)".

Sentencias posteriores del mismo Tribunal han continuado con esta doctrina, reiterando el carácter a la vez de derecho instrumental y de derecho fundamental en sí mismo que cabe afirmar de la llamada "libertad informática", que por otro lado se halla dotada de un contenido mínimo (derivado de la propia Constitución) que comporta, entre otros aspectos, las facultades de conocer la existencia, identidad y responsable de los ficheros informatizados que contengan datos de la persona o, por ejemplo, el derecho de ésta a oponerse a que dichos datos personales sean utilizados para finalidades distintas a las que justificaron su obtención. Son especialmente significativas en este punto las sentencias 143/1994, de 9 de mayo, 11/1998, de 13 de enero (seguida de otras muchas recaídas sobre el mismo supuesto de hecho), y 202/1999, de 8 de noviembre.

En este punto cabe efectuar una primera e importante reflexión; a saber, que con independencia del debate doctrinal acerca de la naturaleza del derecho reconocido en el art. 18.4 del Texto Constitucional, el mismo entraña una ampliación respecto de lo que tradicionalmente ha venido constituyendo objeto de protección a través del derecho a la intimidad personal y familiar. Obviamente, la garantía y protección frente a terceros de un ámbito íntimo o reservado de la persona cuenta con una larga tradición jurídica, y en este sentido la novedad ha venido provocada por el hecho de que las nuevas tecnologías posibiliten el flujo y utilización masiva de la información concerniente a las personas, información que, por otro lado, es necesario facilitar, cada vez con mayor frecuencia, a distintos entes públicos o privados para el ejercicio legítimo de las funciones atribuidas a éstos.

Por ello, el ámbito de la llamada "libertad informática" (también conocido como derecho a la autodeterminación informativa) no abarca únicamente a aquella información que reviste un carácter reservado (por afectar a la esfera más íntima de la persona), sino a cualquier dato o información referida a personas físicas individualizadas o susceptibles de individualización, ya que se parte de que el tratamiento y comunicación de datos personales, aunque éstos en principio y aisladamente considerados no sean sensibles, posibilita la obtención de un determinado perfil de la persona, permitiendo la intromisión en facetas reservadas de su personalidad y generando incluso el riesgo de que dicha información influya en la adop-

ción de determinadas decisiones (sea por sujetos públicos o privados) en relación con el individuo.

Basta, para comprobar la ampliación señalada, una comparación entre el objeto tradicional de protección de la intimidad (señala la Ley Orgánica 1/1982, de 5 de mayo, que "la protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia") y el ámbito de la normativa sobre protección de datos, conforme a la cual se definen los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3.a de la Ley Orgánica 15/1999).

El desarrollo del artículo 18.4 de la Constitución. El ámbito de las Leyes Orgánicas 5/1992 y 15/1999

La concreción del mandato contenido en el art. 18.4 de la Constitución tiene lugar por primera vez, como es sabido, con la Ley Orgánica 5/1992, de 29 de octubre, por la que se regula el tratamiento automatizado de los datos de carácter personal, cuyo ámbito de aplicación reviste algún matiz con relación al precepto constitucional que desarrolla. Así, mientras aquel precepto alude al uso de la "informática", el art. 1 de la Ley Orgánica define su objeto por la limitación del "uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal".

Desde este punto de vista, aun cuando pudiera considerarse más amplio el ámbito de la Ley Orgánica que el que deriva del Texto Constitucional, no hay inconveniente en admitir que en último extremo se trata de atender o satisfacer la misma necesidad jurídica, esto es, la protección de los derechos de la persona (especialmente el de su intimidad personal y familiar, pero también otros) ante los riesgos que para tales derechos supone el inmenso flujo de información posibilitado, merced a las nuevas tecnologías, por el tratamiento masivo de los datos de carácter personal y su constancia en ficheros organizados.

La mayor amplitud del objeto de la Ley Orgánica puede afirmarse por la previsión de otros posibles medios técnicos de tratamiento automatizado de datos distintos de la informática (lo que no deja de plantear un debate semántico), pero en todo caso el fundamento último de la regulación coincide con el fin constitucional previsto en el art. 18.4. No es ocioso señalar que el término automatizado, en su sentido gramatical, hace referencia a procesos o dispositivos automáticos, esto es, basados en mecanismos que funcionan en todo o en parte por sí solos.

No obstante, la cuestión adquiere rasgos de mayor complejidad con la derogación de la Ley Orgánica 5/1992 en virtud de la nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal, uno de cuyos principales efectos, advertido desde un principio por la doctrina, consiste en la ampliación del objeto o ámbito de aplicación de la norma en relación con la normativa ahora derogada.

Es conocido que la promulgación de la Ley Orgánica 15/1999 resultaba obligada con el fin de adaptar el Derecho interno español a la Directiva 95/46/CE, 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; pero no está tan claro que, al menos en este punto concreto que ahora se examina, dicha adaptación se haya llevado a cabo con la precisión que debiera. Por otro lado, las modificaciones que introduce la nueva Ley Orgánica respecto de la anterior no se limitan a aquellos aspectos necesitados de adaptación, sino que alcanza también a otros contenidos de la regulación legal que, aunque pueda considerarse que resultan razonables o comprensibles, no son objeto de justificación expresa por parte del legislador al haberse omitido, inexplicablemente, la exposición de motivos en el nuevo texto legal.

En cualquier caso, y centrándonos en el ámbito de aplicación de la norma, el aspecto más destacable es sin duda su ampliación a cualquier tipo de tratamiento de los datos personales, con independencia de su carácter automatizado o no; así resulta sin más de lo dispuesto en el art. 1 de la Ley Orgánica, que habla del tratamiento de dichos datos sin ningún otro calificativo, por contraste con la redacción, e incluso el título mismo, de la regulación derogada.

La aplicación del marco legal regulador de los datos de carácter personal al tratamiento manual o no automatizado de los mismos es, por tanto, la primera consecuencia que se desprende de la ampliación señalada, y esta misma circunstancia es la que genera importantes dudas respecto al alcance último de la nueva normativa legal en la materia, dudas motivadas en gran medida por la utilización de determinados conceptos cuya definición no termina de perfilar nítidamente el ámbito de protección de la Ley.

Algunos conceptos legales: tratamiento, fichero y cesión de datos

Ya se ha hecho referencia a la noción de “datos de carácter personal”, cuyo alcance aparece en principio como casi ilimitado; y este mismo es el caso del concepto de “tratamiento”, que curiosamente mantiene la misma definición que en la Ley Orgánica 5/1992 (en la que ya se aludía a su carácter automatizado o no), esto

es, como "operaciones y procedimientos técnicos de carácter automatizado o no que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". Como puede observarse, no existe apenas limitación teórica en cuanto al tipo de actividades que pueden entenderse incluidas en el concepto de tratamiento, salvo por la referencia al carácter "técnico" de los citados procedimientos y operaciones, precisión cuyo alcance no despeja en absoluto las dudas interpretativas (el adjetivo "técnico" significa gramaticalmente "perteneciente o relativo a las aplicaciones de las ciencias y las artes").

Otro concepto relevante es el de "fichero", definido en la Ley Orgánica como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", noción indudablemente más amplia que la de fichero automatizado que empleaba la regulación anterior, aun cuando la referencia a su carácter organizado exige en todo caso una mínima estructuración de la información recogida, cualquiera que sea el soporte físico en el que se contenga. En todo caso, la relativa indefinición de los términos utilizados no aclara los contornos que permiten considerar cuándo un fichero, sobre todo en el caso de los no automatizados, se ve afectado o no por las disposiciones legales en materia de protección de datos.

De todas formas, ambos conceptos, los de fichero y tratamiento, guardan una conexión que obliga a interpretarlos de manera conjunta, como lo pone de manifiesto la propia Ley Orgánica 15/1999 al definir en el art. 2 su ámbito de aplicación por referencia a "los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de" los mismos, o al definir, también de manera indistinta, la figura del responsable del fichero o tratamiento.

Las dificultades interpretativas son patentes; si se tiene en cuenta la amplitud del concepto de cesión de datos ("toda revelación de datos realizada a una persona distinta del interesado"), puede comprenderse que la aplicación o no del régimen legal que se examina, y sobre todo de las previsiones sancionadoras que el mismo contempla, va a depender, en el caso de los ficheros no automatizados, de cómo se entienda el carácter más o menos organizado de un fichero o la naturaleza técnica de los procedimientos en que se basa el tratamiento de los datos contenidos en él; y todo ello, según se ha dicho, con independencia del grado de reserva o sensibilidad de los datos que hayan sido objeto de comunicación.

Dicho de otro modo, y sin perjuicio de lo que luego se dirá respecto a la efectividad temporal del régimen legal en el caso de los ficheros no automatizados, desde la perspectiva de las consecuencias prácticas que derivan de esta cuestión, la promulgación de la Ley Orgánica 15/1999 y la extensión de su ámbito de protección a los ficheros no automatizados conlleva, en principio, una notable ampliación, al menos potencial, del número de conductas susceptibles de quedar sujetas al marco legal y sancionador establecido por aquélla, aun cuando vengan referidas a datos o informaciones que no incidan directamente en el ámbito íntimo de las personas. Esto es, la revelación de datos personales no reservados, que efectuada de manera aislada no entrañaría una infracción del derecho a la intimidad ni constituiría, por tanto, una vulneración del deber de confidencialidad, puede no obstante determinar importantes responsabilidades al amparo de la Ley Orgánica citada en la medida en que constituya un tratamiento sujeto a dicha norma legal o afecte a datos contenidos en un fichero regulado por la misma, conclusión que se agrava por la falta de una clara definición del tipo de ficheros y actividades sujetos al régimen legal del tratamiento de datos personales.

Nótese que, llegados a este punto, y aun cuando el amparo de la Ley Orgánica 15/1999 en la Directiva 95/46/CE es incuestionable además de obligado, el distanciamiento entre la norma legal (que se aplica a todo tipo de tratamiento de datos personales) y el art. 18.4 de la Constitución (que utiliza expresamente el término "informática") es más patente. En cualquier caso, y aunque la aplicación práctica de la norma en los próximos años será la que revele las pautas de interpretación de la misma, parece ineludible conectar la nueva regulación legal con el interés jurídico que trata de protegerse, y en este sentido delimitar los conceptos legales de fichero y tratamiento en función de las posibilidades de utilización o circulación masiva de los datos personales objeto de los mismos, toda vez que son estas circunstancias, según revela la doctrina y jurisprudencia elaboradas sobre esta materia, las que evidencian el riesgo para la intimidad y demás derechos de las personas que, a su vez, está en la base de la ampliación del ámbito tradicional de protección de estos derechos.

