SOCIEDAD ESPAÑOLA DE INFORMATICA DE LA SALUD

Navarra de Gestión para la Administración, S.A.

Seguridad de la Información en Entornos Sanitarios

Seguridad de la información en entornos sanitarios

Diseño de cubierta: Julia Bermejo

Primera edición, marzo de 2008

Queda rigurosamente prohibida, sin la autorización escrita de los titulares del "Copyright", bajo las sanciones establecidas en las leyes la reproducción parcial o total de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático.

© SEIS, Sociedad Española de Informática de la Salud, 2002

http://www.seis.es
Secretaría Técnica: CEFIC
C/ Enrique Larreta, 5 – bajo izda. 28036 – Madrid
Tel: 91 388 94 78 Fax: 91 388 94 79
cefic@cefic.com

© Navarra de Gestión para la Administración, S.A.

www.nga.es
Plaza del Castillo, 21 – 2º
Tel: 948 20 39 80 Fax: 948 20 39 81
nga@cfnavarra.es

Printed in Spain – Impreso en España

Depósito legal: NA-663/2008

ISBN: 978-84-934283-2-7

Fotocomposición e impresión:
ONA Industria Gráfica
Polígono Agustinos, Calle F – 31013 Pamplona
Tfno: 948 35 10 14

Seguridad de la información en entornos sanitarios

Coordinadora:

Julia Bermejo Parra

Comité Editorial:

Julia Bermejo Parra
Óscar Blanco Ramos
Javier Carnicero Giménez de Azcárate
Sebastian Hualde Tapia
Ricardo Sáez Crespo

Autores:

Ignacio Alamillo i Domingo
Óscar Blanco Ramos
M. Ramón Gutiérrez Covarrubias
Pilar León
Rafael Ortega García
David Rojas de la Escalera
Ricardo Sáez Crespo

Índice

Presentación..... 7

Prólogo..... 9

Introducción.....13

Capítulo 1 – Fundamentos de seguridad de la información

Conceptos generales 18

Capítulo 2: Aspectos éticos de la seguridad de la información en entornos sanitarios

1. De la ética profesional a la normativa legal 23
2. Naturaleza de la documentación clínica 24
3. Confidencialidad y disponibilidad.....26
4. Seguridad, integridad y conservación.....31
5. Los datos genéticos.....33
6. La telemedicina.....35
7. Resumen y conclusiones.....37

Bibliografía y referencias 39

Capítulo 3: Problemática de seguridad de la información del sector sanitario

1. Introducción.....43
2. La historia clínica tradicional 44
3. La historia clínica electrónica.....45
4. Seguridad de la información = Confidencialidad + Integridad + Disponibilidad 47
5. La historia clínica electrónica como sistema de información compartida.....50
6. La información no clínica.....52
7. El factor humano.....53
8. Resumen y conclusiones.....54

Bibliografía y referencias 56

Capítulo 4: Aspectos legales de la seguridad de la información de salud

1. Los aspectos legales de la seguridad de la información de salud.....59
2. La seguridad en la protección de datos personales de salud.....61

3. Identidad digital y firma electrónica 67
4. La identificación de los titulares de tarjeta sanitaria como medio de acreditación de derechos en el sistema de salud 80
5. Tipología general de certificados de identidad y firma electrónica 82
6. La seguridad y la prestación de servicios de la sociedad de la información 88
7. La custodia y el archivo seguro de documentos electrónicos 95
8. La prevención del uso inadecuado de los sistemas de información sanitaria 98

Capítulo 5: Gestión de seguridad de la información en la Organización

1. Introducción 103
2. Modelos de Gestión de la Seguridad de la Información 104
3. Modelos de defensa 109
4. Resumen y conclusiones 114

Capítulo 6: Tecnologías aplicadas a la seguridad de la información

1. Introducción 117
2. Elementos y mecanismos de seguridad 118
3. Seguridad física de los soportes y de los sistemas informáticos 118
4. Seguridad de la información y de los datos: preservar información frente a observadores no autorizados. 122
5. Seguridad en los periféricos o dispositivos finales 128
6. Seguridad del sistema de comunicación 134
7. Seguridad en los accesos a los sistemas 139
8. Resumen y conclusiones 149
Bibliografía y referencias 154

Glosario de términos 157

Los autores 165

Presentación

A partir de la promulgación de la LORTAD en 1992, en las actividades de la Sociedad Española de Informática de la Salud se incorporan sesiones o ponencias sobre el alcance de la Ley y las necesarias modificaciones que habría que realizar en las aplicaciones informáticas del Sistema Sanitario, así como las medidas organizativas que había que adoptar, contando ya entonces con la colaboración de profesionales de la Agencia Española de Protección de Datos.

En el año 2000 la Sociedad Española de Informática de la Salud edita el III INFORME SEIS "La seguridad y confidencialidad de la información clínica", en el que participan como autores y expertos cerca de 30 profesionales: sanitarios, jurídicos, tecnológicos y gestores. Edición muy bien acogida por nuestro sector y que fue presentada en mayo de 2001 por Don Enrique Múgica, Defensor del Pueblo.

Uno de los claros resultados de estas actividades era la necesidad de impulsar que en la fase de diseño de los SIS se analizasen e incluyesen los requerimientos que la LOPD impone, otro factor clave detectado era la necesidad de difusión de las obligaciones éticas y legales hacia los profesionales sanitarios y por ultimo tratar de acercar a las autoridades en materia de protección de datos los problemas que se encontraban en el sector salud para cumplir la ley sin reducir sus funciones de asistencia, docencia, investigación y control sanitario.

Con estos objetivos la Sociedad Española de Informática de la Salud crea en 2004 el Foro de Protección de Datos de Salud que pretende ser una vía de comunicación y de transmisión de conocimientos sobre todos los aspectos que afectan a los sistemas de información de salud, a su confidencialidad y seguridad.

Uno de los objetivos esenciales de este foro es transmitir, a los directivos del sistema sanitario y a los profesionales de la salud, que la protección de datos es un factor clave para la implantación de las tecnologías de la información y comunicaciones en el ámbito sanitario.

Para ello, es necesario que en las fases iniciales de la concepción de un nuevo proyecto se estudien y resuelvan como un requerimiento funcional más, todos los aspectos precisos para el cumplimiento de la normativa legal y ética a la que pueda estar sujeta la información que se vaya a tratar, y además considerando las diferentes organizaciones que van a intervenir en su utilización o mantenimiento.

Es conocida la complejidad de nuestros sistemas de información y la alta protección que debemos asegurar al tratarse de datos de salud, por ello las medidas a adoptar no solo deben ser tecnológicas y de procedimiento, es preciso impulsar esta cultura de confidencialidad y seguridad de la información a todos los profesionales que intervienen en la protección de la salud.

Creemos que es necesario que se realice una labor difusora, a los profesionales de la salud implicados, de las medidas que en materia de seguridad y confidencialidad llevan incorporados todos los proyectos en implantación y que para su operatividad real se necesita su colaboración y apoyo.

Se han realizado cuatro reuniones anuales de este Foro, en Madrid en 2004 con la colaboración de la Agencia de Protección de Datos de la Comunidad de Madrid y la Agencia Española de Protección de Datos, en Bilbao en 2005 con la colaboración de la Agencia Vasca de Protección de Datos y la Consejería de Sanidad del Gobierno Vasco, en Barcelona en 2006 con la colaboración de la Agencia de Protección de Datos de Cataluña y la Consejería de Salud y por último en Pamplona en 2007, coincidiendo las tres primeras con la sede de las Agencias autonómicas existentes y esta última en base al acuerdo de colaboración con la empresa publica Navarra Gestión para la Administración (NGA), entidad que entre sus líneas estratégicas de actividad está el impulsar todos los aspectos sobre seguridad en el sistema sanitario.

Con la publicación "Seguridad de la información en entornos sanitarios" la SEIS pone a disposición de todos los profesionales un instrumento de referencia para hacer frente a la tarea de garantizar la seguridad de la información. Este trabajo es fruto de la permanente colaboración entre Navarra de Gestión para la Administración, empresa pública del Gobierno de Navarra y la SEIS, ejemplo de colaboración entre una sociedad científica y una entidad pública.

Luciano Sáez Ayerra
Presidente de la Sociedad Española de Informática de la Salud

Prólogo

En la sociedad actual, con la incorporación de las tecnologías de la información y las comunicaciones, se están modificando tanto los hábitos de consumo de la población como los procesos de negocio, las relaciones y la toma de decisiones de las organizaciones. En este contexto, la seguridad lógica es un elemento crítico e imprescindible que aporta confianza y garantiza que los procesos funcionen y se establezca un nuevo modelo digital del siglo XXI.

El Gobierno de Navarra considera que la seguridad puede ser un elemento diferenciador del desarrollo de la Comunidad Foral y que puede dinamizar la competitividad en todos los sectores económicos.

La creación de conocimiento de seguridad aplicado a diversos sectores es una línea de actuación de la iniciativa “Navarra Digital Segura” y en este marco, el Gobierno de Navarra, a través de su empresa Navarra de Gestión para la Administración S.A. continúa colaborando con la SEIS con el fin de desarrollar herramientas que ayuden a la difusión, concienciación y capacitación sobre la seguridad de la información en el ámbito de la salud.

En esta ocasión les presentamos la publicación “Seguridad de la Información en Entornos Sanitarios” dirigida a profesionales del ámbito de la salud con perfiles diversos, como gestores, técnicos, sanitarios, etc. con el objetivo de acercar conceptos y terminología sobre la seguridad lógica que puedan servir de ayuda para la concienciación y sensibilización sobre la misma y también de capacitación para abordar proyectos y relaciones con profesionales tecnológicos con más conocimiento y por lo tanto con mayor entendimiento.

Quiero agradecer el esfuerzo y la dedicación de los autores, editores y coordinadora que han hecho posible esta publicación.

Es nuestro deseo que esta publicación sea el inicio de una serie que trate temas de seguridad de la información y la salud para ir conformando una base de conocimiento útil para los profesionales del sector de la salud.

Les invito a leer los distintos capítulos de este número porque estoy seguro que, como en ocasiones anteriores, encontrarán en ellos información, opiniones, documentación y referencias que les puedan ser de utilidad y aplicación en sus respectivas áreas de actividad.

Juan Santafé Rodrigo
Consejero Delegado de NGA

Introducción a la Seguridad de la Información en Entornos Sanitarios

Javier Carnicero

Director de la Oficina de Innovación de Sistemas de Información Sanitaria. Consejería de Sanidad. Gobierno de Cantabria.

Miembro de la Junta Directiva de la SEIS.

Confidencialidad y disponibilidad

La información relacionada con la salud de las personas siempre ha tenido un carácter altamente confidencial. El paciente cuenta a su médico aspectos de su vida íntima que no comparte con otras personas, con la certeza de que éste guardará absoluto secreto de todo ello. Esa certeza se debe tanto a la confianza en la deontología profesional como a las disposiciones legales que se han ido estableciendo a lo largo del tiempo. Sin embargo, ese mismo paciente también confía en que su historia clínica estará siempre a disposición de su médico, y de cualquier profesional que deba atenderle, cuando sea preciso, sin demoras innecesarias y en un formato que sea fácilmente legible y procesable. Por muy protegida que se encuentre, la información no es útil si no está disponible cuando se necesita.

Los conceptos de confidencialidad y de disponibilidad, que pueden ser contradictorios, son los que definen las principales cuestiones de seguridad y protección de datos: que la información sea confidencial y que esté disponible. Es decir, que la información sea confidencial implica que sólo acceda a la misma quien esté autorizado y cuando esté autorizado y que esté disponible supone que se pueda acceder a ella en cualquier momento en el que sea necesario. Además, es preciso que esa información se haya mantenido íntegra y que quien haya accedido a ella no pueda negarlo, pues también este dato forma parte de la información.

La gestión de la seguridad

Existe un consenso casi general en que la incorporación de las Tecnologías de la Información y de la Comunicación (TIC) a la actividad sanitaria permite una mayor calidad y eficiencia de la atención. Sin embargo, esa incorporación se ha visto acompañada de cierta inquietud por parte de los profesionales sanitarios acerca de la protección de datos. Puede afirmarse con contundencia que existen mecanismos para garantizar las medidas de seguridad y protección de datos con mayor efectividad utilizando medios tecnológicos para tratar la información, que cuando se emplean los tradicionales medios en soporte papel. No obstante, la implantación de las TIC en el sector sanitario debe ser especialmente cuidadosa en cumplir todas las medidas de seguridad necesarias; en primer lugar, por respeto a los derechos de los ciudadanos; en segundo lugar, porque se deben cumplir las leyes y normas éticas que reflejan esos derechos; y en tercer lugar, porque la implantación de medidas de seguridad es una oportunidad para mejorar la calidad y eficiencia de los sistemas de información.

La gestión de la seguridad de la información en los entornos sanitarios, como cualquier otro aspecto de la incorporación de las TIC a estos entornos, adquiere una complejidad especial que se debe, entre otros factores, a la diversidad de profesionales que intervienen y a la dificultad de estandarizar los procesos ("no hay enfermedades sino enfermos"). Al mismo tiempo, los administradores sanitarios, los gerentes de las instituciones y los profesionales contemplan cómo las TIC tienen cada vez mayor presencia en la actividad diaria, y manifiestan su inquietud sobre las medidas de protección que deberían implantarse. Esta inquietud suele resolverse encargando a una empresa especializada que lleve a cabo un plan de seguridad, o simplemente no tomando ninguna medida específica, y confiando en los recursos y buen hacer de los servicios propios.

La seguridad de los sistemas de información no es un asunto cuya responsabilidad deba recaer en exclusiva ni en los servicios de informática de las instituciones ni en empresas externas. La estrategia de seguridad debe ser fijada por la alta dirección y formar parte de la planificación estratégica. Las políticas que se fijen en esta planificación deben tener en cuenta que la seguridad comienza por la organización y que la tecnología es parte del plan de seguridad, pero que por sí sola no es suficiente. Por otra parte, también debe considerarse que la seguridad y protección de datos son un componente de la calidad de los sistemas de información.

La **"Guía de seguridad de la información en entornos sanitarios"** tiene como objetivo servir de ayuda a los profesionales y gestores sanitarios para emprender la tarea de garantizar que los derechos de los ciudadanos se cumplen, y que la implantación de las TIC contempla como uno de sus componentes esenciales la protección de la información.

Se ha tratado de seguir un orden lógico para fijar la estructura del libro. En primer lugar, se tratan los aspectos éticos que constituyen el origen del concepto de confidencialidad de la información de salud. Los valores de la sociedad contemplan que la información que un paciente transmite a un profesional sanitario es privada, y que esta privacidad debe garantizarse. Esta necesidad genera una serie de problemas que las organizaciones deben resolver, y también unas disposiciones legales que son la respuesta de las instituciones a esos principios éticos. Para cumplir con esas obligaciones éticas y legales, y resolver los problemas de las organizaciones, existen tanto procedimientos de gestión como tecnologías. Todos estos aspectos se tratan en la guía de seguridad, precedidos de un primer capítulo que revisa los principales conceptos en materia de seguridad de la información, cuya clarificación resulta necesaria para la comprensión de todos los apartados que se tratan después.

Aspectos éticos

Como nos recuerda Pilar León, y ya se ha indicado antes, aunque la regulación específica sobre la información y la documentación clínicas es reciente, ya estaba contenida en su mayor parte en los códigos deontológicos de las profesiones sanitarias. En este capítulo, la autora revisa la naturaleza de la documentación clínica y recuerda que lo decisivo es la conexión de la información que allí se recoge y la persona a la que corresponde. Se continúa con la relación entre confidencialidad y disponibilidad, conceptos que traen consigo el secreto profesional y la obligación de custodia de la información, que corresponden tanto a los profesionales como a las instituciones.

Se estudia la facultad de acceso a la información por parte de los profesionales, los pacientes y su familia, así como distintos aspectos relacionados con la conservación de la información.

El capítulo también introduce dos aspectos de actualidad en el sistema sanitario, como son aquellos relacionados con los datos genéticos y con la implantación de proyectos de telemedicina.

Las necesidades de seguridad de la información

David Rojas y Óscar Blanco establecen el concepto de seguridad como resultado de la confidencialidad, la integridad y la disponibilidad. Describen cada uno de ellos y presentan las medidas que deben adoptarse para garantizar su cumplimiento. No se olvidan de la información no clínica, y hacen una especial mención al factor humano como una de las claves tanto de éxito como de fracaso en la implantación y ejecución de las medidas de seguridad.

Aspectos legales

Ignacio Alamillo efectúa una revisión exhaustiva de los aspectos legales de la seguridad de la información de salud. Esta revisión no se reduce a una mera exposición de las distintas normas existentes sobre esta materia, sino que las explica y clarifica de forma que consigue que las disposiciones se transformen en conceptos y en pautas que deben seguir las organizaciones.

El autor se detiene para analizar la identidad digital, los distintos métodos de firma electrónica y el modelo ISO de certificación de identidad y firma electrónica.

No termina aquí el apartado de aspectos legales, porque también se tratan otros apartados referidos a la seguridad y prestación de servicios de la sociedad de la información, como las obligaciones de identificación e información y la custodia y archivo seguro de documentos en soporte electrónico.

Gestión de seguridad de la información

En el capítulo que trata sobre la gestión de seguridad, Rafael Ortega revisa los modelos de seguridad de la información y define ésta como el conjunto de medidas tecnológicas, de normas, procedimientos y de formación que aseguren la confidencialidad, integridad y disponibilidad de la información, en los estados de proceso, almacenamiento y transmisión.

En este capítulo se considera la seguridad como un servicio, que requiere implantar unos procesos que conducen al nivel de seguridad que se ha fijado como objetivo de la institución.

Tecnologías aplicadas a la seguridad de la información

Los miembros del Servicio de Informática del Hospital Universitario Marqués de Valdecilla, Ricardo Saéz y M. Ramón Gutiérrez, clasifican los elementos y mecanismos de seguridad desde la perspectiva de la seguridad física y lógica, pero completan esa clasificación según los sistemas de comunicación, dispositivos de acceso y clientes.

El capítulo termina con una tabla muy útil en la que se clasifican los problemas potenciales, el aspecto de seguridad sobre el que inciden y las tecnologías o soluciones disponibles para afrontar esos problemas.

Glosario de términos

La Guía de seguridad de la información en entornos sanitarios concluye con un glosario elaborado por los autores de los distintos capítulos, que ayudará sin duda a aquellos que se enfrenten por primera vez a estos conceptos.

Conclusión

La seguridad de la información es un derecho de los ciudadanos y de los pacientes, reconocido en distintas disposiciones legales. Pero también es una oportunidad de mejora de la calidad de los sistemas de información. Para resolver posibles problemas de seguridad se dispone de medidas organizativas y técnicas. Todo ello conduce a la necesidad de gestionar la seguridad de la información, que debe ser considerada como un aspecto esencial de las instituciones sanitarias.

1 Fundamentos de Seguridad de la Información

Conceptos generales

Con cierta frecuencia se confunden conceptos básicos relacionados con la seguridad de la información. Por ello, se ha considerado oportuno incluir la siguiente terminología básica que puede ayudar a sentar conceptos que resultan claves para entender en toda su dimensión el alcance los distintos capítulos de este libro.

Activo: Es todo aquel recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Identifica a uno de los elementos siguientes:

- Información: es el objeto de mayor valor en una organización, y por ello su salvaguarda debe ser una prioridad, independientemente del lugar en donde se encuentre registrada, y de la naturaleza del medio que lo soporte, electrónico o físico.
- Equipamiento: se identifica con ello al Software, hardware, elementos de comunicación y demás componentes estructurales, que dan soporte a la información.
- Usuarios: son los profesionales que utilizan el equipamiento en el manejo de la información, con el objetivo de intercambiar y generar conocimiento útil a la organización.

Amenaza: es cualquier potencial violación (accidental o intencionada) de la seguridad, es decir, cualquier acción o acontecimiento que pueda provocar una pérdida o daño en la confidencialidad, integridad o disponibilidad de la información (posible fuente de peligro o catástrofe).

Atendiendo a su procedencia, las amenazas se agrupan en:

- Errores accidentales, originados por fallos en los programas informáticos, procedimientos erróneos u omisiones de usuarios autorizados.
- Errores provocados, que causan alteraciones maliciosas para beneficio o venganza.
- Desastres naturales o provocados, que habitualmente llevan a la destrucción o inutilización de los recursos informáticos: entorno arquitectónico, soportes hardware y/o software, y de los datos.
- Interferencias de terceros, que interrumpen o interceptan programas o datos.

Dependiendo del nivel de penetración de las amenazas, se pueden categorizar también en los grupos siguientes:

- Interrupción: un recurso del sistema de información es destruido o se vuelve no disponible. Es un ataque contra la disponibilidad. Ejemplos de este tipo de amenaza son la destrucción de elementos hardware como el disco duro, o el corte de la línea de comunicación.
- Intercepción: una entidad no autorizada (persona, programa, equipo) consigue acceso a un recurso. Es un ataque contra la confidencialidad. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red, la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de cabeceras de paquetes para desvelar la identidad del usuario implicado en la comunicación (intercepción de identidad).
- Modificación: una entidad no autorizada consigue acceder a un recurso y manipularlo. Es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, o alterar un programa para que funcione de forma diferente.
- Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o la adición de registros a un archivo

Ataque: Un ataque es la realización de una amenaza.

Vulnerabilidad: Es la posibilidad de que se materialice una amenaza sobre un Activo.

Impacto: Es la consecuencia de la materialización de una amenaza, y el resultado de la agresión sobre el activo. El impacto puede ser cuantitativo (si representa pérdidas directas o indirectas, cuantificables económicamente) con o sin pérdidas funcionales, o cualitativo con pérdidas orgánicas (por ejemplo daño de personas). En otra categorización, puede ser teórico o efectivo; el teórico es aquel que entra dentro de unas probabilidades evaluadas a partir de posibles riesgos, el efectivo sería la consecuencia real de la materialización de una amenaza.

Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización. Es un indicador resultante de la combinación de la vulnerabilidad y el impacto que procede de la amenaza actuante sobre el activo. Hay cinco acciones que se pueden tomar cuando se trata de un riesgo definido: evitarlo, transferirlo, reducirlo, asumirlo, y provocarlo. A veces puede resultar más interesante acelerar el proceso, aunque sea nocivo, que esperar a que concluya.

Controles, medidas o salvaguardas: Un control se define como “una medida adoptada para disminuir un riesgo determinado”. Pueden ser “preventivos”: que tienen por objeto reducir el riesgo de

que algo nocivo nos ocurra), “detectores”: orientados a identificar riesgos que se han manifestado, o “correctivos”: orientados a impedir o reducir el impacto que producirían los incidentes de seguridad.[1]

Seguridad: Algunos autores acostumbran a definir el término como aquel estado del sistema (informático o no) libre de peligro, daño o riesgo. Hoy en día, entendemos por "sistema seguro" el que cumple las características siguientes:

- Integridad. Garantiza que la información no ha sufrido modificaciones ni supresiones parciales ni totales por agentes no autorizados.
- Confidencialidad. Confianza en la información por parte del emisor y del receptor de la misma.
- No Repudio. Propiedad por la cuál el emisor de una información no puede negar haberla emitido y el receptor de esa información no puede negar haberla recibido.
- Disponibilidad. La información estará disponible siempre que un agente autorizado la solicite.
- Autenticación, o garantía de que la información ha sido generada por agentes autorizados.
- Control de Acceso. La información únicamente debe ser accesible por agentes previamente autorizados.

Cabe decir que en la bibliografía es habitual encontrar variaciones en la terminología y en la descripción de las características referenciadas.

[1] Como ejemplo sencillo se puede citar la típica situación de la sala de reuniones con sus carteles “Prohibido Fumar” (control preventivo), sistemas de detección de incendios (control detector), y el sistema automático de extinción de incendios (control correctivo).

2 Aspectos éticos de la Seguridad de la Información en Entornos Sanitarios

Pilar León

Departamento de Humanidades Biomédicas
Universidad de Navarra

1. De la ética profesional a la normativa legal

Las cuestiones relacionadas con la seguridad de la información clínica están ampliamente reguladas en todo el mundo, lo que exige iniciar este capítulo con una distinción entre el ámbito ético y el jurídico.

La ética profesional busca inspirar la conducta entera de los profesionales de la salud y les impone el compromiso de proporcionar al paciente una atención de calidad. La ética profesional potencia la relación con el paciente basada en la confianza, en la que ambas partes, partiendo de su mutua dignidad, se reconocen y respetan. La ética es un elemento esencial de toda profesión. Las relaciones de los profesionales con los pacientes, las de los profesionales entre sí, o la de éstos con terceros son aspectos que no pueden ser regulados tan sólo mediante disposiciones legales. La vigencia de las normas y recomendaciones éticas no necesita del refrendo jurídico, no es algo añadido o impuesto por una autoridad externa, es algo que la sociedad reclama y exige a los profesionales.

Idealmente, ética profesional y normativa legal deberían ser concurrentes. En efecto, la regulación de las cuestiones relacionadas con la seguridad de la información médica muestra que es posible la coincidencia entre el plano ético-deontológico y el jurídico, pues la mayor parte de la legislación vigente estaba ya contenida en los códigos deontológicos y en las recomendaciones éticas de las profesiones sanitarias. Lo que se ha producido en los últimos años ha sido la conversión de ciertos deberes éticos en deberes jurídicos: la sociedad puede ahora exigir esa responsabilidad. La regulación legal específica sobre la información y la documentación clínica es cosa reciente; tradicionalmente estas cuestiones se trataban en el ámbito ético-deontológico de las profesiones de la salud.

En este capítulo nos referiremos a la naturaleza de la documentación clínica, de la que derivarán los principios éticos que han de ser aplicados a las cuestiones relacionadas con la seguridad: confidencialidad, disponibilidad, integridad y conservación. Por su relevancia, nos detendremos, finalmente, en la consideración de los aspectos éticos relacionados con la documentación generada por la información genética y la telemedicina.

Son muchos los documentos y las declaraciones que exponen la ética profesional de la seguridad de la información clínica. En ellos nos apoyaremos para el desarrollo de este capítulo.[1]

---

[1] Además de las Declaraciones de la Asociación Médica Mundial y del Comité Permanente de Médicos Europeos, citadas en la bibliografía, el tema ha sido objeto de estudio de las asociaciones profesionales

2. Naturaleza de la documentación clínica

La historia clínica tiene su origen en la medicina hipocrática. Laín Entralgo señala que los relatos hipocráticos del curso clínico de los enfermos supusieron “un saber susceptible de enseñanza, basado principalmente en la observación sensorial de la realidad del enfermo y del medio físico”.[2] La documentación derivada de la asistencia al enfermo fue incorporando los avances de la medicina y se desarrolla, sobre todo, con el impulso que adquiere la institución hospitalaria, a partir del siglo XIX.

La historia clínica es un relato patográfico: expresa la realidad del enfermo a lo largo de un curso temporal e incluye aspectos físicos, psíquicos y sociales. Se señala que la historia clínica ha de ser completa, lo cual implica que haya unos límites, temporales y temáticos que la definen: ha de contener las alteraciones propias del estado de enfermedad y referirse a los elementos descriptivos que “sean” o “puedan ser” necesarios para el tratamiento.[3] En general, comprende toda la información generada en la relación del médico y de otros profesionales con el paciente en cada uno de los actos médicos, por ello, “debe contener la justificación fundamentada de los diversos procedimientos diagnósticos y terapéuticos empleados, así como los documentos acreditativos de la información recibida por el paciente y del consentimiento otorgado por éste a dichos procedimientos (…), debe ser completa, dinámica y realizada con un orden coherente e integrado que permita su consulta global, selectiva y diferenciada por todos y cada uno de los episodios asistenciales que se hayan producido”.[4]

Laín destaca cinco tipos de tensiones que manifiestan la complejidad de la historia clínica: la tensión entre la individualidad del relato y la universalidad del conocimiento científico a que ese relato se halla dirigido; la tensión entre la necesidad y la contingencia de los diversos “estados” que integran el curso de la enfermedad; la tensión entre la evidencia y la conjetura en los juicios que acompañan a la descripción de cada momento; la tensión propia de la selección de los datos, ya que no todo lo que acontece en la vida del enfermo ha de estar en la historia clínica; y la tensión entre la intención

nacionales. En el caso español: Declaración de 31 de mayo de 2002 de la Comisión Central de Deontología: “Ética de la Historia: su propiedad, conservación y el acceso a ella del paciente o terceros” (en adelante: "Ética de la Historia"). También nos referiremos al Código de ética y Deontología Médica de la OMC (CEDM), Madrid; 1999.

[2] Laín Entralgo P. La historia clínica: historia y teoría del relato patográfico. Madrid: C.S.I.C.; 1950. p. 730.

[3] Ibídem, p. 752.

[4] "Ética de la Historia", n. 7. Comenta este documento Yuguero del Moral L. Definición, contenido y archivo de la historia clínica: visión deontológica-legal. En León Sanz, P. director. La implantación de los derechos del paciente. Comentarios a la Ley 41/2002. Pamplona: EUNSA; 2004. p. 259-269.

teorética y la intención operativa de este documento, que simultáneamente ha de contribuir a “saber ver” y a “saber hacer”.[5]

Como señala la Declaración “Ética de la historia”: “los bienes y valores que se relacionan con la historia clínica son de una importancia extraordinaria, ya que están directamente relacionados con derechos fundamentales de la persona tales como el derecho a la intimidad, a la integridad física, a la salud, a la libertad, a la confidencialidad y a la privacidad.” ("Ética de la Historia", n. 2).

En el caso de la documentación clínica, lo decisivo, desde un punto de vista ético, es la conexión entre los datos allí recogidos y las personas a las que corresponden. Cualquier información que de ellos se obtenga se traduce en datos personales, a los que pertenece el respeto que se asigna a la persona humana. Por el contrario, si con fines epidemiológicos, de inspección o de investigación se separan los datos clínicos de los de identificación, esos documentos se anonimizan, dejan de tener condición personal, lo que permite su utilización en los procedimientos para los que hayan sido aprobados.

Las nuevas tecnologías de la información y de la comunicación (TIC) han convertido la historia clínica, en papel y documento exclusivamente médico, en una historia clínica informatizada que puede abarcar todo lo referente al estado de salud de una persona.[6] La historia de salud electrónica amplía las posibilidades de acceso y de almacenamiento, permite separar, más fácilmente, la información clínica de la administrativa y controlar qué usuario del sistema accede a la información.

La finalidad de la historia clínica -facilitar la atención médica del enfermo y dejar constancia de ella (CEDM, art. 13.4)- determina los preceptos deontológicos que le afectan y que condicionan el acceso a esta documentación. Aunque están descritos más usos de la historia clínica que el asistencial (circunstancialmente puede interesar a la administración de justicia, a las compañías de seguros, a los académicos, a los investigadores, etc.), la historia clínica ha adquirido el carácter de documento prioritario en la relación médico-enfermo. Es, en lo ético y lo jurídico, un documento decisivo (CEDM, art. 13). Lo cual explica el derecho y la obligación -mandato deontológico- que tiene el médico de redactarla y de que “todos los actos médicos en relación a un paciente queden fielmente reflejados en su historia” ("Ética de la Historia", n, 6).

---

[5] Laín Entralgo P. La historia clínica: historia y teoría del relato patográfico. Madrid: C.S.I.C.; 1950. p. 739.

[6] Analiza los cambios que se han producido Carnicero J, coordinador. Informes SEIS. De la historia clínica a la historia de salud electrónica. Pamplona: Sociedad Española de Informática de la Salud; 2002.

La historia clínica es un documento complejo por la multiplicidad de personas e instituciones que participan en su elaboración y uso, por la intervención de los organismos en la custodia y conservación. No es de extrañar que su manejo origine conflictos y que éstos no siempre sean fáciles de resolver. En ocasiones, los problemas que surgen “derivan de una legislación claramente insuficiente en esta materia.” ("Ética de la Historia", n. 3).

3. Confidencialidad y disponibilidad

Entre los derechos de los pacientes destacan tanto el derecho a ser debidamente informado, como el derecho a la confidencialidad de los datos sanitarios, también cuando éstos son objeto de tratamiento informático. Ambos derechos tienen una relación directa con la documentación clínica.

La confidencialidad y la protección de la intimidad son derechos fundamentales que se apoyan en la dignidad de la persona. La privacidad es el derecho de cada persona a determinar libremente a quiénes, en qué medida y en qué circunstancias permite acceder a su esfera privada.

Cuando los pacientes revelan su intimidad lo hacen para ser curados y cuidados, no para que sus confidencias o datos clínicos sean divulgados: la documentación comprende aquello que el enfermo ha relatado o autorizado a saber, basado en la confianza de que aquello no se revelará, por lo que el quebrantamiento del secreto constituye, desde el punto de vista ético, una grave e injusta agresión a la persona del paciente. Revelar injustificadamente información clínica llevaría consigo una devaluación de la libertad del paciente que vería recortada su capacidad de autodeterminación.

La enfermedad sitúa a las personas en una posición de debilidad, por lo que es necesaria la confianza en los profesionales por parte de la sociedad. En efecto, la custodia de la confidencialidad manifiesta la lealtad del profesional; si faltara, se vería afectada la confianza y la sinceridad de la comunicación en la relación médico-paciente. [7]

De ahí que la custodia de la confidencialidad haya sido una tradición constante de las profesiones sanitarias: el secreto profesional, desde el Juramento Hipocrático, ha sido un elemento esencial del *ethos* sanitario. La guarda de la confidencialidad por parte del profesional de la salud, ante los pacientes y sus allegados, ante los propios colegas y colaboradores, o ante instituciones sociales, no es

[7] Pellegrino ED, Thomasma DC. The Virtues in Medical Practice. New York: Oxford University Press; 1993. p. 89.

un privilegio, sino un deber legal y, sobre todo, un compromiso ético-deontológico grave. Es una manifestación de respeto, actitud ética fundamental del profesional.

Sin embargo, hay situaciones en las que el médico o el profesional de la salud están obligados a revelar datos confidenciales del paciente porque el bien público o común prevalece sobre el particular. Son casos en los que el principio de justicia prevalece sobre el de autonomía del paciente. En cualquier caso, el profesional que tenga que revelar una información confidencial, "siempre lo hará de forma restringida, con discreción, revelando lo estrictamente justo y necesario, y haciéndolo exclusivamente ante quien proceda" (CEDM, art. 16.2). Los expertos en ética de las profesiones sanitarias señalan que los deberes éticos que salvaguardan la intimidad de los pacientes son más amplios y exigentes que las leyes que los contienen, también recomiendan que los Estados desarrollen el marco legal apropiado que regule y limite las ocasiones en que este derecho pueda ser conculcado.

Del secreto profesional nos dicen las prescripciones deontológicas:

a) Es un deber personal porque, aunque existe una responsabilidad colegiada, cada actuación está sujeta a la responsabilidad individual del profesional que la realiza, motivo por el cual todas las anotaciones o intervenciones que se hagan en una historia clínica tienen que estar identificadas con el nombre y la firma del responsable.

b) Es universal (CEDM, arts. 14.2, 15.1-2, 17.2): afecta a todos los profesionales que atienden a un paciente, cualquiera que sea la modalidad de su ejercicio (médicos y enfermeras, auxiliares, físicos, ingenieros y técnicos, especialistas en informática, gestores de las redes de telecomunicación,...).

c) Es omnicomprensivo (CEDM, art. 14.3), es decir, incluye lo relatado, lo observado y lo deducido; engloba todo lo que, acerca del paciente y su entorno, llegue al conocimiento de los profesionales, en el curso de su relación profesional con el paciente.

d) Es, por último, intemporal (CEDM, art. 14.4.) porque la muerte del paciente no desliga del deber de guardar secreto.[8]

En las páginas que siguen nos limitaremos a analizar cómo se compaginan el derecho a la intimidad y a la privacidad, con la disponibilidad de la documentación clínica.

---

[8] Comité Permanent des Médecins Européens (CP98/090Rev 2). La confidentialité entre médecin et patient et les renseignements exigés par les compagnies d'assuraces privées. 25/02/1999. Bruselas.