En esta línea parece que cabe interpretar la propia normativa comunitaria cuya adaptación al Derecho interno lleva a cabo la Ley Orgánica 15/1999. El artículo 3 de la Directiva citada circunscribe su ámbito de aplicación 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"; esto es, su objeto queda definido en principio por el tratamiento de carácter

automatizado, y alcanza también al no automatizado en la medida en que afecta a datos incluidos en un sistema organizado de información.

Aplicación transitoria de la Ley Orgánica de Protección de Datos a los ficheros no automatizados

El propio legislador es consciente, sin duda, de la repercusión que entraña la ampliación llevada a cabo por la Ley Orgánica 15/1999, y de ello es muestra el contenido de la Disposición Adicional primera esta norma legal, que pospone la plena aplicación de la Ley a los ficheros y tratamientos no autorizados hasta octubre de 2007, con la única excepción relativa al ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados, que se entiende que pueden hacerse valer, por tanto, desde la propia entrada en vigor de aquélla.

Por otro lado, y a pesar de que pueda existir alguna opinión discrepante, parece también indudable que el ámbito de aplicación del 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, queda limitado, según expresa su propio título, a los ficheros de tal carácter, sin que pueda hacerse extensivo, por tanto, a los ficheros manuales o no automatizados.

Esta conclusión se impone a la vista de lo establecido en la Disposición Transitoria tercera de la Ley Orgánica 15/1999, conforme a la cual, y en tanto no se dicten las oportunas normas reglamentarias por el Gobierno, continuarán en vigor, en cuanto no se opongan a la Ley, las normas reglamentarias existentes, y en concreto, y entre otros, el citado Real Decreto 994/1999. A pesar de que la regulación legal se extiende a los ficheros no automatizados, el sentido de la norma transitoria comentada no es el de ampliar a su vez el ámbito de aplicación del Reglamento de medidas de seguridad, efecto éste que requeriría una declaración expresa en tales términos y que, además, resultaría contradictoria con la citada Disposición Adicional primera de la Ley Orgánica en cuanto que el cumplimiento de las normas de seguridad de los datos no se encuentra entre las previsiones de la Ley que tienen eficacia inmediata respecto de los ficheros no automatizados.

A mayor abundamiento, sería inadmisible pretender aplicar el régimen sancionador dispuesto en caso de incumplimiento de la regulación legal del tratamiento de datos personales mediante una extensión de los requerimientos contenidos en el Real Decreto 994/1999 a los ficheros no automatizados, no expresamente incluidos en el ámbito del reglamento.

El resultado no deja de ser paradójico; es incuestionable la ampliación del objeto legal de la regulación del tratamiento de datos de carácter personal, y las dificultades interpretativas que ello suscita, si bien la repercusión inmediata de esta ampliación es muy relativa al limitarse, y no sin problemas de aplicación, al ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Esta consideración reduce, de momento, el estudio de las normas sobre seguridad de ficheros a los de carácter automatizado. Una matización mayor debe hacerse, no obstante, en lo que concierne a las normas sobre confidencialidad de los ficheros; entendida en sentido amplio, abarcando, por tanto, todas las previsiones contenidas en la Ley Orgánica 15/1999 que regulan el acceso y la comunicación de los datos de carácter personal, hay que entender que, conforme a la Disposición Adicional primera ya examinada, la aplicación plena de tales normas sólo puede predicarse respecto de los ficheros automatizados. Sin embargo, es también indudable que los ficheros no automatizados quedan sujetos a las normas generales que protegen el derecho al honor y a la intimidad personal y familiar del individuo, y en tal sentido es obligado afirmar un deber estricto de confidencialidad en relación con los datos personales de carácter reservado o íntimo que se contengan en tales ficheros.

EL ACCESO A LA INFORMACIÓN CLÍNICA Y LA CESIÓN DE DATOS

De acuerdo con el concepto amplio antes apuntado, el estudio de la confidencialidad de los sistemas de información permite abarcar, por un lado, las normas que contemplan las personas habilitadas para el tratamiento y acceso a los datos de carácter personal, y por otro, la regulación de la comunicación o cesión a terceros de dichos datos.

A) EL ACCESO A LA INFORMACIÓN CLÍNICA

Comenzando por el primero de los aspectos señalados, y desde la óptica de los sistemas de información clínica, cabe señalar que precisamente una de las cuestiones de mayor trascendencia, y al mismo tiempo dificultad, que suscita la historia clínica y que se agrava con su tratamiento automatizado viene constituida por la determinación de las personas que, además del propio paciente, deben considerarse autorizadas para el acceso a la misma; ello es debido a que no es éste un extremo que venga concretado normativamente.

Normativa sanitaria y legislación sobre protección de datos

La legislación sanitaria se limita a enunciar un principio general de restricción en cuanto al acceso a la historia, según se deduce de los términos que utiliza el art. 61 de la Ley General de Sanidad, conforme al cual se contempla el acceso a la misma, además de por el propio paciente, por parte de los facultativos implicados directamente en el diagnóstico y tratamiento del paciente. Esta última mención legal no es suficiente por cuanto, al referirse en exclusiva al personal facultativo implicado directamente en el diagnóstico y tratamiento del enfermo, no prevé, por tanto, que otros diversos colectivos profesionales que trabajan en el ámbito de las instituciones sanitarias pueden también acceder o manejar, bien es cierto que de modo más limitado, la historia clínica (piénsese en el personal de enfermería que debe consultarla para el ejercicio de las funciones que le son propias, o incluso en el personal administrativo que deba reflejar en ella determinados datos).

La Ley Orgánica 5/1992 no aportaba mayor solución a este problema, por cuanto se limitaba a exigir que quede constancia del órgano (en el caso de las Administraciones Públicas) o la persona (en el caso de ficheros de titularidad privada) que tiene la consideración de responsable del fichero; determinación que por sí sola no permite concretar la totalidad de personas que pueden utilizar o acceder, con fines más amplios o más restringidos, a la historia clínica informatizada, si bien contribuye a delimitar responsabilidades en caso de acceso o utilización no autorizada de aquélla.

La Ley Orgánica 15/1999 introduce alguna modificación respecto de la regulación precedente. Se mantiene la figura del responsable del fichero o tratamiento, definido como “persona física o jurídica, de naturaleza pública o privada, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”; pero junto a ella aparece el encargado del tratamiento, que es “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”.

Además, y afectando de manera específica a los sistemas de información clínica, constituye una novedad destacable de la Ley Orgánica 15/1999 la previsión contenida en su artículo 7.6, que, siguiendo en gran medida el criterio de la Recomendación de 13 de febrero de 1997 del Consejo de Europa, autoriza el tratamiento, entre otros, de los datos relativos a la salud siempre que el mismo se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Esta última norma contribuye bastante más a delimitar el perfil de las personas autorizadas para el acceso y tratamiento de los datos de salud; no obstante, tampoco está exenta de algunas dudas interpretativas en lo que afecta a determinar cuáles son esas otras personas con obligación de secreto equivalente a la de los profesionales sanitarios. En efecto, si se parte de que toda persona que por razón de su actividad laboral o profesional tenga acceso a información de carácter reservado (y la que afecta a datos de salud lo es) viene obligada por un deber de confidencialidad respecto de la misma, habrá que entender que esa obligación de secreto equivalente a la de los profesionales sanitarios debe representar un plus sobre aquel deber genérico; pero por otro lado, tampoco es pacífica, al menos en el Derecho español, la cuestión relativa a en qué actividades cabe afirmar un deber de secreto profesional en sentido propio, cuestión con importantes consecuencias legales y procesales (el vigente Código Penal, sin ir más lejos, tipifica como delitos distintos la vulneración del secreto profesional y la revelación de datos reservados conocidos por razón de la actividad laboral o profesional).

Esta previsión normativa está llevando a entender, al menos en ámbitos no sanitarios, que cuando los sistemas de información incluyan datos de esta naturaleza su tratamiento debe encomendarse a profesionales de la salud. No obstante, este criterio, tal vez válido en aquellos sectores de actividad donde el tratamiento de información sanitaria sea una excepción, no resulta satisfactorio en el ámbito sanitario, en el que parece ineludible, al menos en el modelo organizativo actual, admitir un cierto grado de acceso, aunque sea limitado, a colectivos profesionales no afectados por un deber de secreto profesional en sentido estricto.

Previsiones del Real Decreto 994/1999, de 11 de junio

En todo caso, la regulación legal respecto a las personas autorizadas para el acceso y tratamiento de datos personales debe completarse, a su vez, con lo establecido en el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, normativa que incide más en la exigencia de una previa constancia e identificación de las personas con acceso autorizado a cada fichero, que en el establecimiento de criterios generales respecto a quiénes deban ser objeto de autorización.

En este sentido, la relación de todas y cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información, con indicación además de sus funciones y obligaciones concretas, forma parte del contenido necesario del denominado documento de seguridad, que constituye la pieza clave en la ordena-

ción de las medidas de seguridad de todos los niveles. A esta obligación se añade, además, la exigencia dirigida al establecimiento de procedimientos de identificación y autentificación para el acceso al sistema de información, así como de controles de acceso con el fin de que los usuarios puedan acceder a aquellos contactos y recursos estrictamente necesarios para el desarrollo de sus funciones.

Estas previsiones, establecidas para el nivel básico pero exigibles para todos los niveles, se incrementan en los niveles medio y alto mediante un reforzamiento de las exigencias de identificación y autentificación, hasta llegar a la implantación, en los ficheros de nivel alto, de un registro de accesos que permita guardar en relación con cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En suma, el conjunto de normas legales y reglamentarias examinadas permiten establecer un principio restrictivo en cuanto al acceso y manejo de la información de carácter personal, en el sentido de que, aun admitiendo diversas posibles formas de organización del trabajo, el volumen de información accesible a cada persona es el estrictamente imprescindible para el correcto desempeño de sus funciones, aspecto éste que en cualquier caso puede ser revisado y fiscalizado con base en el citado documento de seguridad.

Todo ello con independencia de que, en cualquier caso, es también indudable el deber general de secreto que se impone a toda persona que por razón de su trabajo tenga acceso a información de datos relativos a la intimidad de las personas; deber cuya infracción acarrea además importantes consecuencias legales.

Contratación externa del tratamiento de datos

El tratamiento de esta materia no puede cerrarse sin hacer una referencia a la posibilidad del acceso de los datos por cuenta de terceros, actualmente prevista en el art. 12 de la Ley Orgánica 15/1999, que representa una importante novedad con respecto a la regulación anterior y que permite solventar ciertas dudas surgidas al amparo de ésta última. La afirmación contenida en dicho precepto, en el sentido de que “no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento”, constituye en realidad una habilitación para la posible contratación externa del tratamiento de datos de carácter personal, cuestión siempre debatida por los riesgos que entraña en orden a la seguridad y confidencialidad de la información.

Téngase en cuenta que la no consideración como comunicación de datos conlleva la innecesariedad del consentimiento del afectado. Por ello, a partir de esta modificación legal es patente la admisión de esta figura, si bien sometida a determinados requerimientos legales como son, básicamente, la necesaria constancia en contrato escrito (u otra forma que permita acreditar su celebración y contenido), la necesidad de pactar expresamente determinadas obligaciones del encargado del tratamiento (acatamiento de las instrucciones del responsable del tratamiento, no aplicación de los datos a fin distinto al del contrato y no comunicación de los mismos al tercero) y de estipular las medidas de seguridad aplicables, y la obligación de destrucción o devolución de los datos al responsable del tratamiento una vez cumplida la prestación contractual.

Esta regulación legal viene, en gran medida, a otorgar rango normativo a determinados criterios que la práctica había venido aplicando para la utilización de la contratación externa, ya que en todo caso la conclusión contraria a la admisión de la misma, aun a pesar del silencio de la Ley Orgánica 5/1992, no parecía una solución razonable.

B) COMUNICACIÓN DE DATOS. EL CONSENTIMIENTO DEL AFECTADO Y SUS EXCEPCIONES

El segundo gran apartado, el referido a la determinación de los supuestos en que la información clínica es accesible a terceros, obliga a considerar conjuntamente los dos ámbitos normativos implicados, a saber, la legislación sanitaria por un lado, y la regulación legal del tratamiento de datos de carácter personal. Con base en una y otra normativa, no obstante, el fundamento que legitima el acceso por parte de terceros a información de carácter personal es el mismo; a saber, el derecho del paciente a la confidencialidad de la información sanitaria relativa a su proceso, caracterizado como derecho fundamental en cuanto expresión al derecho a la intimidad personal del sujeto, no está exento de límites o excepciones, del mismo modo que sucede con cualquier otro derecho reconocido por el ordenamiento jurídico que, por definición, nunca es absoluto sino que encuentra su límite en la protección de otros derechos o intereses legítimos.

Comenzando por el segundo bloque normativo señalado, debe indicarse que las previsiones de la Ley Orgánica 15/1999 relativas a los supuestos expresamente admitidos de cesión y comunicación de datos son indudablemente aplicables, dado su carácter de regulación general, a los sistemas de información clínica.

En este sentido, el principio general que consagra la norma es el de la necesidad del previo consentimiento del interesado para que los datos de carácter perso-

nal objeto de tratamiento puedan ser comunicados a un tercero, siempre y cuando, además, dicha comunicación obedezca al cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Mayor interés que el principio general reviste, sin embargo, la determinación de los supuestos en que la necesidad de aquel consentimiento queda exceptuada, ya que son éstos los supuestos que plantean mayor conflictividad en su aplicación práctica y los que generan asimismo importantes dudas de interpretación.

Exepciones de carácter general

a) La primera de las excepciones viene referida a aquellos casos en que la cesión esté autorizada por una ley. Por esta vía es necesario efectuar una remisión a la regulación específica en el ámbito sanitario, a la que luego se aludirá.

b) Queda exceptuada también del consentimiento del afectado la comunicación de datos recogidos de fuentes accesibles al público, aspecto éste en el que la Ley Orgánica 15/1999 introduce, en relación con la legislación derogada, la novedad importante de definir de modo exhaustivo cuáles son las fuentes que tienen tal carácter.

c) Una excepción importante es la que contempla la ley al excluir el consentimiento "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros". Las dificultades interpretativas de este precepto son notables, aún cuando en principio parece extender al ámbito de la comunicación de los datos la misma excepción al consentimiento del afectado que rige para el tratamiento de los mismos (esto es, la existencia de una relación negocial que exija necesariamente la cesión). Teniendo en cuenta la amplitud de los conceptos manejados por la propia regulación legal y los términos en que se expresa este precepto, no sería descartable su aplicación a supuestos tradicionalmente problemáticos y discutibles, como son los de acceso por parte de un tercero a datos personales (incluso sensibles) con base en el interés legítimo derivado de un contrato suscrito entre dicho tercero y el afectado; el ejemplo típico, en el caso de los sistemas de información clínica, viene constituido por las peticiones de acceso a datos de la salud de las personas formuladas por entidades aseguradoras con quienes el interesado tiene suscrito un determinado contrato de seguro para cuyo cumplimiento puede resultar necesario el conocimiento de aquella información.

d) La Ley Orgánica 15/1999 contempla también, como excepción al consentimiento del afectado, la comunicación de datos que deba efectuarse a favor del

Defensor del Pueblo, el Ministerio Fiscal, los Jueces y Tribunales y el Tribunal de Cuentas (incluyendo a las instituciones autonómicas con funciones análogas al primero y último de los citados), cuando se enmarque en el ejercicio de las funciones que tienen atribuidas. La previsión legal no resulta novedosa en relación con la disposición de la información clínica a favor de los órganos judiciales, conforme a un criterio y una práctica comúnmente admitidos, aunque no exentos de dudas y conflictos planteados, sobre todo, en relación con las condiciones en que debe facilitarse esa información a los Juzgados y Tribunales. Sin embargo, la nueva regulación legal sí añade una mayor claridad al incluir, junto a los órganos judiciales, a las demás instituciones que cita, respecto de las que el acceso a información de carácter personal, incluso reservada, se fundamenta en el ejercicio legítimo de las funciones que constitucional y legalmente tienen atribuidas.

La cesión entre Administraciones Públicas

Mención especial merece el tratamiento de la cesión de datos entre las Administraciones Públicas, ya que en este caso se amplían de modo considerable las posibilidades de cesión de la información de carácter personal con fundamento, asimismo, en el ejercicio de las funciones que legalmente se atribuyen a las Administraciones Públicas.

De la redacción del art. 21 de la Ley Orgánica se desprende que no es necesario el consentimiento del afectado (como se encarga de aclarar su apartado cuarto) en diversos supuestos; en primer lugar, la redacción inicial del precepto permite entender que la cesión entre Administraciones Públicas distintas está autorizada cuando se trata de ejercer las mismas competencias sobre idéntica materia (sólo así se entiende la formulación de la norma en términos negativos).

Pero además, aun no concurriendo esta circunstancia, la cesión o comunicación se permite, de acuerdo con el mismo precepto, siempre que haya sido prevista por las disposiciones de creación del fichero o por una disposición de rango superior que regule su uso, y en todo caso cuando la comunicación tenga por objeto el posterior tratamiento de los datos con fines históricos, estadísticos o científicos. En suma, la ampliación de los supuestos admitidos de comunicación de datos en el caso de las Administraciones Públicas es notable con respecto a los ficheros de titularidad privada, que quedan sujetos sin más a las normas generales señaladas.

Estas conclusiones, no obstante, deben ser revisadas a tenor de la reciente sentencia 292/2000, de 30 de noviembre, dictada por el pleno del Tribunal Constitucional en el recurso de inconstitucionalidad promovido por el Defensor del Pueblo respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, cuyo

fallo, estimatorio del recurso interpuesto, declara inconstitucionales, y por tanto nulos, determinados incisos de los preceptos impugnados. Sin perjuicio de un examen más profundo del citado pronunciamiento (que excede del objeto del presente estudio), debe resaltarse, por lo que aquí interesa, que la declaración de inconstitucionalidad afecta a la previsión legal de la posibilidad de cesión de datos entre Administraciones Públicas, para el ejercicio de competencias distintas o sobre materias diferentes, siempre que aquélla hubiera sido prevista por la norma de creación del fichero o por una disposición de superior rango que regule su uso.

Esta declaración, de consecuencias ciertamente notables (y que debiera obligar en buena lógica a una reforma de la Ley que delimite en mayor medida los supuestos admisibles de cesión de datos entre Administraciones Públicas), descansa en un motivo ("claro", según señala el Tribunal) expresado en el fundamento decimocuarto de la sentencia, que no obstante suscita importantes dudas. El vicio de inconstitucionalidad viene provocado, a juicio del Alto Tribunal, por el hecho de que la Ley haya renunciado a fijar "los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado", afirmación esta última que no deja de resultar peculiar si se tiene en cuenta que precisamente el ejercicio legítimo de las funciones encomendadas a la Administraciones Públicas habilita a éstas para el tratamiento (y por tanto la recogida) de datos sin necesidad de consentimiento del interesado, conforme al artículo 6 de la propia Ley Orgánica 15/1999, excepción que, salvo que en sí misma fuera declarada también inconstitucional, parece coherente en su fundamento con la previsión legal ahora anulada.

Excepciones propias de los sistemas de información clínica

a) La última de las excepciones que contempla la Ley Orgánica, en cuanto a la comunicación de datos sin consentimiento del interesado, viene referida a un supuesto específico o propio del ámbito sanitario como es "la cesión de datos de carácter personal relativos a la salud (que) 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". El inciso primero de la norma prevé lo que podría considerarse un supuesto de estado de necesidad sanitaria, reflejo de la consideración que al legislador le merece la especial problemática que puede suscitarse en relación con los sistemas de información de datos sanitarios, de la que es ejemplo a su vez el tratamiento específico que recibe la transferencia internacional de datos que "sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o trata-

miento médicos o la gestión de servicios sanitarios", a la que se exime del cumplimiento de los requisitos generales exigibles para el movimiento internacional de datos.

b) Por otro lado, es obligada la remisión a la propia legislación sanitaria para completar el régimen legal de habilitación de la cesión o comunicación de datos, remisión que, como se ha visto, la Ley Orgánica ordena en dos ocasiones, una con carácter general (supuestos de cesión autorizada por una Ley) y otra específica en el supuesto de cesión necesaria para la realización de estudios epidemiológicos conforme a la legislación sobre sanidad.

En este sentido, la propia regulación legal de la historia clínica contempla diversos supuestos en los que el carácter reservado de la información contenida en aquélla cede ante determinados fines; así lo establece el art. 61 de la Ley General de Sanidad, que permite la posible utilización de la información contenida en las historias clínicas con fines científicos o para la realización de estudios epidemiológicos, así como para las actuaciones de inspección médica (excepción justificada en el ejercicio legítimo de las funciones de inspección y control atribuidas legalmente a las Administraciones sanitarias).

No obstante, cabe destacar la existencia de un proyecto de modificación en esta materia, que se plasma en un borrador de regulación legal básica en materia de información y documentación clínica, elaborado en 1999 por el Ministerio de Sanidad y Consumo, y que modificaría en este y en otros puntos la normativa vigente contenida en la Ley General de Sanidad. Por su interés merece hacer mención de las previsiones contenidas en dicho borrador en relación con el acceso y disposición de la historia clínica, materia en la que establece un grado de concreción mayor, al contemplar las siguientes situaciones:

1) Como regla general, la historia estará disponible para todos los profesionales que intervengan en el proceso asistencial. Nótese que el término utilizado (profesionales y no facultativos) es más amplio que el actual y permite solventar algunas de las dudas que han quedado apuntadas.

2) Se contempla, asimismo, el acceso en supuestos de requerimiento judicial, seguridad y salud pública, investigación y docencia debidamente autorizados, y demás situaciones previstas en la Ley.