3.1 Disponibilidad de los datos clínicos

Para los profesionales de la salud

Como se ha señalado, el carácter y la finalidad de la historia clínica exigen que puedan acceder a los datos clínicos sólo y exclusivamente los que intervienen en la atención del paciente y en la medida en que necesiten conocerlos para prestar esa atención. Insisten en esta consideración numerosos documentos emanados de las organizaciones profesionales.

Esta circunstancia implica la obligación del profesional de proporcionar a sus colegas los datos necesarios para completar el diagnóstico, así como, ante la solicitud y en beneficio del paciente, facilitar datos sobre las pruebas realizadas (CEDM, art. 13.6).

El respeto al paciente excluye formalmente la oficiosidad en la información clínica. Y fomenta la seriedad con que han de protegerse los sistemas de control de acceso a la información almacenada, por ejemplo, a través del cuidado de las claves de acceso, individuales y secretas, que se asignan a cada persona.

Podría suponerse que el hecho de que un médico u otro profesional de la salud examine o curiosee la historia clínica de un paciente que no está a su cuidado, es una acción éticamente neutra o, en todo caso, irrelevante, puesto que puede hacerlo con la intención de mantener reservados los datos que ha revisado. Sin embargo no es así, esa acción sería una falta contra la justicia, porque se estaría abusando de un privilegio profesional para entrar en la intimidad ajena y lesionando con ello uno de los derechos del paciente.[9]

Para el paciente y su familia

Durante los dos últimos siglos ha habido un progresivo desarrollo de la ética de las profesiones de la salud acerca del derecho a la información por parte de los pacientes. Actualmente es reconocido el derecho del paciente o de su representante legal a acceder a la documentación clínica; así como a los familiares o allegados que éste haya autorizado. Sin embargo, tal acceso no es completo porque hay que contar con “la incorporación a la historia clínica de datos aportados por terceros, especialmente los

[9] Cf. Opinion E-7.025 Council on Ethical and Judicial Affairs. Code of Medical Ethics. Current Opinions. Chicago: American Medical Association; 1997. No sólo es una cuestión ética, a esta cuestión le afecta la Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica (BON 129, 30-V-2002), Art. 5.1.

provenientes del ámbito familiar, así como las apreciaciones y comentarios subjetivos realizados por médicos, diplomados en enfermería u otros profesionales, sobre juicios diagnóstico-terapéuticos, sobre el propio enfermo o su entorno, su comportamiento, actitudes o colaboración,… constituyen elementos añadidos y justifican la limitación de acceso del paciente a la totalidad de su historia clínica" ("Ética de la Historia", n. 16).

Por otra parte, como en tiempos pasados, se sigue ocultando la información o limitando el acceso a la documentación a los pacientes si se sospecha que su conocimiento pueda perjudicarles. Determinadas enfermedades psiquiátricas o ciertos datos genéticos incluidos en la historia, por ejemplo, podrían desaconsejar el acceso del enfermo, ya que podrían no ser correctamente interpretados o crear una situación de angustia e incertidumbre. La tradición médica ha recurrido frecuentemente a los familiares para transmitir la información, cuando el facultativo estimaba que era lo que más beneficiaba al enfermo. En esos casos era importante elegir bien al interlocutor. Lo habitual no ha sido tanto el derecho a no ser informado, como la decisión del médico o incluso de la familia sobre qué no tenía que ser comunicado al paciente. Esta práctica es conservada y admitida en la actualidad a través de la llamada "necesidad terapéutica".[10]

Para otros accesos a la documentación

Ya hemos visto que el médico no puede entregar a terceros la historia clínica completa o parte de ella, a no ser que el paciente lo autorice o que lo impongan deberes superiores de protección de la salud pública o la normativa legal. El código deontológico contempla los supuestos siguientes (CEDM, art. 16): evitar daños al paciente, a terceros o a la comunidad; la exigencia legal (para realizar un parte de lesiones o declarar como testigo ante un juez); la protección de la salud pública (enfermedades de declaración obligatoria); las certificaciones de nacimiento y defunción (datos públicos, certificables en el registro civil); no causar perjuicios injustos por mantener el silencio; o en la gestión de un expediente disciplinario. Brevemente nos referiremos a algunos de estos casos:

- En lo que se refiere a la colaboración con la administración de justicia, los jueces pueden, en el ámbito penal, ordenar el secuestro de la historia clínica cuando constituye elemento de prueba de un acto presuntamente delictivo; “pero en otros muchos procedimientos no penales no está justificado el acceso judicial a la historia clínica completa”. En todo caso, los jueces,

[10] Definida legalmente como “la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave." Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE 274, 15-XI-2002), Art. 5.

“deberían motivar su requerimiento y precisar qué elementos concretos de la misma son de su interés” ("Ética de la Historia", n. 18). No parece que exista, a priori, un deber de entregar, sin motivación judicial suficiente, la totalidad de la historia clínica de un paciente o de un grupo de pacientes, por lo que el médico o el profesional tendrá derecho a exigir que la autoridad judicial precise qué datos de la historia clínica se consideran necesarios para el buen fin de la investigación.

- Con relación a fines epidemiológicos o de salud pública, prevalece el interés por evitar el peligro para la seguridad de todos los ciudadanos. Aunque habrá que evitar situaciones discriminatorias para el paciente, sobre todo en los ambientes educativos y laborales.
- Los estudios estadísticos, las inspecciones de los servicios sanitarios, o las auditorias de calidad asistencial o de control del gasto médico o farmacéutico, son de innegable valor sanitario y social. En esos casos, no es necesaria la identificación del paciente, motivo por el que se pueden anonimizar las historias clínicas, de forma que puedan utilizarse los datos sin desvelar la identidad del paciente “y solo pudieran, en determinadas circunstancias, cruzarse con sus datos de identificación” ("Ética de la Historia", n. 19).
- El acceso a la historia clínica para la docencia y la investigación científica, aun siendo tareas imprescindibles para el progreso y desarrollo de la medicina, no anula la obligación de preservar los datos de identificación personal del paciente, salvo que éste haya dado el consentimiento para que con tal fin se acceda y se utilice la documentación clínica.

  Habitualmente, los documentos propios de los proyectos de investigación se conservan separados de las historias clínicas, ya que se refieren a cuestiones diversas y pueden ser sometidos a revisión e inspección por instancias administrativas no asistenciales. Sin embargo, pueden contener datos clínicos relevantes, por lo que al finalizar el proyecto de investigación también habrán de custodiarse y conservarse siguiendo las pautas que corresponden a los documentos de carácter clínico.
- Un caso particular de acceso a la historia clínica lo constituye la necesidad que tienen las compañías de seguros y las mutuas de contar con información de los asegurados para poder calcular los riesgos y hacer la provisión de fondos. Es habitual que los asegurados, como condición para la suscripción de una póliza, otorguen a estas entidades su autorización para la cesión de los datos a otras bases de datos o para el acceso a todas las informaciones referentes a su estado de salud. Por lo tanto, la custodia de la confidencialidad de la información médica de los pacientes frente a las entidades aseguradoras no se plantea en términos de legalidad o ilegalidad, aunque desde el punto de vista ético cabría cuestionar la licitud de tales cláusulas.

En todos esos casos, los médicos y los responsables de las instituciones sanitarias son quienes han de salvaguardar el derecho de los pacientes. Los médicos han de facilitar a sus colegas de las aseguradoras, con toda veracidad, la información limitada a lo estrictamente necesario en función de su finalidad, contando siempre con la conformidad o la autorización del paciente-asegurado (CEDM, art. 11.2).

Los responsables de las instituciones, por su parte, han de ser conscientes de que son garantes de la confidencialidad de las historias clínicas depositadas en sus archivos (CEDM, arts. 15.2 y 17.2) y no han de ceder a la presión de las compañías a quienes facturan la asistencia médica.

Como resumen podemos decir que, frente a la prioridad de los derechos de la persona a la confidencialidad de sus datos en la historia clínica, sólo podrá prevalecer el justo y superior interés de la sociedad, que se ha de concretar siempre de forma motivada y con el suficiente reconocimiento legal. Esta autorización o esta obligación de revelar los datos no afecta a la discreción del profesional, que procurará siempre mantener la confianza social hacia la confidencialidad.

4. Seguridad, integridad y conservación

La seguridad de los documentos clínicos es objeto de preocupación internacional. Primordialmente hace referencia a la necesidad de establecer controles al acceso a las historias clínicas, ya sean electrónicas o en papel; a mantener íntegra la historia clínica; y a garantizar que los datos médicos no serán modificados o alterados por personas no autorizadas.

Desde el punto de vista ético-deontológico, la protección de la documentación clínica está encomendada tanto a los profesionales como a los centros asistenciales.[11] Ambas instancias están imbricadas en tal cometido. De ahí la reiterada recomendación de los organismos nacionales e internacionales para que el responsable del archivo de historias clínicas y de los bancos de datos

[11] “El médico, por mandato deontológico (CEDM, art. 13.2) y, en su caso, la institución en la que trabaja están obligados a poner en práctica los medios para impedir el acceso o uso no autorizados, la falsificación o eliminación de datos, el robo, la adulteración maliciosa, y la pérdida o destrucción accidental de la historia clínica durante el tiempo que se estime necesaria su conservación”. "Ética de la Historia", n. 9. También, CEDM, art. 15.2.

clínicos sea un médico. También se subraya la necesidad de que las bases de datos médicos sean estancas, es decir, que no estén conectadas a otros bancos de datos (CEDM, art. 19.3).[12]

La informatización de los documentos clínicos exige definir las facultades del "administrador de datos sanitarios". La autoridad o persona responsable de la obtención y conservación de datos personales relativos a la salud se enfrenta, en lo que respecta a su administración, con una pluralidad de necesidades que aconseja establecer diferentes niveles de acceso a la información.

4.1. Conservación de la historia clínica

Ni el Código de Ética y Deontología Médica de la Organización Médica Colegial de España, ni las normas deontológicas de otros países europeos fijan un límite temporal al deber de conservar las historias clínicas de los pacientes. La regulación legal tampoco es unánime: cada país, cada CC.AA., ha establecido plazos diferentes para la conservación de la historia clínica.[13]

La finalidad fundamental de la historia clínica -facilitar la asistencia al paciente- es la que debería determinar hasta cuándo se ha de conservar la documentación clínica. Pero, además, existen factores de naturaleza jurídica, histórica, epidemiológica y de investigación que aconsejan la conservación incluso después del fallecimiento del paciente.[14]

El problema que se plantea es el coste y el espacio necesarios para almacenar la documentación, cuestión que el desarrollo de nuevos sistemas informáticos está facilitando, aunque todavía no haya un soporte ideal.

---

[12] Cf. también los Principios de Ética Médica Europea, art. 8. La Declaración "Ética de la Historia" comenta la necesidad de que para esa función el médico cuente con amplios conocimientos informáticos.

[13] Cf. capítulo 4 de esta Guía y lo legislado por las Comunidades Autónomas: la Ley catalana (Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica, BOE 29, 2-II-2001) establece un plazo de veinte años a contar desde la muerte del paciente, mientras que la gallega (Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes, BOE 1583-VII-2001) señala un plazo mucho más corto: cinco años desde la última asistencia prestada o desde el fallecimiento del paciente, aunque algunos documentos tienen que conservarse indefinidamente.

[14] Un caso especial sería la conservación de los archivos de un médico con ejercicio privado, en el caso de su jubilación o fallecimiento. Para estas situaciones se recomienda que la documentación, o bien sea transferida al médico que se haga cargo de los pacientes, o bien sea puesta bajo la custodia del Colegio de Médicos, o bien sea destruida (CEDM, art. 34.3). Pero un archivo de esta naturaleza no puede quedar bajo el dominio de los familiares del médico.

La deontología también prevé la posibilidad de que, previa valoración médica, se puedan destruir aquellos documentos que no son relevantes para la asistencia (CEDM, art. 13.2), debiendo respetarse: los datos de identificación del paciente, los informes de alta, los relativos a los procedimientos anestésicos, quirúrgicos y obstétricos, los de las exploraciones complementarias, los formularios de los consentimientos informados y voluntades anticipadas, así como el informe de necropsia, en caso de que lo hubiera.

5. Los datos genéticos

La información genética es especial porque, además de importantes implicaciones personales, puede tener decisivas derivaciones familiares y sociales. Los datos genéticos afectan a la misma identidad del ser humano, contienen información relativa al presente y al futuro del individuo y de su familia. Desde un punto de vista ético, la información genética más relevante suele ser la que hace referencia a la reproducción humana y a las escasas posibilidades terapéuticas de muchas enfermedades genéticas.

La precaución con que han de ser tratados los datos genéticos guarda relación también con la complejidad propia de este tipo de información: se refiere a realidades dispares por la diversidad de alteraciones genéticas y enfermedades de ellas derivadas. Los informes pueden ser claramente positivos o negativos. En la mayoría de los casos, los resultados suponen una estimación de riesgo para los individuos, sus familiares y su presunta descendencia.

5.1 El acceso a los datos genéticos

Cada persona tiene derecho a decidir cuándo, cómo y hasta qué punto desea conocer y transmitir su información genética. Habrá que garantizar, por tanto, la confidencialidad de los resultados de los análisis genéticos y establecer restricciones de acceso incluso a los familiares de las personas analizadas. De ahí la tendencia que ha llevado a algunos hospitales a mantener un archivo diferenciado para la información genética. La información genética, insisten los documentos de consenso, ha de ser utilizada para el fin o fines que la originó, no pudiéndose transmitir a terceros ajenos al ámbito asistencial.[15]

[15] Declaración Universal sobre el Genoma Humano y los Derechos Humanos, de la UNESCO; 1997.

Sin embargo, la cuestión sigue suscitando vivos debates. Se discute si es ético que alguien pueda negarse a proporcionar información genética a personas a las que afectan esos datos. Se plantea si existe un "derecho a saber" e incluso un “deber de saber” por parte de terceros. Algunos consideran que habría que revelar a los familiares el riesgo que tienen de padecer la enfermedad. No revelar estos datos supondría dañar a esas terceras personas, lo cual sería suficiente razón para quebrantar la confidencialidad. Habría que hacerlo, insisten, incluso en el caso de que la enfermedad no tuviera tratamiento o no pudiera prevenirse, ya que esa situación podría cambiar, o bien podría ser útil conocer esos resultados.[16]

5.2 La no discriminación

El interés especial de la confidencialidad de la información genética está orientado a evitar la discriminación.[17] Se suelen citar, sobre todo, el ámbito laboral y el de los seguros. Pero no son los únicos: los avances de la farmacogenómica, que tiene como objetivo lograr una medicina personalizada en la que cada paciente reciba un tratamiento de acuerdo con su perfil genético, lleva a la exclusión terapéutica de quienes no tengan suficiente sensibilidad genética a los medicamentos.[18]

La información genética puede ayudar a evitar enfermedades profesionales o puede ocasionar una discriminación del trabajador, si se utiliza como criterio de selección. Son muchas las empresas que desean conocer la aptitud física y psicológica de sus trabajadores. Desean conocer el absentismo predecible por la manifestación de futuras enfermedades.

Por su parte, las aseguradoras quieren eliminar al máximo el "factor riesgo". Pretenden conocer unos datos de los que va a derivar la estimación de riesgo y de gasto. Las señas de identidad genética de una persona constituyen un objeto muy apetecible para las compañías de seguros a la hora de establecer las condiciones de las pólizas o de rechazar a un futuro cliente. Sin embargo, y, aunque no exista en España, de momento, una legislación expresa sobre la cuestión, el acuerdo es unánime: "Sólo podrán hacerse pruebas predictivas de enfermedades genéticas o que permitan identificar al sujeto como portador de un gen responsable de una enfermedad, o detectar una predisposición o una

[16] Bowles Biesecker asegura que el que una persona se niegue a revelar la información genética a su familia, es excepcional y hay que intentar convencer al paciente para que lo autorice. Bowles Biesecker B. Practice of Genetic Counselingin. En: Encyclopedia of Bioethics. New York: Macmillan; 2004, 3ª ed. p. 952-955.

[17] Convenio relativo a los derechos humanos y la biomedicina, Oviedo, 4 de abril de 1997 (BOE 20-10-99 y 11-11-99). Art. 11.

susceptibilidad genética a una enfermedad, con fines médicos o de investigación médica y con un asesoramiento genético apropiado".[19]

La Declaración Universal sobre el genoma y derechos humanos (1997) presenta la confidencialidad como una garantía del derecho al respeto de la dignidad y derechos del individuo, cualesquiera que sean sus características genéticas.[20]

Los avances en el ámbito de la genética y la naturaleza de la información que generan anuncian, para un futuro inmediato, la aparición de problemas éticos y jurídicos de extraordinaria complejidad y repercusión.

6. La telemedicina

El término telemedicina se refiere a la práctica de la medicina a distancia. En la telemedicina, las intervenciones diagnósticas o terapéuticas y las recomendaciones se basan en datos, documentos, imágenes o información transmitida a través de sistemas de telecomunicación. Continuamente se están desarrollando nuevas técnicas de información y comunicación por lo que aumentan las posibilidades de la medicina telemática dirigidas a la atención al paciente y a la consulta con expertos. También son numerosos en todo el mundo los documentos que comentan los aspectos éticos de este tipo de asistencia.

En la telemedicina continúan vigentes los principios éticos propios de la asistencia clínica. Ni la distancia ni la interposición de instrumentos disminuyen la plena relación de confianza que ha de existir entre el profesional de la salud y el paciente, ni difuminan el carácter interpersonal de su relación.[21] Por lo que también se aplican las normas de consentimiento del paciente para decidir qué

[18] Committee for Propietary Medicinal Products (CPMP). Position paper on terminology in Pharmacogenetics. EMEA/CPMP/3070/01. London, 13 December 2001.

[19] Resolución del Parlamento europeo sobre los problemas éticos y jurídicos de la manipulación genética, 16 de marzo de 1989; Convenio relativo a los derechos humanos y la biomedicina, Art. 12.

[20] La Declaración Universal sobre el Genoma Humano y los Derechos Humanos, de la UNESCO, Art. 6.

[21] En el debate ético que precedió a la aprobación del documento: The practice of telemedicine in Europe: analysis, problems and CPME recommendations (CPME 2002/027), se identificaron los siguientes principios: Principio de responsabilidad: la telemedicina ha de ser considerada como un acto médico; Principio de seguridad: obliga a proteger los datos cuando son transmitidos, reproducidos y conservados; Principio de confidencialidad: por la importancia del secreto en la relación a distancia entre médico y paciente; Principio de precaución: para proteger los datos de la criminalidad informática; Principio de transparencia: se ha de facilitar al paciente la información correspondiente; Principio de no-maleficencia: implica la abstención de toda

documentos se transmiten y a quién; y la confidencialidad y seguridad de la documentación obtenida telemáticamente. La dificultad de seguir estas pautas ha llevado a que, unánimemente, las directrices ético-deontológicas nacionales e internacionales recomienden un uso restrictivo de la telemedicina. Se propone para situaciones en las que no es posible la presencia física y lo requiera la asistencia del paciente.[22] En esos casos, la utilización de Internet como medio para el envío de documentación clínica, obtener confirmación de un diagnóstico, plantear y resolver dudas o requerir opiniones especializadas, es "plenamente aceptable ética y deontológicamente" ("Ética de la Historia", n. 37).

En este tipo de consultas es obligado obtener una identificación inequívoca y segura del consultante y del médico consultor, por lo que, además de registrar adecuadamente la información y documentar cualquier actuación médica (hallazgos, recomendaciones y servicios de telemedicina utilizados), la medicina telemática ha de añadir el registro de la identificación del paciente. La custodia de la confidencialidad se reforzará si se transmiten sólo aquellos datos que sean pertinentes o relevantes para resolver el problema en cuestión.[23]

El profesional ha de ser muy cuidadoso para evaluar los datos y la información que recibe. Su contestación sólo puede darse si la calidad y la cantidad de los datos o la información recibida es suficiente y relevante. En cualquier caso, habrá que establecer medidas regulares de evaluación de la calidad, a fin de asegurar el mejor diagnóstico y tratamiento posibles.

Para cerrar este capítulo sobre los aspectos éticos de la seguridad de la información en los entornos sanitarios cabría volver a aludir a las características de la documentación clínica. Lo haremos, del modo como Laín Entralgo cierra su amplio estudio sobre la historia clínica, enumerando las notas que hacen tan peculiar esta información: "Idoneidad, integridad, claridad, precisión, elegancia: he aquí el

operación éticamente injustificada. Cf. Haehnel P. L'impact de la télémedecine sur la deontologie medical en Europe. En: Colloque Deontologie medicale et télémedicine, du 6 mai 1996.

[22] Además de las declaraciones mencionadas, apoyan esta recomendación un buen número de documentos de asociaciones profesionales: el CEDM español; el Código de los médicos alemanes (Bundesärztekammer. Muster-Berufsordnung für die deutel schen Arztinnen und Arzte. Deutsche Arzteblatt 1997;94:A2354-A2363. n. 7); el de la Asociación Médica Americana (Council on Ethical and Judicial Affairs. Code of Medical Ethics. Current Opinions. Chicago: American Medical Association; 1997. Opinión 5.025); la Orden de los Médicos de Francia, (Qualíté et déontologie sur Internet, abril de 2000); etc.

[23] Así, por ejemplo, la instalación de un equipo de videoconferencia en la habitación del enfermo no autorizaría a curiosear en su vida privada. El paciente ha de autorizar cuándo y para qué fines se conecta la transmisión y quienes pueden presenciarla.

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".[24]

La información clínico-asistencial se refiere a las instituciones, pero el factor más importante para la seguridad de la información de los datos asistenciales son los profesionales de la salud que intervienen en los procedimientos. A ellos han de ir dirigidos los programas de formación continuada, las guías y las directrices.

La confidencialidad, la integridad y la necesidad de la disponibilidad de los datos asistenciales son cuestiones de gran relevancia para los pacientes y para la sociedad, lo cual lleva a buscar la implantación de procedimientos que sean lo más seguros posibles.

7. Resumen y conclusiones

La regulación legal específica sobre la información y la documentación clínica es reciente, pero en su mayor parte estaba contenida en los códigos deontológicos y en las recomendaciones éticas de las profesiones sanitarias.

La finalidad de la historia clínica, facilitar la atención médica del enfermo y dejar constancia de ella, determina los preceptos deontológicos que le afectan y condicionan el acceso a esta documentación. Lo decisivo, desde un punto de vista ético, es la conexión entre los datos allí recogidos y las personas a las que corresponden.

La confidencialidad y la protección de la intimidad son derechos fundamentales que se apoyan en la dignidad de la persona, por lo que la guarda de la confidencialidad por parte del profesional de la salud es, además de un deber legal, un compromiso ético-deontológico grave. Sin embargo, no se trata de un derecho absoluto: hay situaciones en las que el profesional de la salud está obligado a revelar datos confidenciales del paciente porque el bien público o común prevalece sobre el particular. Aun en estos casos, el profesional procurará siempre mantener la confianza social hacia la confidencialidad.

La protección y la conservación de la documentación clínica está encomendada tanto a los profesionales como a los centros asistenciales. Hay una reiterada recomendación de los organismos nacionales e internacionales para que el responsable del archivo de historias clínicas y de los bancos

[24] Laín Entralgo P. La historia clínica: historia y teoría del relato patográfico. Madrid: C.S.I.C.; 1950. p. 763.

de datos clínicos sea un médico. También se subraya la necesidad de que las bases de datos médicos estén aisladas de otros bancos de datos.

Ni las normas deontológicas ni la regulación legal fijan un límite temporal para la conservación de las historias clínicas de los pacientes. Existen factores de naturaleza jurídica, histórica, epidemiológica y de investigación que aconsejan su conservación después del fallecimiento del paciente.

En cuanto a la información genética, cada persona tiene derecho a decidir cuándo, cómo y hasta qué punto desea conocer y transmitir su información genética. El interés especial de la confidencialidad de la información genética está orientado a evitar la discriminación.

Por último, la telemedicina mantiene vigentes los principios éticos de la asistencia clínica. La dificultad de seguir estas pautas ha llevado a que, unánimemente, las directrices ético-deontológicas recomienden un uso restrictivo. Se propone para situaciones en las que no sea posible la presencia física y en las que lo requiera la asistencia del paciente.

Bibliografía y referencias

Asociación Médica Mundial. Declaración sobre las responsabilidades y normas éticas en la utilización de la telemedicina. Adoptada por la 511 Asamblea General, Tel Aviv, Israel, octubre de 1999 http://www.wma.net/s/policy/17-36-s.html.

Carnicero J, Coord. Informes SEIS. De la historia clínica a la historia de salud electrónica. Pamplona: Sociedad Española de Informática de la Salud, 2002.

Organización Médica Colegial de España, Código de ética y deontología médica. Madrid, 1999.

Comisión Central de Deontología, Declaración "Ética de la Historia: su propiedad, conservación y el acceso a ella del paciente o terceros". Madrid, 31 de mayo de 2002.

Herranz Rodríguez G. Comentarios al Código de Ética y Deontología Médicas. Pamplona; 1992.

Herranz Rodríguez G. Aspectos éticos de la telemedicina. En: VII Congreso nacional de derecho sanitario. Madrid; 2000,

Laín Entralgo P. La historia clínica: historia y teoría del relato patográfico. Madrid: C.S.I.C.; 1950.

León Sanz P., director, La implantación de los derechos del paciente: comentarios a la Ley 41-2002. Pamplona: EUNSA; 2004.

Lusignan, S. de, Chan, T., Theadom, A., Dhoul, N. The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics.* 2007*;* 76 (4):261-268.

Comité Permanent des Médecins Européens, The practice of telemedicine in Europe: analysis, problems and CPME recommendations (CPME 2002/027). CP guidelines for e-mail correspondence between a doctor and a patient (CP 2001-112). En: Handbook of Policy Statements; Bruxelles; 1959-2000.

3 Requisitos de Seguridad de la Información del Sector Sanitario

David Rojas de la Escalera
Óscar Blanco Ramos

Oficina de Innovación de Sistemas de Información Sanitaria (ISIS)
Consejería de Sanidad. Gobierno de Cantabria

You have zero privacy anyway. Get over it.
Scott McNealy, Consejero Delegado de Sun Microsystems. Enero 1999

Here is my dilemma. I want my notes to be strictly confidential but readily accessible to those who need them.
Rhona MacDonald, BMJ. Febrero 2001

1. Introducción

La historia clínica de un paciente constituye el instrumento fundamental del proceso asistencial, ya que es el elemento básico de información para la actividad diaria del profesional sanitario. Los datos que contiene, en resumen, son los siguientes[1]:

- Identificación del paciente
- Identificación del centro
- Datos clínicos
- Procedimientos y datos diagnósticos y terapéuticos
- Consentimiento escrito del paciente o representante legal

Este concepto de historia clínica es válido tanto para el modelo tradicional, cuyo soporte mayoritario es el papel, como para el modelo en soporte electrónico, que gracias al importante progreso de las Tecnologías de la Información y las Comunicaciones (TIC) se está extendiendo durante los últimos años.

La historia clínica electrónica salva gran parte de las limitaciones de la historia tradicional al permitir una mayor accesibilidad y disponibilidad de la información del paciente, independientemente del lugar y momento en que esta información se haya generado, e independientemente del lugar y momento en que se produzca la consulta[2]. Esta mayor disponibilidad de la historia clínica electrónica, así como las facilidades que ofrece para procesar de forma más eficiente los datos, tienen un impacto muy importante en los procesos de negocio de la asistencia sanitaria, y obligan a servicios de salud, a centros asistenciales y a profesionales sanitarios a acometer una serie de medidas que garanticen la seguridad de la información clínica.

Desde este punto de vista, la disponibilidad y la confidencialidad de la información son dos intereses en permanente conflicto. Por un lado, el profesional necesita disponer de la información más completa posible para prestar una asistencia sanitaria de calidad, que es el primer derecho del paciente. Por otro, la confidencialidad de dicha información es también uno de sus derechos más importantes, máxime cuando los datos relativos a la salud de las personas afectan a toda la población y son los que mayor preocupación pueden suscitar. Paradójicamente, la mayor disponibilidad de la información permite una asistencia de mayor calidad, pero supone un mayor riesgo para su confidencialidad[3], lo que obliga a la búsqueda de una solución de compromiso entre ambas que permita la prestación de una asistencia sanitaria de calidad y garantice el cumplimiento de la ley[4, 5].

Esta conciliación entre disponibilidad y confidencialidad de la información debe llevarse a cabo en situaciones tan complejas como las que caracterizan a los servicios de salud, derivadas tanto de la presión asistencial como del entorno crítico (por ejemplo, los servicios de urgencias) en el que se desarrolla parte de la actividad clínica, con la aplicación de las medidas necesarias para garantizar la protección de los datos del paciente.

2. La historia clínica tradicional

El soporte clásico y prácticamente único de la información clínica ha sido siempre el papel. Este material permite al profesional sanitario registrar la información con entera libertad de forma y contenido, lo cual ha supuesto siempre una gran ventaja desde el punto de vista del usuario. Sin embargo, el soporte papel presenta varios inconvenientes:

- Escasa estructuración de la información y falta de uniformidad en la presentación, lo que dificulta la búsqueda de información. Esto se debe fundamentalmente a la libertad que la historia clínica tradicional otorga al usuario a la hora de introducir la información, aunque este problema no es exclusivo de los sistemas basados en soporte papel.
- Existencia de información ilegible.
- Riesgo para la integridad de la información, debido a las posibilidades de alteración de los datos y de deterioro o extravío del soporte físico.
- Disponibilidad y accesibilidad muy limitadas.
- Imposibilidad de independizar la forma de recoger los datos que se incorporan a la historia clínica de la forma en la que éstos se visualizan, a pesar de que las necesidades de los usuarios no tienen por qué ser las mismas en ambos casos[6].
- Dudosa garantía de confidencialidad, a causa del movimiento de la historia clínica por el interior, e incluso en ocasiones el exterior, del centro sanitario.
- Dificultad de explotación estadística de la información.

A pesar de todas estas limitaciones, el papel sigue siendo el bien más preciado en los servicios de salud, ya que hasta hace poco se ha carecido de soportes alternativos para la información clínica.

Figura 1: Historia clínica tradicional

3. La historia clínica electrónica

El progreso de las TIC ha permitido la aparición de soportes alternativos al papel para almacenar y transmitir la información clínica. Los sistemas de historia clínica electrónica, y más recientemente los de historia de salud electrónica, intentan resolver los problemas de la historia clínica tradicional anteriormente mencionados:

- Registro completo y estructurado de los datos y posibilidad de configuración de la presentación, lo que facilita la búsqueda de información.
- Legibilidad perfecta de la información.
- Interoperabilidad con otros sistemas de información, como las soluciones departamentales.
- Inalterabilidad y no repudio: no se produce ninguna alteración de los datos sin que queden registradas las modificaciones efectuadas y el autor o autores de las mismas.
- Amplia disponibilidad de la información clínica, con acceso concurrente y multiusuario.
- Mayor garantía de integridad de la información, ya que no hay necesidad de contacto directo con el soporte de almacenamiento ni de traslado del mismo. Además, se pueden habilitar mecanismos de copia de seguridad.
- Confidencialidad de la información, gracias a la definición de permisos de acceso y a la instalación de mecanismos de autenticación de los usuarios.
- Posibilidad de explotación estadística automatizada de la información, así como de "despersonalización" de la misma para su tratamiento con fines de investigación, estudios epidemiológicos, etc. Esta información puede utilizarse también con fines no asistenciales: administración sanitaria, actividades docentes y académicas, compañías aseguradoras, etc.

Sin embargo, el soporte electrónico también presenta inconvenientes[7]:

- *Financieros*: inversión en el diseño y desarrollo de nuevos sistemas de información corporativos.

- *Organizativos*: convivencia con la historia clínica tradicional. La historia clínica electrónica no parte de cero y es necesario afrontar un extenso periodo de transición entre la historia clínica tradicional y la electrónica.
- Técnicos:
    - Necesidades de infraestructura: despliegue de equipamiento teleinformático para su utilización por los profesionales sanitarios.
    - Ausencia de estándares de aceptación universal: no existe un estándar universalmente aceptado para el intercambio de datos clínicos, por lo que la comunicación entre las diferentes soluciones es difícil y cara, ya que los estándares existentes pertenecen con frecuencia a entidades privadas y deben abonarse los correspondientes costes de las licencias, además de asumir una relación de dependencia tecnológica respecto del proveedor correspondiente. Esta tendencia ha cambiado en los últimos años, con la aparición de estándares abiertos que permiten una mayor interoperabilidad, entre los que destaca el Clinical Document Architecture (CDA), basado a su vez en el formato eXtensible Markup Language (XML) y englobado en el estándar Health Level 7 (HL7).
- Culturales:
    - Concienciación del profesional: el clínico aún considera las TIC como un elemento poco importante para la práctica asistencial, investigadora y docente. Esto se debe en parte a que el proceso automatizado de la información exige una codificación y estructuración de los datos, que puede colisionar con la necesidad de utilizar texto libre por parte del clínico, muy común debido a su flexibilidad y comodidad y a la aparente ventaja que supone para el usuario. La historia clínica en soporte papel puede organizarse de manera intuitiva, ya que permite acciones como escribir en los márgenes, emplear varios colores diferentes, símbolos y marcas personalizados, etc.
    - Necesidad de codificar y estructurar la información: en línea con lo explicado en el punto anterior acerca de la necesidad de adoptar unos estándares universales para el intercambio de datos clínicos, se requiere un gran consenso por parte de los usuarios, lo que puede ralentizar y encarecer el desarrollo de la historia clínica electrónica.

No obstante, los servicios de salud deben contemplar este cambio como una oportunidad de mejora de la calidad del proceso asistencial, siendo plenamente conscientes de sus implicaciones, así como del éxito obtenido en otros sectores profesionales que optaron por la utilización de las tecnologías hace años[8]. Uno de los mejores ejemplos se puede encontrar en el sector financiero, donde la banca ha automatizado completamente su método de trabajo, agilizando considerablemente los trámites necesarios para su funcionamiento, y sin embargo, la gran cantidad de información que manejan

diariamente está sometida a una seria de estrictas medidas de protección que garantizan la seguridad de todos sus procesos.

Finalmente, no debe olvidarse que el desarrollo de la historia clínica electrónica está orientado al beneficio del ciudadano, que en último término podrá recibir una mejor atención al generarse un importante valor añadido para el profesional sanitario.

4. Seguridad de la información = Confidencialidad + Integridad + Disponibilidad

La normativa vigente en materia de protección de datos establece los requisitos de seguridad que deben cumplir todos los sistemas de información sanitaria, en lo referente tanto a la confidencialidad de la misma como a su integridad, pero como se ha explicado anteriormente, es imprescindible que el profesional sanitario disponga de esta información para prestar una atención sanitaria de calidad. Por lo tanto, el concepto de seguridad debe incluir los tres requisitos: confidencialidad, integridad y disponibilidad[9].

4.1 Confidencialidad

Los profesionales sanitarios implicados en el proceso asistencial están obligados a guardar el secreto médico, que es inherente al ejercicio de su actividad profesional y constituye uno de los derechos más importantes del paciente, hasta el punto de que no se extingue ni siquiera después del fallecimiento de este último. Por consiguiente, el requisito de confidencialidad consiste en garantizar que sólo accede a la información quien dispone de autorización para ello, y sólo cuando este acceso resulta necesario.

Los requisitos que deben cumplirse para asegurar la confidencialidad de la información son las siguientes:

- Determinar quién puede acceder al sistema y a qué información puede acceder. Deben existir unas directrices de *autorización* que especifiquen los permisos y privilegios de cada profesional en función de su perfil y de las atribuciones del puesto que desempeña. Es decir, debe llevarse a cabo una *definición y asignación de roles y permisos*. De este modo, se garantiza que sólo accede al sistema el profesional *autorizado* a tal efecto, y que dicho acceso

queda restringido a la *información pertinente y necesaria para* la prestación asistencial, así como al *tiempo* durante el cual ésta se prolongue.

- Conocer quién accede realmente al sistema y a qué información accede. Debe disponerse de un sistema de *gestión de identidades* destinado a la *autenticación* del profesional, con el fin de evitar suplantaciones, además de sistemas de *monitorización, registro y auditoría* de los accesos de ese usuario. Así se asegura que toda la *actividad* relativa al acceso y tratamiento de los datos queda debidamente *registrada* y *auditada*.
- Proteger la información clínica. Además de las medidas anteriormente expuestas, relativas al control de accesos, se deben implantar unos mecanismos de *cifrado* de la información, destinados a impedir que, en caso de que se produzca un ataque contra el sistema, el responsable del mismo no pueda interpretar los datos a los que ha tenido acceso.