3) También se permite la utilización de la historia clínica para el ejercicio de funciones de inspección sanitaria, actividades de evaluación y acreditación y otras

motivadas por la autoridad sanitaria que tengan por objeto mejorar la calidad de la asistencia.

4) Y por último, se prevé el acceso a la historia en defensa de los intereses generales en casos de urgencia o necesidad.

En suma, y aun con dificultades de interpretación en algunas de las excepciones previstas, la aplicación conjunta de la normativa sanitaria y de la regulación del tratamiento de datos permite concretar con relativa precisión los supuestos en que es legalmente admisible el acceso por parte de terceros a la información clínica, configurando de esta manera el contorno y los límites del deber de confidencialidad exigible en relación con los datos de carácter personal.

ASPECTOS PRINCIPALES DE LA REGULACIÓN CONTENIDA EN EL REAL DECRETO 994/1999, DE 11 DE JUNIO

El 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, constituye el desarrollo de lo dispuesto en el art. 9 de la Ley Orgánica 5/1992, precepto legal cuya redacción, con la única salvedad referida a la inclusión del encargado del tratamiento junto al responsable del fichero como sujeto obligado, se mantiene intacta en la Ley Orgánica 15/1999.

Este precepto legal, a través de los tres párrafos en que se redacta, contempla en realidad tres previsiones distintas. Por un lado, se establece un deber, definido en términos genéricos, de adoptar "las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado". Como puede observarse, este apartado no efectúa una remisión al reglamento en orden a la determinación de cuáles son esas medidas, sino que contiene una obligación, en principio jurídicamente exigible, que se concreta en función de las propias circunstancias, o, como señala el propio precepto, de acuerdo con el "estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos".

La llamada al Reglamento se efectúa propiamente en los dos restantes apartados de la norma legal comentada, con carácter general para todo tipo de datos de carácter personal, por un lado, y de modo específico para los datos especialmente protegidos, entre los que se encuentran los relativos a la salud de las personas, por otro. Dicha norma reglamentaria debe regular, según el mandato legal, las condiciones de integridad y seguridad de los datos y de los centros de tratamiento, loca-

les, equipos, sistemas y programas, así como los de los ficheros y las personas en el caso de tratamiento de datos sensibles.

Cabe destacar que el régimen sancionador dispuesto por la propia Ley Orgánica tipifica como infracción grave el incumplimiento de las condiciones que se establezcan reglamentariamente en relación con los ficheros, locales, programas o equipos que contengan datos de carácter personal, si bien el incumplimiento del deber genérico contenido en al apartado primero del precepto legal que se examina podría, probablemente, encontrar acomodo en alguna otra de las conductas susceptibles de ser sancionadas conforme a aquel régimen.

Abordada con anterioridad la cuestión relativa al ámbito de aplicación del Reglamento, el estudio debe centrarse en un breve análisis de algunos de los aspectos destacables de una regulación que, no obstante su carácter esencialmente técnico, merece también ciertas consideraciones de índole jurídica, comenzando por la primera y esencial referida a su fundamento o razón de ser, que, como expresa su propia exposición de motivos en concordancia con la norma legal objeto de desarrollo, radica en la necesidad de garantizar la confidencialidad e integridad de la información como modo de protección de los derechos al honor y a la intimidad personal y familiar y demás derechos de la persona.

Debe reseñarse, igualmente, el carácter básico o mínimo que revisten las previsiones establecidas en el Reglamento, en cuanto aplicables a todo tipo de ficheros que contengan datos de carácter personal con independencia de las medidas especiales que puedan establecerse para ficheros que, por la peculiar naturaleza de los datos contenidos en ellos, exijan una mayor protección.

Niveles de seguridad

Las disposiciones reglamentarias se articulan en torno a tres niveles de seguridad, que se establecen atendiendo a la naturaleza de los datos que son objeto de tratamiento. Las exigencias y medidas de seguridad se disponen de manera acumulativa, de tal forma que todos los ficheros deben cumplir las previsiones establecidas para el nivel básico y además las vinculadas a los niveles medio y, en su caso, alto en el supuesto de que el fichero en cuestión contenga datos de los que obligan a su adopción.

Los ficheros que contengan datos referidos a la salud y a la vida sexual de las personas se clasifican entre los de nivel alto, lo que implica, en principio, el sometimiento de los sistemas de información clínica al grado más elevado de protección dispensado por la norma reglamentaria.

El establecimiento de tres niveles de protección trasciende asimismo al ámbito de aplicación temporal del Reglamento, que dispone la implantación de las medidas de nivel básico en el plazo de seis meses desde su entrada en vigor (prevista para el día siguiente a su publicación oficial), en el de un año en el caso de las medidas de nivel medio, y en el de dos años para las de nivel alto. El primero de los plazos resulta, por lo demás, ampliado hasta el 26 de marzo de 2000 en virtud de la modificación introducida por el Real Decreto 195/2000, de 11 de febrero.

Ámbito de aplicación

El Reglamento es de aplicación, según se ha visto, a los tratamientos de datos personales de carácter automatizado, si bien la norma se encarga de precisar que sus previsiones resultan aplicables íntegramente a tales ficheros ya sean permanentes o temporales, ordenando respecto de estos últimos su borrado una vez que dejen de ser necesarios para los fines que motivaron su creación. Asimismo, las medidas establecidas para cada uno de los niveles se aplican al acceso a datos de carácter personal a través de redes de comunicaciones, según señala el art. 5 del Reglamento.

El documento de seguridad.

La regulación descansa, como elemento básico, en el documento de seguridad, en el que deben integrarse y contenerse las medidas, normas y procedimientos de seguridad establecidos por el responsable del fichero conforme a las propias exigencias del Reglamento; de ahí que éste defina un contenido mínimo del documento de seguridad, respecto del que se ordena asimismo su permanente revisión y actualización en función de las modificaciones operadas en el propio sistema de información o en las disposiciones normativas aplicables en materia de seguridad.

Las normas establecidas para el nivel básico, y aplicables por tanto a todo fichero, vienen referidas a las funciones y obligaciones del personal, a la existencia de un registro de incidencias, a la identificación y autentificación de usuarios, a los controles de acceso, a la gestión de soportes y a las copias de respaldo y seguridad. En los niveles superiores, con carácter general, se incrementan las exigencias impuestas para cada uno de tales aspectos, incorporando en algunos supuestos obligaciones añadidas, como es el caso de la figura del responsable de seguridad y la auditoría (interna o externa) en los ficheros de nivel medio (y por tanto, también en los de nivel alto), o la necesidad de cifrado de datos para la distribución de soportes de datos, o transmisión de los mismos a través de redes de comunicaciones, en el caso de los ficheros de nivel alto.

Algunas consideraciones de carácter jurídico

a) A la vista del criterio establecido para determinar la aplicación de las medidas de seguridad de uno u otro nivel, reviste un notable interés, desde un punto de vista jurídico, la delimitación del concepto de "datos de salud" a que alude el Reglamento. A falta de una definición legal del término, parece que debe considerarse incluida dentro del mismo toda información referida al estado de salud física o mental de la persona, no estando tan claro que constituyan datos de tal naturaleza (aunque puede resultar discutible) aquellas informaciones de tipo administrativo o burocrático referidas al proceso asistencial. Tampoco la jurisprudencia aclara demasiado al respecto, ya que los escasos pronunciamientos recaídos hasta el momento se han dictado sobre supuestos de hecho no dudosos, como es el caso de la sentencia 202/1999, de 8 de noviembre, ya citada, del Tribunal Constitucional, que considera de tal naturaleza la información relativa al diagnóstico médico contenida en una base de datos de absentismo laboral.

b) Por otro lado, y aun cuando afecta a aspectos de naturaleza esencialmente técnica, es llamativo, desde una perspectiva legal, el alto nivel de exigencia que deriva de la aplicación estricta del Reglamento de medidas de seguridad, que en ocasiones plantea dudas reales respecto de la posibilidad misma de cumplimiento de sus previsiones. A efectos ilustrativos cabe citar, por ejemplo, el ya comentado registro de accesos que es obligatorio para los ficheros de nivel alto, y cuya efectiva implantación parece requerir, desde un punto de vista estrictamente técnico, una capacidad de los sistemas de información muy superior a la necesaria para el propio tratamiento de los datos. La referencia al "estado de la tecnología" que se contiene en el artículo 9 de la Ley al establecer el deber de adopción de las medidas de seguridad de los datos queda, en cierto modo, puesta en entredicho con previsiones como la que se examina.

c) Como último aspecto de la regulación en materia de seguridad, cabe mencionar la remisión al régimen sancionador de la Ley Orgánica 5/1992 (referencia que hay que entender hecha en la actualidad a lo dispuesto en la Ley Orgánica 15/1999) para el caso de incumplimiento de las medidas de seguridad impuestas por el Reglamento; régimen que, como es sabido, determina la inaplicación de sanciones económicas a las infracciones cometidas por las Administraciones Públicas, sustituidas por la facultad de la Agencia de Protección de Datos de dictar resolución con las medidas de obligado cumplimiento para el cese de la conducta infractora y de proponer la iniciación de las actuaciones disciplinarias oportunas.

A MODO DE CONCLUSIÓN

El examen jurídico de la regulación relativa al tratamiento de datos de carácter personal, y específicamente en materia de seguridad y confidencialidad, parece arrojar más dudas que certezas en relación con un marco legal que, sin demasiados

riesgos, puede calificarse como exigente y riguroso. Las críticas, sin embargo, no deben dirigirse contra esta última caracterización (fruto de una determinada opción legislativa), sino contra la falta de una clara delimitación de aspectos y elementos esenciales que afectan al propio ámbito de protección dispensado por de la norma o a la aplicación de instrumentos y garantías esenciales previstos por la misma.

Las incertidumbres sobre la interpretación y aplicación que definitivamente se dé a la Ley Orgánica 15/1999 son por ello importantes, y frente a las mismas cabe reclamar más que nunca la necesidad de un criterio ponderado que conjugue los intereses que se tratan de proteger con la debida consideración de la realidad social en que la norma debe ser aplicada.

ANEXO. RELACIÓN DE NORMAS Y SENTENCIAS CITADAS

1. Ley 14/1986, de 25 de abril, General de Sanidad. BOE 29-4-1986, núm. 102.
2. Ley Orgánica 5/1992, de 29 de octubre, por la que se regula el tratamiento automatizado de los datos de carácter personal. BOE 31-10-1992, núm. 262.
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal. BOE 14-12-1999, núm. 298.
4. Directiva 95/46/CE, 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. DOCE nº L 281/39.
5. 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. BOE 25-6-1999, núm. 151.
6. Ley Orgánica 1/1982, de 5 de mayo, reguladora de la protección civil del honor, de la intimidad personal y familiar y de la propia imagen. BOE 14-5-1982, núm. 115.
7. Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. BOE 18-8-1993.
8. Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo. BOE 13-6-1994.
9. Sentencia del Tribunal Constitucional 11/1998, de 13 de enero. BOE 12-2-1998.
10. Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre. BOE 16-12-1999.
11. Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. BOE 4-1-2001.

FUNCIONES DE LA AGENCIA DE PROTECCION DE DATOS. TRATAMIENTO Y CONFIDENCIA-LIDAD DE DATOS DE SALUD

Jesús Rubí Navarrete

Adjunto Director Agencia Protección de Datos

LA AGENCIA DE PROTECCIÓN DE DATOS

El art. 18 de la Constitución española tiene como objeto la regulación del derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como la inviolabilidad del domicilio y el secreto de las comunicaciones.

Su apartado 4 contiene previsiones específicas para garantizar el honor y la intimidad personal y familiar frente al uso de la informática.

La jurisprudencia del Tribunal Constitucional ha reforzado la configuración constitucional del derecho reconocido en el art. 18.4 afirmando que se trata de un derecho fundamental autónomo que obliga a todos los poderes públicos y que reviste el carácter de un auténtico derecho subjetivo, origen inmediato de derechos y obligaciones y no el de un mero principio programático.

La protección constitucional de este derecho se encuentra recogida, fundamentalmente, en la Ley Orgánica 15/1999, de 13 de diciembre, que desarrolla el art. 18.4 de la Constitución.

El órgano encargado de dicha protección es la Agencia de Protección de Datos (APD/La Agencia). La Ley Orgánica configura a la Agencia como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

La independencia de la APD se articula en torno a un triple orden de elementos.

Por una parte, previendo que el Director de la Agencia, una vez nombrado, tendrá un mandato de cuatro años, sin que pueda producirse su cese por decisión del Ejecutivo, salvo que concurra alguna de las circunstancias tasadas normativamente: Incumplimiento grave de las obligaciones del cargo, incapacidad sobrevenida para el ejercicio de sus funciones, incompatibilidad o condena por delito doloso. De este modo la actuación del Director de la Agencia se sustrae a una posible remoción por parte del Gobierno, cualquiera que sea aquélla.

En segundo lugar, estableciendo que ejerce sus funciones con plena independencia y objetividad, no estando sujeto a instrucción alguna en el desempeño de aquéllas.

Finalmente, contemplando que sus resoluciones no puedan ser objeto de revocación por autoridad administrativa alguna, sino por órganos jurisdiccionales independientes y, en particular, por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

FUNCIONES DE LA AGENCIA DE PROTECCIÓN DE DATOS

La Ley Orgánica atribuye a la APD la función de velar por el cumplimiento de la normativa de protección de datos personales contemplando, a tal efecto, un conjunto de funciones que, sintéticamente, se exponen a continuación.

Registro General de Protección de Datos

La primera de ellas es una función de carácter informativo respecto de los ciudadanos. Esta función consiste en facilitarles información sobre los ficheros existentes, sobre la finalidad de los mismos y sobre la identidad del responsable del fichero.

El instrumento previsto específicamente para hacer efectiva esta función es el Registro General de Protección de Datos al que, imperativamente, deberán ser notificados tanto los ficheros de titularidad pública como los de titularidad privada con objeto de que, si cumplen las exigencias legales, sean objeto de inscripción.

La creación de ficheros de titularidad pública deberá ser habilitada por medio de una disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente antes de ser notificados e inscritos en el Registro. Los de titularidad privada podrán crearse para el logro de actividades u objetos legítimos de su titular debiendo notificarse previamente a su inscripción al Registro mencionado.

La inscripción debe incluir, entre otros aspectos, los datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición que la Ley reconoce. El acceso al mismo es gratuito por parte de los ciudadanos.

La inscripción, acorde con su finalidad informativa, es meramente declarativa sin que constituya una autorización para la existencia de los ficheros ni sane las posibles actuaciones contrarias a la normativa de protección de datos personales.

De este modo, el Registro se configura como un órgano que permite a los ciudadanos conocer la existencia de los ficheros en los que pueden estar incluidos sus datos personales, así como informarse acerca de dónde y ante quién pueden ejercer los derechos de acceso, rectificación, cancelación y oposición.

Tutela de los derechos de acceso, rectificación, cancelación y oposición

La segunda de las funciones atribuidas a la Agencia es la de tutelar el ejercicio de los citados derechos.

Estos tienen carácter personalísimo y deben ser ejercitados, en primer lugar, ante el responsable del fichero que contenga sus datos personales. No obstante, si dicho ejercicio es negado u obstaculizado por el responsable del fichero, la Ley atribuye a la APD la competencia para garantizarlo.

A tal efecto, se tramitará el correspondiente procedimiento administrativo en el que deberá analizarse la conformidad o disconformidad de la negativa respecto de las previsiones legales y, en caso de apreciarse que la negativa al ejercicio de los derechos es ilícita, la Agencia impondrá el ejercicio de los mismos, incurriendo en infracción administrativa sancionable el responsable del fichero que impide su ejercicio.

Además de la responsabilidad administrativa por el incumplimiento de la Ley, los afectados que como consecuencia de la misma sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados. Esta responsabilidad deberá exigirse conforme al régimen de responsabilidad de las Administraciones Públicas en el caso de los ficheros de titularidad pública y, ante los órganos de jurisdicción ordinaria en el caso de los ficheros de titularidad privada.

Vigilancia del cumplimiento de la normativa de protección de datos

Además de garantizar los derechos de los interesados, la competencia de la Agencia de velar por el cumplimiento de la normativa de protección de datos personales se lleva a cabo declarando la existencia de infracciones e imponiendo las correspondientes sanciones.

Tal declaración se realiza mediante la instrucción de un procedimiento administrativo sancionador, con plenas garantías para las partes.

Antes de iniciar el expediente la Agencia puede realizar actuaciones previas, que no forman parte de aquél, a fin de acreditar las circunstancias de hecho concurrentes.

Para ello la Ley le atribuye la potestad de inspección en cuya virtud, los funcionarios inspectores pueden solicitar la exhibición o el envío de documentos y datos examinados en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados. Los inspectores tienen la con-

sideración de autoridad pública en el desempeño de sus cometidos, estando obligados a guardar secreto sobre las informaciones que conozcan en ejercicio de las mismas, incluso después de haber cesado en el desempeño de su actividad.

Las actuaciones inspectoras pueden realizarse como consecuencia de denuncia o de oficio, siendo cada vez más frecuente la realización de planes de inspección de esta última naturaleza dirigidos a comprobar el cumplimiento de la normativa de protección de datos, especialmente en aquellos sectores como el sanitario en el que se tratan datos especialmente protegidos, o en los que se produce un tratamiento masivo de datos (entidades financieras, operadores de telecomunicaciones, prestadoras de servicios básicos, etc..). Las inspecciones de oficio suelen concluir con la adopción por parte de la Agencia de recomendaciones que faciliten el cumplimiento de la normativa de protección de datos. No obstante, de apreciarse presuntas infracciones de ésta, se producirá la iniciación de expedientes sancionadores.

En el caso de acreditarse una infracción, si se hubiera producido por parte de una Administración Pública, el Director de la Agencia declarará la responsabilidad de la misma, sin imposición de sanción económica, pudiendo recabar la exigencia de responsabilidad al funcionario responsable de aquélla. Estas declaraciones, así como las medidas que se hayan adoptado para cumplir la Ley deben ser comunicadas al Defensor del Pueblo.

De resultar responsable de la infracción el titular de un fichero privado debe imponerse las sanciones económicas previstas en la ley que comprenden un abanico entre 100.000 y 100.000.000 de pesetas.

Sin embargo, las posibilidades que la Ley atribuye a la Agencia para garantizar la privacidad no se agotan en la imposición de sanciones. La norma atribuye a su Director la competencia de adoptar medidas cautelares dirigidas a exigir a los responsables de los ficheros la adopción de las medidas necesarias para adecuarse a las exigencias legales, pudiendo ordenar, en su caso, la cesación de los tratamientos y la cancelación de los ficheros. De este modo, es posible garantizar la intimidad de los afectados, incluso con carácter previo a la declaración de existencia de infracciones, en situaciones urgentes o cuando pueda apreciar que el contenido de la resolución definitiva no será efectivo sin la adopción de medidas cautelares. Asimismo, la Ley permite con dichas medidas velar por la privacidad en aquellos casos en los que la cuantía de la sanción económica no resultar disuasoria para que el infractor cese en el tratamiento ilícito de datos personales.

Las exigencias de la Ley Orgánica para la protección de los datos personales tienen el carácter de mínimos, pudiendo los responsables de los ficheros intensifi-

car o ampliar dicha protección. A tal efecto, la Ley contempla la posibilidad de que se adopten códigos-tipo, mediante acuerdos sectoriales, convenios administrativos o decisiones de una empresa. Los códigos.tipo tienen el carácter de códigos deontológicos o de buena práctica profesional debiendo ser inscritos, para su conocimiento por los ciudadanos, en el Registro General de Protección de Datos, previa decisión del Director de la Agencia.

Finalmente, la APD debe autorizar las transferencias internacionales de datos en los casos previstos en la Ley Orgánica. Los datos personales sólo podrán ser transferidos a terceros países cuando, además de cumplir las exigencias de la Ley, el país de destino tenga un nivel de protección adecuado o equiparable al que garantiza la norma española.

Las transferencias son posibles a los países de la Unión Europea ya que, por exigencia de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, los Estados Miembros gozan de dicho nivel de protección, estando garantizada la libre circulación de datos personales entre ellos.

En el caso de no existir un nivel de protección adecuado, es preciso exigir garantías específicas que pueden ser acordadas por la Comisión Europea o por las autoridades nacionales de protección de datos, entre las que se encuentra la Agencia española. Como novedad reciente en esta materia debe citarse la Decisión de la Comisión Europea, de 26 de julio de 2000, que declara la existencia de un nivel adecuado de protección si la transferencia se realiza a una empresa en Estados Unidos acogida a los principios de “puerto seguro” que se recogen en ella.

Por su parte, la Agencia española ha autorizado transferencias internacionales a países sin nivel de protección adecuado, exigiendo garantías contractuales al cedente y al destinatario de los datos. Las garantías exigidas pueden resumirse en el compromiso de las partes de respetar la Ley Orgánica 15/1999, limitar el tratamiento de datos exclusivamente a la finalidad de la transferencia, adoptar las medidas de seguridad requeridas por el derecho español, responsabilizarse solidariamente de los incumplimientos, garantizar de forma asequible el ejercicio de sus derechos a los afectados y permitir las inspecciones independientes que estime necesarias la autoridad española.

Fuera de los supuestos expuestos, las transferencias internacionales sólo serán posibles cuando concurra alguna de las excepciones contempladas en el art. 34 de la Ley Orgánica.