4.2 Integridad

Los servicios de salud deben garantizar que la información contenida en la historia clínica de los pacientes es veraz y completa. En otras palabras, el requisito de integridad exige:

- Que la información se encuentre *protegida* contra accidentes, ataques y extravíos, minimizando la posibilidad de alteración o pérdida total o parcial de la misma y garantizando su *recuperación* en caso de que sea necesario. Esta condición se aplica a todo proceso de consulta, tratamiento, almacenamiento o transporte del que puedan ser objeto los datos.

  La protección de la información requiere disponer de mecanismos de *prevención y detección de ataques* y de sistemas de *copia de seguridad* orientados a la recuperación de datos.
- Que ninguna de las partes implicadas ya identificadas y autenticadas pueda *negar* parcial o totalmente su *participación* en cualquier proceso al que haya sido sometida la información. Es decir, debe garantizarse el *no repudio* por parte del profesional. Para ello existen sistemas de *certificación digital*, como la firma electrónica.

4.3 Disponibilidad

Uno de los requisitos más importantes para que los profesionales sanitarios puedan prestar una atención de la máxima calidad durante un episodio asistencial, como se adelantaba en la introducción, es que la información clínica del paciente sea accesible para dichos profesionales. En otras palabras, la información necesaria debe estar disponible para su consulta por parte de los usuarios debidamente

autorizados, en cualquier momento en que se precisen estos datos y desde cualquier punto de la red asistencial en el que pueda prestarse la atención sanitaria.

Para asegurar la disponibilidad de la información es preciso contemplar los siguientes aspectos:

- Definición de unos *niveles de servicio* de los sistemas de información, adecuados a las necesidades de la prestación sanitaria.
- Adaptación de los sistemas de información ya existentes a los niveles de servicio definidos.
- Dotación y mantenimiento de los *recursos*, tanto humanos como materiales, necesarios para garantizar la *operación* de los diferentes sistemas de información, cumpliendo los acuerdos de nivel de servicio previamente establecidos.

La siguiente tabla presenta un resumen de necesidades de seguridad en el sector sanitario y medidas para su solución:

Necesidad	Medidas
Confidencialidad	Definición de permisos: determinar quién *puede* acceder al sistema y a qué información *puede* acceder.
	Control de accesos: conocer quién accede realmente al sistema y a qué información accede.
	Protección del sistema: *impedir* accesos no autorizados
Integridad	Protección de la información: evitar la *alteración* o *pérdida* de datos, y garantizar su *recuperación* en caso necesario.
	No repudio: impedir que un agente implicado en el tratamiento de la información niegue su participación.
Disponibilidad	Definición de los niveles de servicio correspondientes.
	Adaptación de los sistemas de información a los niveles de servicio.
	Dotación de los recursos necesarios para garantizar el nivel de servicio.

4.4 La seguridad en la historia clínica

Los requisitos de confidencialidad, integridad y disponibilidad son inherentes al concepto de historia clínica e independientes del soporte, ya sea físico o electrónico, en el que se almacene la información. Sin embargo, el formato tradicional en soporte papel es susceptible de incumplir gran parte de los requisitos expuestos, a diferencia de los sistemas de información basados en el desarrollo de las TIC.

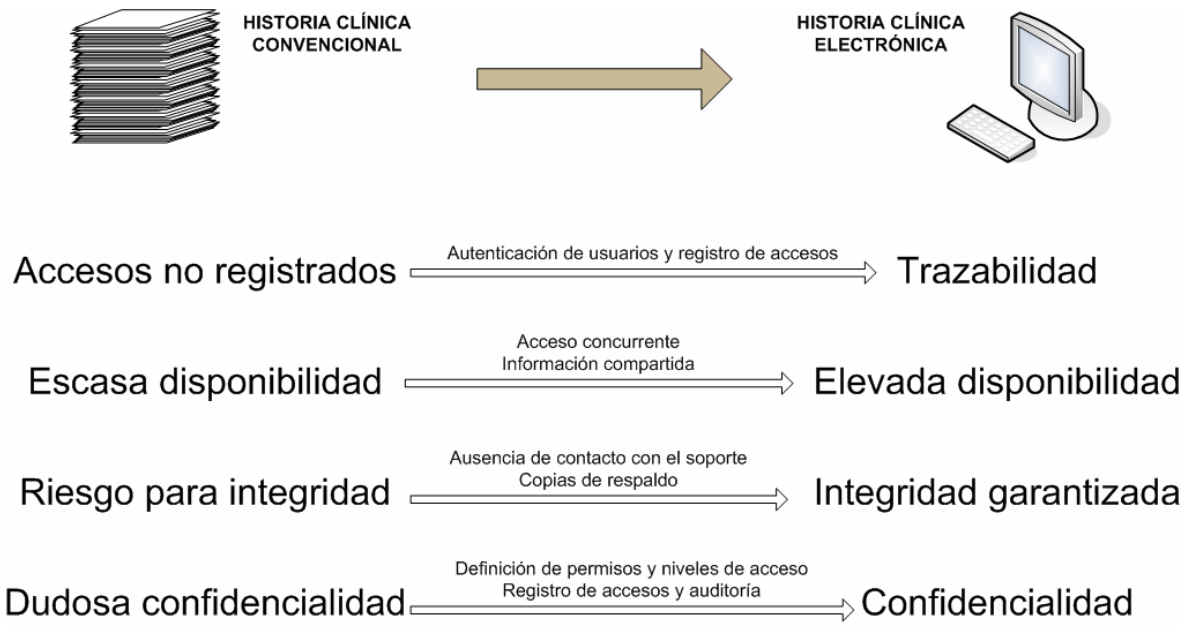


Figura 2: La seguridad en la historia clínica tradicional y en la historia clínica electrónica

5. La historia clínica electrónica como sistema de información compartida

Un servicio de salud o un centro asistencial dispone de distintos sistemas de informaicón, tanto corporativos como, sobre todo, departamentales:

- Información clínica o asistencial: Sistema de Información Hospitalaria (HIS), Fichero Maestro de Pacientes, Gestor de Peticiones Clínicas, Sistemas de Información de Laboratorios (LIS), Prescripción y Dispensación de Medicamentos, Gestor de Citación, Estación Clínica, etc.
- Información administrativa: Contabilidad, Suministros, Nóminas, Facturación, etc.

La sustitución del papel como soporte de la información de la historia clínica ofrece la posibilidad de compartir los datos de manera ágil entre los diferentes profesionales de los servicios de salud, lo que obliga a que dichos datos se transmitan entre los diferentes sistemas de información existentes[10,11]. Todas estas transacciones entre sistemas deben estar protegidas por medidas de seguridad que garanticen la confidencialidad de la información.

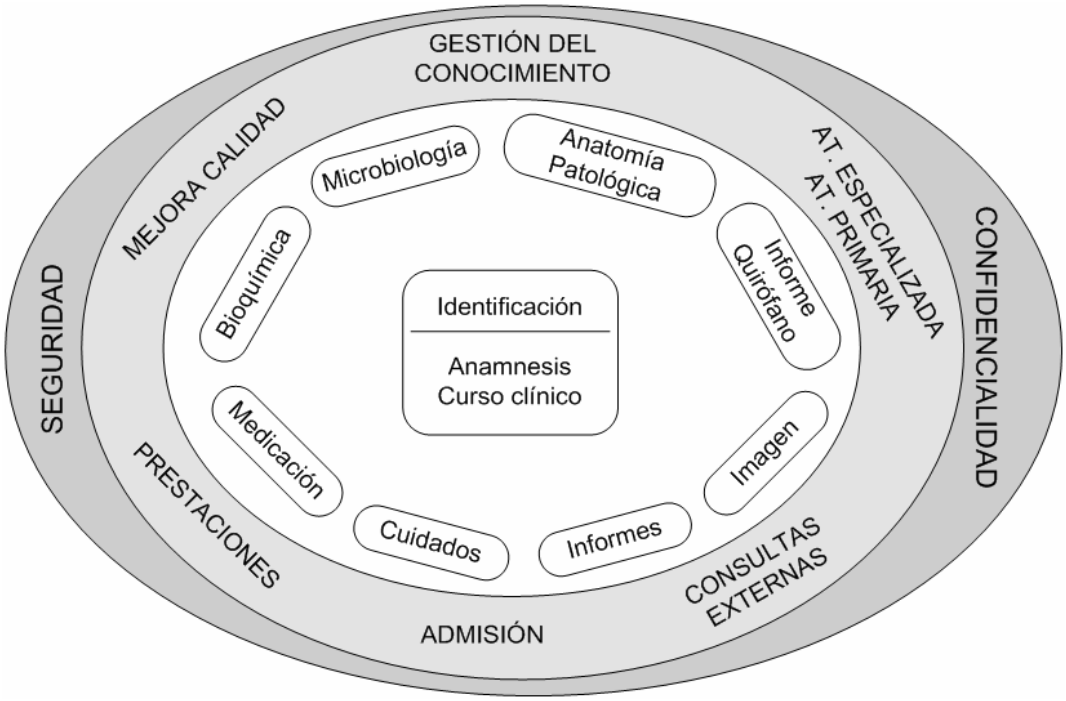


Figura 3: Modelo de historia clínica electrónica. Fuente: [2]

Por lo tanto, uno de los fundamentos de la eficacia de la historia clínica electrónica es el intercambio de información entre todos estos sistemas, con las consecuencias que ello supone en materia de seguridad. A continuación se exponen, brevemente, algunas medidas de seguridad imprescindibles en el entorno sanitario, ya adelantadas en el apartado anterior y elevadas ahora a una escala corporativa:

- Protección de cada sistema de información:
    - Definición de permisos y niveles de acceso para los diferentes usuarios.
    - Registro de la actividad de los usuarios sobre el sistema.
    - Procedimientos de copia de respaldo y recuperación de información.
- Protección del conjunto de sistemas de información:
    - Definición de permisos y niveles de acceso para el intercambio de información entre sistemas. Estos parámetros no tienen por qué coincidir con los individuales de cada aplicación. Los privilegios que un usuario puede tener en un sistema de información pueden no ser extensibles a otros.
    - Gestión corporativa de identidades. Además de aplicar la política de permisos de usuario, es necesario garantizar que el profesional pueda trabajar en un entorno amigable que le permita un eficaz desempeño de su labor. Una de las demandas más frecuentes de los profesionales sanitarios es que sólo tenga que autenticarse una vez en

el sistema, para lo que es necesario que la comunicación entre los diferentes sistemas se realiza de forma automática y transparente al usuario.

- Protección de las comunicaciones entre los diferentes sistemas. Cuando se trabaja con más de un sistema de información, surgen dos nuevos puntos de vulnerabilidad: las líneas de comunicación y las plataformas de integración entre sistemas (repositorios compartidos, transmisión de ficheros, interfaces, etc.), que se convierten así en nuevos elementos que proteger. En esta situación se colisiona nuevamente con la necesidad de disponibilidad de la información, ya que cuanto más estrictos sean los mecanismos de seguridad, menos ágil será la comunicación. Otro ejemplo es la redundancia de líneas, con canales de transmisión secundarios para emplear en caso de fallo de los primarios, que ofrece mayores garantías de funcionamiento del sistema pero introduce más elementos a proteger.

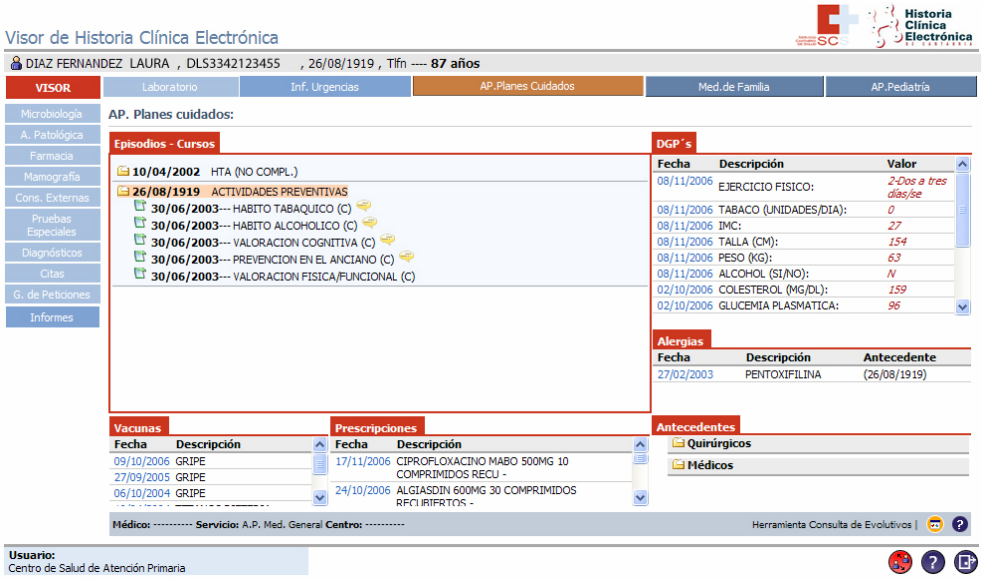


Figura 5: La HCE como sistema de información compartida. El Visor de HCE de Cantabria permite compartir información entre Atención Especializada y Atención Primaria.

6. La información no clínica

Al hablar de gestión de la información en los servicios de salud, es frecuente asumir que los únicos datos sensibles que se manejan son aquellos relativos a la salud de los pacientes. Si bien es cierto que esta información es la que presenta unos requisitos de confidencialidad más estrictos, no hay que

olvidar que las organizaciones sanitarias manejan también otro tipo de información confidencial con el fin de poder llevar a cabo su propia gestión:

- Datos demográficos de los pacientes.
- Datos personales de los empleados: demográficos, financieros, etc.
- Datos de pacientes relativos a citas e interacciones con el centro sanitario. A pesar de que esta información no se considera estrictamente clínica y por lo tanto no forma parte de la historia clínica del paciente, estos datos deben estar sometidos a los mismos criterios de seguridad y control, ya que a partir de ellos puede llegar a extraerse información de carácter clínico, con el consiguiente perjuicio para el paciente. Por ejemplo, el hecho de que un paciente esté citado a una fecha y hora determinadas en una consulta no es de por sí revelador, pero si se trata de una consulta del Servicio de Oncología de un hospital, el conocimiento de este dato puede dar lugar a conjeturas bastante fundamentadas sobre la salud del paciente, con lo que se estaría vulnerando su derecho de confidencialidad.

7. El factor humano

Al igual que sucede en otros sectores profesionales, el factor humano es el eslabón más débil en la cadena que constituyen las medidas de seguridad en los servicios de salud, ya que la responsabilidad del registro, recopilación, tratamiento y difusión de la información recae, en primera y última instancia, sobre los usuarios del sistema. De aquí se deduce que la mayor parte de las incidencias relativas a la seguridad tienen su origen en la intervención de un usuario del sistema de información, ya sea de forma inconsciente o dolosa.

Una de las primeras medidas que debe llevarse a cabo es la sensibilización de los profesionales. Esto no significa en modo alguno que el personal asistencial no tenga presente el deber de secreto inherente a su profesión, sino que la revolución de las TIC es reciente y se necesitan varios años para que los usuarios se familiaricen con las nuevas tecnologías, y aún más para que sean conscientes de los riesgos y oportunidades que ello supone y aprendan a gestionarlos.

Por ello es necesario concienciar a los profesionales de las ventajas que van a obtener en el desarrollo de su actividad cotidiana con la incorporación de las nuevas tecnologías[12]. Se trata de un caso parecido al de la telefonía móvil, el acceso a Internet o la utilización del correo electrónico, cuya utilidad ha quedado ya sobradamente demostrada a pesar de lo reciente de su incorporación al mundo laboral. De hecho, muchos profesionales los consideran actualmente imprescindibles para el desempeño de su trabajo.

8. Resumen y conclusiones

La naturaleza de la historia clínica del paciente la convierte en el elemento básico de información para la actividad diaria del profesional sanitario y por extensión, en el instrumento fundamental del proceso asistencial. Además, la información de la historia clínica puede explotarse con fines no asistenciales, como la docencia e investigación, la administración sanitaria, etc.

De la existencia de la historia clínica surge la colisión entre los dos derechos fundamentales del paciente, que son el de recibir una asistencia sanitaria de calidad y el de confidencialidad de la información. El primero implica que la información clínica del paciente debe estar disponible en el momento y forma que así se requiera, pero el segundo exige que este acceso quede restringido a los datos pertinentes y a los profesionales sanitarios correspondientes. Por lo tanto, es necesario buscar una solución de compromiso que garantice el cumplimiento de ambos derechos, en beneficio del paciente.

La historia clínica tradicional, basada en la utilización del papel como soporte único de la información, dificulta el cumplimiento de ambos derechos, y sólo el progreso de las Tecnologías de la Información y las Comunicaciones ha permitido la aparición de soportes alternativos, en este caso electrónicos, que ofrecen mayores garantías de seguridad de la información. Cabe destacar que el concepto de seguridad engloba la confidencialidad, la integridad y la disponibilidad de la información, es decir, significa: que nadie puede acceder a los datos del paciente sin identificarse adecuadamente y sin la debida autorización; que éstos no pueden ser destruidos ni modificados, ya sea por accidente o a causa de un ataque; y que la información que se precisa durante un episodio asistencial (y únicamente dicha información) se encuentra a disposición del profesional que la necesite para poder prestar la mejor asistencia posible.

El enfoque corporativo de los nuevos sistemas de información sanitaria introduce el concepto de información compartida, de modo que no existe un único sistema en el que residan todos los datos, sino que éstos son almacenados en diferentes sistemas, tanto corporativos como departamentales, y compartidos entre ellos. Para que esta estructura sea eficaz es necesario garantizar la comunicación entre los diferentes sistemas, implantando los canales de comunicación y las plataformas de integración entre sistemas que sean precisos. Esta nueva visión multiplica la cantidad de puntos de acceso a los mismos, por lo que aparecen nuevos requisitos de seguridad a considerar: definición de perfiles de usuario y niveles de acceso, gestión de identidades, protección de las comunicaciones entre los diferentes sistemas de información, mecanismos de monitorización y auditoria, etc.

Además de la información de carácter clínico, no debe olvidarse que los servicios de salud manejan otro tipo de datos que, sin formar parte de la historia clínica del paciente, presentan unos requisitos de confidencialidad establecidos por la normativa vigente. Por lo tanto, las medidas de seguridad deben comprender también esta información no clínica, aunque el nivel de protección no sea el mismo.

Por último, el factor humano es, al igual que sucede en otros entornos profesionales, el punto crítico en la aplicación de las medidas de seguridad en los servicios de salud. Es imprescindible que el usuario sea perfectamente consciente de la necesidad de seguir rigurosamente las políticas corporativas de seguridad de la información, del mismo modo que la organización debe asumir el esfuerzo necesario para llevar a cabo esta labor de sensibilización, contemplando ambos estas necesidades no como un inconveniente, sino como una oportunidad para la mejora de la calidad del proceso asistencial, cuyo beneficiario último no es otro que el ciudadano.

Bibliografía y referencias

(1) Mazón, P.; Carnicero, J. La informatización de la documentación clínica: oportunidad de mejora de la práctica clínica y riesgos para la seguridad y confidencialidad. En: Carnicero, J.; Hualde, S., editores. La seguridad y confidencialidad de la información clínica. Informes SEIS (3). Sociedad Española de Informática de la Salud (SEIS). Pamplona, 12 de diciembre de 2000. Págs. 19-33.

(2) Blanco, O.; Elicegui, I.; Rojas, D. La gestión de la contratación. Relaciones con el equipo ejecutor, gestión del contrato. Propiedad intelectual. En: Carnicero, J., coordinador. La gestión de los proyectos de Tecnologías de la Información y de las Comunicaciones en los servicios de salud. Informes SEIS (7). Sociedad Española de Informática de la Salud (SEIS). Pamplona, 25 de enero de 2007. Págs. 211-222.

(3) Mitjans, E. La información sanitaria y la protección de datos. En: Aced, E.; García, C., coordinadores. Especial Protección de Datos. Revista Informática y Salud, nº 57. Sociedad Española de Informática de la Salud (SEIS). Pamplona, junio 2006. Págs. 12-13.

(4) MacDonald, R. Commentary: A Patient's Viewpoint. BMJ, 2001; 322; 287.

(5) Mandl, K.D.; Szolovits; Kohane, I.S. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ, 2001; 322; 283-7.

(6) Escolar, F.; Iraburu, M.; Manso, E. Modelos de historia de salud electrónica. En: Carnicero, J., coordinador. De la historia clínica a la historia de salud electrónica. Informes SEIS (5). Sociedad Española de Informática de la Salud (SEIS). Pamplona, 18 de diciembre de 2003. Págs. 119-145.

(7) Carnicero, J. La historia clínica informatizada. En: León, P., editora. La implantación de los derechos del paciente. Ediciones Universidad de Navarra, S.A. (EUNSA). Barañáin (Navarra), 2004. Págs. 271-294.

(8) Castells, M. La era de la información. Economía, sociedad y cultura. Vol 1. La sociedad red. Alianza Editorial. Madrid, 2000:225.

(9) Garbayo, J.A.; Sanz, J.; Carnicero, J.; Sánchez, C. La seguridad, confidencialidad y disponibilidad de la información clínica. En: Carnicero, J., coordinador. De la historia clínica a la historia de salud electrónica. Informes SEIS (5). Sociedad Española de Informática de la Salud (SEIS). Pamplona, 18 de diciembre de 2003. Págs. 255-286.

(10) Kohane, I.S.; Van Wingerde, F.J.; Fackler, J.C.; Cimino, C.; Kilbridge, P.; Murphy, S.; et al. Sharing electronic medical records across multiple heterogeneous and competing institutions. Proc AMIA Annu Fall Symp, 1996:60812.

(11) Gostin, L.O. Health Information Privacy. Cornell Law Review, 80. 1995.

(12) Nygren, E.; Wyatt, J.C.; Wright, P. Medical records. Helping clinicians to find data and avoid delays. Lancet 1998; 352: 1462-66.

4 Aspectos legales de la Seguridad de la Información de Salud

Ignacio Alamillo i Domingo

Director de asesoría e investigación

Agencia Catalana de Certificación

1. Los aspectos legales de la seguridad de la información de salud

Las cuestiones de índole jurídica representan una de las preocupaciones más frecuentes en las estrategias de seguridad de la información de salud, por la especial sensibilidad de esta categoría de informaciones, que indudablemente afecta de forma particularmente intensa a los derechos de las personas.

Diversos factores han contribuido a este protagonismo de las cuestiones jurídicas, entre los que debe considerarse la aparición, relativamente reciente, de normativa legal que regula de forma específica la seguridad de la información, en especial cuando se trata de información personal, información propiedad del sector público o que afecta a las denominadas infraestructuras críticas y a la seguridad nacional.

En concreto, en el ámbito de la información de salud, cabe considerar la importancia de una serie de normas que resultan de referencia obligada cuando nos referimos a estas cuestiones, y que, en consecuencia, deben ser conocidas y realmente comprendidas por los gestores de servicios seguros de salud. Las más importantes, listadas en orden cronológico, son las siguientes:

- La Ley 14/1986, de 25 de abril, general de sanidad.
- La Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.
- La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico.
- La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- La Ley 59/2003, de 19 de diciembre, de firma electrónica.

A este breve listado debe añadirse la legislación propia de las comunidades autónomas, la normativa de desarrollo reglamentario correspondiente y las Directivas de la Unión Europea, al menos a título de interpretación, excediendo del ámbito de este trabajo citar el detalle de dicha normativa.

La importancia creciente de los aspectos legales de la seguridad de la información ha sido reconocida en normas de mejores prácticas en la gestión de la seguridad de la información, como la

norma internacional ISO 17799:2005, que dedica al cumplimiento legal la sección 15.1 de sus recomendaciones.

Dicha sección establece como objetivo de control el "*evitar infracciones de cualesquiera obligaciones legales, reglamentarias, administrativas o contractuales, así como de cualquier requisito de seguridad*", partiendo de la consideración de que el diseño, la operación, el uso y la gestión de los sistemas de información puede encontrarse (y de hecho, suele ser el caso habitual) sujeto al cumplimiento de regulaciones jurídicas.

La norma ISO 17799:2005 identifica una serie de controles habituales, orientados al cumplimiento legal y de la seguridad de la información:

- Identificación de la legislación aplicable.
- Cumplimiento con los derechos de propiedad intelectual e industrial de terceros.
- Protección de los ficheros y archivos de la organización.
- Protección de los datos de carácter personal.
- Prevención del abuso de los sistemas de información.
- Uso de los controles criptográficos, incluyendo la firma electrónica y el cifrado de la información.

La aplicación de los controles identificados en la ISO 17799:2005 facilita de forma importante el cumplimiento de la legislación ya que se orientan a disponer de procedimientos dentro de la organización específicamente diseñados para dicho cumplimiento.

Dada la naturaleza de la norma internacional ISO 17799:2005, en este caso recopilando las mejores prácticas en materia de seguridad, cabe completar los controles que propone y adaptarlos a la práctica de cada Estado y cada tipo de organización, realizando una asesoría continua del grado de cumplimiento legal y gestionando los riesgos jurídicos correspondientes.

En España la normativa general sobre seguridad de la información se ha centrado en la protección de los datos de carácter personal, en un primer momento, y en la promoción de la identidad digital y la firma electrónica, más recientemente, cuestiones ambas íntimamente interrelacionadas. Asimismo, en materia específica de salud, la normativa resalta el deber legal de secreto que se impone, como principio general, a toda persona que elabore o tenga acceso a la información y documentación clínica.

Aunque parece innecesario, hay que resaltar que la Ley 41/2002 declara, en su artículo 17, que resultan de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal

Adicionalmente, se han ido produciendo normas más concretas relativas a la seguridad general de la información - de salud o de otras categorías - como la regulación de la identificación e información mínimas en Internet de los prestadores de servicios de la sociedad de la información, el establecimiento de fuertes restricciones a actividades como las comunicaciones comerciales no solicitadas (SPAM) y de obligaciones de conservación de documentos electrónicos originales.

2. La seguridad en la protección de datos personales de salud

Sin duda alguna, el motor que legalmente ha impulsado la adopción de medidas de seguridad en los sistemas de información generales, especialmente en el sector privado, ha sido la normativa de protección de datos de carácter personal, y que en materia de datos de salud resulta particularmente estricta.

Nuestra vigente Ley Orgánica 15/1999, de 13 de diciembre, establece el marco referencial para todo tratamiento de datos de carácter personal, mientras que el Real Decreto 994/1999, de 11 de junio, establece el conjunto mínimo de medidas de seguridad aplicables a los ficheros que contienen datos personales y a los sistemas de información que tratan dichos ficheros.

El concepto de fichero de datos personales viene referido legalmente a "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*". Se trata de un concepto lógico, que abarca las diferentes formas técnicas de organizar la información, como ficheros de datos en unidades de almacenamiento, bases de datos y otras formas de organizar, guardar y acceder a los datos.

Conviene indicar que las medidas de seguridad exigibles a los sistemas de información son diferentes en función de la categoría de datos personales tratados, diferenciándose en tres niveles, de acuerdo con el artículo 4 del reglamento, que establece lo siguiente:

> "*1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.*
>
> *2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.*

3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes."

Los datos de salud, así como los de vida sexual, se consideran datos especialmente protegidos en la LOPD, junto a datos como la ideología, afiliación sindical, religión o creencias, o el origen racial.

En este sentido, el artículo 7.3 exige que los datos de salud puedan ser recabados, tratados o cedidos en las siguientes circunstancias:

- Cuando lo exija una Ley, por razones de interés general.
- Cuando exista consentimiento expreso del afectado.

2.1 Tratamiento de los datos de salud

Asimismo, el artículo 7.6 permite que los datos personales de salud sean tratados cuando resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos personales de salud cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

A pesar del tratamiento estricto y restrictivo de los datos de salud, el artículo 8 de la LOPD establece una habilitación legal expresa para el tratamiento de los datos de salud de las personas que acuden a los centros de salud, cuando determina que las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

El criterio a seguir con respecto a la aplicación de ambos supuestos (artículo 7.6 y artículo 8) es el de la aplicación restringida a los dos supuestos en que únicamente será de aplicación; esto es, que una disposición normativa establezca y disponga con carácter específico un tratamiento de tales datos, o bien que el mismo resulte efectivamente necesario e imprescindible, y ello se justifique debidamente en cada caso concreto, debiendo aplicarse en los restantes supuestos el régimen general.

En general, la LOPD impone la obligación de proteger la seguridad de los datos, mediante la prescripción contenida en el artículo 9 de la misma, que establece que el responsable del fichero (el centro sanitario, por ejemplo) y, en su caso, el encargado del tratamiento (cuando exista, pudiendo por ejemplo, ser una empresa de informática que asiste al centro sanitario en sus procesos y, por tanto, accede a datos personales), deberán 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, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio natural.

Muestra el artículo 9 de la LOPD las características y objetivos clásicos de la seguridad: el análisis de riesgos y la política de seguridad, la autenticidad e integridad de la información, así como el control del acceso a la misma (que a su vez requiere la previa identificación de las personas y dispositivos que deben acceder) y el secreto y la disponibilidad de la información, necesidades que conectan con la función de la seguridad como proceso de negocio clave en el sector sanitario, y con el empleo de productos de seguridad y con productos seguros.

2.2 El Reglamento de Medidas de Seguridad

El Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS), aprobado por Real Decreto 994/1999, de 11 de junio, resulta de indudable aplicación a la informática de salud, partiendo de la calificación de los ficheros que contengan datos de salud como de nivel alto, el máximo previsto en el RMS, en relación con la cual establece un conjunto de obligaciones, que expondremos sucintamente a continuación.

Las obligaciones del RMS competen a toda organización o persona que gestione datos personales, bien en su consideración de responsable del fichero o de encargado del tratamiento, de acuerdo con el artículo 12 de la LOPD.

Podemos distinguir entre obligaciones formales y materiales.

Las obligaciones formales son las siguientes:

- Inscribir el fichero en la Agencia Española de Protección de Datos (ficheros de titularidad pública y privada) o en la Agencia de la Comunidad Autónoma correspondiente, cuando exista y haya decidido crear registro propio (ficheros de titularidad pública, aún los gestionados por entidades privadas mediante fórmulas de gestión por cuenta de entidades públicas).

  Hay que aclarar que el Registro General de Protección de Datos de la Agencia Española de Protección de Datos tiene la función de publicitar todos los ficheros y por tanto, las Agencias de las Comunidades Autónomas que dispongan de Registro propio deben comunicar a dicho Registro General todas las inscripciones que se produzcan.

  Sin dicho mecanismo de coordinación, se debe inscribir el fichero siempre en el Registro General de Protección de Datos, dado que los registros de las Agencias de las Comunidades Autónomas son facultativos, y se pueden establecer para el ejercicio de sus propias competencias, pudiendo optar también por no establecer registro propio y ejercer sus competencias con base en el Registro General de Protección de Datos.
- Disponer de un documento de seguridad, con los siguientes contenidos (artículos 8 y 15 RMS):
  - El ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
  - Las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
  - Las funciones y obligaciones del personal.
  - La estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
  - Los procedimientos de notificación, gestión y respuesta ante las incidencias.
  - Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
  - La identificación del responsable o responsables de seguridad.
  - Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
  - Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.
- Disponer de al menos un responsable de seguridad, encargado de coordinar y controlar las medidas definidas en el documento de seguridad (artículo 16 RMS).

- Disponer en la organización de un procedimiento de notificación y gestión de incidencias de seguridad, que contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma, así como los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación (artículos 10 y 21 RMS).

Las obligaciones materiales, correspondientes a la calificación legal de los datos de salud como de nivel alto, son las siguientes:

- Garantizar la equivalencia de la seguridad de los accesos de aplicaciones, sistemas y redes locales y a través de redes de comunicaciones (artículo 5 RMS), incluyendo el cifrado de la información transmitida (artículo 26 RMS).
- Autorizar de forma previa y expresa los trabajos con datos personales fuera de los locales y aplicar las medidas de seguridad pertinentes (artículo 6 RMS).
- Aplicar a los ficheros temporales las medidas de seguridad correspondientes al nivel de datos que contienen, y destruirlos tan pronto hayan cumplido su función (artículo 7 RMS), así como abstenerse de emplear datos reales en las pruebas de sistemas y programas (artículo 22 RMS) cuando no se apliquen las correspondientes medidas de seguridad.
- Describir y documentar las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información, y adoptar medidas para que dicho personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento (artículo 8 RMS). El control de acceso ha ganado una relevancia importante después de la aprobación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, dado que en dicha norma se establece el derecho al acceso a la información por parte de:
    - Los profesionales del centro donde se asiste a un paciente (artículo 16.1 de la Ley 41/2002), así como del personal administrativo, en cuanto resulte necesario para el cumplimiento de sus funciones propias (artículo 16.4 de la Ley 44/2002). En este caso, resulta preciso listar en el documento de seguridad a todos los usuarios que podrán acceder, empleando mecanismos que les identifiquen de forma inequívoca y personalizada, así como establecer controles que garanticen la autorización del acceso (artículo 18 del RMS).

- Los pacientes o sus representantes (artículo 18.1 de la Ley 44/2002), con excepción del acceso a las anotaciones subjetivas de los profesionales sanitarios (artículo 18.3 de la Ley 44/2003). En este caso, el documento de seguridad deberá incorporar de forma genérica la posibilidad de este acceso mediante el uso de roles, referidos al titular o los diferentes tipos de representantes legales. Cabe diferenciar entre el acceso directo, como usuarios del sistema, o a través de un usuario interno autorizado (por ejemplo, un médico), que actuará como intermediario entre el sistema y el paciente o su representante. La opción para el acceso directo se puede realizar mediante certificado de firma electrónica del paciente o mediante un sistema de gestión o federación de identidad con el servicio de salud que otorga identidad digital al paciente (por ejemplo, mediante comprobación en tiempo real de la identidad de un poseedor de tarjeta sanitaria frente a la Administración sanitaria correspondiente).

- Disponer de relaciones de usuarios identificados de forma inequívoca y personalizada con acceso a los datos, así como procedimientos seguros de autenticación, incluyendo normas especiales relativas a la seguridad de las contraseñas (artículos 11 y 18 RMS) y al uso de certificados digitales para este propósito (cuya adopción promueve la reglamentación de medidas de seguridad propuesta).
- Establecer mecanismos y procedimientos de control de acceso, incluyendo los de acceso físico (artículos 12 y 19 RMS), y disponiendo de un registro de accesos con ciertas características (artículo 24 RMS)
- Implantar procesos de gestión de los soportes informáticos que contienen datos personales, respecto a su entrada y salida, incluyendo la destrucción de la información (artículos 13 y 20 RMS), así como el cifrado de la información contenida en los soportes (artículo 23 RMS).
- Definir y aplicar los procedimientos de realización de copias de respaldo y de recuperación de los datos, con unas garantías mínimas (artículo 14 RMS), incluyendo el almacenamiento fuera de los locales donde se tratan (artículo 25 RMS), con cumplimiento de las medidas de seguridad correspondientes.
- Finalmente, es preciso realizar una auditoria de las medidas implantadas al menos cada dos años (artículo 17 RMS).

3. Identidad digital y firma electrónica

3.1 Identidad digital

Bajo la expresión "identidad digital" se han venido agrupando, de forma reciente, las técnicas que permiten a las personas y a las organizaciones identificarse y actuar en las redes, mediante mecanismos de autenticación de mayor o menor robustez.

En general, la identidad digital se construye empleando datos o atributos que nos diferencian de forma suficiente de otras personas o entidades, siempre dentro de un ámbito concreto, como por ejemplo el nombre y los apellidos, los diferentes números de identificación que se nos asignan desde organizaciones públicas o privadas (DNI, tarjeta sanitaria individual, otros...)

La identidad debe ser asignada de acuerdo con la legislación vigente, si bien puede ser acreditada mediante múltiples documentos, en función de las necesidades concretas. De esta forma, mientras que la identidad personal y la condición de nacionalidad se acreditan mediante el documento nacional de identidad, los extranjeros son también identificados mediante otros instrumentos, como por ejemplo el número de identidad de extranjero (NIE). En el ámbito corporativo, son habituales las tarjetas de trabajadores, mientras que en las relaciones comerciales es frecuente la emisión de tarjetas de identificación de cliente.

Por este motivo, hay que asumir que todos disponemos de diversas identidades parciales, a lo largo de nuestra vida, adecuadas a los diferentes roles y actividades que realizamos, variedad que, como no puede ser de otra forma, se ha proyectado a la identificación digital en las redes de comunicaciones electrónicas.

El Sistema Nacional de Salud dispone de normas sobre identificación de pacientes y profesionales, así como los registros de identidades, que ofrecen una base legal para la construcción de aplicaciones y sistemas de información en su ámbito de influencia.

Desde la perspectiva que interesa en este trabajo, hay que considerar que las organizaciones públicas y privadas han venido asignando mecanismos de identidad digital a pacientes, profesionales sanitarios y a su personal en general, al objeto de permitir que dichas personas, ya identificadas por ejemplo con un código personal, pudieran autenticarse electrónicamente frente a los sistemas de información y realizar procedimientos y trámites electrónicos, informáticos y telemáticos.

Habitualmente se utiliza como identidad digital en los sistemas el nombre de usuario y la contraseña, aunque se aprecia un avance de los sistemas basados en certificados de firma electrónica, especialmente debido al incremento de la cultura de la seguridad y a la nueva regulación administrativa, que fomenta la adopción de mecanismos de identificación más robustos, especialmente en entornos de trabajo distribuidos, como por ejemplo el acceso integrado a historias clínicas de un mismo paciente en centros hospitalarios o servicios de salud diferentes.

En estos nuevos escenarios, en que un paciente o un profesional se relaciona con múltiples instituciones, se produce un incremento de la complejidad de los modelos de relación entre usuarios y aplicaciones, y la identificación y autenticación directa entre el usuario y la aplicación de la organización presenta algunas limitaciones, técnicas, jurídicas y de modelo de confianza, que se tratan de superar con nuevas técnicas, y, en concreto, con la autenticación distribuida (y, por tanto, delegada) y la federación de la identidad.

En este sentido, la norma ISO 17799:2005 recomienda el establecimiento de las oportunas relaciones contractuales entre las personas identificadas y la organización, regulando el empleo de dicha identidad digital, y por supuesto cabe aplicar los controles jurídicos, técnicos y organizativos derivados de la normativa de protección de datos de carácter personal.

3.2 Firma electrónica

La expresión "firma electrónica" se refiere a los mecanismos técnicos que, además de permitir identificarse y actuar en las redes, facilita la producción de documentos originales y auténticos en forma electrónica, así como la prestación del consentimiento y la producción de las oportunas evidencias documentales electrónicas.

Cabe indicar que toda firma electrónica es una identidad digital, pero que no toda identidad digital permite firmar electrónicamente.

Las principales aplicaciones en que se prevé el empleo de certificados electrónicos como mecanismo de identidad digital, de firma electrónica y, en su caso de cifrado, son las siguientes:

- Solicitudes de acceso a información de pacientes en sistemas de información hospitalaria (HIS).
- Solicitudes de acceso realizadas entre distintas aplicaciones empleadas dentro de sistemas hospitalarios, incluyendo administración de pacientes, gestión clínica, patología, radiología, historial y otros sistemas de información.
- Historia clínica electrónica (HCE) e historia de salud electrónica (HSE).

- Correo electrónico seguro.
- Aplicaciones de facturación, de acuerdo con la legislación vigente.
- Aplicaciones de diagnóstico por la imagen, que requieren una vinculación entre las imágenes y la identidad del paciente, así como la autenticación de los profesionales sanitarios que acceden a las imágenes.
- Aplicaciones de control de acceso remoto.
- Aplicaciones de receta electrónica.
- Documentos de consentimiento de pacientes, o de negativa a tratamientos.

Sin embargo, cabe advertir también que existen diversos niveles o tipos de firma electrónica, en función de los riesgos de la aplicación a considerar.

Por otra parte, en relación con los documentos (ficheros, bases de datos, etc) a los que se incorpora la firma electrónica, la Ley 59/2003 de firma electrónica aporta una definición de documento electrónico, con la finalidad de indicar que la información firmada electrónicamente tiene en todo caso la consideración de documento electrónico. En este sentido, de acuerdo con el artículo 3.5, "*se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente*". Por su parte, el artículo 3.6 establece que "*el documento electrónico será soporte de:*

e) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

f) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

g) *Documentos privados*".

Continúa el artículo 3.7 señalando que "*los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable*", en muestra del principio de neutralidad que informa la firma electrónica, y que no varía las condiciones legales aplicables a cada documento.

En el artículo 3.8 de la Ley 59/2003 se reconoce que es admisible como prueba documental en juicio el "*soporte en que se hallen los datos firmados electrónicamente*", matizando los aspectos probatorios de cada modalidad de firma electrónica en la propia Ley de firma electrónica, puesto que la disposición adicional 10ª de la Ley 59/2003 ha añadido un tercer apartado al artículo 326 de la Ley

1/2000, de 7 de enero, de enjuiciamiento civil, indicando que "*cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica*".

Resulta finalmente necesario referirse a la norma contenida en la disposición adicional primera, apartado 2, que determina que "*en el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa*", y que configura a dichos prestadores como archiveros de la prueba electrónica

Firma electrónica ordinaria

El primer tipo de firma electrónica puede identificarse como "firma electrónica ordinaria", y, de acuerdo con el artículo 3.1 de la Ley 59/2003, es "*el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*".

Esta definición permite que todos los mecanismos técnicos de autenticación sean potencialmente considerados como la firma electrónica de una persona, dado que, de acuerdo con el artículo 3.9 de la Ley 59/2003 señala que "*No se negarán efectos jurídicos de una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación con los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica*".

Todos los mecanismos de autenticación, como el número personal de identificación (PIN, en sus siglas en inglés) o el nombre de usuario y contraseña, pueden servir como firma electrónica, y de hecho, en gran cantidad de contratos de acceso a servicios telemáticos se establece de esta forma, al amparo de la previsión legal contenida en el artículo 3.10 de la Ley 59/2003, que establece que "*a los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas*".

A pesar de que esta consideración es correcta, no elimina la realidad de las cosas, y es que el PIN y la contraseña – al igual que sucede con los mecanismos de seguridad simétricos, en los que ambas partes conocen los datos para la autenticación – pueden utilizarse para lograr una autenticación en el sentido de identificar a la entidad (en este caso, a la persona), pero difícilmente van a permitir una autenticación en el sentido de vincular un mensaje de datos con esa persona.

Por tanto, cabe concluir que la firma electrónica ordinaria es sencillamente un mecanismo de identidad digital, y que no resulta idóneo para la firma de documentos, de acuerdo con la propia dicción legal. En particular, y aunque una contraseña pueda calificarse contractualmente como "*firma electrónica del usuario*", hay que recordar que este mecanismo no goza de la declaración legal de equivalencia *ex lege* entre la firma electrónica y una firma manuscrita, contenida en el artículo 3.4 de la Ley 59/2003, porque no cumple los requisitos legalmente exigibles para ser firma electrónica reconocida.

Este hecho tiene un impacto directo en la efectividad potencial de la contraseña como firma electrónica: porque la lectura correcta del artículo 3.9 de la Ley 59/2003 es que no se negarán efectos a la firma electrónica precisamente por presentarse en forma electrónica; es decir, será una firma válidamente producida, siempre que cumpla las condiciones para ello establecidas, habitualmente por las partes, de acuerdo con lo establecido en el artículo 3.10 de la Ley 59/2003, pero los tribunales podrán negar efectos jurídicos en un caso concreto por otras circunstancias, como por ejemplo que la contraseña que actúa como firma electrónica no pueda considerarse suficientemente segura, o que haya sido divulgada (caso cada vez más frecuente, especialmente en casos de robo de identidad digital, por ejemplo mediante *phishing*) o que no permita establecer un vínculo suficientemente fiable entre firmante y mensaje firmado.

En el caso de la contraseña, la ausencia de este vínculo es muy palpable, puesto que no hay operación objetiva que permita verificar que mensaje y contraseña ("firma electrónica") corresponden el uno al otro, a diferencia de lo que sucede con una firma digital ("firma electrónica avanzada"). Por el contrario, este vínculo es puramente arbitrario, establecido en un registro ("log" o bitácora) de la entidad que dispone el mecanismo de autenticación, como por ejemplo un hospital que establece un control de acceso o de firma de recetas electrónicas basado en contraseña, que realmente podría incluso conocer o reproducir la contraseña que ha asignado al usuario y que, por tanto, podría crear o manipular los "datos firmados".

Resulta evidente que no es del interés de las entidades realizar estas actuaciones, pero en caso de conflicto con un usuario que haya podido cometer una infracción, dicha entidad se puede encontrar con dificultades para poder aportar una evidencia o prueba suficiente de la infracción, o incluso recibir una acusación de manipulación indebida por parte del verdadero infractor.

En conclusión, la contraseña (y en general todos los mecanismos de identidad digital o autenticación) pueden servir para establecer un mecanismo de firma electrónica jurídicamente válido, especialmente con el recomendable soporte contractual o la pertinente autorización administrativa,

pero su eficacia jurídica práctica dependerá de la seguridad efectiva y de la prueba real de que se pueda disponer.

Cabe notar que la Ley 59/2003 no establece ninguna norma en cuanto al tratamiento de la prueba de la firma electrónica ordinaria, más allá de indicar que el soporte en que se contienen los datos firmados será admisible como prueba documental (artículo 3.8), lo que dificulta la determinación previa de la diligencia que debe aplicarse a la generación y gestión posterior de las evidencias, así como el procedimiento en caso de impugnación judicial del documento "firmado".

Finalmente, no se recomienda el uso de la firma electrónica ordinaria en aplicaciones que realmente requieran el equivalente a la firma escrita de una persona, especialmente cuando la legislación aplicable exija la presencia de una firma escrita (como por ejemplo, en los casos de informes clínicos, prescripciones y otros).

Firma electrónica avanzada

La firma electrónica avanzada es aquélla que cumple los siguientes requisitos (artículo 3.2 de la Ley 59/2003):

a) Permite identificar al firmante.

b) Permite detectar cualquier cambio ulterior de los datos firmados.

c) Está vinculada al firmante de manera única.

d) Está vinculada a los datos a que se refiere,.

e) Ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

La definición de firma electrónica avanzada se basa, por supuesto, en la definición de firma electrónica, que ya adelantamos en el apartado 3.2.1; es decir, los datos en forma electrónica consignados a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación (artículo 3.1 de la Ley 59/2003). Se trata de un tipo de firma electrónica de mayor seguridad y calidad, idónea para cumplir las funciones de la firma escrita y, por tanto, susceptible de recibir efectos jurídicos.

La firma electrónica avanzada es un concepto neutral desde un punto de vista tecnológico, permitiendo que diferentes tecnologías reciban equivalentes efectos jurídicos. Actualmente, la tecnología más extendida para implementarla es la firma digital basada en criptografía asimétrica.

Las características principales de la firma electrónica avanzada son las siguientes:

1. La identificación del firmante

La firma electrónica avanzada es un mecanismo de identificación superior del firmante, típicamente sustentada en algoritmos de firma digital, una técnica de identificación de entidades de suficiente seguridad y calidad como para recibir efectos jurídicos.

2. La vinculación única con el firmante

La firma electrónica avanzada tiene una vinculación única con el firmante del mensaje de datos, considerándose firmante a la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa (artículo 6.2 de la Ley 59/2003).

La vinculación entre firma y firmante – que se denomina autenticación de origen de datos – se logra mediante el empleo de técnicas informáticas basadas en determinados problemas matemáticos: el firmante posee un dispositivo de creación de firma, como una tarjeta sanitaria individual o una tarjeta de profesional sanitario, en ambos casos con microprocesador que contiene los datos que se emplean para crear la firma.

Dichos datos poseen una vinculación matemática con otros datos, que se emplean para verificar la firma electrónica. Los datos de verificación de firma deben ser conocidos por el destinatario del mensaje, que puede emplearlos para comprobar que la firma fue creada por la persona que posee los datos de creación de firma, y no por otra persona.

Precisamente esta característica es la vinculación entre firma y firmante: podemos saber que esa firma corresponde a ese firmante, y no a otro. Esta propiedad viene garantizada gracias a la existencia del par de claves vinculadas matemáticamente y a la posesión de la clave privada sólo por el firmante.

3. La vinculación con los datos firmados

La firma electrónica avanzada debe permitir la detección de las modificaciones que sufra el mensaje de datos firmado electrónicamente: esta funcionalidad se denomina integridad de los datos firmados.

La firma digital, que se emplea para obtener autenticación (identificación de entidades y de origen de datos), garantiza también la integridad de los datos, característica de la firma electrónica avanzada.

Esto es posible por una propiedad de las funciones de resumen que se emplean en las firmas digitales, para la comparación del resumen cifrado por el emisor con el resumen generado por el

destinatario. Cualquier cambio en el mensaje conlleva la creación por el destinatario de un resumen diferente al resumen que cifró el firmante, de modo que los resúmenes no coincidirán y la firma se verificará incorrectamente; en este caso, la firma ya no está vinculada a los datos firmados, porque el documento no ha permanecido íntegro.

4. El control exclusivo de los medios de creación de firma

La firma electrónica avanzada debe ser "creada por medios que el firmante puede mantener bajo su exclusivo control"(artículo 3.2 de la Ley 59/2003).

Este requisito es una medida de control del uso de la clave privada por parte del firmante, al objeto de sustentar la vinculación real del firmante con la firma.

Si se pudiera demostrar que personas diferentes del firmante tiene acceso a la clave privada, entonces ya no se podría garantizar que las firmas son generadas por el firmante, y por lo tanto, no se podría garantizar la identificación del firmante, ni la vinculación con el firmante, ni la relación existente entre el firmante y el documento supuestamente firmado por él.

Las medidas para cumplir con este requisito de control exclusivo pueden ser diversas, pero en general se refieren a la necesidad de que el firmante disponga de algún elemento para activar o desactivar la firma electrónica.

Cuando se emplea un dispositivo seguro de creación de firma, el control exclusivo viene integrado como parte de dicho dispositivo; por ejemplo, la tarjeta sanitaria individual electrónica, con capacidades de identificación y firma electrónica, debería implantar la autenticación del paciente mediante una contraseña de acceso a la tarjeta, o mediante el empleo de biometría (por ejemplo el uso de la huella digital).

5. El reconocimiento jurídico de la firma electrónica avanzada

El régimen de reconocimiento jurídico de la firma electrónica avanzada es similar al de la firma electrónica ordinaria, dado que tampoco la firma electrónica avanzada goza de la declaración de equivalencia entre firma electrónica reconocida y firma escrita.

Sin embargo, la firma electrónica avanzada ya contiene en su definición legal los elementos que permiten sustentar de forma razonable su uso en los casos en que se exige legalmente la firma escrita, quedando condicionada su eficacia a la prueba de que se pueda disponer, que será habitualmente mayor que en la firma electrónica ordinaria.

Cabe indicar que para que se pueda emplear sin riesgos legales la firma electrónica avanzada en aquellos casos en que una norma imperativa exige la firma escrita deberá existir la oportuna autorización legal, generalmente en forma de normativa administrativa, dado que, como veremos en el apartado 3.2.3, sólo la firma electrónica reconocida se presume legalmente equivalente en todo caso a la firma escrita.

En el caso de la receta médica, por ejemplo, sucede que para resultar válida debe obligatoriamente incorporar la firma del médico, que no puede ser objeto de mecanización, tal como prevé el artículo 3.1.a) de la Orden del Ministerio de Sanidad y Consumo de 23 de mayo de 1994. En este caso, y a salvo de una posible autorización también por Orden referida al uso de otras modalidades de firma electrónica, resultaría imperativo el uso de la firma electrónica reconocida para el cumplimiento de este deber legal de "firmar".

Respecto a los aspectos probatorios de la firma electrónica avanzada, el artículo 3.8 *in fine* de la Ley 59/2003 que "*si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil*", que ofrece la posibilidad de "*pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto*", de forma que se pueda determinar la autenticidad del documento, en cuyo caso las costas, gastos y derechos que origine el cotejo o comprobación serán exclusivamente de cargo de quien hubiese formulado la impugnación, más la multa de 120 a 600 euros que el tribunal pueda imponerle en caso de impugnación temeraria.

Caso de no proponerse prueba alguna, o en caso de no poder determinar la autenticidad del documento, el mismo será valorará conforme a las reglas de la sana crítica.

Hasta la fecha, la firma electrónica avanzada se ha venido empleando de forma habitual en la mayoría de trámites de los ciudadanos y las empresas con las Administraciones Públicas, sin perjuicio de la admisión generalizada de los sistemas de firma electrónica reconocida.

Firma electrónica reconocida

La definición de la firma electrónica reconocida se recoge, como novedad con respecto a la regulación anterior, en la Ley 59/2003, de 19 de diciembre. Se trata de un concepto nuevo demandado por el sector de prestadores de servicios de certificación, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio RDL 14/99 venían exigiendo. Con ello se aclaran las condiciones para la equivalencia directa por Ley entre la firma electrónica y la firma escrita, en el sentido de que no basta sólo con una firma electrónica avanzada,

sino que, de acuerdo con el artículo 3.3 de la Ley 59/2003, se necesitan dos elementos adicionales; "*se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*".

En este sentido, se puede establecer que la diferenciación entre firma electrónica ordinaria, firma electrónica avanzada y firma electrónica reconocida viene dada por los efectos de la firma frente a terceros, en función exclusivamente de la calidad de la firma, que deriva de la tecnología y de los procedimientos empleados.

La firma electrónica reconocida es un mecanismo de seguridad jurídica que aporta certeza y protección de la actuación realizada por medios electrónicos frente al Estado y a los restantes ciudadanos. Este formalismo emplea unas tecnologías que deben ofrecer unas garantías de calidad y seguridad elevadas, que de algún modo son "reconocidas" por el Estado, sin que sea preciso dictar una nueva norma jurídica para cada posible uso de la firma o llegar a un acuerdo previo con cada persona con la que vayamos a firmar documentos electrónicamente, como suele realizarse en los restantes casos de firma electrónica, incluso aunque no sea legalmente exigible en todos los casos.

Por supuesto, esto no resta validez a los restantes tipos de firmas electrónicas, sean ordinarias, avanzadas o que no cumplan todos los requisitos de la firma electrónica reconocida, tal y como dispone el artículo 3.9 de la Ley 59/2003. Sencillamente, el empleo de una firma electrónica reconocida nos garantiza ya el cumplimiento del requisito jurídico de existencia de una firma manuscrita.

En los restantes casos, la firma electrónica se podrá emplear en entornos de contratación entre las partes o, en los casos de uso de la firma electrónica en las relaciones con las Administraciones Públicas, con sustento en normativa administrativa específica dictada en cumplimiento de los requisitos de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común. Y como hemos analizado, en el caso de que la normativa exija de forma imperativa que un documento incorpore una firma manuscrita, se deberá valorar si resulta viable emplear una firma electrónica diferente a la firma electrónica reconocida.

Las características principales de la firma electrónica reconocida son las siguientes:

1. La firma electrónica reconocida es una modalidad cualificada de la firma electrónica avanzada (art. 3.2 de la Ley 59/2003), y por tanto, cumple y reúne todas las características de ésta última.

No todas las firmas electrónicas avanzadas son susceptibles de ser calificadas firmas electrónicas reconocidas; sin embargo, todas las firmas electrónicas reconocidas son necesariamente firmas electrónicas avanzadas.

2. El certificado reconocido

La firma electrónica reconocida se basa en un certificado digital, que presenta unas elevadas características de calidad y fiabilidad, denominado "certificado reconocido".

Frente al resto de tipos de certificados electrónicos, el certificado reconocido se encuentra cualificado por su uso relevante, conforme al artículo 3.4 de la Ley 59/2003; la equiparación del valor jurídico de una firma electrónica avanzada con el mismo valor jurídico de una firma manuscrita, siempre que dicha firma electrónica avanzada haya sido producida por un dispositivo seguro de creación de firma y esté basada en un certificado reconocido.

El concepto de certificado reconocido viene recogido en el artículo 11.1 de la Ley 59/2003: "*Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la presente Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten*". A continuación, el artículo 11.2 de la Ley 59/2003 recoge el contenido mínimo que debe reunir un certificado reconocido, y el artículo 20 de la misma describe las obligaciones exigibles a los prestadores de servicios de certificación que expiden certificados reconocidos.

La fiabilidad del certificado la proporcionan, entre otros:

a) Los datos de identificación del firmante y otras informaciones que se muestran al usuario en el momento de la verificación del certificado.

b) Los procedimientos de identificación y comprobación de los datos que figurarán definitivamente en el certificado.

c) Las medidas de seguridad adoptadas por el prestador de servicios de certificación en todos los procesos relacionados con la generación, emisión y gestión de los certificados digitales.

Resulta de especial relevancia que el prestador de servicios de certificación haya realizado los procedimientos de comprobación de la identidad y demás circunstancias personales de los solicitantes

con arreglo a lo dispuesto en el artículo 13 y en el artículo 17 de la Ley 59/2003 (protección de datos de carácter personal), así como la garantía que ofrece en el servicio que presta, ajustando sus procedimientos a los estándares y mejores prácticas del sector.

3. El dispositivo seguro de creación de firma electrónica

Además de reunir las características de firma electrónica avanzada y estar basada en un certificado reconocido, la firma electrónica reconocida debe ser generada empleando un dispositivo seguro de creación de firma electrónica.

El artículo 24 de la Ley 59/2003 define los datos de creación de firma como "*los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica*", y a continuación define un dispositivo de creación de firma como "*un programa o sistema informático que sirve para aplicar los datos de creación de firma*", como por ejemplo una aplicación web o de escritorio para firmar electrónicamente, que ya suelen venir incorporados a las aplicaciones ofimáticas más populares, como Adobe Acrobat PDF, OpenOffice o Microsoft Word 2007.

Un dispositivo seguro de creación de firma se define en la ley como "*un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:*

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los datos de verificación de firma o de la propia firma, y que quedará además protegida contra la falsificación, con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma".

Para proceder a la clarificación de los requisitos enumerados en el artículo 24.3 de la Ley 59/2003, hay que referirse a las especificaciones técnicas publicadas por el Comité del artículo 9 de la Directiva de Firma Electrónica, o a sus equivalentes técnicos, que suelen considerar que la forma idónea de dispositivo seguro es un microprocesador criptográfico, que se puede presentar en forma de tarjeta, token USB o incluso PDA.

4. El reconocimiento jurídico de la firma electrónica reconocida

Consiste en el establecimiento del efecto típico de la equiparación con la firma manuscrita: "*La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel*" (art. 3.4 de la Ley 59/2003).

La ley le otorga directamente la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica. Esta declaración, sin embargo, es tan genérica que en la práctica se recomienda establecer contratos referentes al empleo de la firma electrónica en las relaciones negociales electrónicas – firma electrónica convencional – o dictar normas administrativas para el empleo de la firma electrónica en la Administración electrónica o en documentos privados regulados por la Administración – firma electrónica normativa.

En este segundo supuesto, además hay que tener en cuenta que el artículo 4 de la Ley 59/2003 permite el establecimiento de condiciones adicionales en el uso de la firma electrónica - incluso sobre el uso de la firma electrónica reconocida - por parte de las Administraciones Públicas, con el objeto de salvaguardar las garantías de cada procedimiento. Esta posibilidad permite exigir una auditoría previa a la admisión del uso de los certificados emitidos por los prestadores de servicios de certificación.

Respecto a los aspectos probatorios de la firma electrónica reconocida, el artículo 3.8 de la Ley 59/2003 establece que "*si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes*".

Se trata de una norma algo oscura, que configura al prestador del servicio de certificación como participante activo en la verificación, custodia y archivo de la prueba electrónica, cuando realmente no parece ser ésta la función del prestador, que habitualmente se limita a emitir los certificados, norma cuya modificación se encuentra propuesta en el borrador de la Ley de Impulso de la Sociedad de la Información.

La recomendación desde el punto de vista legal es el empleo, siempre que resulte posible, de mecanismos de firma electrónica reconocida, que son los que ofrecen las máximas garantías de

equivalencia con la firma escrita y el menor riesgo legal de rechazo de los documentos, a pesar de la deficiente configuración del procedimiento probatorio en la vigente Ley de firma electrónica.

4. La identificación de los titulares de tarjeta sanitaria como medio de acreditación de derechos en el sistema de salud

La necesidad de identificar a una persona sin ambigüedades, sea ciudadana, paciente, profesional sanitario o personal al servicio de la administración sanitaria, y los métodos para hacerlo, es uno de los debates más importantes en la seguridad de la información sanitaria.

De los diferentes mecanismos para identificar y, posteriormente, autenticar a las personas, la tarjeta sanitaria ha despertado un especial interés para todas las partes involucradas en el sector, incluyendo las Administraciones Públicas.

La tarjeta sanitaria, por su carácter de elemento único de identificación poblacional dentro de cada Servicio de Salud, permite la asignación de una identidad única a cada ciudadano, que posteriormente puede emplearse en trámites sanitarios y no sanitarios.

Las Administraciones sanitarias de las Comunidades Autónomas actúan como emisoras de las tarjetas sanitarias individuales, cada una de las cuales dispone de su propia numeración, situación que genera dificultades para la acreditación del derecho cuando el titular de la tarjeta se encuentra fuera de su Comunidad.

En el futuro, las identidades de los titulares de tarjeta sanitaria deben funcionar de forma coordinada, objetivo que se puede lograr mediante el reconocimiento cruzados de los diferentes sistemas de numeración empleados por las Comunidades Autónomas, o mediante el cruce centralizado de los diferentes números en un sistema central.

Las líneas de actuación en cuanto a la identidad de los usuarios del Sistema Nacional de Salud, de acuerdo con lo establecido en el artículo 57 de la Ley 16/2003, son las siguientes,:

- El acceso de los ciudadanos a las prestaciones de la atención sanitaria que proporciona el Sistema Nacional de Salud se debe facilitar a través de la tarjeta sanitaria individual, que se prevé en soporte informático.
- Los datos básicos de los usuarios deben figurar de manera normalizada en todas las tarjetas sanitarias individuales.

- El Ministerio de Sanidad y Consumo debe asignar un código de identificación personal único para cada ciudadano dentro del SNS, que coordine los diferentes códigos de identificación personal asignados por las Comunidades Autónomas.
- Se debe desarrollar una base de datos de población protegida por el Sistema Nacional de Salud que genere el código personal único y que actúe como sistema de mantenimiento y actualización de datos básicos para todas las CCAA y otras administraciones competentes en aseguramiento sanitario.

Esta orientación a la centralización en una base de datos única, formada a partir del intercambio de datos entre las diferentes Administraciones sanitarias mediante la red de comunicaciones prevista en el artículo 58 de la Ley 16/2003, contrasta en primer lugar con las posibilidades que ofrecen los sistemas de gestión federada de la identidad, propugnada a nivel técnico por entidades como HL7/IHE o Liberty Alliance. Estos sistemas de gestión federada de identidad permiten el mismo objetivo de autenticación única y coordinada del usuario, mediante su número personal en la tarjeta sanitaria, pero sin que exista un punto central único que deba intermediar todos los accesos, y que parece una mejor opción en términos legales, precisamente a la vista de la LOPD.

En segundo lugar, la existencia de diferentes formatos de tarjeta, con características diversas en las diferentes Comunidades Autónomas (incluyendo tarjetas electrónicas y en soporte plástico), y la actual distribución de competencias en la materia, dificultan que el Ministerio pueda aspirar a la normalización y uniformidad que propugna la normativa.

La existencia de la tarjeta sanitaria europea aporta, en tercer lugar, un elemento de complejidad adicional a gestionar, ya que el colectivo que la recibe es un subconjunto de las personas que reciben la tarjeta sanitaria individual, formado por los trabajadores y sus beneficiaros, que podrán emplearla para evitar avanzar el pago de los servicios de salud que reciban en la Unión Europea. En este caso, el esquema de numeración es el propio de la afiliación a la Seguridad Social.

La gestión federada de la identidad resulta de nuevo una forma eficiente de gestionar esta identidad adicional, y permite construir un sistema de acreditación del derecho completo, en el que un proveedor de servicios de salud pueda aceptar cualquiera de estas identidades (basadas en las correspondientes tarjetas) y comprobar en línea y en tiempo real la existencia del derecho y el grado de cobertura.

El empleo de la tarjeta sanitaria individual en un entorno de gestión federada de identidad, y por tanto, de forma conjunta y segura con las redes electrónicas ha de permitir cumplir los siguientes objetivos:

- Permitir la colaboración entre pacientes y profesionales sanitarios, así como compartir información sanitaria para prestar servicios continuos de salud.

- Permitir a proveedores de servicios sanitarios, aseguradoras y administraciones sanitarias establecer procesos fiables y eficientes de comunicación, y, en consecuencia, la prestación de servicios de alta calidad orientados al paciente, con ahorros considerables procedentes de la mejora de los procesos administrativos.
- Ofrecer sistemas seguros individualizados para permitan a los pacientes acceder al seguimiento de su información médica personal.
- Ofrecer sistemas seguros interactivos amigables y personalizados de información general de salud, así como guía personal en materias sensibles.
- Ofrecer soporte seguro a la movilidad de pacientes con necesidades especiales o en casos de emergencia, así como a la movilidad de profesionales sanitarios, con acceso seguro a la información médica, de forma ubicua.

5. Tipología general de certificados de identidad y firma electrónica

En la actualidad existe una variada tipología de certificados de identidad y firma electrónica, adaptados para usos y comunidades de usuarios concretos:

- *Certificados ordinarios*, que no cumplen los requisitos legales para la identificación de las personas. Se suelen emplear para el aseguramiento de correo electrónico. No se recomiendan ni se suelen admitir en el ámbito de las Administraciones Públicas, por su limitada o nula garantía jurídica.
- *Certificados reconocidos*, sean empleados en la firma electrónica avanzada (sin dispositivo seguro) o en la firma electrónica reconocida (con dispositivo seguro), que cumplen todos los requisitos legales para la identificación de las personas, y que pueden a su vez, clasificarse de la siguiente forma:
    - Certificados de persona física. Resultan idóneos para la identificación de los pacientes o usuarios del Sistema Nacional de Salud, especialmente si se producen dentro de la Tarjeta Sanitaria Individual electrónica e incluyen el código de identificación personal de la Administración sanitaria correspondiente.
    - Certificados de persona jurídica y de entidad sin personalidad jurídica. Se emplean para la realización de los actos de las personas jurídicas que se encuentran incluidos dentro del giro o tráfico ordinario de las mismas, o cuando han sido expresamente habilitados para realizar transacciones con las Administraciones Públicas,. Ofrecen la

interesante posibilidad de automatizar muchos de los actos que deben realizarse, como la facturación o el envío de informaciones, admitiendo el cifrado de forma adicional.

- Certificados de representación, en los que deben tomarse en cuenta los apoderamientos y capacidades de actuación de la persona, indicadas o no en el certificado, antes de confiar en la firma. Debe incluir como subtipos los certificados de representación orgánica, voluntaria, etc. Resultan idóneos para la realización de los actos que requieren, de acuerdo con la legislación vigente, la acreditación de la representación legal, como podría ser el caso del acceso por el tutor a la historia clínica de un incapaz o un menor de edad, con las debidas cautelas en relación con la necesidad de obtener consentimiento, en su caso.
- Certificados de empleados, en los que además de la identidad personal se indica su vinculación con una organización, sin indicación de apoderamiento. Resultan especialmente interesantes para el acceso por el personal administrativo a los datos de la historia clínica o a los datos administrativos de los usuarios, en las debidas condiciones de seguridad jurídica y técnica.
- Certificados de profesional colegiado, en los que además de la identidad personal se indica su colegiación en un colegio profesional. Resultan imprescindibles para la realización de las actuaciones que requieren la acreditación de la colegiación, como paso previo a la comprobación de los restantes requisitos que deben cumplir los profesionales (por ejemplo trabajar para el servicio de salud correspondiente o acreditar determinadas especialidades).

- *Certificados para dispositivos informáticos*, incluyendo certificados para servidores seguros, aplicaciones informáticas, firmado de código o estampación de fecha y hora. Resultan idóneos para aportar seguridad estrictamente tecnológica a los sistemas de información.

5.1 Los certificados digitales y las tarjetas sanitarias

Una de las cuestiones más polémicas e interesantes en la actualidad se refiere a la necesidad, o no, de disponer de certificados electrónicos propios para la e-Salud, frente a la posibilidad de emplear los certificados de identidad y firma electrónica que prevé la Ley dentro de una tarjeta sanitaria individual y electrónica.

En opinión de EHTEL, la Asociación de Telemática Sanitaria Europea, la introducción de estas tarjetas sanitarias electrónicas, con funciones criptográfica (la firma digital, el cifrado, la

autenticación) en los sistemas sanitarios europeos requiere la existencia de infraestructuras de clave pública (PKI) y de otras medidas de seguridad.

Adicionalmente, los Estados miembros de la Unión Europea deben aclarar la situación normativa con respecto a la posibilidad real de sustituir documentos en papel por sus versiones electrónicas, acción que conecta con la Directiva Europea de Firma Electrónica y, en gran medida, con las iniciativas del Programa IDABC de la Comisión Europea y los correspondientes programas nacionales, como la red SARA del MAP y la red propia de Cataluña, operada por el Consorcio para la Administración Abierta de Cataluña (Consorci AOC).

Por su parte, el "Plan de Acción eEurope: Una Sociedad de la Información para Todos", inició a principios del año 2000 y en relación con las tarjetas inteligentes, una serie de trabajos bajo la denominación común de "Smart Card Charter", con especial atención al sector sanitario y, en concreto, a la identificación basada en tarjeta sanitaria.

En general, el Smart Card Charter considera imprescindible la generación de confianza para el desarrollo de la sociedad de la información, entendiendo además que la confianza se encuentra íntimamente ligada a los derechos de las personas, como la seguridad, la identificación, la autenticación, la privacidad y la confidencialidad.

En este sentido, se consideran la tarjeta inteligente y la PKI como elementos esenciales para la construcción de infraestructuras de confianza. En particular, una de las áreas de interés dentro del Smart Card Charter ha sido la tarjeta sanitaria (Trailblazer 11).

Uno de los aspectos más interesante de estos trabajos es un cambio de orientación en relación con el uso de la tarjeta sanitaria, que debe pasar de ser un mero contenedor de ciertos datos, a ser el elemento esencial en relación con las infraestructuras de seguridad en la e-Salud.

En algunas de las experiencias realizadas, el ciudadano dispone ya de su certificado y lo puede inscribir o “cargar” en la tarjeta sanitaria, si bien la opción que nos parece más correcta es la emisión de un certificado específico y propio para el usuario, con generación de las claves dentro de la tarjeta sanitaria, que deberá ser un dispositivo seguro de creación de firma, de acuerdo con la legislación de firma electrónica.

En relación con el DNI electrónico, hay que de decir que no todos los usuarios o asegurados sanitarios tienen DNI, bien por ser menores de edad, bien por ser nacionales extranjeros residentes, de forma que la identidad entre ambos sistemas es difícil de encontrar, y por otra parte no resulta admisible introducir informaciones adicionales en dicho DNI electrónico, al menos de momento, de acuerdo con la política del emisor del DNI.

Los certificados a incluir en las tarjetas sanitarias se deben centrar, más bien, en la identificación de condición de usuario del Sistema Nacional de Salud. En segundo lugar, dichos certificados pueden incluir determinadas informaciones adicionales de los usuarios, como el tipo de aseguramiento.

En tercer lugar, las tarjetas sanitarias deben ofrecer capacidades de firma electrónica para cumplir con las previsiones del derecho de acceso por parte de los usuarios a su información, y para dar cumplimiento pleno al control de los datos personales por parte del propio usuario afectado.

5.2 El modelo ISO de certificación de identidad y firma electrónica sanitaria

Atendiendo a las propuestas técnicas internacionales, como la especificación técnica ISO 17090:2002, la vía más correcta es la expedición de certificados propios y diferentes de otros, aunque igualmente reconocidos y cumpliendo la legislación de firma electrónica correspondiente.