Tratamiento de datos de salud

Para concluir, se hará a continuación referencia específica al tratamiento de datos de salud.

En la Ley los datos de salud tienen el carácter de datos especialmente protegidos que sólo pueden ser recabados, tratados y cedidos cuando así lo disponga una Ley o el afectado consienta expresamente. Dicho tratamiento será posible cuando resulte necesario para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrá llevarse a cabo cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona.

A tal efecto, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes pueden proceder al tratamiento de datos relativos a la salud de las personas que acudan a ellos o hayan de ser tratados en los mismos, en los términos previstos en la legislación estatal o autonómico sobre sanidad.

Es, igualmente, posible la transferencia internacional de datos cuando sea necesaria para las finalidades expuestas o para la salvaguarda de un interés público en el ámbito sanitario, por estar contempladas tales excepciones en el art. 34 de la Ley Orgánica.

Mención específica requiere una breve referencia a la relación entre el secreto profesional del médico y la protección de datos personales a la vista de la reciente Sentencia de la Sala de lo Contencioso-Administrativo –Sección Octava– del Tribunal Superior de Justicia de Madrid, de 12 de julio de 2000.

En ella se afirma que las relaciones de un médico profesional liberal, que ejerce su actividad profesional a título personal, sin dependencia laboral de ninguna clase, con sus clientes –arrendamiento de servicios– están regidas por un insuprimible deber de secreto profesional. A juicio del Tribunal el contenido del ordenador personal de profesional queda fuera del ámbito de aplicación de la derogada Ley Orgánica 5/1992, de 24 de octubre (LORTAD, que ha sido sustituida por la Ley Orgánica 15/1999) pues las eventuales violaciones del deber de confidencialidad del médico tienen sus propios cauces jurídicos de reacción distintos y al margen de los establecidos en la LORTAD.

Adicionalmente, la Sentencia afirma que, aún admitiendo a efectos meramente dialécticos la aplicación de la LORTAD, la conducta del profesional negando a los

inspectores de la APD datos obrantes en su ordenador relativos a pacientes no constituye obstrucción alguna a la actuación inspectora de la Agencia, sino una discrepancia absolutamente razonable en orden al alcance de la actuación de la Agencia respecto de unos datos cuya confidencialidad quedaba garantizada y salvaguardada por el secreto profesional.

En la actualidad la competencia revisora de las resoluciones del Director de la Agencia no corresponde a los Tribunales Superiores de Justicia sino a la Audiencia Nacional. Este órgano no ha dictado sentencia en la materia comentada, por lo que no es posible conocer en qué medida compartirá, disentirá o matizará el pronunciamiento de la sentencia comentada. Ello no obsta para que resulte oportuna su mención dada la novedad del planteamiento contenido en la misma.

C O N C L U S I O N E S *

* Las conclusiones del informe fueron acordadas en el curso de la reunión por todos los asistentes a la jornada.

INTRODUCCIÓN

En la jornada llevada a cabo el 12 de diciembre del 2000 en Pamplona, para elaborar el Informe SEIS sobre "La Seguridad y la Confidencialidad de la Información Clínica", se expusieron y debatieron las 8 ponencias incluidas en este documento, y se desarrolló una sesión de trabajo para obtener las conclusiones globales.

Aquí se recogen las conclusiones acordadas por los participantes en la jornada de trabajo, que se apoyan en sus aspectos de detalle en las 8 ponencias, a las que se hace referencia más concreta cuando ello es necesario.

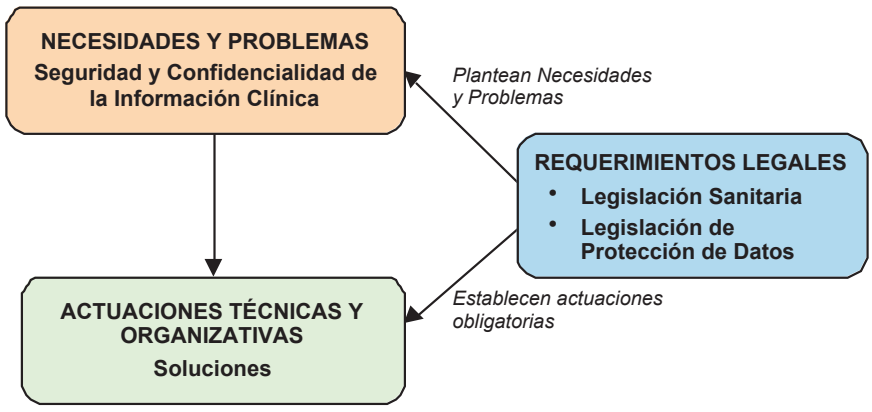
El primer aspecto a considerar es la propia estructura argumental de las conclusiones, para lo cual, teniendo en cuenta que las propias ponencias se agrupan en 3 bloques de forma natural:

–La visión de los usuarios (médicos, gestores e investigadores): ponencias 1, 2 y 3,

–La visión de los técnicos en SS.II.: ponencias 4, 5 y 6,

–La visión legal: ponencias 7 y 8,

se decidió seguir el siguiente esquema:



En cada apartado se discutieron los siguientes aspectos principales:

–Necesidades y problemas

- Aspectos previos: Necesidad de información sanitaria (recogida, tratamiento, difusión); el problema de la estandarización; qué información se ha de proteger.

- Quién ha de acceder a la información, para qué, con qué seguridad. Problemas para garantizar la seguridad y confidencialidad.

–Requerimientos legales: los requerimientos legales, producto de la propia legislación sanitaria y de la legislación en materia de protección de datos de carácter personal, afectan tanto a las necesidades y problemas, como a las actuaciones técnicas y organizativas. Por ello, en las conclusiones no se ha desarrollado como un apartado independiente, sino que se ha integrado en los otros dos. Por otra parte, un tratamiento detallado del marco legal se puede encontrar en la ponencia "Aspectos legales de la seguridad y confidencialidad en la información clínica".

–La titularidad de los derechos de la información clínica fue ampliamente discutida. Esta cuestión está tratada además de en la ponencia sobre aspectos legales, en otros trabajos del mismo autor* a los que pueden recurrir las personas interesadas en estos aspectos

–Actuaciones técnicas y organizativas: una vez identificadas las necesidades y problemas fundamentales, se identificaron las principales actuaciones a realizar, tanto técnicas como organizativas, para atender las necesidades en materia de seguridad y confidencialidad de la información clínica, que deben enmarcarse en un plan global de seguridad.

NECESIDADES Y PROBLEMAS

Aspectos previos

Tratamiento y disponibilidad de la información

El objetivo de cualquier sistema de salud ha de ser prestar la mejor asistencia posible a los ciudadanos. Un elemento necesario para proporcionar una mejor asistencia es el tratamiento y disponibilidad de la información, tanto para la propia asistencia, como para los aspectos de gestión e investigación asociados.

* Andérez A, Historia Clínica e informática: aspectos legales.
I. Informática y salud 1999, n.º 18 (896-899). II. Informática y salud 1999, n.º 19 (968-969). III. Informática y salud 1999, n.º 20 (1022-1026).

Estandarización de la información

Un aspecto que se trató en la jornada de trabajo, y que se reseña también en alguna ponencia, es el problema que supone la falta de estandarización de la información clínica. Aunque éste no era el objeto del informe, resulta interesante incluir una breve síntesis de las reflexiones efectuadas:

–Los diferentes servicios de salud requieren en muchos casos compartir información clínica. Este proceso actualmente no está automatizado, ya que cada servicio de salud estructura la información recogida en la historia clínica de manera diferente. El intercambio de información se ha de hacer de modo manual, lo cual es lento y costoso, amén de susceptible de errores de transcripción. A la escasa estandarización de las historias clínicas, se une la inexistencia de un número de identificación único por paciente de ámbito estatal, porque los códigos de identificación de la Tarjeta Individual Sanitaria (TIS) son diferentes en los distintos servicios de salud.

Teniendo en cuenta estos problemas, parece lógico que se establezca una estructura estándar mínima de historia clínica informatizada, en el ámbito nacional e incluso en el ámbito europeo, que vaya más allá del Conjunto Mínimo Básico de Datos (CMBD).

–Además de los intercambios de información entre servicios de salud, para estandarizar la historia clínica, se deberán tener cuenta los niveles de atención sanitaria, atención primaria y especializada, porque la necesidad de información clínica de ambos niveles es diferente.

En definitiva, existe consenso a la hora de considerar como necesario para un mejor aprovechamiento de la información, la estandarización de los aspectos fundamentales de la historia clínica, así como la existencia de un identificador único para la TIS.

Seguridad y la confidencialidad de la información

El tratamiento de la información clínica siempre ha tenido asociada la necesidad de seguridad y confidencialidad, debido al carácter especialmente sensible de los datos de salud.

Esta necesidad, los problemas que plantea satisfacerla, y las formas de abordarlos son el objetivo del presente informe.

Qué información se ha de proteger

Se considera que información clínica es la relativa a la salud de una persona identificada o identificable.

Necesidades y problemas en materia de seguridad y confidencialidad

La seguridad y confidencialidad de la información clínica es un mandato claro para todas las personas que intervienen en el proceso asistencial, y en sus aspectos derivados como la gestión e investigación. Esta obligación está establecida desde diferentes fuentes:

–Legislación en materia sanitaria.

–Legislación en materia de protección de datos de carácter personal.

–La propia ética profesional.

Además de ser una obligación ética y legal, la seguridad y confidencialidad de la información clínica es una condición para que los profesionales sanitarios acepten usar las Tecnologías de la Información y las Comunicaciones (TIC), y las aprovechen para prestar un mejor servicio a los pacientes.

Aunque la necesidad del secreto y la confidencialidad es anterior al desarrollo de las tecnologías de la información; su desarrollo y difusión, a la vez que permite un mejor manejo de la información, plantea necesidades y problemas adicionales.

Los problemas básicos de la seguridad de la información clínica, al igual que la de cualquier tipo de información, son cuatro:

–Autentificación.

–Integridad.

–Confidencialidad.

–No Repudio.

Entre las necesidades y problemas identificados en las ponencias incluidas en este informe, en la sesión dedicada a conclusiones se identificaron algunos por su carácter destacado.

A continuación, se detallan las necesidades y requerimientos del sistema sanitario relacionados con la seguridad y confidencialidad que se identificaron como fundamentales:

Regulación de la seguridad y confidencialidad de la información clínica

La seguridad y confidencialidad de la información clínica están reguladas por diferentes leyes y normas, que en la actualidad no siempre son congruentes. Esta falta de coherencia puede provocar una confusión que lleve a desaprovechar algunas de las posibilidades de las TIC bien por temor a infringir alguna norma, bien por excederse en su cumplimiento.

Se hace necesario unificar criterios en lo que respecta a la confidencialidad de la información clínica, lo que en una primera instancia podría resolverse con códigos tipo como permite la Ley Orgánica de Protección de Datos, y con el tiempo en una regulación legal más clara.