Dicha especificación técnica se centra en una infraestructura de clave pública (PKI) sanitaria, definiendo los conceptos y requisitos básicos de la misma, así como los tipos de certificados que se precisan, y guías de práctica para la creación y operación de las correspondientes entidades de certificación.

Todo ello con la intención clara de disponer de una infraestructura segura interoperable para los servicios y las comunicaciones sanitarias. Distingue el documento ISO entre diferentes actores, que deberán obtener los certificados:

- *Personas*. Incluyendo profesionales sanitarios regulados y no regulados, pacientes/consumidores y empleados sanitarios. En este caso, las personas recibirán certificados con la consideración de reconocidos.
- *Organizaciones*. Incluyendo organizaciones sanitarias y organizaciones de soporte (por ejemplo, ciertos proveedores). Podrían ser certificados de persona jurídica o de entidad sin personalidad jurídica. Asimismo se deberían incluir los certificados de representación.
- *Dispositivos médicos regulados y no regulados*. Se trata de certificados no reconocidos, dado que el concepto de certificado reconocido contenido en la Ley 59/2003 se reserva a los certificados de personas.
- *Aplicaciones sanitarias*. Se trata de certificados no reconocidos, por el mismo motivo, si bien en este caso se propugna una aproximación basada en la posibilidad de cualificar la firma electrónica de aplicación como "sello electrónico", posibilidad que se recoge en el borrador de la Ley de Acceso Electrónico de los Ciudadanos a las Administraciones Públicas.

1. Certificados para los pacientes

En cuanto a los certificados para los pacientes, éstos son, en general, certificados de asegurado de un sistema sanitario, público o privado, quizá parecidos a los certificados de los ciudadanos, pero con sus propias características y particularidades:

- El certificado debería incluir, además de los datos de identidad de la persona física, el número o código de asegurado del sistema sanitario, como base para la acreditación de dicha condición, en relación con sus diferentes prestaciones, y para el establecimiento posterior del sistema de gestión federada de la identidad, que permite el control del acceso a los diferentes prestadores, dentro y fuera del servicio de la salud de la propia Comunidad Autónoma.
- El certificado debería ser expedido a todos los usuarios, porque sirve para su identificación y autenticación, con independencia de que también puedan o no firmar documentos, dado que se trata de funciones completamente diferentes.
- Los certificados no deben estar protegidos de forma que únicamente el usuario pueda emplearlos, sino que, en muchas aplicaciones, la simple presentación física de la tarjeta ha de servir para la autenticación, sin necesidad de emplear un dato de activación de la firma, como una contraseña. Esto implica que la tarjeta sanitaria disponga de diversas aplicaciones de identidad digital, apropiadas a los diferentes usos, como la identificación consciente o el acceso a determinadas informaciones incluso sin la intervención del usuario, como determinados datos vitales.
- Adicionalmente, el certificado ha de permitir producir firmas electrónicas equivalentes a firmas escritas, para que ciertas aplicaciones se puedan beneficiar de ello, como por ejemplo la autorización o la negativa expresa a un tratamiento.

En este sentido, algunos proyectos internacionales han planteado el desarrollo e implantación de infraestructuras de clave pública específicas para el sector sanitario, como por ejemplo Austria, Reino Unido o Francia. Cabe notar, además, que en el proyecto de Austria esta tarjeta sanitaria sirve como tarjeta de ciudadano de propósito general, fuera del sector de salud.

Sin embargo, en algunos Estados de la Unión Europea y, dentro de España en algunas Comunidades Autónomas se ha propugnado la utilización del mismo sistema de certificación para las aplicaciones generales y para las sanitarias; en algunos casos sólo para los pacientes, y en otros, también para los profesionales.

En este caso se inscriben las iniciativas de Finlandia o Eslovenia, por una parte, y de la Comunidad Autónoma de Valencia o el País Vasco, que expiden certificados reconocidos en una tarjeta sanitaria

segura, o incluso de la Comunidad Autónoma de Galicia o de Madrid, que inscriben dentro de una tarjeta sanitaria criptográfica el certificado en software de la FNMT-RCM.

2. Certificados de profesionales

Respecto a los certificados de profesionales, más allá de la identificación de la persona física y de su condición de profesional, hay que tratar el rol de dicho profesional, como por ejemplo, la especialidad médica de un profesional, o que trabaja para un centro contratado por el servicio de salud.

No resulta recomendable incluir estas informaciones en los certificados, dada su potencialmente elevada frecuencia de cambio. En este caso, la solución más correcta legalmente es incluir esta información dentro de certificados de atributos o en bases de datos, y en este segundo caso suministrarla bajo demanda dentro de esquemas de federación de identidad y de capacidades de actuación.

Sin embargo, también se prevé la posibilidad de certificar estas informaciones en origen, mediante un campo especial de “rol sanitario”, para aquellos casos en que muchos destinatarios deban recibir y poder confiar en esta información.

Los certificados de profesionales son habitualmente expedidos por los Colegios profesionales correspondientes, cumpliendo con la Ley de firma electrónica y aportando el correspondiente dispositivo seguro de creación de firma, que frecuentemente es una tarjeta que actúa cono carné colegial.

En esta línea se pueden citar las experiencias de la Autoridad de Certificación de la Organización Médica Colegial o la iniciativa de Firmaprofesional SA, compañía que comercializa certificados a profesionales colegiados.

3. Certificados de persona jurídica o de entidad sin personalidad jurídica

En el caso de los certificados de persona jurídica o de entidad sin personalidad jurídica parece evidente que dichos certificados no resultan en absoluto idóneos para aplicaciones sanitarias, aunque sí, por ejemplo, para aplicaciones de índole administrativa o tributaria (por ejemplo, cuando el hospital deba expedir facturas o presentar su documento de resumen de retenciones e ingresos a cuenta)

Los certificados de representante pueden tener un mayor número de casos de usos, dado que, en función del tipo de representación, la firma en cuestión podrá emplearse para que tutores autoricen actos con relevancia sobre sus tutelados, por ejemplo personas menores de edad, o incapaces.

6. La seguridad y la prestación de servicios de la sociedad de la información

La prestación de servicios de salud por vía de Internet y sus actividades relacionadas, se encuentra sometida a requisitos jurídicos por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico.

Algunas de las actividades que se sujetan a la Ley incluyen:

- Disponer de una página web con información sobre salud o sobre servicios de salud. Como ejemplos podemos citar las páginas web de proveedores de servicios y productos de salud, sin que sea necesario que en dichas páginas web se realicen operaciones comerciales.
- Realización de publicidad de productos, como medicamentos, a través de redes de comunicaciones electrónicas, incluyendo la telefonía móvil, en especial cuando se trata de comunicaciones comerciales no solicitadas.
- La realización de operaciones comerciales, como la venta telemática de bienes y servicios que además debe cumplir la reglamentación al respecto en salud o por ejemplo la contratación de seguros privados de salud.

6.1 Las obligaciones de identificación e información

La Ley 34/2002 establece la necesidad de que los prestadores de servicios se identifiquen electrónicamente y ofrezcan ciertas informaciones mínimas al público en su comunicación telemática, complementando la regulación que ya existía anteriormente.

Las obligaciones de información previstas en la Ley 34/2002 que resultan relevantes en materia de salud son las siguientes:

- La constancia registral del nombre de dominio.
- El suministro de determinada información sobre el prestador del servicio.
- El suministro de información sobre el empleo de "cookies" en las páginas web.
- El suministro de información en caso de prestación de servicios tarificada mediante el empleo de programas y aplicaciones de acceso a números especiales, como la serie 800, posibilidad que no creemos jurídicamente viable.

1. La constancia registral del nombre de dominio

El artículo 9.1 de la Ley 34/2002, de 11 de julio, establece la obligación de inscribir en el Registro el nombre de dominio empleado por el prestador de servicios de la sociedad de la información, como refuerzo de la tendencia a que la identificación electrónica coincida con la identificación tradicional.

"*Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro*".

Esta obligación ha sido muy criticada, por defectos de técnica legislativa en cuanto al procedimiento de "comunicación" a emplear, y no cabe duda de que tiene todo el sentido que el destinatario de servicios de la sociedad de la información pueda obtener la información registral del prestador del servicio a partir del nombre de dominio o la dirección de Internet.

Esta finalidad, sin embargo, se alcanza también mediante la obligación de publicar precisamente la información registral del prestador de servicios de la sociedad de la información, como se establece en el artículo 10.1 de la Ley 34/2002, de modo que puede cuestionarse el acierto de esta prescripción legal, que impone un coste adicional a los prestadores de servicios de la sociedad de la información; el coste de la "comunicación" del nombre de dominio o la dirección de Internet, y no aporta mayor seguridad a los destinatarios de servicios.

En este sentido, cabe indicar que el borrador de Ley de Impulso de la Sociedad de la Información ha propuesto la derogación de este artículo 9, aún vigente.

2. Información a suministrar por el proveedor del servicio

El artículo 10 de la Ley 34/2002 establece la información mínima que se debe suministrar:

"*1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:*

a) Su nombre o denominación social, su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España, su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro a que se refiere el artículo 9.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión

d) Si ejerce una profesión regulada, como el ejercicio de la medicina y otros casos indicados en la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, deberá indicar:

1.ª Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.ª El título académico oficial o profesional con el que cuente.

3.ª El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.ª Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.”

La primera nota de interés al artículo es su carácter de mínimos, que no excluye la necesidad de cumplir otros requisitos adicionales de información, que pueden venir dados por la aplicación de las normas de comercio minorista – en sede de venta a distancia – o de protección de los consumidores y usuarios. Por ejemplo, la normativa de viajes combinados establece requisitos de información concretos para la oferta al público.

En segundo lugar, hay que señalar que dicha información deberá encontrarse a disposición de los usuarios y de las autoridades de control, en forma electrónica, permanente, fácil, directa y gratuita.

Esta obligación del prestador hay que relacionarla con el deber general existente en las relaciones comerciales con consumidores, de redactar las cláusulas de forma comprensible y transparente, evitando oscuridades, criterio que se encuentra recogido en nuestro Código Civil y en la Ley General de Defensa de Consumidores y Usuarios.

Resulta interesante señalar el criterio establecido en el apartado segundo del artículo 10, que facilita la seguridad jurídica en el cumplimiento de la Ley, indicando que el lugar en cierto modo idóneo para la publicación de la información es la página de Internet del prestador.

En la práctica, la forma de cumplir esta obligación es incluir la información en una página, accesible desde la página principal de la sede web del prestador, que se suele denominar “Aviso legal”. En esta página aparecerá la información exigida por el artículo 10 de la Ley 34/2002, de 11 de julio, y también otras menciones o avisos legales importantes, especialmente referidos a la propiedad intelectual e industrial de los elementos de la página, precauciones que debe tener en cuenta el usuario del servicio y, frecuentemente, la política de protección de datos personales que sigue el prestador de los servicios.

3. Información en servicios que hacen uso de "cookies"

Las "cookies" son pequeños ficheros de texto incluidos dentro de los programas de navegación por Internet por las sedes o páginas web, con informaciones personales de los usuarios que se conectan a las mismas. Se emplean para que la página web "recuerde" datos del usuario, como su preferencia de idioma o de personalización de la página, pero también se pueden emplear para almacenar informaciones sin el conocimiento del usuario, que podrían permitir rastrear sus actuaciones por Internet o crear perfiles de usuario.

Estos usos de las "cookies" pueden ser especialmente graves en relación con las páginas web que anuncia o prestan servicios de salud, en especial en relación con la creación de perfiles para la publicidad a través de Internet.

Las "cookies" también han planteado problemas de robo de la información contenida en las mismas, por lo que en general no se recomienda su empleo. Cuando se empleen para la inclusión de datos personales de salud, e incluso para datos administrativos y de aseguramiento, se recomienda incluirlos cifrados.

La Ley 34/2002 las denomina "dispositivos de almacenamiento y recuperación de datos" y establece, en su artículo 22.2, las obligaciones en relación con su empleo:

"*Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.*

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario."

Con estas obligaciones se trata de contrarrestar los posibles efectos negativos del empleo de este tipo de dispositivos, tanto desde la perspectiva de la seguridad como desde la perspectiva de la protección de los datos de carácter personal.

6.2 SPAM de medicamentos y otros productos de salud

La Ley 34/2002, de 11 de julio, regula en su artículo 20 la información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos, normativa que se añade a la ya existente en materia de publicidad en materia de salud, como la contenida en el artículo 27 de la Ley General de Sanidad, que establece el control de la publicidad y la propaganda comerciales en materia de salud, de forma que se ajusten a criterios de veracidad en lo que atañe a la salud, o en el artículo 102 de la Ley General de Sanidad, que determina la posibilidad de autorización previa para la realización de publicidad de medicamentos y otros productos sanitarios dirigidas a profesionales, así como de clasificación y autorización previa de publicidad de dichos productos cuando la publicidad se dirige al público.

Nótese que una parte muy importante de las comunicaciones comerciales no solicitadas que se reciben en Europa en la actualidad se refieren a medicamentos o dietéticos, como son los casos Cialis, Viagra o Anatrim. Asimismo proliferan en Internet las actividades de farmacia y de parafarmacia, con su correspondiente publicidad, generalmente emitida desde otras jurisdicciones y sin respetar la normativa vigente.

Por supuesto, no todas las actividades publicitarias en materia de salud son ilícitas, resultando perfectamente posible realizar determinadas comunicaciones comerciales por Internet, en su caso con la autorización previa que resulte preceptiva, en cuyo caso deberán cumplir con los requisitos legales que establece la Ley 34/2002.

Como medidas para el control de esta actividad, la Ley 34/2002 establece que las comunicaciones comerciales deben identificarse como tales, e indicar la persona física o jurídica en nombre de la cual se realizan. Asimismo, y en el caso en que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente (como por ejemplo SMS o MMS), deben incluir al comienzo del mensaje la palabra «publicidad».

Por otro lado, en los supuestos de ofertas promocionales como las que incluyan descuentos, premios, regalos y de concursos o juegos promocionales, previa la correspondiente autorización, se debe asegurar, además del cumplimiento de los requisitos antes comentados, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso de participación, se expresen de forma clara e inequívoca.

El legislador somete a especial cautela el envío de comunicaciones comerciales a usuarios que no las han solicitado específicamente, dado que el artículo 21 de la Ley 34/2002 prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En este sentido, la prestación de consentimiento expreso exige la manifestación de una voluntad libre, informada, específica e inequívoca de aceptación del envío de comunicaciones comerciales realizadas por correo electrónico u otro medio de comunicación individual equivalente.

Por ello, se entendería cumplido este requisito, por ejemplo, si el prestador de servicios de sociedad de la información, después de informar al usuario sobre el uso al que destinará su dirección o número de teléfono, le ofrece la oportunidad de manifestar su conformidad con el envío de comunicaciones comerciales haciendo “clic” en una casilla dispuesta al efecto.

Por otro lado, puede entenderse que el requisito no se cumpliría cuando, sin haber autorizado de forma expresa la recepción de comunicaciones comerciales, el destinatario tolera o no se opone a su envío, cuando no responde a los mensajes por los que se solicita su consentimiento y, por supuesto, cuando se hubiera opuesto a su recepción.

El rigor de la norma contenido en el artículo 21 expuesto ha sido suavizado mediante la inclusión de una excepción, en virtud de la disposición final 1.1 de la Ley 32/2003, de 3 de noviembre, de telecomunicaciones, que determina un nuevo apartado 2 del artículo 21 de la Ley 34/2002, indicando que “*lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o*

servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija".

Se trata del caso en que el que un prestador de servicios de la sociedad de la información dispone ya de datos de contacto de correo electrónico de sus clientes, porque ciertamente en este caso obligar a recabar un nuevo permiso del cliente para remitir información adicional sobre productos y/o servicios similares no parecía justificado ni para comerciante ni para cliente.

La referencia a la captación lícita de los datos de contacto resulta algo confusa, dado que la norma parte de la existencia de una relación contractual previa, en la que por supuesto se han obtenido los datos. Probablemente haya que poner este término en relación con la normativa de protección de los datos de carácter personal; es decir, que se debe haber informado al cliente de que sus datos serían tratados para el mantenimiento de la relación comercial.

Más importante resulta el hecho de que la excepción es aplicable para el caso de publicidad sobre productos o servicios similares a los inicialmente adquiridos, y no para los que sean sustancialmente diferentes, lo que limita mucho las posibilidades de uso de esta posibilidad de remitir comunicaciones comerciales no solicitadas.

Se completa el régimen expuesto relativo al SPAM con el establecimiento de los derechos de los destinatarios de servicios expuestos en el artículo 22.1 de la Ley 34/2002, en su redacción dada por la disposición final primera de la Ley 32/2003:

"*El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.*

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos."

7. La custodia y el archivo seguro de documentos electrónicos

A medida que se va implantando el documento electrónico original, cobra mayor importancia la estrategia de custodia y archivo seguro de dichos documentos, especialmente a la luz de la normativa de conservación ya existente referida a los documentos en soporte papel, que a veces establecen periodos de conservación relativamente largos, cuando no indefinidos.

En consecuencia, y desde una óptica general, la norma ISO 17799:2005 considera como control que los registros importantes sean protegidos de pérdidas, destrucción, y falsificación conforme a los requisitos legales, reguladores, convenidos y de negocio.

Los sistemas de almacenamiento de datos deben ser escogidos de tal forma que los datos requeridos puedan ser recuperados en un período y formato aceptable, según las necesidades identificadas.

Los registros deben ser clasificados en diferentes tipos, por ej. registros contables, registros de base de datos, “logs” de transacciones, “logs” de auditoria y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ej. papel, microfichas, medios magnéticos u ópticos.

Cualquier material criptográfico relacionado y programas asociados con archivos cifrados o firmas digitales, también deben ser almacenados para permitir el desciframiento de los registros durante el tiempo que los registros son conservados, considerando la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros.

Los sistemas de almacenamiento de datos deben seleccionarse de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un Tribunal de justicia, por ejemplo, que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable, y de forma que se puedan cumplir las normas aplicable de archivo histórico, en su caso.

Para cumplir estos objetivos, la norma recomienda el establecimiento de los siguientes controles:

e) Se debe emitir normativa interna para la retención, almacenamiento, manipulación y eliminación de registros e información;

f) Se debe preparar un calendario de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

g) Se debe mantener un inventario de fuentes de información clave.

h) Se debe implementar adecuados controles para proteger los registros y la información esenciales contra pérdida, destrucción y falsificación.

Uno de los elementos cuya custodia resulta más sensible es la historia clínica electrónica. El artículo 3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica define la historia clínica como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Por su parte, amplía el artículo 14 de la citada Ley 41/2002 esta definición, determinando que la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

De acuerdo con el artículo 15 de la Ley 41/2002, la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Asimismo, se determina que todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado – por tanto, incluyendo el electrónico – de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud.

La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella, que por tanto deben ser identificados y autenticados previamente, de forma segura. Idealmente, con firma electrónica reconocida, al objeto de salvaguardar su responsabilidad en caso de anotaciones por personas no autorizadas.

En relación con la historia clínica, se deben distinguir dos casos:

- El acceso y el tratamiento de la historia clínica de cada centro, donde el centro determina, de acuerdo con el correspondiente análisis de riegos, las medidas de identificación y firma electrónica a exigir.
- El acceso por profesionales en diferentes centros a una historia clínica centralizada o, más probablemente, a un fichero índice que permita posteriormente el acceso a los documentos de

las diferentes historias clínicas. En este segundo caso, entendemos que la normativa de la Administración sanitaria debe establecer los criterios y condiciones de identificación y firma electrónica a exigir a los centros que acceden o intercambian información.

En este segundo caso, resulta especialmente importante el disponer de sistemas de federación de identidad, que permitan delegar a los centros las tareas de identificación dentro de un esquema de confianza, para controlar de forma distribuida las autorizaciones de acceso.

A continuación, determina el artículo 14.2 de la propia Ley que cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información; es decir, con aplicación de las medidas que hemos venido exponiendo y, en concreto, mediante el uso de la firma electrónica reconocida, mientras que, de acuerdo con el artículo 16.2 de la propia Ley, cada centro debe establecer los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

Ello sin perjuicio de la facultad que otorga el artículo 14.3 de la Ley a las Administraciones sanitarias, para establecer los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura, y el apartado 4 del mismo artículo para que las Comunidades Autónomas aprueben las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental, o de la facultad que les otorga el artículo 16.7 de la misma Ley, para regular el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

En este sentido deben entenderse los instrumentos aprobados hasta la fecha, entre lo que podemos citar la Orden de 22 de noviembre de 2004, del Consejero de Sanidad del Gobierno Vasco, por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Sistema Sanitario de Euskadi o la Orden de 14 de julio de 2004, de la Conselleria de Sanitat de la Generalitat Valenciana, por la que se regula la utilización de la firma electrónica reconocida en los documentos sanitarios de la Conselleria de Sanitat.

Resulta necesario establecer normas internas respecto a la tutela o custodia de la información. En este sentido, hay que traer a colación el contenido de los párrafos 4 y 5 del artículo 17 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que determinan lo siguiente:

- La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.
- Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

Asimismo, hay que indicar que el artículo 19 de la Ley 41/2002 establece que el paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la Ley.

Respecto a la cancelación de la documentación electrónica sanitaria, el criterio general es que la documentación e información, en cualquier soporte (papel, fax, correo electrónico o disquete, etc.), así como la documentación temporal, debe ser destruida tan pronto surta sus efectos o su función, sin proceder a su conservación o archivo, salvo cuando ello sea legalmente exigible.

Precisamente en este sentido cabe recordar que el artículo 17.1 de la Ley 41/2002 determina que los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial; y que, por su parte, el párrafo 2 del mismo artículo 17 establece que la documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud de forma que en su tratamiento se evite, en lo posible, la identificación de las personas afectadas.

8. La prevención del uso inadecuado de los sistemas de información sanitaria

Finalmente, resulta de especial importancia establecer las bases jurídicas para la regulación del uso de los sistemas de información por parte de los usuarios, especialmente en el caso del uso no autorizado o del abuso de los sistemas.

A esta problemática dedica un control específico la norma ISO 17799:2005, que parte del dato que la dirección debe aprobar el empleo de instalaciones y sistemas de procesamiento de información, de forma que cualquier empleo de estas instalaciones para cualquier propósito no autorizado por la dirección, debería ser considerado como un empleo inadecuado de dichos sistemas y, en su caso, sancionada.

La necesidad de control de las actividades de los usuarios de los sistemas de información resulta esencial para reducir los riesgos del negocio, pero también, de forma particularmente intensa en los datos de salud, para el cumplimiento de los derechos de los afectados, en especial en relación con la protección de su intimidad y evitar la divulgación no autorizada de datos de carácter personal.

Esta norma implica la necesidad de establecer medidas de supervisión del empleo de los sistemas de información, actividad siempre conflictiva, dado que el derecho legal de control del trabajo por las organizaciones nunca puede conculcar derechos fundamentales Un caso límite de este conflicto es la monitorización del correo electrónico, que puede ser tipificada como un delito caso que se realice sin las debidas garantías legales.

En cualquier caso, y con independencia del necesario y delicado análisis jurídico previo al establecimiento de medidas técnicas para el control de las actividades de las personas que trabajan o colaboran con una organización, si se identifica cualquier actividad no autorizada, esta actividad debe ser atendida por la dirección, y se deben aplicar las medidas disciplinarias apropiadas y, en su caso, las acciones legales oportunas.

Como contrapartida del derecho de supervisión de la organización, todos los usuarios deben ser conscientes de su acceso permitido y de las medidas de supervisión implantadas con el objetivo de detectar el empleo no autorizado de sistemas de información.

Manifestación legal de estas necesidades es el artículo 9.2 del RD 994/1999, Reglamento de medidas de seguridad de la LOPD, que determina que "*el responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento*", en conexión evidente con la definición clara de las funciones y obligaciones del personal y de la necesidad de concesión de autorización de acceso.

Asimismo, cabe recordar la obligación establecida por el artículo 12.2 del RD 994/1999, de relativa a que "*el responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados*", que incluyen mecanismos de prevención

y detección, incluyendo la supervisión y monitorización, con los límites derivados de la dignidad e intimidad de los trabajadores a que nos hemos referido.

Típicamente, esta concienciación se instrumenta concediendo a los usuarios la autorización de uso y acceso por escrito, mediante una copia que debería ser firmada por el usuario y conservada por la organización.

En definitiva, todos los empleados de una organización, contratistas y usuarios terceros deben ser informados de sus accesos autorizados, así como de las medidas de supervisión a implantar de acuerdo con la política de seguridad, con pleno respeto al principio de proporcionalidad y a los derechos fundamentales de los mismos.

5 Gestión de Seguridad de la Información en la Organización

Rafael Ortega García

Departamento de Technology and Security Risk Services
Ernst & Young

1. Introducción

Cuando se habla de seguridad de la información en el ámbito sanitario, inmediatamente se piensa en la Ley de Protección de Datos y en la Ley de Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y documentación clínica. Si bien las obligaciones que conlleva el cumplimiento de estas leyes, es el punto de preocupación de cualquier organización que trata este tipo de datos, el entorno de seguridad por el que una entidad sanitaria debe preocuparse es mayor.

Estamos hablando de términos como *disponibilidad* y *continuidad* de la actividad, puestos en boga últimamente, por ejemplo por los problemas de suministro eléctrico en Barcelona este pasado verano. ¿Se imaginan un ataque lógico combinado a las infraestructuras críticas de la red sanitaria con el objetivo de interrumpir los servicios que prestan los dispositivos críticos? No olvidemos que todos estos dispositivos ya están conectados en red y al exterior aunque sea solo para realizar tareas de telemantenimiento.

Asimismo, además de preservar la *confidencialidad* en las aplicaciones que dan soporte a los datos confidenciales de los pacientes, estamos hablando de robustecer la infraestructura tecnológica que da soporte a estas aplicaciones, ya que en todos los años que tiene Internet el objetivo del ataque no ha cambiado pero sí las técnicas, que han evolucionado llegando a un nivel de sofisticación extrema.

Ya no se trata de esos “románticos” cerebros que, al final del día, aportaban su conocimiento a la comunidad. Existen grupos organizados que realizan sus delitos utilizando diversas tecnologías con distintos fines como la sustracción monetaria, el espionaje empresarial/industrial, subastas de vulnerabilidades de los sistemas en la red, chantaje a organizaciones, etc. ¿Se imaginan un mensaje en el que se amenace la paralización de toda la infraestructura de un hospital?.

En la actualidad, estas organizaciones delictivas trabajan con el objetivo fundamental del robo de las identidades de los usuarios de sistemas intentado, bien con métodos de engaño y abuso de confianza (ingeniería social) o bien con métodos técnicos que aprovechan las vulnerabilidades de los sistemas, conocer o sustraer los datos de autenticación y firma y/o los datos clave de tarjetas de crédito, con los que es posible el quebranto económico a los ciudadanos. Prácticamente la totalidad de problemas de fraude electrónico en la banca electrónica se basa en la sustracción de identidades.

El reto que tiene la Seguridad de la Información en las organizaciones es la implantación de un entorno de control que impacte de forma mínima en los procesos de negocio y que los procesos de

control se conviertan en tareas habituales del trabajo. Es decir, el objetivo es proporcionar confianza sin reducir la eficiencia. En el entorno sanitario, se trata de una problemática más compleja y vital que los términos económicos utilizados normalmente: **las personas**. Se trata de eficiencia y de confianza, con una variable única en este sector como es la salud y la vida de la persona.

En este capítulo trataremos de métodos y modelos de organización de seguridad, es decir, cómo podemos integrar las personas, las actividades que realizan y las herramientas que utilizan para crear un entorno de control de seguridad eficaz y eficiente.

- Figura 1 -

2. Modelos de Gestión de la Seguridad de la Información

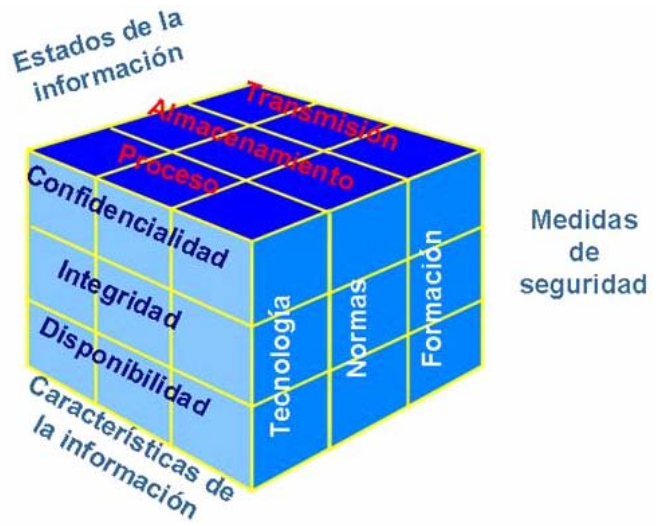
Todo sería más fácil si pudiésemos aplicar esta frase de dos de los más importantes conocedores de seguridad en Internet:

> *"Es muy sencillo tener un sistema seguro.*
>
> *Simplemente tiene que desconectar todas las conexiones remotas y permitir únicamente los terminales directamente conectados, colocar la máquina y sus terminales en una sala protegida, y un guardia en la puerta."*
>
> *F.T. Grampp & R.H. Morris*

El primer punto clave en una estrategia de seguridad es la implantación de un Plan de Seguridad. Sin embargo, antes de presentar algún modelo y cómo desarrollarlo, es preciso recordar algunos de los principios que hay que tener presentes cuando se quiere abordar un modelo y arquitectura de seguridad:

- La seguridad no es un valor absoluto.
- No se puede hablar de un sistema informático que sea seguro sino más bien que no se conocen tipos de ataque que puedan vulnerarlo.
- El último eslabón de la seguridad descansa en la confianza en alguna persona.
- El personal usuario de los sistemas de información constituye el eslabón más débil en la cadena de la seguridad, puesto que sus actuaciones no alineadas con las buenas prácticas en seguridad, pueden acarrear importantes impactos en la misma.

El primer modelo que se presenta es un modelo fácil y comprensivo de seguridad, independiente del entorno, arquitectura o tecnología que gestione nuestra información. Este modelo fue expuesto por John R. McCumber en el "Datapro on Information Security IS09-800-201 Concepts&Issues", de Junio de 1.992.



- Figura 2 -

Este modelo de tres dimensiones se convierte en un cubo con 27 celdillas como marco de actuación.

A partir de este modelo, se puede definir la Seguridad de la Información como todas aquellas medidas tecnológicas, de normas y procedimientos y de formación que aseguren la confidencialidad, integridad y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión.

No significa que en todos los casos haya que actuar en cada una de ellas, pero conviene analizarlas todas previamente a la elaboración de cualquier Plan de Seguridad de la Información si se quiere conseguir un resultado realmente eficaz y no dejar lagunas.

Como ocurre en todos los Planes de Seguridad, de poco vale la acumulación de medidas encaminadas a la protección de un determinado aspecto, si otros quedan totalmente olvidados. En más de una ocasión se observan medidas aplicadas sin esa visión global, y el resultado final presenta debilidades incomprensibles.

Este modelo servía para construir un modelo de seguridad para implantar en la empresa y también como una herramienta de evaluación de la situación actual en seguridad en una organización.

Cada vulnerabilidad descubierta llevará implícita un medida de seguridad a implantar correspondiente a su celdilla del cubo.

En el año 1994 algunos autores iban más allá de las tres características de la información, ya que la problemática se complicaba; la transmisión de datos era vital para las empresas, el uso masivo de motores de base de datos relacionales, la aparición del concepto de propietario de la información y de legislaciones de seguridad y protección de datos en diversos países, hacía necesario que aumentasen las características de la información.

Así, Don M.Parker, en la conferencia que impartió en la 14th National Computer Security Conference con el titulo de “Restating the Foundation of Information Security” desdoblaba las características de la información en parejas:

- Confidencialidad-Posesión
- Integridad-Autenticidad
- Disponibilidad-Utilidad

Las nuevas características se definen de la siguiente manera:

- Posesión: tenencia o propiedad y control.
- Autenticidad: conforme a los hechos y a la realidad, válido, verdadero o cierto, real y genuino para un propósito.
- Utilidad: útil para un propósito.

Entonces, como ejemplo de este desdoblamiento se citaba el caso del robo y destrucción de un fichero cifrado. En él no se ha perdido la confidencialidad, ya que el ladrón no va a poder ver su contenido, pero en caso de no tener copia de la información almacenada,, el propietario, va a perder su posesión.

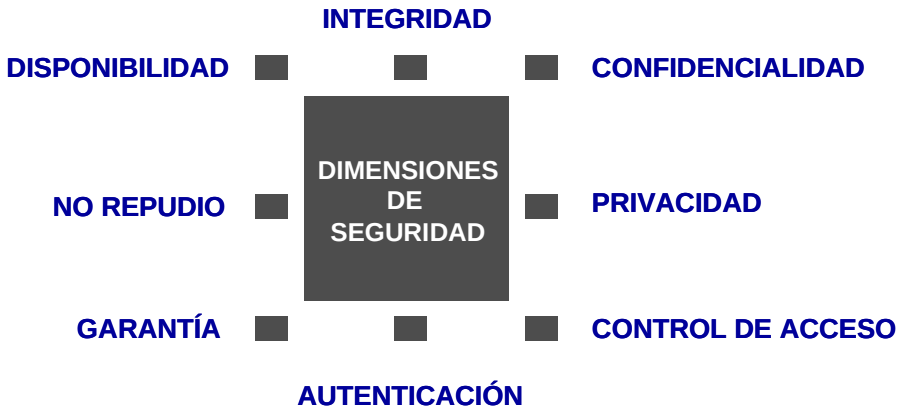
Dependiendo del tipo de información que se maneje, se ampliaban las características de la información y en vez de tener un sistema con 27 celdillas o áreas de actuación, se tenía un sistema con 54 áreas de actuación

Al final del siglo/milenio, la Seguridad se definió como un proceso, ya que no era una foto fija sino que evolucionaba en el tiempo. Esto daba un salto cualitativo en el concepto de Seguridad de la Información, ya que como tal, empezaba a alinearse con calidad y con los enfoques ISO de mejora continua (ISO 17799-2005 e ISO 27001).

En la actualidad y con la aparición de nuevos estándares de facto para la gestión de sistemas como ITIL (Librería para la Gestión de Infraestructuras) y los conceptos que en él se definen, desde mi punto de vista, la seguridad no es un proceso, sino un SERVICIO que requiere implantar un conjunto de procesos que soportados por la tecnología adecuada, consigue llegar al nivel de seguridad objetivo (objetivo de control) y que la Dirección debe aprobar, definiendo el nivel de riesgo que la organización está dispuesta a asumir.

Por tanto, el modelo habitual de seguridad basado en las tres dimensiones de confidencialidad, integridad y disponibilidad resulta insuficiente para definir los objetivos del servicio en grandes organizaciones y con la visión puesta en el futuro.

Es necesario redefinir el servicio de Seguridad TIC como un vector más complejo, de “n” dimensiones (n > 3), que aunque difícilmente representable en el espacio físico, es más real, habida cuenta las necesidades a cubrir.