Esos criterios claros en el tratamiento de la información se han de establecer en las distintas funciones del proceso sanitario: asistencia, docencia, investigación, evaluación y gestión.

Acceso a la información

Dentro de la seguridad y confidencialidad de la información un aspecto clave es el control de acceso a la información, es decir, quién y a qué puede acceder.

Entre los problemas en el acceso a la información, se pueden destacar algunos:

–Como los datos clínicos son información especialmente sensible, es necesario establecer perfiles de usuarios, delimitando el acceso a la información dependiendo de las funciones a desarrollar en cada puesto de trabajo. Del mismo modo habrá que definir por cada perfil establecido el tipo de operaciones que puede realizar (escritura, solo lectura…). También se deberán ocultar los datos de carácter personal en aquellas tareas en las que no sea necesario la identificación del paciente, como por ejemplo en la realización de estadísticas.

Acceso con autorización, sólo a la información necesaria y para operaciones necesarias.

–Del mismo modo que es necesario establecer los niveles de acceso a la información, será necesario que se garantice la autenticidad de los accesos a los sistemas de información, es decir que tanto las personas, como los recursos (conexiones externas, servidores en red...) que acceden a los sistemas de información estén correctamente identificados y se asegure su autenticidad.

Verificar quién accede y comprobar que está autorizado a ello.

–Debido a la alta rotación del personal de enfermería en los servicios de salud, la gestión de los usuarios de los sistemas de información se hace muy complicada, lo que hace que se generen usuarios genéricos, y por tanto se pierde el control de la información tanto consultada, como introducida.

Gestión ágil de altas y bajas de autorizaciones.

–El proceso de automatización de la historia clínica permite en muchos casos delegar tareas en personal administrativo, que debe ser autorizado para acceder a

información sensible, pero se requiere que esté formado en la importancia de la confidencialidad, en los procedimientos de seguridad y en la responsabilidad en que incurre. Por otra parte, el contenido de la información clínica sigue siendo responsabilidad del personal sanitario que debe asegurarse de su validez y fiabilidad.

La desburocratización y la delegación de tareas exigen hacer explícitos los procedimientos y normas de seguridad, y la responsabilidad de todos los implicados en el proceso asistencial.

Intercambio de información

El intercambio de información clínica con terceros plantea dos tipos particulares de problemas:

–Técnicos: El uso de las redes públicas de comunicaciones plantea problemas a la hora de garantizar que la información circulante por dichas redes esté lo suficientemente protegida. Por ello, para salvaguardar la confidencialidad, dicha información se deberá transmitir cifrada. Además, este requerimiento lo establece el Reglamento de Medidas de Seguridad de la LOPD para los datos relativos a la salud.

Red segura.

–Legales: La cesión de información a terceros está regulada legalmente. Por lo que, cuando se realice, deberán cumplirse las normas establecidas, y seguir los procedimientos adecuados. Se deberá delimitar la información que se suministra, de manera que se cedan únicamente los datos estrictamente necesarios. Excepto en los casos previstos legalmente, para realizar la cesión será necesario el consentimiento expreso del afectado.

Cesión de información en los casos estrictamente necesarios, y de acuerdo con las normas y procedimientos legales establecidos.

Coste de la seguridad

Alcanzar los niveles de seguridad necesarios en el tratamiento de la información clínica, requiere de una dotación de recursos específica:

–Estructura. La función de seguridad en la organización debe contar con una estructura que garantice la disponibilidad de personal con sólidos conocimientos en materia de seguridad de sistemas de información.

–Recursos Económicos: La implantación de medidas de seguridad en los sistemas de información implica un coste de equipamiento, personal y programas. Esta situación debe tenerse en cuenta y valorar el coste de oportunidad que suponen las medidas de seguridad, frente a proyectos nuevos en sistemas de información, continuamente demandados en el sistema sanitario. Por ello debe buscarse un equilibrio entre inversión y seguridad, valorando que ningún sistema de seguridad garantiza el riesgo cero.

Necesidad de un cambio cultural

La necesidad de la seguridad y confidencialidad en la información clínica no está comúnmente asumida de forma práctica por el personal. Si no se consigue un cambio cultural en materia de seguridad, todas las medidas de índole técnico que se acometan estarán condenadas al fracaso.

Los síntomas de esa necesidad de cambio cultural son múltiples, pero pueden destacarse algunos:

–En la mayoría de los centros existen multitud de aplicaciones departamentales y bases de datos particulares que no se encuentran vigiladas o tuteladas por el personal técnico. Este tipo de aplicaciones no cumplen las normas legales vigentes en materia de protección de datos, y por lo tanto se deberían adecuar a dichas normativas o promover normas que se puedan cumplir y aseguren este tipo de ficheros de usuario.

–Existe una actitud reacia de los usuarios a utilizar los sistemas de información corporativos, y además es habitual en estos la cesión de contraseñas entre usuarios.

–La seguridad se concibe como un asunto secundario, ya que como norma general existe confianza en que no va a pasar nada. En muchos casos no se percibe la necesidad de la seguridad hasta que ocurre algo.

–Frecuentemente, se presta mas atención en disponer de la tecnología más avanzada, como por ejemplo la firma digital, que a solucionar los problemas básicos de seguridad, como las copias de seguridad o la cesión de contraseñas. Generalmente, estos problemas básicos son más organizativos que tecnológicos.

–En algunos casos el personal hace un uso indebido de los recursos y de la información clínica, por ejemplo comunicando información a pesar de su carácter confidencial.

–El personal directivo no tiene como una prioridad la seguridad y confidencialidad de la información clínica a la hora de asignar recursos.

Para conseguir el cambio cultural deseado en materia de seguridad se han de tener en cuenta varios aspectos:

–Parece más eficaz enfocar el problema de la seguridad como un problema de coste y riesgo, es decir, evaluar el coste que tendría la pérdida de un número elevado de historias clínicas, o la fuga de la información clínica de determinados pacientes. Para solventar estos problemas es necesario impulsar el cambio de cultura.

–Para impulsar el cambio se requiere una política de seguridad que marque las estrategias, fije las responsabilidades y delimite lo que se puede y no se puede hacer en lo que a seguridad de la información se refiere.

–Tanto para tener éxito en la implantación de las medidas de seguridad, como para conseguir mentalizar y concienciar al personal de los servicios de salud en la confidencialidad de la información y el correcto uso de los Sistemas de Información, será estrictamente necesario que los puestos directivos estén comprometidos con la implantación de las medidas de seguridad, así como en la concienciación del resto del personal.

ACTUACIONES TÉCNICAS Y ORGANIZATIVAS

Se han de acometer actuaciones técnicas y organizativas para satisfacer los requerimientos sanitarios, y además cumplir los requerimientos legales en lo que a protección de datos se refiere. De hecho, en el RD 994/1994 que aprueba el "Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal", se establecen una serie de actuaciones técnicas y organizativas concretas con carácter obligatorio.

Solución global de seguridad

La implantación de medidas de seguridad, para que proporcionen el nivel de seguridad requerido, se debe hacer de una manera organizada y coherente, planificando las actividades y proyectos que se deben llevar a cabo. El resultado ha de ser un Plan Integral de Seguridad en el ámbito de la información, que forme parte del Plan global de la empresa o entidad. La seguridad es uno de los componentes del Plan de Sistemas de Información.

Para llevar a buen termino el Plan Integral de Seguridad es imprescindible la implicación de los puestos directivos, de forma que el resto del personal acate las políticas y normas establecidas en materia de seguridad de la información.

El Plan Integral de Seguridad de la Información se deberá abordar mediante las siguientes actividades:

–Como punto de partida se realizará un Diagnóstico de Seguridad de la información y un Análisis de Impacto y de Riesgo.

–Definir y desarrollar la estrategia y políticas de seguridad, articulando y difundiendo las normativas de seguridad al resto de la organización.

–Definición de la estructura organizativa de seguridad y elaborar el manual de funciones y responsabilidades para cada puesto de la estructura definida. El propio Reglamento de medidas de seguridad de la LOPD obliga a tener un Documento de Seguridad que recoja estos aspectos.

–Seguridad Preventiva: Elaborar el Plan de Seguridad Preventiva Física, Lógica y de Comunicaciones, en el cual se incluirán las medidas necesarias a implantar para salvaguardar los elementos críticos de los sistemas de información de posibles ataques o vulnerabilidades.

> *La solución técnica a los problemas de autentificación, confidencialidad, integridad y no repudio estará basada en técnicas criptográficas.*

–Seguridad Correctiva: Elaboración del Plan de Contingencias y Recuperación de Desastres, de forma que se minimice el impacto ante un desastre sea del tipo que sea, recuperando un nivel de servicio aceptable en el menor tiempo posible.

–Por último, se deberá establecer un Plan de Auditorías mediante el cual se controle y verifique que se están cumpliendo las normativas y procedimientos establecidos.

Cambio Cultural

La técnica no puede solucionar los problemas de seguridad, salvo que vaya acompañada por un uso correcto por parte de las personas.

En el sector sanitario, es necesario un cambio cultural de las personas que lo componen, de forma que:

–Los profesionales sanitarios hagan uso de las posibilidades de los sistemas de información, para lo que se precisa, entre otras cuestiones, que confíen en su seguridad y confidencialidad.

–Las personas sean conscientes de la importancia de la seguridad y confidencialidad (no revelar datos, no compartir contraseñas, hacer copias de seguridad, etc.)

–Se recabe y use la información personal estrictamente necesaria.

–Se asuman los derechos del paciente, y de las personas en general, sobre sus datos.

Para conseguir este cambio cultural las actuaciones básicas son:

–Implicar a la Dirección.

–Clarificar, ordenar y hacer inteligible la normativa aplicable para que los profesionales sepan a qué atenerse.

> *En primera instancia recopilar la normativa aplicable y ejemplos prácticos de su aplicación en diferentes entornos sanitarios. A más largo plazo una forma de clarificar la situación sería la promulgación de un "Código Tipo" para el sector.*

–Implantar mecanismos técnicos de seguridad que sean lo más "amigables" posible para los usuarios. La seguridad no ha de suponer una falta de disponibilidad de la información para los profesionales sanitarios.

> *Si los profesionales han de recordar un gran número de contraseñas, se está abocado a que las escriban o sean muy fáciles.*

–Formación ética y técnica en materia de protección de datos personales.