- Figura 3 -

En este modelo y respecto a la información, se definen los siguientes conceptos:

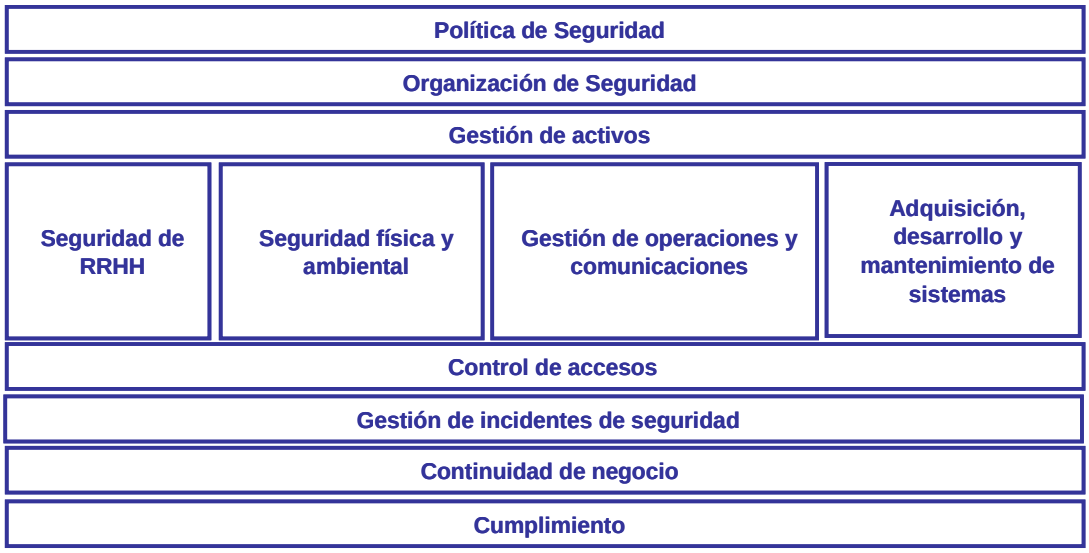
- Integridad: no variación indeseada de los datos

- Confidencialidad: los datos solo los conoce quien está autorizado
- Privacidad: la tenencia de datos está justificada
- Control de Accesos: por necesidades y responsabilidades
- Autenticación: quien accede es quien dice ser
- Garantía: el sistema hace lo que se espera
- No repudio: el autor de un hecho no puede negar la autoría del mismo
- Disponibilidad: la información está accesible cuando se necesita

El ISO/IEC, viene realizando un trabajo de emisión de buenas prácticas y estándares de seguridad, a través del JC1 Subcomité 27. Desde mi punto de vista, el más importante y base para cualquier estructuración exhaustiva de la seguridad en una organización, proceso, sistema de información o infraestructura tecnológica es el ISO/IEC 17799:2005, código de buenas prácticas de seguridad.

El nuevo estándar es una guía clara, estructurada y detallada para construir un entorno de control de seguridad, pudiéndose acometer su aplicación desde un punto de vista global en la compañía, en un proceso o un departamento, en un sistema de información o en la infraestructura tecnológica.

Las "Clauses" o dominios de control se describen por un objetivo general, los 11 dominios definidos se representan en la siguiente figura.



- Figura 4: Dominios de control del ISO/IEC 17799:2005 -

Cada Dominio, se divide en un subconjunto de controles, en total 133 controles, y para una mejor comprensión se han desarrollado tres apartados descriptivos:

- Control: descripción del control especifico, que con su correcta implantación se consigue cumplir con el objetivo de control del dominio.

- Guía de implantación: desarrollo en detalle de cómo implantar el control para poder cumplir con el objetivo del dominio
- Otra Información: información adicional de ayuda, como por ejemplo, referencia a otros estándares.

3. Modelos de defensa

La evolución de las tecnologías y el uso que se está haciendo de las mismas conlleva que las amenazas cambien y ha hecho que las estrategias de defensa evolucionen.

En un principio, en sistemas centralizados la idea era proteger el interior, protegiendo todo como si de un castillo se tratase, la securización era a modo de silo de los elementos informáticos. Este tipo se denominaba la "defensa por aislamiento".

Con la evolución de los sistemas a entornos distribuidos, hacia estándares abiertos y con la interconexión de redes, la estrategia para proteger la información y los sistemas tiene que cambiar. Nadie se imagina vivir en una gran ciudad y en el momento que ves el cartel de "Bienvenido" estuviese todo abierto. La defensa cambia a una estrategia de "Seguridad por Autorizaciones" en la que se produce una descentralización de los recursos en base a privilegios otorgados a entidades autorizadas correctamente.

Pero en entornos como el Sanitario, las exigencias son mayores y no hay que hablar de entidades, sino que hay que bajar a nivel de contenidos, autorizar a personas el acceso o modificación de contenidos en función de las necesidades de conocimiento del puesto de trabajo concreto. Se trata de una "Seguridad por contenidos".

En este sentido ha aparecido el concepto de Digital Right Management (DRM) o Gestión de Derechos Digitales. Según Wikipedia DRM se define *como el conjunto de tecnologías orientadas a ejercer restricciones sobre los usuarios de un sistema, o a forzar los derechos digitales permitidos por comisión de los poseedores de derechos de autor e independientemente de la voluntad de uso del usuario del sistema*.

Si bien este concepto nació para su aplicación en entornos de protección de derechos de autor para contenidos multimedia en la red (libros electrónicos, música, video, etc.), se ha ampliado para cualquier contenido en formato electrónico, permitiendo ampliar el concepto de autorización, no solo por la clasificación tradicional de la información (confidencial, restringida, etc.) sino también a otros atributos ligados a la utilidad y el conocimiento.

Algunas compañías utilizan un modelo diferente de clasificación de la información basado en distintos niveles respecto a cuestiones como la Sensibilidad, Criticidad, Carácter Regulatorio y Factor de Exposición de la información. Debido a que las únicas personas que conocen con total certeza los requisitos de Sensibilidad de la información son las que pertenecen a las áreas funcionales que manejan dicha información para el desempeño de sus funciones, es más operativo establecer dichos valores no para la información, sino para el *Servicio Tecnológico*, es decir, para el sistema o aplicación que presta servicio a procesos de negocio o asistenciales.

Con esta disquisición, dichas variables serán únicas con independencia de los procesos que soporte, puesto que dependerá únicamente de la información y la configuración de los componentes de la Infraestructura Tecnológica que lo integran.

A continuación, se presentan los niveles identificados para los aspectos de sensibilidad, Carácter regulatorio y Factor de exposición del activo:

- *Sensibilidad*: indica los requerimientos de confidencialidad e integridad imprescindibles de la información gestionada por el Servicio Tecnológico.

Nivel	Descripción
Muy alto	Se considera que el nivel de sensibilidad de la información gestionada por un Servicio Tecnológico es muy alto, si atendiendo a su confidencialidad la información está catalogada como secreta o confidencial, o atendiendo a su integridad compromete la información de los pacientes
Alto	Se considera que el nivel de sensibilidad de la información, gestionada por un Servicio Tecnológico es alto, si por su confidencialidad es clasificada como restringida para facultativos que necesitan el acceso a la misma o por su integridad puede comprometer un diagnóstico de un paciente.
Medio	Se considera que el nivel de sensibilidad de la información gestionada por un Servicio Tecnológico es media, si por su confidencialidad es catalogada como uso restringido al entorno hospitalario interno o por su integridad puede comprometer a información de control económico o de gestión.
Bajo	Se considera que el nivel de sensibilidad de la información gestionada por un Servicio Tecnológico es baja, si por su confidencialidad es considerada de carácter público o por su integridad afecta a información no incluida en los niveles previos, y cuya modificación no implica responsabilidades del hospital frente a terceros, ya que no debe responder por los errores derivados de su modificación.

- *Carácter regulatorio*: indica los requerimientos legales impuestos por la legislación vigente a la información, y en consecuencia a los sistemas que gestiona cada Servicio Tecnológico.

Nivel	Descripción
Muy alto	El Servicio Tecnológico está sujeto a normas de seguridad técnicas impuestas por la legislación vigente.
Alto	El Servicio Tecnológico está sujeto a la legislación vigente, que no especifica la implantación de medidas de seguridad en los sistemas de información.
Medio	Se desconoce si el Servicio Tecnológico está sujeto a restricciones derivadas de la legislación vigente del país.
Bajo	El Servicio Tecnológico no está sujeto a ninguna restricción derivada de la legislación vigente.

- *Factor de exposición*: cada servicio de acceso (entendido como puerto de comunicaciones) habilitado en un Servicio Tecnológico lleva asociado un 'Factor de Exposición' definido con base a su accesibilidad, considerando esta accesibilidad desde las diferentes redes.

Nivel	Descripción
Muy alto	Se considera que el nivel de exposición es muy alto para un Servicio Tecnológico si existen servicios (entendidos como puertos de comunicaciones) habilitados para la conexión directa desde redes no confiables, y para aquellos que pertenecen a la organización y están ubicados fuera de las redes confiables.
Alto	Se considera que el nivel de exposición es alto para un Servicio Tecnológico que no es accesible directamente desde redes no confiables pero es accedido desde Servicios Tecnológicos con Factor de Exposición muy alto.
Medio	Se considera que el nivel de exposición es medio para un Servicio Tecnológico que no es accesible directamente desde redes no confiables pero es accesible desde Servicios Tecnológicos cuyo Factor de Exposición es alto.
Bajo	Se considera que el nivel de exposición es medio para un Servicio Tecnológico del que se desconoce si es accesible desde Servicios Tecnológicos cuyo Factor de Exposición es muy alto, medio o alto.

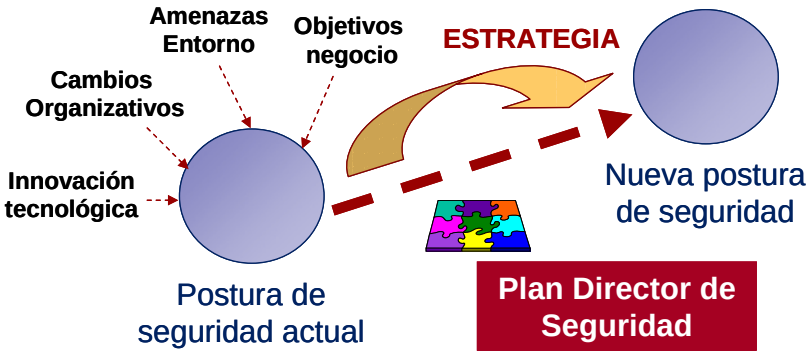
Con esta clasificación, se pueden trasladar estos niveles, por un sistema de herencia de atributos, a los activos que soportan los servicios tecnológicos, y a partir de ahí definir las medidas de seguridad (controles ISO) que se deben implantar en los mismos.

La *criticidad* como atributo de seguridad para la clasificación de la información está ligada a la disponibilidad y continuidad de negocio. En el sector sanitario cobra vital relevancia por los impactos que puede ocasionar desde distintos puntos de vista (vidas humanas, imagen, legal, etc.) por lo que debe tratarse de forma independiente al definir un Plan de Continuidad.

A partir de este momento, cada organización debe diseñar un Plan Director de Seguridad. No existe una metodología concreta para desarrollar este tipo de planes y se pueden abordar a partir de la

realización de un análisis de riesgos y organizar las medidas en proyectos o bien haciendo un simple diagnóstico.

Si definimos el concepto de *"Postura de Seguridad"* como el conjunto de iniciativas, procesos y actividades de seguridad que se llevan a cabo en la Organización con el fin de alcanzar los objetivos de seguridad planificados y que tienen como referencia la misión, visión y valores vigentes; un Plan Director se definiría como la "evolución planificada de la postura de seguridad".



- Figura 5 -

En mi opinión, un *Plan Director de Seguridad* no es sólo un análisis de riesgos, un diagnóstico de seguridad, una auditoria de técnica de seguridad, un conjunto de medidas y salvaguardas a aplicar y un proceso de certificación de la seguridad. Desde un punto de vista conceptual, debería ser:

- La línea maestra que la organización debe implantar para alinear la seguridad a su actividad empresarial, su cultura organizativa y a los sistemas y tecnología que utiliza.
- La definición de los objetivos de seguridad que son necesarios para asegurar este alineamiento.
- La definición del entorno de control/medidas/salvaguardas necesario para conseguir los objetivos marcados.
- La definición de la organización de seguridad (responsabilidades y procesos) para gestionar, administrar y revisar el entorno de control definido.
- La definición de la arquitectura de seguridad necesaria para obtener el nivel de control objetivo.
- La cuantificación de los gastos e inversiones necesarios para llegar a la meta deseada.
- La estimación de recursos necesarios, distribución de esfuerzos y la planificación de acciones a realizar en el marco temporal fijado.

La experiencia nos dice, y muchas veces se olvida, que el verdadero énfasis debe concentrarse en la elaboración del Plan de Acción y en la estimación de esfuerzos y presupuestos. Se tiende a llevar a cabo un diagnóstico demasiado detallado, sin que esto aporte una concreción significativa en el resultado final del Plan, más bien, puede trastocar su resultado, haciendo muy compleja su implantación posterior.

Por último, hay que tener en cuenta las siguientes consideraciones:

- El diagnóstico se debe abordar de forma positiva, y no con "espíritu auditor". Es imprescindible contar con la colaboración y las aportaciones del personal implicado.
- Si es necesario evaluar el estado de la seguridad de la organización o identificar vulnerabilidades importantes, esta actividad se puede acometer antes de abordar el proyecto.
- Aprovechar las entrevistas y tomas de datos iniciales para explotar sinergias con otras iniciativas planificadas o en curso (p.ej: análisis de Impacto de procesos o aplicaciones críticas)
- El gran problema de un Plan Director no está en la definición, sino en una efectiva y eficiente implantación del mismo y es recomendable:.
    - Evaluar los esfuerzos de implantación y la posibilidad de constituir una Oficina de Proyectos para dicho fin.
    - Únicamente desarrollar la normativa de primer nivel en los ámbitos de actuación de seguridad. Cada uno de los proyectos tendrá que incluir la implantación técnica de la solución y la normativa específica y procedimientos asociados.
    - Establecer indicadores para seguimiento y grado de implantación del Plan.
- Los procesos de aprobación, comunicación y "venta interna" del Plan son críticos para el éxito del Plan y su posterior implantación

4. Resumen y conclusiones

Como resumen, podemos afirmar que para poder implantar un entorno confiable que proteja la información de nuestra organización, es necesario diseñar y/o seleccionar un modelo de seguridad y conocer las necesidades de seguridad de la información que se gestiona para, a partir de ahí realizar un Plan Director que nos permita llegar a un nivel de seguridad objetivo.

En la actualidad el ISO 17799 es el estándar más utilizado, permitiendo certificar su implantación, a través de la ISO 27001. El punto clave de la implantación de un estándar de este tipo es la particularización de los controles al entorno particular de la empresa. Hay que tener en cuenta que el entorno burocrático a desarrollar es importante y que es necesario establecer una función de seguridad, que organice y coordine todas las actividades de seguridad de la información que se realicen en la organización.

Dadas las características del sector sanitario, se recomienda considerar y tratar de manera específica aspectos clave de seguridad, entre otros:

- Concepto de seguridad como servicio.
- Organización de la seguridad en base a procesos.
- Concienciación sobre seguridad de la información.
- Control de accesos y derechos digitales.
- Continuidad del servicio.
- Gestión de incidentes de seguridad.

Por último, indicar que la seguridad no es una tarea que se realice en un momento determinado, sino que como otras actividades de la organización, tiene que tener su sistematización y seguimiento. No hay peor amenaza que tener una falsa sensación de seguridad.

6 Tecnologías aplicadas a la Seguridad de la Información

Ricardo Sáez Crespo
M. Ramón Gutiérrez Covarrubias

Servicio de Informática. Hospital Universitario Marqués de Valdecilla

1. Introducción

La seguridad es un aspecto inherente al ser humano. Desde el principio de los tiempos ha necesitado amparar su intimidad, y para conseguirlo, se ha apoyado en la tecnología existente, que le ha facilitado herramientas para superar ese objetivo.

Algunos fenómenos recientes relacionados con la evolución de las Tecnologías de la Información y de las Comunicaciones (TICs) como son la microinformática, los virus, los sistemas abiertos, las redes de comunicación o Internet, han contribuido a que hoy entendamos la enorme importancia que tiene preservar la seguridad de la información. Hoy en día está presente desde las fases iniciales de análisis, en cualquier proyecto de software de aplicación. Sin embargo, el interés por preservar la seguridad se intensifica cuando el proyecto, software o entorno de trabajo, utiliza datos sensibles. Prácticamente cualquier proyecto de sistemas de información desarrollado en entornos sanitarios cumple este perfil.

Los problemas asociados con la seguridad informática no pueden ser tratados individualmente porque la fragilidad del sistema está condicionada por la del punto más débil. El uso de sofisticados algoritmos y métodos criptográficos, resultan inútiles si, por ejemplo, no se considera la confidencialidad de las estaciones de trabajo.

Por otra parte, el factor educacional de los usuarios resulta fundamental para que las tecnologías que se implanten resulten efectivas, como lo demuestra el hecho de que gran parte de las técnicas de intrusión contra la seguridad van orientadas a conseguir -mediante engaño- (*Fishing*) que los usuarios autorizados revelen sus identidades y contraseñas. Esto evidencia que por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de los equipos directivos y una sensibilidad por parte de los usuarios, no se conseguirá implantar un sistema eficaz.

En este capítulo se analiza la contribución de las TICs en garantizar la “integridad”, la “confidencialidad”, la ”disponibilidad” y el “no repudio de la información”, términos que en su conjunto definen a un sistema seguro, y se profundiza en los distintos niveles que delimitan su marco de referencia tecnológico.

2. Elementos y mecanismos de seguridad

No resulta fácil definir un patrón que permita abordar de forma homogénea los distintos conceptos, estrategias, mecanismos y elementos tecnológicos relacionados con la seguridad, cuando las expectativas del análisis son distintas (auditoria informática, gestión de red, tests de intrusión, etc).

La bibliografía relacionada estudia la seguridad desde dos niveles distintos:

i) *Seguridad Física*: se interesa por las condiciones de los edificios e instalaciones que albergan los soportes de datos y el resto del hardware, con el objetivo de garantizar la integridad, la disponibilidad y la recuperación de los datos. Contempla diversas situaciones tales como incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Algunos mecanismos representativos son el control de accesos a las instalaciones, CPD's, servidores (hardware), medios y procesos de almacenamiento, copias de seguridad, sistema de discos (RAID..), etc.

j) *Seguridad Lógica*: se refiere a todo lo demás, a las condiciones en el uso de software, la protección de los datos, procesos y programas, así como la identificación de usuarios y el acceso autorizado de los usuarios a la información.

Abarca entre otros los siguientes aspectos: arquitecturas, servidores (sistemas operativos), filtrado del Firewall, configuración de electrónica de red, detección y eliminación de virus.

Para facilitar el estudio, emplearemos una clasificación alternativa considerando perspectivas adicionales: física, información y datos, sistema de comunicación, dispositivos de acceso, clientes. En cada uno de los niveles se acota el ámbito de actuación, se describen los mecanismos que intervienen, se identifican aquellas tecnologías de protección que resultan más apropiadas, y finalmente se aportan algunas recomendaciones que contribuyen a minimizar los riesgos.

3. Seguridad física de los soportes y de los sistemas informáticos

La seguridad física de los soportes y de los sistemas informáticos tiene por objeto garantizar el funcionamiento del sistema de información de la empresa. Está relacionada con los controles que protegen de los desastres naturales (incendios, inundaciones o terremotos), de los intrusos (ataque, robo o daño), de los peligros medioambientales y de los accidentes. También está relacionado con los

controles que protegen de los fallos en el hardware, y de las pérdidas voluntarias o involuntarias de datos, así como del control de acceso a las instalaciones.

Proporciona en definitiva, una primera barrera de protección ante accesos no autorizados, daños e interferencias a las instalaciones de la organización y a su información.

Sus requisitos varían considerablemente de unas organizaciones a otras, y dependen fundamentalmente de los activos que se desean proteger aunque en cualquier caso y con carácter general son aplicables criterios de control perimetral, control de las entradas físicas, de protección de áreas restringidas, o de instauración de sistemas y equipamientos de seguridad.

El Centro de Proceso de Datos (CPD) es el escenario habitual donde residen los soportes de los sistemas de información (activos) de una Organización y donde realiza su actividad el personal técnico que los custodia y administra. Son, por tanto, áreas especialmente sensibles que deben de estar protegidas adecuadamente.

No es objeto de este capítulo abordar qué características técnicas o qué tecnologías son las más adecuadas en un sala o edificio de esta naturaleza, pero dada su trascendencia, se ofrece una visión general referente a los criterios que deben estar presentes en su definición.

El proyecto de construcción de un CPD debe contemplar distintos aspectos: el entorno de las instalaciones y de la ubicación, la obra civil, los sistemas de climatización, el sistema eléctrico, el cableado estructurado, los sistema de detección y extinción de incendios, el sistema de iluminación, el sistema de control de accesos, etc., pero un aspecto que cobra especial importancia y que no puede pasar inadvertido en la definición de un CPD es la necesidad de garantizar el servicio en situaciones críticas. Para ello se precisa un modelo de respaldo que redunde el CPD y su información en un lugar remoto (otro edificio, otra ciudad) de modo que en caso de catástrofe la información esté a salvo y los sistemas de información de la empresa puedan rearmarse en un tiempo mínimo.

3.1 Técnicas de redundancia y de tolerancia a fallos

Las técnicas de redundancia en los sistemas informáticos tienen por misión incrementar su fiabilidad de forma que el fallo de uno de los componentes, normalmente en el hardware, no afecte a su operatividad.

En este contexto la redundancia se suele ligar a la alta disponibilidad, y en definitiva con la tolerancia a fallos. Esta última se define como la capacidad de un sistema en responder a un suceso inesperado; un

fallo de suministro eléctrico, un fallo de hardware, etc., de forma que no se pierdan datos, y que se mantenga su funcionalidad.

La redundancia, junto con los sistemas de alimentación ininterrumpidos (UPS y grupos electrógenos), proporciona seguridad física solamente en caso de cortes de suministro eléctrico o fallos del hardware, pero no ofrece protección contra las acciones negligentes o el borrado accidental, y se debe evaluar desde dos perspectivas distintas:

- *Local*, inherente al equipo informático. En ella los fabricantes de hardware se anticipan a los fallos en los componentes aplicando la redundancia en áreas clave como son las unidades de disco, las fuentes de alimentación, controladoras de red, ventiladores.

  Merecen una atención especial las técnicas RAID para salvaguardar los datos. Un RAID (Redundant Array of Inexpensive Disks o array redundante de discos) es un conjunto de unidades de disco que aparecen como una sola unidad lógica. Los datos se reparten entre dos o más particiones de los diferentes discos, aspecto que incrementa el rendimiento y proporciona redundancia y protección contra el fallo de uno de los discos de la formación. Existen varios niveles RAID; en el nivel 0 los datos se dispersan en varias unidades pero no hay redundancia (gran rendimiento pero nula seguridad), en el nivel 1 (espejo) los datos se escriben duplicados en distintas unidades (no incrementa el rendimiento pero si la seguridad, mayor protección - más caro). Los demás niveles RAID son una combinación de los conceptos anteriores y buscan aumentar la seguridad y el rendimiento simultáneamente.

  Casi todos los sistemas operativos actuales incorporan administración RAID.

- *Global*, para lo cual se redunda el sistema informático completo (por ejemplo, un servidor de aplicaciones con un equipo gemelo alternativo, en una arquitectura típica denominada *cluster*).

  Aunque tiene otras acepciones, un “cluster” es un conjunto de computadoras independientes (también denominados nodos) interconectadas mediante enlaces de alta velocidad que ejecutan una serie de aplicaciones de forma conjunta, y aparecen ante los usuarios como un solo sistema.

  Permiten aumentar la escalabilidad, disponibilidad y fiabilidad de los datos y de las aplicaciones que los gestionan, por tanto es una técnica que nos aporta seguridad, aunque su mayor utilidad estriba en utilizar varios computadores de bajo coste para crear un sistema con rendimiento cercano al de un supercomputador (“grid” o granja).

Una de las tecnologías que está teniendo mas empuje en la actualidad (aunque el invento data de 1994) es la de “cluster Beowulf” pensada para agrupar computadores con sistema operativo Linux y formar un supercomputador virtual paralelo.

3.2 Copia de seguridad

Respalda el sistema de información y garantiza su recuperación ante un hipotético desastre al estado que tenía inmediatamente antes de lanzar el proceso de copia.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que:

- Sea fiable, es decir, refleje fielmente el original y utilice como destino un soporte seguro.
- Permanezca en lugar seguro, tanto en lo que se refiere a los aspectos medioambientales, como a los mecanismos de acceso físico y lógico.
- Facilite una recuperación rápida y eficiente.

La técnica de respaldo que permite llevar a cabo la copia se denomina “backup”, y junto a la técnica de redundancia descrita en el apartado previo, protegen los datos ante interrupciones que se presenten de formas muy variadas: fallos de electricidad, incendios, inundaciones, virus informáticos, caídas de red, pérdidas por borrado accidental. Ambas técnicas, respaldo y redundancia, resultan por tanto complementarias.

La ejecución de un protocolo de copia supone haber completado un análisis previo del sistema de información, en el que se han valorado un conjunto de parámetros que lo condicionan:

- *Estrategia*. ¿Copiar programas y datos o únicamente los datos?. Esta última es poco recomendable, ya que en caso de incidencia, puede ser preciso recuperar también el entorno que proporcionan los programas, y esto influye negativamente en el tiempo de recuperación.
- *Tipo de copia*. Se consideran varios mecanismos que con frecuencia se complementan:
    - Completa: en la cual se realiza la copia integral de todos los activos. Es el mecanismo más efectivo y el recomendable siempre que las condiciones (tiempo de copia, presupuesto disponible), lo permitan.
    - Incremental: trata exclusivamente las modificaciones realizadas (fechas) desde la última copia. La restauración resulta mas compleja porque precisa de una copia original, y a partir de ahí se restauran las distintas copias incrementales.

- Diferencial: copia las diferencias reales sobre la última total. Tiene como ventaja que la restauración es más rápida, precisando la información de la copia total y de la última diferencial, y como inconveniente que requiere más espacio en disco.

- *Soporte.* Siendo habituales los basados en medios magnéticos y ópticos (cintas, discos, CD's), ligados a unidades fijas o extraíbles que se encuentran controladas por sistemas informáticos.
- *Volumen de información a copiar*, que dependerá especialmente de los factores enunciados: tipo de copia, estrategia, y soporte.
- *Tiempo de copia*. Es el margen temporal disponible para efectuar la copia. Supone un condicionante importante en aquellos casos en los que el proceso exige que los usuarios no se encuentren trabajando mientras se realiza la copia. Afortunadamente los gestores de bases de datos actuales y los software comerciales de respaldo permite efectuar las copias sin necesidad de parar los procesos de los usuarios. En cualquier caso, es recomendable realizar la copia en periodos de tiempo donde la actividad sea mínima.

Finalmente queda por resaltar que de nada sirve hacer backups si cuando se necesitan no funcionan. Debemos comprobar que los backups realizados pueden ser restaurados correctamente, o de lo contrario se estará confiando a un sistema de respaldo inútil cuyo funcionamiento no está garantizado.

4. Seguridad de la información y de los datos: preservar información frente a observadores no autorizados.

La seguridad de la información en este caso, hace referencia a uno de los niveles más importantes ya que afectan directamente a los contenedores de la información. Incluye aspectos relativos a los datos y aspectos propios de los programas que los manejan.

4.1 Seguridad de los datos

Existen mecanismos que actúan no tanto en los soportes sino en los datos propiamente dichos, en la identidad de los agentes que intervienen en el intercambio de los datos y en la integridad de la información desde que se envía de una fuente y llega a un destino.

Aunque no hay sistema totalmente seguro, una buena práctica de salvaguarda de datos consiste en proteger los programas que los gestionan.

4.2 Seguridad de los programas

El usuario se comunica con su ordenador a través de un interfaz, ya sea gráfico o no, utilizando los programas que componen el sistema informático que se maneja; por ejemplo Windows con un Office.

Normalmente el software que utilizamos está basado en múltiples tipos de programas que exceden el conocimiento de un usuario final, las operaciones que realiza un procesador de textos o un programa de hoja de cálculo no están supervisados por el usuario final y éste supone que son las correctas.

Pero, ¿qué pasaría si ese programa, además de hacer lo que dice que hace, realiza otras operaciones que pueden llegar a comprometer la seguridad del sistema donde está instalado?.

Para poder certificar las funcionalidades de los programas que existen en un sistema informático, sería preciso analizarlos todos en detalle, y este extremo no parece una solución muy práctica. En cambio, lo que sí podemos hacer es fiarnos en un grado mínimo de programas de los cuáles conocemos su procedencia y nos inspiran confianza. Esos programas normalmente son los pertenecientes al sistema operativo y a algunos paquetes cerrados de software (Ofimáticos, Gestión de Redes, ...) de ciertos fabricantes. Por el contrario, por norma general, no podemos confiar en los programas que se descargan desde Internet, a través de enlaces directos o P2P, ya que esos no suelen estar validados por ningún fabricante y han podido ser alterados, por ejemplo, para fines fraudulentos o ilegales.

Existe una celebre frase que dice "seguro que no hay programa totalmente seguro". En realidad, existen multitud de técnicas de ataque a través de programas, ideadas para generar un malfuncionamiento intencionado en un programa y que implica que se comporte de forma distinta a como se concibió por su propietario o usuario. Las razones obedecen a intereses diversos; por ejemplo, desde corrupción de datos, acceso a datos confidenciales e incluso bromas. Estos intereses permiten establecer una clasificación de técnicas de ataque que se realizan con programas según su enfoque:

- *Funcionamiento anómalo del sistema / bloqueo del sistema y corrupción de datos*. Es un mecanismo orientado a provocar daños en los datos del sistema atacado. Se trata de programas especializados en corromper ficheros de tal manera que queden truncados o inaccesibles. Además, tienen por finalidad causar un malfuncionamiento o comportamiento anómalo del sistema víctima. Causan grandes estragos en los sistemas informáticos, llegando a bloquear los accesos, borrando ficheros necesarios para el buen rendimiento del sistema, modificando el sector de arranque o, incluso, formateando el soporte donde se encuentran lo datos. Los ejemplos mas representativos son:

- *Virus*. Es un programa que se auto-copia para generar un funcionamiento anómalo del sistema donde está instalado, de manera no controlada por los usuarios y administradores del sistema. Para replicarse y extenderse normalmente modifican un programa del sistema atacado y se instalan en él, para que en el momento en el que el usuario lo utilice, poder saltar a la memoria ram, desde donde continúa su labor de infección a otros programas, asi como a otros equipos.
- *Gusanos*. Son programas que actúan como los virus, pero a diferencia de estos no necesita de un anfitrión, son autónomos.

- *Accesos no autorizados*, o mecanismos que en función de su finalidad se subdividen en:
  - *Auditores*. Son programas que están relacionados con las labores que suelen realizar los administradores, y se usan como ayuda para identificar los posibles puntos débiles de un sistema, para lo cual utilizan técnicas invasivas para probar las medidas de seguridad de un sistema. También se utilizan en la formación de administradores de sistemas.
  - *Dañinos*. Son programas que persiguen normalmente el robo de datos, aunque existe literatura reciente indicando que también se hacen pagos por terceros para causar graves problemas de seguridad y así perjudicar a la empresa propietaria del sistema atacado.

A continuación se indican algunos ejemplos representativos de programas actuales que atacan la seguridad muy extendidos en Internet:

- *Honeypots.* Son programas especializados en captar la atención de posibles atacantes con la finalidad de descubrirlos, espiarlos y detectar sus intenciones. En si mismo, es un programa de defensa o prevención ante ataques, pero lo incorporamos en este apartado para referenciar su uso como programa de ataque.
- *Troyanos (o caballos de Troya).* Programas que están ocultos detrás de otros con apariencia legal y que tienen un mecanismo programado de activación por el cuál pueden realizar distintas operaciones, ya sea enviando información privada a otros equipos (spyware), permitiendo accesos no controlados al sistema mediante control remoto, etc. Unos de los más llamativos y peligrosos son los *keyloggers* ya que son capaces de grabar todas las pulsaciones realizadas en los teclados y enviarlas a un equipo remoto con el consiguiente riesgo de obtener información estratégica como claves de acceso, etc.
- *Backdoors (Puertas traseras).* Programas que permanecen residentes en el sistema esperando una llamada específica. Una vez recibida esa llamada, habilitan un acceso no controlado al

sistema. Tienen una naturaleza común con los troyanos y de hecho se les puede considerar un subgrupo de ellos.

- *Exploits.* Es un método por el cuál el atacante se aprovecha de alguna debilidad o vulnerabilidad del programa atacado, para conseguir un acceso privilegiado no autorizado a la línea de comandos del sistema.
- *Shellcodes.* Es una técnica de programación consistente en la inyección de código en el programa original con la finalidad de que el intruso consiga un acceso privilegiado no autorizado a la línea de comandos (shell) del sistema atacado.
- *Rootkits.* Conjuntos de utilidades que se instalan en el sistema víctima con el fin de ganar acceso a muchos servicios del sistema y obtener privilegios de una forma no autorizada. Están provistos de herramientas para eliminar sus huellas del sistema atacado, y normalmente instalan puertas traseras (backdoors) y otros mecanismos para poder conseguir acceso al sistema en un futuro.

Para asegurar los programas de un sistema informático, un protocolo sencillo y a la vez efectivo consiste en limitar al máximo los accesos a la *shell* del sistema. Los administradores deben ser los únicos autorizados para acceder al sistema en modo comando. Posteriormente se pueden generar resúmenes (*hash*) de los programas del sistema, por ejemplo mediante el algoritmo MD5. Los ficheros resultantes se guardarán en un lugar seguro, fuera de accesos por red y en un soporte de sólo lectura. Periódicamente (depende de la frecuencia de accesos al sistema y del grado de compromiso que tenga el sistema) se puede validar cada uno de los programas generando de nuevo el *hash* y comparándolos con los guardados, obteniendo así un listado de los programas que han sido alterados.

Otro buen hábito puede ser la comprobación de los permisos de los programas del sistema, comparándolos con una lista guardada al estilo de los *hash* explicados anteriormente.

4.3 Seguridad de la información

A lo largo de la historia se ha podido observar la relación entre la comunicación, el lenguaje y la criptología, como forma de mantener en secreto una información. Por ejemplo, la codificación de un mensaje en lenguaje Morse que se envía a través de una comunicación basada en ondas y es recogido por un destinatario que utilizando el mismo lenguaje puede acceder a la información. No obstante, ese mensaje podría ser interceptado y leído por un tercero, ya que tanto la codificación como la comunicación se realizan con/sobre sistemas públicos muy extendidos y conocidos.

La seguridad de la información está pues muy relacionada con la efectividad de las técnicas de ocultación utilizadas. Este aspecto lo estudia la ciencia de la criptología.

El término deriva del griego *kryptos* (ocultación) y *logos* (ciencia), y su definición precisa conocer otros términos con los que está relacionado como son la criptografía, los criptogramas, los criptosistemas y el criptoanálisis.

La criptografía es una "*técnica para ocultar la escritura*". Aquí cabe matizar entre la criptografía clásica y la criptografía moderna. Si bien la primera básicamente ha sido el arte de ocultar una información dada mediante una clave secreta, hoy en día la criptografía moderna abarca una gran abanico de disciplinas, fundamentalmente matemáticas, para llevar a cabo la labor de la ocultación de la información sin usar únicamente una clave secreta. Así, una definición más académica y más moderna podría ser "*el conjunto de técnicas/métodos utilizados para cifrar una información dada*", es decir, a un mensaje "en claro" (inteligible) una vez aplicadas esas técnicas genera un mensaje cifrado (ininteligible). Ese mensaje cifrado se denomina criptograma.

En resumen, la criptografía intenta cumplir con las normas básicas de seguridad: confidencialidad de la información, autenticidad del emisor, integridad de esa información y no repudio (el emisor está claramente identificado y no puede negar la autoría del mensaje).

En la criptografía clásica, existen dos tipos de cifrado básicos o elementales: los de transposición, que reordenan los elementos del mensaje en claro siendo clave el criterio de reordenación empleado, y los de sustitución, que cambian los elementos del mensaje original por otros siendo clave el criterio de sustitución. El resto de cifrados de la criptografía clásica se basan en uno u otro, o en la unión de ambos.[1]

En la criptografía moderna el factor diferencial son las claves utilizadas, que permiten diferenciar dos modalidades:

- Métodos simétricos, en los que la clave de cifrado coincide con la de descifrado. La clave debe ser secreta, acordada entre el emisor y el receptor y conocida únicamente por ellos. Se les

[1] A partir del texto: "MAÑANA VOY A MADRID", si ciframos con un criptosistema de transposición con clave k=7, indica que cada 7 caracteres el orden se invierta. Así tenemos los grupos "MAÑANA ", "VOY A M" y "ADRID". Aplicando el criterio, resulta "ANAÑAM", "M A YOV" y "DIRD". Finalmente lo uniremos y el criptograma resultante será "ANAÑAMM A YOVDRID".

Para obtener un cifrado a partir de un criptosistema de sustitución con clave k=3 (utilizada por César en la antigua Roma), cada carácter del mensaje original se sustituye por el posterior k posiciones en el abecedario; A se cambia por D, B por E, etc. Aplicando el criterio del criptosistema, el cifrado resultante es "ODQDPD YRB D ODGULG"

conoce como criptografía de clave secreta o clásica. Un ejemplo lo representa el algoritmo DES (*Data Encryption Standard*).

- Métodos asimétricos, donde la clave de cifrado es distinta de la de descifrado. Se basa en un par de claves, una privada y otra pública. La privada utilizada para cifrar y la pública para descifrar. Se les conoce como criptografía de clave pública. Muestras de ellos son los algoritmos RSA (*Ronald Rivest, Adi Shamir y Leonard Adleman*) ó *ElGamal*. Un uso común es el siguiente: en una comunicación emisor y receptor generan un par de claves privada/publica y envían al otro su clave pública. Para enviar un mensaje de E (emisor) a R (receptor), E cifrará el mensaje con la pública de R, asegurándose de que el mensaje solamente puede descifrarlo R con su privada.

Estas técnicas son precisamente las que se implementan en las soluciones de firma electrónica.

Por su parte, el criptoanálisis se encarga exactamente de la labor contraria a la criptografía y puede ser definido como "*un conjunto de técnicas/métodos utilizados para descifrar una criptograma o mensaje cifrado*". A través del criptoanálisis se puede recuperar el mensaje original así como probar la robustez del criptosistema empleado para cifrarlo. Se trata de uno de los elementos más importantes de la criptografía y de su estudio han surgido nuevas técnicas para cifrar la información cada vez más resistentes y fiables.

Entonces, de manera general, podemos definir criptología como "*la ciencia que engloba el estudio de la criptografía y el criptoanálisis*".

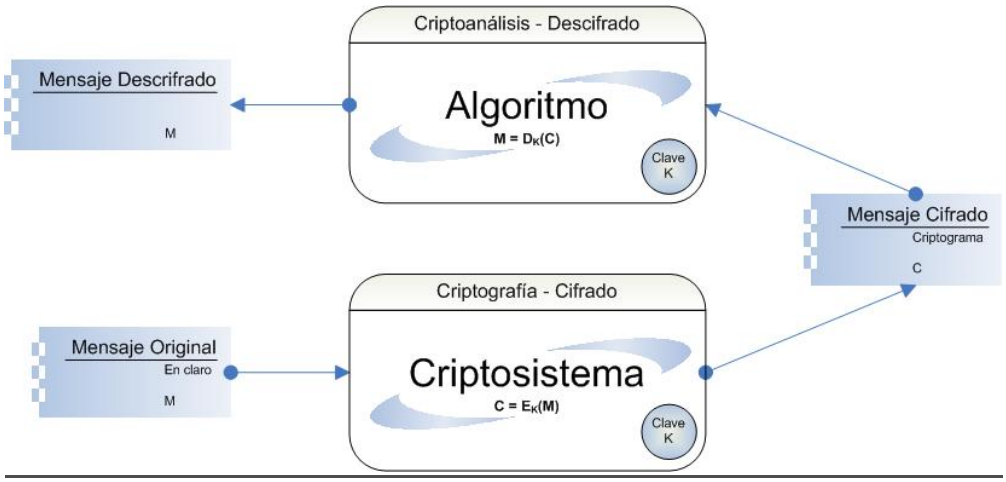


Figura 7.1 - Las técnicas de la criptología

Los criptosistemas son susceptibles de registrar un gran número de ataques debido al interés que suscita la información que se protege.

Un aspecto que resulta relevante en el éxito de un ataque de esta naturaleza es la información disponible del criptosistema. Por ello, a priori los públicos son mas vulnerables, mientras que la ausencia de información de los criptosistemas no públicos les hace mas fuertes y es una de las razones por la que muchas organizaciones, entre ellas las militares, utilizan estos últimos con el fin de ocultar al máximo el secreto. Además, la capacidad de cifrado también es importante y unido al criterio anterior puede hacer que el descifrado de los mensajes esté al alcance del atacante. Siempre que el criptosistema sea conocido se podría hacer un ataque llamado por *fuerza bruta* (ataque más elemental sin necesidad de conocimientos criptográficos) consistente en generar todas las claves posibles y conseguir la verdadera. Con este tipo de ataque, dependiendo del criptosistema, el espacio de claves (conjunto máximo de claves que puede utilizar) y de los recursos empleados (procesador y tiempo, básicamente), podrá conseguirse la clave del criptosistema atacado.

Por último, queda indicar un área de la criptología llamada *esteganografía* que se encarga de ocultar la existencia del mensaje en sí y no su contenido. Es una técnica que incluye el mensaje a proteger dentro de otro mensaje sin interés, utilizando una clave secreta acordada entre el emisor y el receptor. La utilización de la esteganografía aumenta la seguridad del mensaje cifrado ya que aplica una capa más de ocultación.[2]

5. Seguridad en los periféricos o dispositivos finales

Hace referencia a la seguridad física del hardware y a la que puede ejercerse desde una administración informática. Tiene una relevancia especial por ser la más cercana al usuario y por tanto la que se encuentra más expuesta a peligro de mal uso o de uso malintencionado.

Es preciso configurar estas máquinas y dispositivos de red de forma que sea lo más complicado posible realizar manipulaciones sobre ellos, tanto en el nivel físico como en el nivel informático.

Aunque una serie de pautas son comunes a todos los dispositivos, la distinta naturaleza de los mismos (de sobremesa o portátiles, de conexión fija o de conexión inalámbrica, etc.) recomienda que estudiemos en este capítulo los controles y aspectos diferenciales de la seguridad en función del periférico.

[2] Como ejemplo curioso tenemos el de la Grecia Clásica en que algunos mensajes se escribían (tatuaban) en el cuero cabelludo de los mensajeros (normalmente esclavos), se dejaba que creciera el pelo y el mensaje quedaba oculto pudiendo el mensajero transportarlo sin temor a ser descubierto.

Son medidas y controles de naturaleza más organizativa que tecnológica, que contribuyen a minimizar los riesgos de seguridad asociados a un equipo de usuario final, y creemos que pueden contribuir a entender mejor esta faceta

5.1 Control de los ordenadores personales fijos

Se recogen aspectos de control a tener en cuenta en los equipos de usuario más habituales y extendidos como son los ordenadores personales fijos.

Son consejos de cómo mejorar la seguridad física de estos dispositivos, impidiendo su manipulación por parte del usuario final. Si el acceso directo al hardware por parte del usuario es necesario (disqueteras, CDROMS, impresoras, etc.) se precisa una política clara de uso del hardware, donde el usuario conozca exactamente lo que puede hacer y lo que no debe hacer.

- Control de acceso del personal al hardware

  Es una medida previa. Se puede realizar dedicando personal que verifique la identidad de las personas que supuestamente tienen permiso de acceso, o disponiendo dispositivos electrónicos (claves, sistemas biométricos) o físicos (puertas blindadas, cerraduras seguras, etc.) que permitan controlar quién tiene acceso al hardware y quién no.

  Siempre será preferible la intervención de personal encargado del acceso al hardware que la utilización de llaves, tarjetas o dispositivos electrónicos, pues estos últimos son más susceptibles de ser burlados.

  En lo que respecta a la seguridad de los equipos propiamente dicha, la única medida eficaz pasa por responsabilizar de alguna forma al usuario final del hardware que está a su cargo.

  Los dispositivos y servidores situados fuera de los centros de datos o de computación o en las zonas departamentales deberán ser protegidos en armarios cerrados con llave (racks) y deberá seguirse un protocolo específico de accesos desde el departamento de informática / sistemas.

- Control de acceso del personal de servicios

  Un aspecto poco conocido pero muy a tener en cuenta en la seguridad física de los sistemas es el control de acceso del personal de mantenimiento del edificio. El personal de limpieza, de mantenimiento del edificio y otro personal de servicios debe pasar por los mismos sistemas de control de acceso que los administradores o usuarios de las máquinas.

- Las cajas de los ordenadores y el acceso interno

La caja común de un ordenador personal está preparada para facilitar el acceso a su interior al técnico de mantenimiento, y por tanto no presenta dificultad mayor su apertura y acceso, en la mayoría de los casos sin necesidad de herramientas. Esto, evidentemente va en contra de su seguridad.

Hay varias soluciones que se pueden aplicar para mejorar la seguridad de estos sistemas: el sellado de la caja alertará ante cualquier intrusión, perforar y poner un candado que impida su apertura es otra posibilidad, o incluso alternativas más radicales como la soldadura de la tapa de la caja con el armazón. Todas estas acciones sin embargo van en detrimento y perjuicio de las tareas de soporte y mantenimiento del equipo.

Diversos fabricantes proporcionan hoy cajas que tienen cerraduras y sistemas de anclaje de la tapa con el armazón, que proporcionan una seguridad considerable contra intrusos. También se puede usar cajas de metacrilato fabricadas a medida para nuestros sistemas (opción engorrosa y difícil de mantener).

Todas estas opciones son parches para el problema principal, que es el mantener datos importantes en una máquina expuesta al usuario final y a posibles intrusos. La opción correcta es mantener estos datos en lugar seguro (un servidor de archivos dentro de un armario o rack) y que el usuario trabaje de forma remota sobre estos datos, con lo que la seguridad física del ordenador del usuario final será poco importante.

- Seguridad de la BIOS

  La seguridad que proporciona incorporar contraseña (password) en la BIOS es absolutamente ficticia. Habitualmente se suele confiar excesivamente en este mecanismo, cuando su seguridad está condicionada físicamente; si es posible abrir la caja del ordenador, es posible actuar sobre el puente de anulado del password de la bios o puede simplemente ser intercambiado por otro chip alterado en cuyo caso implicaría además un acceso total (robo de chip original).

- Grabación de datos (grabadoras de CD, disqueteras, etc.)

  Son puertas potenciales de salida de información, y el mecanismo de seguridad más efectivo consistiría en anularlas.

  Sin embargo, aunque es posible anular las grabadoras de CDs, las disqueteras, ninguno de los métodos es absolutamente seguro para prevenir la extracción de datos del periférico. Por otro lado, estas medidas tan drásticas pueden suponer serios inconvenientes en el uso normal y habitual del puesto de trabajo.

Sin descartar totalmente las medidas anteriores, entendemos que una medida complementaria como mantener los datos lo mas alejados posible del usuario final, aumenta sensiblemente la eficacia en seguridad.

Si la naturaleza de los datos requiere preservar especialmente el sistema de posibles fugas (por ejemplo los datos de salud), la forma de "alejar" los datos del usuario final consiste en almacenarlos y gestionarlos desde dispositivos de almacenamiento centralizados (NAS, SAN, DAS), e impedir el acceso masivo a lotes de datos. El usuario trabaja sobre ellos de forma remota y la replicación local se torna más compleja.

- Llaves USB y Sistemas de Almacenamiento USB. Otros puertos Serie Paralelo

  Su peligro estriba en lo que puede entrar por ellos: virus, software pirateado, juegos, etc., y lo que se puede exportar en ellos: datos de la empresa, software licenciado para otros, etc.

  Los mecanismos de protección son los indicados para las grabadoras y CD's: alejar los datos del usuario, e inhabilitar los puertos USB, ya sea mediante métodos software o hardware.

  Los puertos serie y paralelo no son menos peligrosos, ya que aunque algunos dispositivos precisan programas de conexión (drivers) cuya instalación se puede controlar y bloquear desde el sistema operativo de una forma sencilla y eficaz, en otros casos como los fax/modem no es así ya que actúan normalmente sin necesidad de drivers.

  Los puertos Ethernet también presentan un peligro potencial ya que un simple cable cruzado permite simular una red y con ello es posible habilitar la transferencia de datos o la fuga de información impresa

  Los dispositivos USB son un problema mayor, especialmente en sistemas operativos como el Windows (en software libre como Linux se puede anular el soporte USB de almacenamiento fácilmente anulando los respectivos módulos del kernel). En Windows XP es harto difícil porque incorpora de serie drivers para todo este tipo de dispositivos (y dispositivos como el ratón, teclado o impresora que deben autodetectarse, cada vez mas hacen uso del puerto USB).

  Y por supuesto, siempre está la alternativa más radical (pero menos recomendable) de sellar, desoldar de la placa base o anular físicamente los puertos USB.

Un caso peligroso relacionado con los puertos USB y también con las unidades de CD es el de una tecnología reciente denominada U3 que se implementa en la mayoría de las llaves o pendrives actuales, y que permite la auto-ejecución de programas desde el propio dispositivo sin dejar rastro de su ejecución. Esto es debido a que, mediante U3, el USB es capaz de tener dos particiones, una de almacenamiento y otra de auto-arranque al estilo de los CDs, a través de ficheros AUTORUN. Si bien estos ficheros contienen normalmente menús de selección para el usuario, también podrían contener programas que se ejecuten silenciosamente sin su conocimiento. Esto puede conllevar graves riesgos de seguridad, ya que simplemente la inserción y visualización de un USB dotado de U3 y previamente tratado por un hacker, puede auto-arrancar un programa que agrupe silenciosamente ficheros (cuentas de correo, mensajes, ...) e incluso instalase un keylogger para luego enviar la información generada a través de Internet al atacante.

- Dispositivos “keycatchers”y sistemas para captar claves secretas

  Los dispositivos “keycatchers” son llaves que se interponen entre el teclado y el ordenador para captar las pulsaciones del usuario, grabando los datos que se introducen, buscando sobre todo la adquisición de claves y contraseñas que el usuario pueda teclear. Son dispositivos visibles y fáciles de detectar, aunque también son fáciles de instalar y desinstalar. Han sido empleados con éxito en el pasado en la banca y en el comercio electrónico para captar números de tarjetas de crédito, números de cuenta y otro tipo de datos secretos. Con la tecnología actual cada vez son menos útiles y frecuentes.

5.2 Control de los ordenadores portátiles

La portabilidad de estos dispositivos y sus reducidas dimensiones, los hace susceptibles de ser robados con facilidad, sobre todo cuando se encuentran fuera de la empresa.

El valor real estriba más en la información y datos contenidos, que en el coste económico del equipo. Por ello es importante mantener un control sobre los mismos.

Una forma de minimizar el riesgo consiste en evitar guardar cualquier dato que pueda resultar estratégico o sensible en el disco duro local. Es menos comprometida la conexión remota desde el mismo a un repositorio central de la empresa utilizando un protocolo de comunicación seguro. Si a pesar de todo es imprescindible manejar datos locales, éstos se deben proteger mediante cifrado, garantizando el acceso mediante clave personal de la que el usuario es responsable.

Asimismo son aplicables todas las recomendaciones ya indicadas para los equipos personales fijos, si bien por encima de todas ellas está el hacer un uso responsable por parte del usuario.

5.3 Control de dispositivos de mano: Palm, Pocket PC, Ultra Mobile PC (UMPC)

Deben tomarse medidas aún más exhaustivas que con los portátiles, dado que su escaso tamaño y dimensión les hace más vulnerables frente a la sustracción. Es relativamente frecuente, el robo de estos dispositivos con todos los datos del empleado que luego pueden ser usados para realizar espionaje (*hacking*), dado que puede haberse visto comprometida información estratégica de la empresa (números de teléfono, datos sobre la empresa, *passwords* de acceso a los sistemas, etc.)

La forma de minimizar el riesgo es no mantener datos estratégicos de la empresa sobre este tipo de dispositivos (especialmente passwords de acceso).

5.4 Control de teléfonos móviles y "SmartPhones"

Los móviles y especialmente los *smartphones* [3] cada vez se parecen más a un ordenador personal, por lo que las amenazas y controles seguros mucho tienen que ver con lo expresado en los párrafos previos respecto de los portátiles, PocketPC o PDA.

Las amenazas más frecuentes en los dispositivos móviles son las prácticas de "*hacking*", conocidas como *BlueSnarfing* y *BlueSniping*, dos técnicas que permiten tomar, acceder y robar la información de los terminales móviles equipados con tecnología *Bluetooth*, aprovechando las vulnerabilidades de está última. Así, los teléfonos pueden ser atacados remotamente para acceder y capturar la información contenida en los equipos, como la agenda de contactos, números telefónicos, citas o notas de

[3] Un "Smartphone" o teléfono inteligente, es un dispositivo de mano que integra las funcionalidades de un teléfono móvil, de una PDA (tratar archivos, reproducir mp3, tratar imágenes, ..), con WIFI y bluetooth, conexión a internet, mensajería (SMS, MMS, mensajería instantánea) y email. Pueden instalarse aplicaciones adicionales; desarrolladas por el fabricante, por el operador o por cualquier otro agente. Poseen un sistema operativo definido: Palm OS, Linux, Windows Mobile o Symbian. Su mercado crece rápidamente; no solo está cambiando el sector de la telefonía sino también el de la electrónica, y el de la tecnología de la información.

calendario, mensajes de texto. Los teléfonos son vulnerables cuando la funcionalidad *Bluetooth* está activada.[4]

Algunas recomendaciones que los expertos consideran clave para prevenir o minimizar este tipo de ataques son que el usuario debe conocer las capacidades y aplicaciones de su teléfono, ser muy conservador en el momento de decidir la instalación de una nueva aplicación en el teléfono, especialmente si se lo descarga de Internet (que es lo mas frecuente), y estar alerta cuando utilice tecnologías inalámbricas *Bluetooth*, activándolas sólo cuando lo necesite.

6. Seguridad del sistema de comunicación

Se conoce por sistema de comunicación al conjunto de reglas o principios que permite establecer una comunicación entre dos agentes interlocutores. Está formado por los siguientes elementos:

- *Codificación*. Hace referencia al lenguaje o conjunto de reglas de agrupación de caracteres tipo para formar mensajes. Esta codificación debe ser conocida por emisor y receptor.
- *Mensaje*. Es la información codificada que se desea transmitir.
- *Medio ó Canal* por donde se transmite el mensaje (cable, ondas EM, …). Tiene habilitados controles de errores y flujo para asegurar que el mensaje se transmite correctamente.
- *Emisor* o extremo origen de la transmisión de mensaje.
- *Receptor* o extremo destino del mensaje.

El emisor y el receptor están unidos por un medio o canal con el fin de intercambiar un mensaje cuya codificación es conocida por ambos. Esto representa un sistema de comunicación genérico.

En la figura 7.2.a se muestra una comunicación telefónica entre dos usuarios, emisor y receptor, que se transmiten un mensaje a través de un medio de transmisión, la red de telefonía móvil. El mensaje se transmite codificado (bits) en un lenguaje comprensible por los terminales móviles de cada uno de los usuarios. Los terminales móviles se entienden entre si porque utilizan el mismo lenguaje, pero esto no es siempre así, y entonces se necesitan mecanismos de traducción (intérpretes) para comprender el mensaje.

[4] Cuando el Bluetooth comenzó a implantarse en la industria de la telefonía móvil se dieron casos conocidos como el del Metro de Londres donde usuarios inocentes eran blanco de ataques en los que se usaban sus dispositivos sin su consentimiento merced a un agujero de seguridad del Bluetooth.

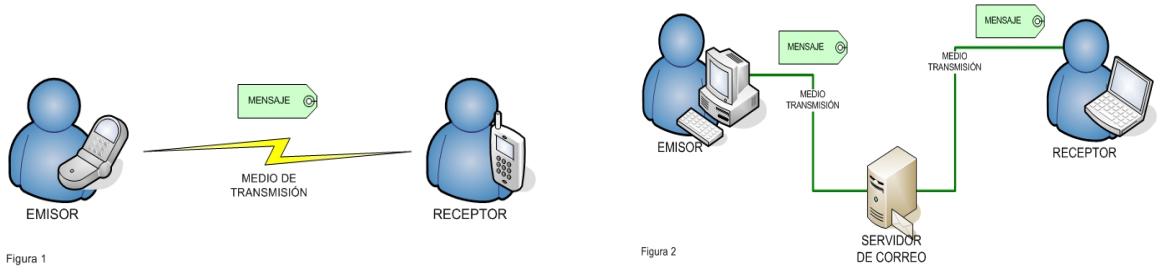


Figura 7.2- Sistemas de comunicación (a) y (b)

La figura 7.2.b, representa el flujo general que emplea el servicio de correo electrónico. El medio de transmisión, en verde, sería por ejemplo una línea ADSL. La comunicación se realiza en dos fases: la primera entre el emisario del mensaje y el servidor de correo, que en este caso, actúa como receptor, y la segunda se establece entre el servidor de correo (emisor) y el receptor final. En cualquier caso los elementos que participan en la comunicación son los mismos que en la figura 7.2.a.

Un sistema de comunicación está en riesgo permanente de sufrir problemas de seguridad dada la variedad de los elementos que intervienen. En la figura 7.3 se ilustra un caso muy común:

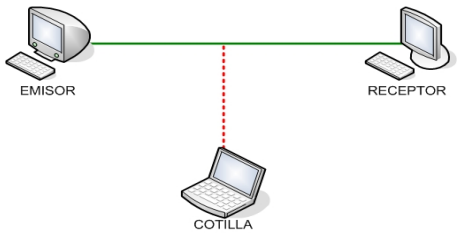


Figura 7.3- Amenazas en un sistema de comunicación

Se establece una comunicación entre dos agentes a través de un medio de transmisión cualquiera (en verde). Los únicos que deben enterarse de lo que se transmite son el emisor y el receptor, pero si un tercero (cotilla) fuese capaz de conectarse al mismo canal y “escuchar” los mensajes, la seguridad de la comunicación quedaría comprometida y el “cotilla” podría hacerse eco de todo los transmitido.

El ejemplo muestra la técnica más comúnmente utilizada para comprometer la seguridad de una comunicación, existiendo distintas variantes, tanto en comunicaciones por cable, como en comunicaciones inalámbricas (Wifi, Bluetooth, Satélite, …).

Los ataques que reciben los canales soportados por cable se realizan desde el propio canal, es decir, el atacante tiene acceso físico al mismo. Esto conlleva un riesgo para el propio atacante ya que puede ser detectado más fácilmente. Por el contrario, los realizados a un canal inalámbrico tienen la ventaja para el atacante de dificultar en alto grado su detección. Para estos últimos, se han implementado diferentes mecanismos de seguridad de comunicación (listas MAC, WEP, WPA, etc.).

6.1 Seguridad de la red de comunicación

Estudia el aspecto más dinámico de la seguridad en los sistemas de comunicación

Se entiende por red informática "*la interconexión de ordenadores autónomos con una finalidad común, normalmente la compartición de recursos*". Así, Internet es una gran red (en realidad, es una red de redes). Esos recursos compartidos podrían ser software como aplicaciones, hardware como impresoras, bases de datos, etc. Se centrará el análisis sobre las redes TCP/IP, por ser las más extendidas y las adoptadas masivamente por las organizaciones sanitarias. A su vez son el protocolo soporte del Internet actual.

Se pueden clasificar las redes atendiendo a distintos criterios, pero uno de los más utilizados es el ámbito geográfico. Desde este punto de vista se distinguen los siguientes tipos:

- *Red de área local (LAN)*. Permiten la interconexión de ordenadores próximos entre sí. Podríamos verla como la red más básica, por ejemplo las desplegadas en las oficinas de cualquier empresa.
- *Red de área metropolitana (MAN)*. Habitualmente en la interconexión participan ordenadores ubicados en diferentes edificios de una misma localidad geográfica, por ejemplo red de una administración local, de metro, etc.
- *Red de área extensa (WAN)*. Interconecta ordenadores de distintas localidades e incluso países.

Actualmente, la red de ordenadores es quizás uno de los términos más extendidos en todas las organizaciones; existen redes en los hospitales, en el servicio de correos, en la administración central, en los bancos, etc., en definitiva, todo el mundo está interconectado mediante redes.

Este entorno ideal donde se comparte información multimedia (voz, datos, imagen, video) conlleva sin embargo un riesgo ya que si no se ponen las barreras adecuadas, la información generada por cada uno de los nodos (elementos de la red, generalmente un ordenador o *host*) quedan a merced de cualquier agente interesado.

Uno de los elementos fundamentales de seguridad son los cortafuegos (*firewall*) que se utiliza para salvaguardar la información que distribuye ó sirve una red de ordenadores. Permite la monitorización de los accesos a una red, validando o rechazando conexiones a la misma en función de su procedencia y/o destino y en función de los servicios informáticos para los que se requiere acceso (Web, Correo, etc.). Es un elemento imprescindible en cualquier organización, con independencia de su tamaño, al menos para controlar los accesos desde Internet.

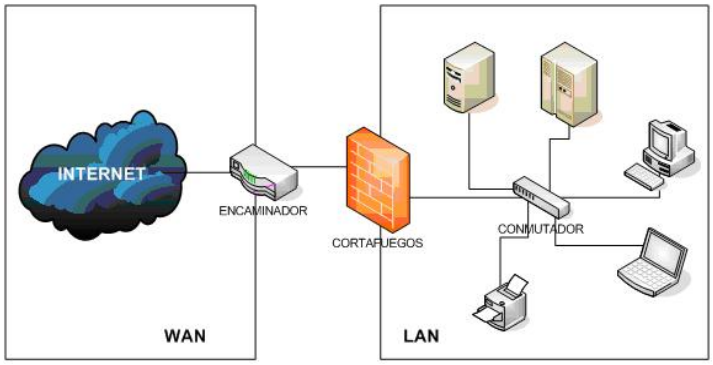


Figura 7.4- Cortafuegos o “firewall”

El esquema de la figura 7.4 representa una configuración típica en la que interviene una LAN, un cortafuegos y distintos dispositivos habituales que participan en la topología de red, tales como conmutadores para conformar la red local o un encaminador que habilita el acceso entre esta y otras redes WAN.

Si no existiese el cortafuegos, la LAN quedaría expuesta a múltiples ataques desde la WAN no controlados. Y quedaría comprometida la información residente en cualquiera de los nodos de la LAN. Pero también, y no menos importante, quedaría comprometida la seguridad por potenciales ataques efectuados desde la propia LAN.

Los cortafuegos pueden ser de tipo hardware o software, siendo preferibles los primeros ya que son máquinas preparadas expresamente para realizar óptimamente la tarea de protección, incorporando una electrónica específica orientada a conseguir mayor rendimiento. Por el contrario, los cortafuegos software suelen estar instalados sobre otras máquinas que no han sido fabricadas para realizar esa función teniendo un rendimiento peor y una menor tolerancia a fallos.

Pueden proteger redes, pero también pueden proteger máquinas (nodos) independientes. Por ejemplo los cortafuegos personales que aparecen embebidos en el software de algunos sistemas

operativos habituales. El funcionamiento de ambos es en origen el mismo. Su gestión se hace a partir de reglas (políticas) definidas según el origen/destino de los paquetes y protocolos que se utilizan.

Últimamente, han aparecido soluciones muy completas que además de cortafuegos, disponen de módulos de antivirus, antispam e incluso detección de intrusión (IDS). Existen distintos fabricantes que disponen de equipos de esta naturaleza (familia Fortinet de Fortigate, Symantec, etc.).

6.2 Disponibilidad de recursos y control de accesos indebidos

La distinta naturaleza y multiplicidad de dispositivos que forman parte de una red (impresoras, ordenadores personales, conmutadores, etc.) y los efectos en el colectivo que puede acarrear el malfuncionamiento de uno de ellos, hacen necesario la utilización de mecanismos capaces de monitorizar todo lo que acontece en la red; tipos y flujos de paquetes en circulación, consumo de recursos como el ancho de banda, colisiones y control de congestión de red.

Estos mecanismos que globalmente se conocen por "herramientas de gestión de red" consisten básicamente en software especializado que se encarga de cubrir alguna o varias de las tareas siguientes:

- *Análisis*. Se utilizan para monitorizar la red. Comprueban la utilización de la red, a partir de los protocolos que se emplean sobre ella. Si tenemos un PC conectado a Internet a través de un P2P (por ejemplo eMule) que está consumiendo cada vez más ancho de banda de la red y ralentizando con ello el tráfico por falta de recursos, podemos detectar esa situación y aislar a ese PC o bien limitarle los recursos de acceso a ese servicio. Un ejemplo real lo tenemos en los gestores de ancho de banda como el de *Allot NetEnforce*.
- *Prevención*. Son herramientas enfocadas a enviar alarmas en función de los eventos que suceden en la red. Si un conmutador está generando errores debido a la pérdida masiva de paquetes por sobrecarga, es posible detectar ese malfuncionamiento e intentar resolver la situación antes que el problema se agrave. Es el caso de productos comerciales como el *HP Open View*.
- *Protección*. El exponente más representativo es el cortafuegos o firewall.

El ejemplo mas representativo de herramientas de gestión de red que actúan por hardware son los "dispositivos Tap", que permiten leer el tráfico de una red sin tener que emitir ningún tipo de dato en la red, por lo que resultan difíciles de detectar. Se suelen usar para instalar dispositivos *IDS stealth* (Detectores de intrusos no detectables como máquinas de la red) y para hacer "*sniffing*" de la red sin ser detectados. Son útiles para el administrador de sistemas en la instalación de detectores de intrusos

y para hacer análisis de red, pero pueden volverse en contra si se instala en la red con un uso malintencionado.

Estos dispositivos, al funcionar incluso sin dirección IP (modo transparente) pueden estar actuando y analizando la red de forma inadvertida para nosotros. El control de direcciones MAC en el envío de información puede ser una manera de minimizar el riesgo.

7. Seguridad en los accesos a los sistemas

Además de los riesgos que puedan provenir de los dispositivos físicos (servidores, puesto de trabajo del usuario, equipos microinformáticos, el sistema de comunicaciones), existen otros inherentes en el acceso proporcionado al usuario para interactuar con el sistema y frente al cual se identifica. Una política errónea en el control y gestión de accesos de los usuarios representa un problema grave de seguridad. En este apartado se analiza este aspecto junto a los mecanismos de protección mas utilizados.

7.1 Tipos y perfiles de usuario

No todos los usuarios realizan las mismas funciones y por lo tanto es preciso definir tipos básicos y con ello perfiles de usuario. De entrada se puede hacer una distinción entre perfil técnico y perfil funcional, aunque resulta excesivamente genérica, por lo que obviaremos esta distinción en la clasificación siguiente

- *Administrador de sistema*. Es el tipo de usuario más relevante, que a priori dispone de un nivel de privilegios que puede configurar y controlar el sistema informático por completo (usuario, recursos, conectividad). Este grupo admite a su vez diferentes grados:
    - *Administrador*, propiamente dicho o "superusuario". Son usuarios que disponen de todos los permisos del sistema y están capacitados para poder aplicar configuraciones y correcciones, así como instalaciones en el mismo. Su labor comprende tanto la gestión de usuarios como el control de los recursos del sistema.
    - *Operador*. Realiza labores rutinarias (copias de seguridad, determinadas monitorizaciones de actividad, comprobación de registros de actividad, etc.) accediendo a una información limitada del sistema. No permite hacer cambios en las configuraciones del núcleo del sistema (core), pero sí realizar funciones básicas de control dirigidas a monitorizar tareas de mantenimiento del sistema. Realiza acciones delegadas por los administradores.

- *Administrador de Base de Datos (DBA)*. Es un usuario autorizado a realizar todas las operaciones de control y administración en el SGBD (Sistema Gestor de Base de Datos). Encargado de administrar las diferentes bases de datos del sistema informático. Sus funciones incluyen la monitorización de los recursos de la base de datos, los accesos a la base de datos, control de consultas, mantenimiento del esquema o diccionario, etc.
- *Usuario de aplicación*. Es el usuario final que tiene autorización para utilizar el software de aplicación previsto por la organización y que puede estar instalado en un sistema central o incluso en su sistema local. Se trata del usuario más limitado, pero que dentro de cada aplicativo informático puede tener otorgados diferentes privilegios. En una aplicación intervienen distintos componentes aunque básicamente esos elementos son dos: el gestor de base de datos (como Informix, Oracle, Ms-SQL, ...) y los programas que realizan los accesos a esa base de datos. Según este modelo puede haber un perfil que permita la visualización de información, listados, estadísticas, ..., distinto de aquel otro que además puede modificarla, crearla e incluso borrarla.

Si resulta importante definir bien los perfiles de usuarios, lo es más el mantenimiento actualizado de usuarios con sus perfiles asociados; un sistema puede tener bien definidos los perfiles, pero si la gestión de usuarios (altas, bajas y modificaciones) no está controlada, el sistema informático es inseguro.

Esta gestión, a veces compleja, se debe realizar de la manera más escrupulosa posible; por ejemplo, un usuario que causa baja en la organización, debe perder todos los derechos de acceso al sistema informático en el momento en el que se produce tal situación. Cada usuario debe tener única y exclusivamente privilegios de acceso únicamente a aquella información y recursos que resulten necesarios para desempeñar su trabajo.

La única forma de salvaguardar esta seguridad es mediante procesos regulares de auditoria informática (manual o automáticamente) sobre los accesos al sistema, los tipos de usuario, perfiles, etc. En estos procesos debe estar presente la revisión de los privilegios de cada uno de los usuarios sin entrar en el detalle de sus accesos (se puede consultar si un usuario ha accedido a Internet, pero no que lo ha hecho a una web en especial). Para esto último se pueden habilitar alarmas destinadas a los mecanismos de monitorización de los administradores.

Otro punto a tener en cuenta es la longitud de las claves de acceso. No debieran medir menos de seis caracteres, entremezclados sin sentido alguno y utilizando mayúsculas y minúsculas indistintamente. Desgraciadamente esta regla no siempre se cumple (por presiones del usuario, desidia, etc.). Otro aspecto importante es la obligatoriedad de que el usuario cambie su clave periódicamente.

La periodicidad del cambio es directamente proporcional a la seguridad, es decir, a mayor frecuencia mayor seguridad.

7.2 Control de Actividad

Como en otras disciplinas, el conocimiento y diagnóstico temprano de un problema, supone una solución más sencilla y rápida. La consulta habitual de los registros de actividad de usuarios en el sistema redunda en un sistema más seguro tanto desde el punto de vista físico como lógico.

Es importante disponer de herramientas que permitan monitorizar la actividad y conocer el estado del sistema puntualmente; por ejemplo, si un usuario ha lanzado un proceso que está bloqueando al resto por consumir muchos recursos o por haber instalado "ilegalmente" un programa que genere ese bloqueo, debemos hacernos eco de ello cuanto antes para que tenga una solución lo más inmediata posible y con las mínimas consecuencias tanto para el propio sistema (resto de usuarios) como para otros sistemas dependientes.

Los controles "mínimos" que se debieran hacer en cualquier sistema informático en relación a los usuarios son los siguientes.

- *Monitorización de las actividades***.** Este control se lleva a cabo a través de los registros de actividad de usuario. Los registros son una sucesión de líneas en las que quedan identificadas las operaciones realizadas, el momento horario, el usuario que accede, el equipo origen y opcionalmente la carga de trabajo del sistema y otros indicadores. Un usuario, inocentemente o no, puede ejecutar un programa de terceros que genere un malfuncionamiento en el sistema informático al que está conectado. Las consecuencias pueden ser muy importantes, pero si estamos alerta podemos mitigar su gravedad.
- *Trazabilidad***.** Detectado un problema, es preciso identificar su origen para lo cual es necesario habilitar mecanismos de rastreo. Para realizar esa operación es necesario disponer de "pistas". Esas pistas son constituidas por la unión del registro de actividad y el registro de accesos.
- *Registro de accesos***.** Cuando un usuario accede a un sistema, es necesario registrar ese acceso. Su finalidad es conocer que usuarios están o se han conectado al sistema en un momento dado y relacionarlo con las actividades y procesos que se han ejecutado. La actual Ley de Protección de Datos (LPD) obliga a registrar todos los accesos.
- *Posibilidad de bloqueo***.** En algunas situaciones, es necesario tener la posibilidad de bloquear al usuario. El bloqueo puede ser de distintos tipos:

- Bloqueo aislado es aquel motivado como reacción a un problema concreto en el sistema (p.e., excesivo consumo de recursos) y se tienen que eliminar (*kill*) los procesos de un usuario.
- Bloqueo temporal es aquel realizado durante un tiempo limitado debido normalmente a labores de mantenimiento en el sistema aunque también puede estar relacionado con el uso indebido del sistema por parte de un usuario.
- Bloqueo total es cuando se ha verificado que el usuario no debe seguir teniendo acceso al sistema (caso de bajas, si se observan dos o mas sesiones del mismo usuario desde dos o más equipos distintos).