PREVISIONES DE FUTURO

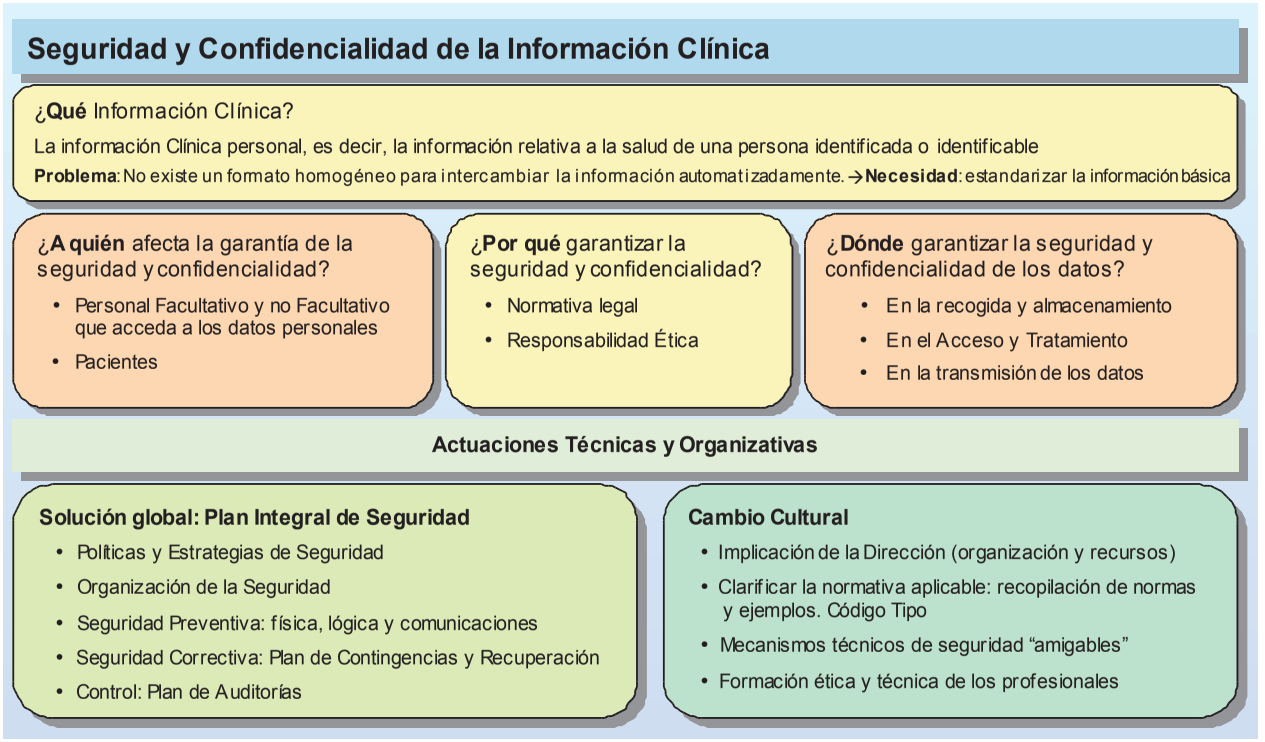
En los próximos tres años, los aspectos más importantes que se pueden prever son:

Se completará y clarificará la normativa, así como se desarrollarán los reglamentos necesarios tanto a nivel de los estados como de las diferentes regiones europeas.

Se estabilizará el mercado de las autoridades de certificación. Se verá si han quedado pocas autoridades que han fidelizado a muchas organizaciones, o bien han surgido muchas autoridades de ámbito menor y con valor añadido, que están relacionadas entre sí a través de entidades supranacionales.

Las políticas de seguridad se habrán establecido en la mayor parte de las organizaciones, estando además implantada la función de seguridad en las mismas, no como algo impuesto sino como necesario e incorporado a la cultura de las personas.

Los clientes y empleados de las organizaciones dispondrán de tarjetas inteligentes como medio de acceso en los terminales (PC, móviles, Web TV, etc.) con los que se comunican con las mismas.


Seguridad y Confidencialidad de la Información Clínica
¿Qué Información Clínica?
La información Clínica personal, es decir, la información relativa a la salud de una persona identificada o identificable
Problema: No existe un formato homogéneo para intercambiar la información automatizadamente. → Necesidad: estandarizar la información básica
¿A quién afecta la garantía de la seguridad y confidencialidad?
• Personal Facultativo y no Facultativo que acceda a los datos personales
• Pacientes
¿Por qué garantizar la seguridad y confidencialidad?
• Normativa legal
• Responsabilidad Ética
¿Dónde garantizar la seguridad y confidencialidad de los datos?
• En la recogida y almacenamiento
• En el Acceso y Tratamiento
• En la transmisión de los datos
Actuaciones Técnicas y Organizativas
Solución global: Plan Integral de Seguridad
• Políticas y Estrategias de Seguridad
• Organización de la Seguridad
• Seguridad Preventiva: física, lógica y comunicaciones
• Seguridad Correctiva: Plan de Contingencias y Recuperación
• Control: Plan de Auditorías
Cambio Cultural
• Implicación de la Dirección (organización y recursos)
• Clarificar la normativa aplicable: recopilación de normas y ejemplos. Código Tipo
• Mecanismos técnicos de seguridad “amigables”
• Formación ética y técnica de los profesionales

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

API (Aplication Program Interface): conjunto de rutinas o funciones que constituyen un interfaz o forma de diálogo entre las aplicaciones de los usuarios y el sistema operativo, ofreciendo una forma estándar de acceso a dichos sistemas, que logran independizar el desarrollo de las palicaciones con el Sistema operativo sobre el que se ejecuten.

Autentificación: mecanismos del sistema de información para poder identificar a los usuarios que acceden a sus recursos, y asegurar la integridad y autenticidad de los datos.

B2B (business to business): término utilizado en el ámbito Internet con el fin de reflejar las relaciones comerciales entre empresas. Fundamentalmente se centra en el proceso de compras y suministros entre organizaciones, aunque puede recoger todo tipo de transacciones comerciales.

Bit: unidad básica de información en un ordenador. Sólo puede tener dos valores, 1 ó 0.

Cifrado: técnicas utilizadas para hacer inaccesible la información a personas no autorizadas. Se suele basar en una clave, sin la cual la información no puede ser descifrada.

Contraseña (password): que es la parte privada de identificación de usuario. El nombre y la contraseña forman una pareja inseparable en los sistemas que identifican a sus usuarios a través de este mecanismo.

Copias de Seguridad (back-up): copias de los datos existentes en un sistema informático, con el fin de preservarlos y asegurar su disponibilidad, de forma que ante su destrucción en el sistema, podrían recuperarse y evitar así su pérdida. Normalmente se realizan sobre discos, CD-ROM o cintas magnéticas.

Cortafuegos (Firewall): conjunto de componentes hardware y software destinados a establecer unos controles de seguridad en el punto o puntos de entrada a la red de comunicaciones a la que está conectado el ordenador.

Encaminador (router): equipo informático conectado a una red con el fin de "encaminar" o dirigir los mensajes a una u otra red, aunque estas sean diferentes. De esta forma permite la interconexión de varias redes de comunicaciones. Se utiliza para establecer determinadas medidas de seguridad, de forma que se permita o impida el acceso a ciertas redes, o se limite su acceso.

Extranet: interconexión de ordenadores en base al protocolo Internet, que permite extender el acceso a determinados datos internos de la organización (que sólo serían accesibles desde la Intranet) a contratistas o empresas o instituciones con las que se tengan relaciones comerciales, institucionales, ... el acceso es restringido, y no es total como en la Intranet, permitiendo el acceso sólo a determinados usuarios (claramente identificados) y a determinados datos.

FTP (File Transfer Protocol): estándar de transmisión de ficheros.

Intranet: Interconexión de varios ordenadores entre sedes dispersas geográficamente de una misma organización. Permite el uso a los empleados y trabajadores de dicha organización, restringiendo totalmente el acceso a la misma desde el exterior. Se basa en los mismos protocolos que Internet, con lo que para el usuario es como si estuviese trabajando en Internet.

Nombre (login): identificador del usuario para poder acceder a los datos de un sistema. Suele ser público.

PKI: combinación de software, tecnologías de cifrado y servicios, que permiten proteger los mensajes transmitidos a través de las líneas de comunicación con el fin de que sean seguros, y que las transacciones comerciales a través de Internet sean seguras.

Proxy: un tipo de servidor cuya misión es comprobar la acreditación del usuario que trata de conectarse, comprobando la máquina origen, la de destino y el puerto a utilizar. Normalmente va unido a un cortafuegos, o él mismo puede actuar como tal.

Puentes (bridges): Permite la interconexión de redes de un mismo tipo.

Puerta de acceso (gateway): equipo para conectar diversas redes que utilizan protocolos de comunicación diferentes. Adpata el formato de los datos para que puedan viajar por la red y llegar a su destino de forma inteligible.

Red de Área Local (LAN o RAL): red física de interconexión a nivel local o departamental de varios ordenadores. Sólo permite conectar un número reducido de ordenadores.

Sistema Operativo: conjunto de programas, funciones o rutinas y datos cuya misión es gestionar los recursos del sistema informático y facilitar su uso a las aplicaciones de los usuarios, además de dotarle de las medidas oportunas de seguridad en dicho uso.

Suma de chequeo (checksum): contador que recoge la suma de los resultados de aplicar un determinado algoritmo a cada octeto de la información a comprobar.

TCP/IP (Transport Control Protocol/Internet Protocol): Protocolo estándar desarrollado por la agencia de investigación de la defensa de USA como base para la red ARPANET (1983) y que es el utilizado por defecto en sistemas operativos abiertos y en la red Internet. Se utiliza para el intercambio de información entre ordenadores conectados a una red.

UIT (Unión Internacional de Telecomunicaciones): Organismo internacional, con sede en Ginegra, cuya misión es definir estándares para las redes de comunicación.

Virus informáticos: son programas, generalmente destructivos, que se introducen en el ordenador y pueden provocar pérdida de la información almacenada en los medios de almacenamiento permanente, principalmente discos.

WAN (Red de Área Amplia): red que permite conectar físicamente varios ordenadores, y cuya titularidad es pública. Son las Redes Públicas de Datos, normalmente. En ellas se basa la Red Internet.

WAP (Wireless Access protocol): protocolo de acceso sin hilos, utilizado para la transmisión de datos a través de Internet desde un teléfono móvil a un servidor internet. Es un protocolo que se puede utilizar siempre que se trate de acceso de ordenadores a internet a través de redes inalámbricas.

Web (World Wide Web o WWW): colección de ficheros que dan lugar a un sitio Web o páginas de Web, que incluyen información multimedia: texto, gráficos, sonidos y vídeos, además de vínculos con otros Web. La Web se identifica por un localizador universal de recursos (URL) que especifica el protocolo de transferencia, la dirección de Internet de la máquina y el nombre de la página a que se desea acceder.

La Sociedad Española de Informática de la Salud desea expresar su más sincero agradecimiento al Fondo de Investigaciones Sanitarias por su apoyo en la publicación del presente informe.

También quiere hacer constar su gratitud al Gobierno de Navarra por su apoyo en la organización de la reunión correspondiente al III Informe SEIS que se celebró en Pamplona el 12 de Diciembre de 2000.