7.3 Identificación versus Autenticación de usuarios

Los sistemas habitualmente utilizados para identificar a una persona, como son el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no es identificar a una persona, sino autenticar que esa persona es quien dice ser realmente.

Los métodos de autenticación se dividen en tres grandes categorías en función del criterio utilizado para verificar la identidad:

k) Algo que el usuario sabe (por ejemplo un password de Unix, o passphrase –PGP)

l) Algo que éste posee (por ejemplo una tarjeta de identidad, una huella digital, una tarjeta RFID)

m) Una característica física del usuario (por ejemplo la huella dactilar) o un acto involuntario del mismo (por ejemplo al firmar, que no se piensa en el diseño de cada trazo individualmente). Esta última categoría se conoce con el nombre de autenticación biométrica

En la práctica, el mecanismo para dar autenticidad a un documento o valor que mayor progresión está experimentando nos lo ofrece el certificado digital. Un certificado digital es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC). Como tanto el emisor como el receptor confían en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad. Una de las certificaciones más usadas y que en la actualidad resulta un estándar en infraestructuras de clave pública PKIs (Public-Key Infrastructure) es X.509.

También merecen una reseña los dispositivos basados en claves de un solo uso, que se solicitan al usuario en el momento de autenticarse. Basados en algo que posee y que genera una clave cuando se solicita y la debe introducir en el sistema como un nivel más de seguridad.

Normalmente los sistemas de autenticación que se utilizan cotidianamente no emplean método único, sino una combinación de estrategias logrando con ello incrementar su fiabilidad (por ejemplo la tarjeta de crédito junto a una contraseña o PIN utilizados en los cajeros automáticos bancarios).

En cualquier caso, un sistema de autenticación demostrará su eficacia en la medida que sea fiable, resulte económicamente asequible para la organización, soporte un cierto nivel de ataques y sea aceptado por quien lo usa.

Atendiendo a esta última clasificación, se distinguen tres mecanismos diferenciados de autenticación de usuarios.

Sistemas basados en algo conocido: contraseñas

El modelo de autenticación más común se basa en decidir si un usuario es quien dice ser si aporta una prueba de conocimiento avalada por una contraseña secreta que únicamente sólo él puede superar.

Es el sistema más vulnerable a todo tipo de ataques, pero también resulta el más barato y por ello es la técnica más ampliamente utilizada en entornos que no precisan una seguridad elevada. La mayoría de los sistemas operativos actuales lo incorporan y se puede aplicar en las aplicaciones que demandan alguna identificación de usuarios. También se encuentra complementando a otros mecanismos de autenticación, como el ejemplo descrito del PIN en las tarjetas de cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) acuerdan una clave secreta. Cuando una de las partes desea autenticarse ante otra, le muestra su conocimiento de esa clave común y si es correcta se le otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior.

Este mecanismo resulta muy fácil de romper, dado que es suficiente que una de las partes no mantenga el secreto de la contraseña para que toda la seguridad del modelo se pierda. Y esa pérdida puede venir de la comunicación de contraseña a un tercero o de la rotura del cifrado. En cualquiera de los casos un intruso puede suplantar la identidad del usuario y autenticarse ante el sistema con la identidad de un usuario que no le corresponde.

Sistemas basados en algo poseído

El ejemplo más representativo de este grupo lo constituyen las tarjetas inteligentes.

Una tarjeta inteligente (o *Smart Card*), es un sistema portador de información electrónica resistente a la adulteración, que utiliza como soporte una tarjeta de plástico con un circuito integrado (chip) incrustado, que ofrece funciones para el almacenamiento seguro de información, puede implementar un sistema de ficheros cifrado y funciones criptográficas y además detectar activamente intentos no válidos de acceso a la información almacenada. El chip inteligente es el elemento diferencial frente a las tarjetas de crédito convencionales que únicamente incorporan una banda magnética en la que almacenan cierta información del propietario de la tarjeta.

Cuando el usuario poseedor de una tarjeta inteligente desea autenticarse debe introducir la tarjeta en un *hardware* lector. Los dos dispositivos se reconocen entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave (CK o CCK, *Company Key* o *Chipcard Communication Key*), lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía; además esta clave puede utilizarse para asegurar la comunicación entre la tarjeta y el dispositivo lector. Tras identificarse las dos partes, se lee la identificación personal (PID) de la tarjeta y el usuario teclea su PIN; se inicia entonces un protocolo desafío-respuesta: se envía el PID a la máquina y ésta desafía a la tarjeta, que responde al desafío utilizando una clave personal del usuario (PK, *Personal Key*). Si la respuesta es correcta, el ordenador ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido.

Entre las ventajas que aporta la tarjeta destacan:

- que es un modelo aceptado universalmente
- es rápido
- incorpora *hardware* seguro, tanto para almacenar datos como para realizar funciones de cifrado
- sirve tanto para controles de acceso físico como para controles de acceso lógico a los ordenadores
- convive y se integra fácilmente con otros mecanismos de autenticación como las contraseñas
- resulta fácil bloquear el acceso de un usuario; basta con que el lector retenga la tarjeta cuando se introduce en el lector y/o marcarla como inválida en una base de datos (por ejemplo, mecanismo de bloqueo en los cajeros automáticos cuando se teclea erróneamente el PIN varias veces).

Por el contrario, sus principales inconvenientes radican en el coste adicional que suponen las tarjetas y los dispositivos lectores, así como la imposibilidad de acceder al sistema si se produce la pérdida o extravío de la tarjeta, o la vulnerabilidad frente a determinados métodos de ataque basados en ingeniería inversa - destructiva contra el circuito de silicio.

Sistemas de autenticación biométrica

Los sistemas biométricos hacen uso de características físicas del usuario para autenticarlo.

Esta autenticación existe desde siempre y es la utilizada en mayor número de situaciones cotidianas. Incorporado este concepto en la tecnología (con ayuda de la inteligencia artificial, el reconocimiento de formas y del aprendizaje) está llamado a convertirse en el modelo de autenticación de usuarios del futuro. Los sistemas resultan más cercanos al usuario y son más difíciles de falsificar que una simple contraseña o una tarjeta magnética. Las principales razones por la que no se han impuesto hay que buscarlas en su elevado precio y en su dificultad de mantenimiento.[5]

Aunque cualquier característica única del individuo que pueda ser medible es potencialmente valida para autenticarlo, lo habitual es trabajar con cinco grandes grupos:

- Verificación de voz: en los sistemas de reconocimiento de voz no se intenta reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser.

  El principal problema del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que se emplea en el protocolo de verificación de voz. Por el contrario posee una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces o se les niegue un acceso porque no se les reconoce correctamente

[5] En Emiratos Arabes Unidos, para acceder al Aeropuerto se utiliza un sistema de reconocimiento del iris. Se permite el acceso de pasajeros una vez sometidos al escaneado del iris y realizada la comparativa en una base de datos de personas non-gratas.

- Verificación de escritura: el objetivo no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

  En los modelos biométricos se utiliza además de la forma de firmar, las características dinámicas (*Dynamic Signature Verification*, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo.

- Verificación de huellas: típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Desde el siglo pasado hasta nuestros días se vienen realizando clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

  El mecanismo se basa en extraer de la imagen dactilar las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que el sistema tiene en su base de datos. El sistema por tanto no analiza la huella sino la posición relativa de cada una de las minucias.

  Los sistemas basados en reconocimiento de huellas son relativamente baratos en comparación con otros biométricos, como por ejemplo los basados en patrones retinales; sin embargo, tienen en su contra la problemática de autenticar usuarios que presenten heridas quemaduras o daños en el dedo a reconocer. Existe un factor psicológico contra estos sistemas, ya que generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

- Verificación de patrones oculares. Se utiliza desde dos tecnologías diferentes: análisis de patrones retinales (forma de los vasos sanguíneos de la retina humana) y análisis del iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

  Las desventajas de los métodos basados en el análisis de patrones oculares son su escasa aceptación, el coste elevado y la lentitud del proceso de autenticación.

  La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales y desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios La empresa estadounidense *IriScan* es la principal

desarrolladora de tecnología (y de investigaciones) basada en reconocimiento de iris que existe actualmente, ya que posee la patente sobre esta tecnología.

- Verificación de la geometría de la mano: Son los más rápidos de los sistemas biométricos; en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser con una probabilidad de error aceptable en la mayoría de ocasiones.

  Uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es su capacidad de aprendizaje: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida). Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica:

- *Captura* o lectura de los datos que el usuario somete a validación.
- *Extracción* de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar).
- *Comparación* de las mismas con las guardadas en una base de datos.
- *Decisión* de acerca de la validez o no del usuario.

En la siguiente tabla se muestra una comparativa de los rasgos más generales de los distintos sistemas biométricos:

MÉTODOS ASPECTOS	**Ojo – Iris**	**Ojo - Retina**	**Huellas dactilares**	**Geometría de la mano**	**Escritura - Firma**	**Voz**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta

Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación/ autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firma fácil o cambiante	Ruido, resfriados .. .
Utilización	Instalaciones nucleares, servicios médicos, penitenciarías	Instalaciones nucleares, servicios médicos, penitenciarías	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio x nodo	Alto	Alto	Bajo	Medio	Bajo	Bajo

Tabla 7A- Comparativa de métodos biométricos

Sistemas de Autenticación basados en LOGIN, NIS y LDAP

Hasta ahora hemos abordado la autenticación del usuario desde el punto de vista individual, pero desde una perspectiva de red, con elevado número de nodos, y complejas relaciones de accesos y privilegios (el ejemplo mas típico es Internet) es donde aparecen mecanismos especiales tendentes a garantizar la autenticación de los nodos de la red (en cuanto a pertenencia de las organizaciones) y de sus usuarios.

A diferencia de los sistemas basados en LOGIN o contraseña, donde el usuario basa su autenticación en la posesión de una información (palabra clave) que presenta a un equipo para que éste le valida el acceso, los sistemas NIS y LDAP surgen para solucionar la gestión de nombres, usuarios y grupos de usuarios en redes con gran número de nodos.

La solución NIS (*Network Information Service*, desarrollado por SUN Microsystems en los 80) incorpora en su diseño un sistema cliente-servidor por el cual la información se almacena en un único lugar y se transmite a los clientes de la red. Este sistema se mejora posteriormente con el NIS+ que distingue diferentes tipos de acceso dependiendo de la confidencialidad de los datos e incluye un sistema en el cual los clientes pueden verificar la autenticidad del servidor. Este concepto propietario

evoluciona para crear un estándar, que es el x.500 o servicio de directorio, en el cual la información se organiza jerárquicamente. Los niveles de jerarquía se identifican mediante etiquetas, y esto permite realizar en el servidor búsquedas inteligentes de información.

El siguiente paso a la definición del estándar x.500 fue la creación de un protocolo denominado DAP (*Directory Acces Protocol*) para permitir a clientes el acceso a la base de datos. El protocolo LDAP aparece como una solución de compromiso combinando el acceso a directorios x.500 a través de redes basadas en TCP/IP. Hoy en día LDAP ("Lightweight Directory Acces Protocol", ó Protocolo Ligero de Acceso a Directorios) se ha convertido en la opción mas adecuada para los servicios de directorio.[6]

Una de las utilidades de los sistemas LDAP es proporcionar una base de datos de usuarios distribuida, con datos de interés como pueden ser direcciones de correo electrónico, tipo de actividad, etc., si bien la utilidad mas importante en relación a la seguridad, es como servidor de autentificación. En este caso, es utilizado como repositorio de información del registro de sucesos (usuarios y claves) que permite la implantación de una autenticación única y consistente para todos los servicios teleinformáticos ofrecidos desde una organización (por ejemplo la sanitaria).

8. Resumen y conclusiones

La tecnología ha facilitado en cada momento de la historia mecanismos que han permitido proteger y garantizar la seguridad de la información. Hoy en día, cualquier proyecto de sistemas de información sanitarios requiere un tratamiento escrupuloso e intenso de la seguridad de la información debido a la utilización de datos sensibles.

Los problemas asociados con la seguridad informática no pueden ser tratados individualmente ya que la fragilidad final del sistema quedará condicionada por la del punto más débil.

Es preciso abordar la seguridad desde distintos planos tecnológicos como son: los soportes y dispositivos informáticos, los sistemas de información y los datos, los periféricos, los sistemas de comunicación y los puestos clientes donde se encuentra el usuario.

---

[6] Cada item (entrada) en el directorio LDAP describe un objeto (por ejemplo: una persona, un recurso de red, una organización) y tiene un único identificador (DN, Distingued Name). La entrada consiste de una colección de atributos (por ejemplo una persona podría tener apellido, organización, e-mail). Para encontrar las entradas hay que navegar a través del Arbol de Información de Directorio (DIT, Directory Information Tree). En la raíz

En cada uno de los niveles intervienen múltiples amenazas, muchas de ellas potenciadas y favorecidas a raíz de entender la sociedad de la información como una sociedad global y abierta, conectada en red. La tecnología actual permite distintos y múltiples mecanismos para mitigar el efecto, si bien el factor que sigue siendo crucial y esencial en la prevención, sigue siendo humano y reside en la sensibilidad de las personas que utilizan las TIC para acceder a información, máxime cuando ésta contiene datos personales que deben ser especialmente protegidos.

En general la efectividad de las medidas protectoras no están en el empleo de tal o cual programa de prevención, o en tal o cual dispositivo hardware, o en tal o cual tecnología, sino en el uso razonable de los sistemas informáticos por parte de los usuarios, en la vigilancia permanente tanto por parte de estos últimos como por parte de los técnicos administradores de los sistemas y en el control actualizado permanente de los mecanismos de seguridad establecidos.

El conocimiento de la Organización y de los sistemas teleinformáticos instalados por parte del personal técnico responsable de su administración contribuye asimismo a minimizar los riesgos. La instalación de programas o funcionalidades en los sistemas informáticos debe de ser una tarea supervisada por el personal técnico responsable de dichas tareas y es necesario que sean lo suficientemente evaluados y contrastados sus efectos y funcionalidades antes de instalarlos. Asimismo, calibrar la utilidad de los nuevos programas para la Organización antes de proceder a instalarlos, es una medida preventiva a considerar.

La Tabla 7B, resumen de lo expuesto a lo largo del capítulo, enumera un conjunto de peligros y amenazas potenciales al alcance de los sistemas y tecnologías de la información, junto a los aspectos de seguridad en los que inciden (confidencialidad, integridad, disponibilidad), y algunas respuestas para solventar o minimizar sus riesgos.

PROBLEMAS POTENCIALES	ASPECTO SOBRE EL QUE INCIDE	TECNOLOGÍAS/ SOLUCIONES DISPONIBLES
1.- Desastres naturales	INTEGRIDAD	1. Diseño y elección de CPD e instalaciones asociadas. 2. Infraestructuras críticas redundantes y tolerantes a fallos.

del árbol se encuentra El Mundo, el cual esta subdividido en el siguiente nivel en países, y en el siguiente en organizaciones. Dentro de las organizaciones se almacenan información de personas, recursos, etc.

PROBLEMAS POTENCIALES	ASPECTO SOBRE EL QUE INCIDE	TECNOLOGÍAS/ SOLUCIONES DISPONIBLES
2.- Ataques de intrusión física por personal no autorizado	INTEGRIDAD CONFIDENCIALIDAD	3. Aplicar medidas de control de acceso del personal técnico al hardware. 4. Controlar el acceso del personal de servicio a las salas técnicas: mantenimiento, limpieza, etc.
3.- Fallos en el hardware y software de base	INTEGRIDAD DISPONIBILIDAD	5. Utilizar técnicas de "clustering" en los sistemas informáticos. 6. Aplicar técnicas de respaldo y técnicas de restauración (copia de seguridad). 7. Infraestructuras críticas redundantes y tolerantes a fallos (eléctricas, comunicaciones, etc.).
4.- Borrado de datos (voluntario o involuntario)	INTEGRIDAD DISPONIBILIDAD	8. Emplear técnicas RAID en el almacenamiento. 9. Utilizar técnicas de protección y de seguridad de los programas y datos: sistemas antivirus, anti-malware, antispam, IDS/IPS. 10. Las indicadas en el problema nº 3
5.- Ataques a programas y datos mediante virus, gusanos, otros específicos de internet (Spyware, Keyloggers), Backdoors, Exploits, Shellcodes, Rootkits)	INTEGRIDAD	11. Limitar el acceso a los sistemas informáticos críticos a la línea de comandos. 12. Control de acceso solo a los administradores. 13. Resúmenes HASH de los programas críticos, y auditarías periódicas. 14. Chequeos de los permisos de los programas.
6.- Ataques a la información mediante criptoanálisis	CONFIDENCIALIDAD	15.Técnicas de cifrado (criptografía moderna): métodos simétricos (clave secreta), métodos asimétricos (clave publica).
7.- Vulnerar los cifrados de información mediante ataques de fuerza bruta	CONFIDENCIALIDAD	16. Mejorar capacidad de cifrado del algoritmo. 17. Empleo de técnicas de estenografía (aumenta la seguridad del mensaje cifrado)
8.- Ataques al puesto de trabajo (terminal de usuario), y a su información.	CONFIDENCIALIDAD INTEGRIDAD	18. Emplear "cajas" con cerradura o sistema de anclaje 19. Vigilar controles de seguridad sobre la BIOS. 20. Anular (en su caso tener controlados) los puertos de salida de información: USB, disqueteras, CD,

PROBLEMAS POTENCIALES	ASPECTO SOBRE EL QUE INCIDE	TECNOLOGÍAS/ SOLUCIONES DISPONIBLES
		etc. Controlar los puertos USB-U3. 21.Conocer las limitaciones de los sistemas operativos en el tratamiento de estos puertos (Windows XP, Linux, ...) 22.Emplear sistemas de almacenamiento centralizado seguros (NAS, SAN, DAS) y acceso remoto, frente a gestión local en el terminal.
9.- Robo de terminal portátil	CONFIDENCIALIDAD DISPONIBILIDAD	23. Evitar datos estratégicos en el terminal, usar sistemas centralizados, y acceder en remoto. 24. Proteger datos locales mediante encriptación.
10.-Accesos no autorizados y ataques sobre dispositivos de mano: Pocket, PALM, etc.	CONFIDENCIALIDAD DISPONIBILIDAD	25. Mismo que portátiles 26. No mantener datos estratégicos en el terminal. 27. Las indicadas en el problema nº 9
11.- Accesos no autorizados y robo de Teléfonos móviles y SmartPhones	CONFIDENCIALIDAD DISPONIBILIDAD	28. Formación en las funcionalidades del terminal. 29. Activar la tecnología (ej. Bluetooth) sólo cuando se precise 30. Las indicadas en problema nº 9
12.- Keycatchers (llaves entre teclado y ordenador)	CONFIDENCIALIDAD	31. Inspección ocular
13.- Ataques al canal y sistema de comunicaciones	CONFIDENCIALIDAD INTEGRIDAD	32.Diseño adecuado de red (arquitectura, topología). 33. Utilización de firewalls (al menos para controlar internet). 34. Análisis de red mediante herramientas de gestión. 35. Control de direcciones MAC en los equipos emisores de información.
14.- Ataques a la Identidad (ataques a la seguridad del usuario)	CONFIDENCIALIDAD	36. Definir perfiles de usuario y roles 37.Actualización de permisos (altas, bajas, modificaciones). 38. Claves de acceso personalizadas. 39. Controlar magnitud de las claves. 40. Cambio periódico de contraseñas.

PROBLEMAS POTENCIALES	ASPECTO SOBRE EL QUE INCIDE	TECNOLOGÍAS/ SOLUCIONES DISPONIBLES
		41. Control de actividad de los usuarios: monitorización, trazabilidad, registro de accesos.
15.- Suplantación de la Identidad	CONFIDENCIALIDAD NO REPUDIO	42. Empleo de mecanismos de autenticación combinados: basados en contraseña (PIN, PGP), basados en tarjeta inteligente, biométricos. 43. Empleo de mecanismos de gestión de identidades (NIS o LDAP) en todos los servicios teleinformáticos.

TABLA 7B -Resumen de amenazas y tecnologías de seguridad

Bibliografía y referencias

1. Chris McNab . “Técnicas y herramientas avanzadas para la evaluación de seguridad de redes”. Editorial Anaya Multimedia - O'Reilly . ISBN:84-415-1751-7

2. Nitesh Dhanjani . “Claves Hackers en Linux y Unix” . Editorial Mc Graw Hill. ISBN:84-481-4050-8

3. Andrew S. Tanenbaum . ”Redes de computadoras. Editorial Pearson “– Prentice Hall. ISBN:970-26-0162-2

4. Ministerio de Administraciones Públicas (MAP). Aplicaciones utilizadas para el ejercicio de Potestades. Criterios de Seguridad.. Junio 2004. NIPO 326-04-044-9

5. Antonio Villalon Huerta. “Seguridad en Unix y Redes”. Universidad Politécnica de Valencia (UPV). Julio 2002

6. KRIPTÓPOLIS: **http://www.kriptopolis.org**

7. WIKIPEDIA: **http://es.wikipedia.org**

8. Revista HACKIN9: **http://www.hakin9.org**

9. Sourceforge: **http://www.sourceforge.net**

10. Insecure.org: **http://www.insecure.org**

11. CyberSeguridad: http://www.cyberseguridad.org

12. IriScan: http: //www.iriscan.com/

13.IrisCERT: http://www.rediris.es/cert/

7 Glosario de términos

Autenticación: acto de confirmación de la identidad de una persona.

Clinical Document Architecture (CDA): estándar abierto que especifica la estructura y la semántica de los documentos médicos, para un intercambio más eficaz entre sistemas de información clínica de naturaleza diferente. Está basado a su vez en el estándar XML.

Cluster: arquitectura informática orientada a aumentar la escalabilidad, disponibilidad y fiabilidad de los datos y de las aplicaciones que los gestionan. Habitualmente está integrada por dos o más computadoras independientes (también denominados nodos), interconectadas mediante enlaces de alta velocidad, que aparecen ante el usuario como un único sistema.

Conmutador (Switch): equipo de comunicaciones que se encarga de distribuir ó repartir los paquetes que se envían entre equipos pertenecientes a una misma red. Algunos conmutadores son capaces de realizar la tarea del encaminador.

Consentimiento escrito: procedimiento formal para la aplicación del principio de autonomía del paciente, cumpliendo los requisitos de información, comprensión y voluntariedad por parte de éste. Es decir, el paciente debe contar con toda la información, comprenderla en su totalidad y decidir libremente si se somete o no a un proceso clínico, y si da su autorización para el registro y tratamiento de los datos generados durante el mismo.

DAS (Direct Attached Storage): es el método tradicional de almacenamiento y el más sencillo. Consiste en conectar el dispositivo de almacenamiento directamente al servidor o estación de trabajo, es decir, físicamente conectado al dispositivo que hace uso de él.

Deontología: ciencia de los deberes profesionales.

Despersonalización de la información clínica: proceso mediante el cual se garantiza la imposibilidad de relacionar un conjunto de datos clínicos con el paciente al que pertenecen.

Dirección de broadcast: dirección de multidifusión. La utilizan algunos programas para distribuir una petición en una red a todos los elementos que la componen.

Direccionamiento IP: numeración consistente en 4 grupos de 8 bits escrito en decimal y separados por puntos (32 bits), que identifica un único elemento en una red. Se divide en dos partes: la primera identifica la red a la que pertenece y la segunda el número de elemento dentro de esa red. La primera es asignada por el NIC (Network Information Center) y ocupa 8, 16 o 24 bits (Clases A, B y C, respectivamente).

Encaminador (Router): elemento capaz de direccionar los paquetes que le llegan hacia un host destino. Conectan redes distintas y encaminan los paquetes entre ellas. Habitualmente se utiliza para conectar una LAN a una WAN.

Enfermedad presintomática: enfermedad que se diagnostica antes de que se manifiesten los síntomas. Término usado frecuentemente en enfermedades genéticas.

eXtensible Markup Language (XML): conjunto de reglas para definir etiquetas semánticas que permiten organizar un documento en diferentes partes. Se trata de un metalenguaje que define la sintaxis utilizada para definir otros lenguajes de etiquetas estructurados.

Farmacogenómica o farmacogenética: caracterización fenotípica y genotípica de los polimorfismos genéticos implicados en el metabolismo de fármacos y en receptores dirigidos a una monitorización de los sujetos sanos o enfermos participantes en ensayos clínicos.

Gestión de identidades: conjunto de procedimientos para la creación, asignación, modificación, suspensión y eliminación de los privilegios correspondientes a los diferentes perfiles de usuario que rigen el acceso a un sistema o servicio.

Health Level 7 (HL7): estándar para el intercambio de información de carácter clínico, desarrollado por el American National Standards Institute (ANSI).

Historia Clínica Electrónica (HCE): conjunto de toda la información generada durante los procesos de asistencia a un paciente, referida a su salud y almacenada en soporte electrónico.

IDS (Intrusion Detection Systems): la detección de intrusos consiste en un conjunto de métodos y técnicas para revelar actividad sospechosa sobre un recurso o conjunto de recursos computacionales, es decir, eventos que sugieran comportamientos anómalos, incorrectos o inapropiados sobre un sistema entendido como el ente que está siendo monitorizado. Un IDS es una herramienta de apoyo en procesos de auditoria, entendida como el control del funcionamiento de un sistema a través del análisis de su comportamiento interno.

IPS (Intrusion Prevention Systems): son dispositivos de hardware o software encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta usualmente consiste en descartar los paquetes involucrados en el ataque o modificarlos (*scrubbing*) de tal manera que se anule su propósito. Este comportamiento los clasifica como dispositivos proactivos debido a su reacción automática a situaciones anómalas.

LDAP (Lightweight Directory Access Protocol): es una versión "aligerada" del protocolo DAP, de modo que sea posible su utilización en redes TCP/IP. Implementa un servicio de directorio

jerárquico y distribuido para acceder a repositorios de información referente a usuarios, contraseñas y otras entidades en un entorno de red, ofreciendo una amplia capacidad de filtrado y mecanismos de seguridad sobre la información.

MAC (Media Access Control address): identificador, único en el mundo, consistente en un número de 48bits representado en notación hexadecimal que es almacenado por el fabricante dentro de la tarjeta de red o interfaces de red.

Malware: todo tipo de software malicioso o código malicioso. Los virus son la principal forma de Malware, pero no la única

Máscara de subred: mecanismo para acotar el número de nodos que existen en una red. Cuando se especifica una red se hace a través de una dirección IP y la máscara de subred.

MD5 (Message-Digest Algorithm 5): es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Se usan extensamente para proporcionar seguridad de que un archivo descargado de Internet no ha sido alterado.

Monitorización: posibilidad de conocer de manera inmediata el estado actual del sistema.

NAS (Network Attached Storage): es un dispositivo de almacenamiento que se conecta directamente a una red local (LAN), normalmente Ethernet, dispone de una dirección IP propia, y permite compartir su almacenamiento desde múltiples servidores conectados a la red.

NIS (Network Information Service): es un servicio que proporciona información, que tiene que ser conocida por toda la red, a todas las máquinas de la red. Se emplea para centralizar ficheros de configuración (por ejemplo de usuarios) que se encuentran replicados en los distintos nodos de la red, en una sola máquina y bajo una administración única.

Paquete: tamaño mínimo de información transmitida por la red. Un mensaje habitualmente consta de múltiples paquetes. A veces, llamado datagrama.

Patografía: descripción del curso de la enfermedad a lo largo del tiempo.

Protocolo: conjunto de especificaciones necesarias para que un cliente pueda acceder a la información que suministra un servidor. Un ejemplo lo tenemos la web que utiliza el protocolo http (Hyper Text Transfer Protocol).

RAM (Random Access Memory ó Memoria de acceso directo): área de la memoria de un ordenador que se usa para mantener los programas mientras se están ejecutando, y los datos mientras se los procesa.

Repudio: rechazo de la existencia de un hecho, de sus consecuencias y/o de la responsabilidad del mismo.

RFID (Radio Frequency Identification / Identificación por Radio Frecuencia): es una tecnología que permite el almacenamiento remoto y la recuperación de datos utilizando dispositivos denominados etiquetas o tags RFID.

SAN (Storage Area Network): es una red específica de almacenamiento y de altas prestaciones basada en tecnología fibre channel (canal de fibra). Su función similar a la del NAS y consiste en centralizar el almacenamiento de los archivos en una red de alta velocidad y máxima seguridad, se trata de una solución global donde se comparte todo el área de almacenamiento corporativo.

Sniffing: hace referencia a la realización de tareas de red empleando un sniffer. Un sniffer es un programa que captura todo el tráfico que pasa por la red, de forma que ejecutado sobre una red local, permite obtener información, por ejemplo pares de usuario:contraseña. Suele funcionar de forma pasiva, siendo muy difíciles de detectar, aunque existen algunas técnicas que permiten averiguar si existen espías en la red.

Spam (SPiced hAM) o "correo basura": es todo tipo de comunicación no solicitada, realizada por vía electrónica. Normalmente hace referencia a cualquier mensaje no solicitado y que generalmente tiene por objeto ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada es el correo electrónico.

Spyware: categoría de software malicioso. Son programas que rastrean los hábitos de comportamiento del usuario y su información personal para luego enviar esta información a terceros sin la autorización o conocimiento del mismo. Se instalan automáticamente en el ordenador, acompañando a otro de apariencia legal e inofensiva.

Tecnologías de la Información y las Comunicaciones (TIC): concepto que engloba al conjunto de tecnologías ligadas a la gestión y transmisión de la información, principalmente la informática y los sistemas de telecomunicación.

Telemedicina: medicina que se practica a distancia, sin que el paciente esté presente.

TCP/IP (Transport Control Protocol / Internet Protocol ó Protocolo de Control de Transmisión): protocolo de Internet.

UPS (Uninterruptible Power Supply): Sistema de alimentación ininterrumpida (SAI), es un mecanismo diseñado para proporcionar energía eléctrica de manera automática, sin retardo ni

transitorios, durante un período de tiempo en el cual el suministro normal de energía eléctrica no puede funcionar de manera aceptable

USB (Universal Serial Bus / Bus de Serie Universal): provee un estándar de bus serie para conectar dispositivos a una computadora (usualmente a un PC).

WEP (Wired Equivalent Privacy): es un protocolo de seguridad para redes inalámbricas WLAN definido en el Standard 802.11b y establecido en 1999 cuyo objetivo es proporcionar seguridad mediante el cifrado de datos. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas. Admite tres configuraciones: Off (ninguna seguridad), 64-bit (seguridad débil), 128-bit (seguridad algo mejor).

WPA (Acceso Protegido Wi-Fi): protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP, creado por la WiFi Alliance que incorpora un sistema de seguridad con encriptación de 128-Bits.

8 Los autores

Natxo Alamillo i Domingo

Licenciado en Derecho. Abogado del Ilustre Colegio de Madrid. Director del área de asesoramiento e investigación de la Agència Catalana de Certificació (desde finales de 2002).

Miembro del grupo directivo europeo de Seguridad de Redes y de la Información y del grupo directivo de la Iniciativa Europea de Normalización de la Firma Electrónica, asesorando a la Comisión Europea. Miembro del Consejo de Certificación de ASIMELEC.

Ha sido miembro del grupo directivo europeo de la Iniciativa Europea de Normalización de la Firma Electrónica, y del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones.

Autor de numerosas publicaciones y ponencias en firma electrónica y su campo de aplicación.

Óscar Blanco Ramos

Licenciado en Ciencias Físicas (Especialidad Electrónica y Computadores) por la Universidad de Cantabria, 1999.

Coordinador técnico del Proyecto de Historia Clínica Electrónica de Cantabria en la Oficina de Innovación de Sistemas de Información Sanitaria (ISIS) de la Consejería de Sanidad y Servicios Sociales del Gobierno de Cantabria, desde 2005.

Manuel Ramón Gutiérrez Covarrubias

Ingeniero Técnico en Informática de Gestión por la UOC, 2006.

Técnico en Informática del Hospital Universitario "Marqués de Valdecilla", desde 1991.

Pilar León Sanz es doctora en medicina y cirugía por la Universidad de Navarra. Ha compaginado puestos de gestión, con la docencia y la investigación. Actualmente es profesora titular de Historia de la Ciencia, directora del Departamento de Humanidades Biomédicas y subdirectora del Centro de Estudios Europeos de la Universidad de Navarra. Es miembro del Steering Committee del Proyecto Sócrates Comparative History of European Public Assistance.

Su investigación abarca la historia de las profesiones sanitarias y el origen y desarrollo de la ética biomédica. Entre sus publicaciones se cuentan: Vicente Ferrer Gorraiz Beaumont y Montesa (1718-1792), un polemista navarro de la ilustración (Pamplona, 2007). "Professional Responsibility and the Welfare System in Spain at the Turn of the 19th Century" (Hygiea *Internationalis,* 2006, 5(1): 75–90). "Profesión y asistencia médico-farmacéutica en los escritos de Jaime Vera, 1859-1918" (Dynamis, 2006, 26: 169-193); "El poder de los médicos. Un análisis de El ejercicio profesional de la medicina en nuestros días (Madrid, 1906)", (Estudos do Século XX, 2005, 5: 223-241); "La práctica de informar a los pacientes y a sus familiares a lo largo de los s. XIX y XX", en León Sanz, P., ed., La implantación de los derechos del paciente. Comentarios a la Ley 41/2002, (Pamplona, 2004, pp. 127-150); "La preocupación por la asistencia a los necesitados en la Navarra ilustrada: la obra del obispo Úriz" (Evora, 2004, pp. 197-223); "La consulta médica. Una práctica de la medicina del siglo XVIII" (Dynamis, 2002, 22: 279-301); "Medical Theories of Tarantism in Eighteenth-Century Spain" (London, 2000, pp. 273-292); "La confidencialidad del médico y la información debida a las entidades aseguradoras" (Revista de Medicina de la Universidad de Navarra 2000; 44 (1): 25-31).

Rafael Ortega García es licenciado en Ciencias Físicas y ha sido miembro del subcomité 27 AENOR de Certificación de Seguridad. Desde 2006 trabaja como Socio en el departamento de Technology and Security Risk Services (TSRS), dentro de Ernst & Young, desempeñando labores de dirección de negocio del área de integración de soluciones de seguridad. En su carrera profesional ha desempeñado los puestos de Director en Arthur Andersen, Deloitte y Vice-Presidente de Azertia.

Cuenta con 22 años de experiencia en proyectos relacionados con tecnología y riesgos, dirección tecnológica y medios y áreas de dirección de desarrollo de negocio.

Ha dirigido proyectos de Continuidad de Negocio, diseño y despliegue de Planes Directores de Seguridad, certificaciones ISO 27001, gestión de seguridad, proyectos tecnológicos de seguridad, estrategia de Firma Electrónica y proyectos de Seguridad en el Ciclo de Vida de Desarrollo.

Entre los clientes en los que ha prestado servicios destacan las más importantes empresas tanto nacionales como internacionales de los sectores financiero, asegurador, servicios, sector público y telecomunicaciones.

Cursos y seminarios:

- Ponente habitual en jornadas de seguridad e IT, colaborador de artículos en prensa y en revistas especializadas.
- Ponente en diversos seminarios de Auditoría (tanto internos como externos) de seguridad informática.
- Profesor de Tecnologías de la Información en el Master de Derecho de Nuevas Tecnologías de varios centros (CEU, Asimelec, ALI)
- Profesor de Seguridad en Nuevas Tecnologías en el Instituto de Empresa

David Rojas de la Escalera

Ingeniero en Telecomunicaciones (Especialidad Telemática) por la Universidad de Cantabria, 2003.

Coordinador técnico del Proyecto de Historia Clínica Electrónica de Cantabria en la Oficina de Innovación de Sistemas de Información Sanitaria (ISIS) de la Consejería de Sanidad y Servicios Sociales del Gobierno de Cantabria, desde 2005.

Ricardo Sáez Crespo

Licenciado en Ciencias Físicas (especialidad Electrónica) por la Universidad de Cantabria, 1985.

Master en Dirección de Sistemas y Tecnologías de la Información y de las Comunicaciones por la Universidad Politécnica de Madrid, 2004.

Jefe del Servicio de Informática del Hospital Universitario "Marqués de Valdecilla", desde 1991.