LA SEGURIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN CLÍNICA

José Antonio Garbayo Sánchez
Jokin Sanz Ureta
Dirección General para la Sociedad de la Información. Gobierno de Navarra

Javier Carnicero Giménez de Azcárate
Coordinador de los Informes SEIS

Carlos Sánchez García
Microsoft Ibérica

INTRODUCCIÓN

Para los médicos el deber de secreto de la información relacionada con los pacientes es tan antiguo como su profesión, como muestra el que esa obligación se encuentre presente entre las descritas en el Juramento Hipocrático. En la actualidad el deber de guardar secreto profesional incluye no sólo a los médicos sino al resto de personal, tanto sanitario como no sanitario, que se relaciona con los pacientes o que accede a la información relacionada con ellos. Ese deber, que obliga a todos, se refleja en la normativa de protección de datos, la normativa sanitaria e incluso el código penal.

Por otra parte, las organizaciones sanitarias tienen entre sus cometidos el preservar la información clínica íntegra y disponible para cuando sea necesaria, y accesible sólo a las personas autorizadas para ello.

La informatización de la historia clínica ha supuesto la introducción de las tecnologías de la información y de las comunicaciones en el núcleo de la actividad sanitaria. Este proceso ha traído consigo la integración de la información dispersa en varias bases de datos de los centros sanitarios, como las de los laboratorios clínicos y los programas de admisión. El siguiente paso ha sido la integración de la información clínica, correspondiente a una persona, que se encontraba ubicada en todos los centros sanitarios en que hubiera sido atendida.

Las tendencia actual es el acceso a la información clínica desde cualquier momento y lugar en el que pueda ser necesario para la debida atención del paciente, con independencia de en qué centro sanitario haya sido generada esa información.

La informatización de la historia clínica, que contiene información del ámbito de la intimidad de las personas, el posible acceso a esa historia desde otros lugares en que pueda ser necesario para atender a ese paciente y la creación de bases de datos centralizadas, generan inquietud por la seguridad y confidencialidad de esa información entre los médicos. Éstos se preguntan si se puede garantizar que esos datos no llegarán a manos de quien pueda utilizarlos con otros fines que aquellos para los que fueron recogidos: diagnosticar y curar a los pacientes (1-5).

Las inquietudes sobre la seguridad y confidencialidad de la información se pueden sintetizar en tres categorías:

– Técnicas: ¿Soporta la tecnología todos los requisitos de seguridad que deberían tener este tipo de sistemas?
– Organizativas: ¿Está la organización capacitada para gestionar esta información con todas las garantías?
– Legales: ¿Está respaldado legalmente el uso que se hace de todas esas herramientas y sistemas?

La seguridad y confidencialidad de la información exigen garantizar los siguientes aspectos de la información:

– Que está disponible. Es decir que cuando la necesitamos, podamos acceder a ella y utilizarla.
– Que a la información solo acceda quien está autorizado para ello y para el uso a que está autorizado. Se requiere identificar a la persona a la que se autoriza, a quien se le concede permiso para determinadas tareas. Son los procesos de identificación, autorización y asignación de perfiles y roles.
– Que la información se mantiene íntegra, es decir que no se ha transformado durante su almacenamiento o transporte. Es la característica de integridad.
– Que quien participe en una transacción no pueda negar haberlo hecho. Es la característica de no repudio.
– Que la organización pueda comprobar quién ha accedido a la información y en qué transacciones ha participado. Es el proceso de auditoría.

Las disposiciones legales en materia de seguridad, confidencialidad e historia clínica informatizada así como los aspectos técnicos y organizativos se tratan en el III Informe SEIS (6 - 8) y en el capítulo de "Aspectos legales de la historia clínica" de este V Informe. En el presente trabajo se revisan algunos de los aspectos técnicos, en especial el de la disponibilidad, que es el que con menos frecuencia se estudia. También se revisan los mecanismos de seguridad de los que se dispone actualmente para proteger los sistemas, se facilitan directrices sobre cómo conseguir un sistema seguro, tanto durante el diseño y construcción de un sistema nuevo, como en el caso de asegurar un sistema ya existente, y se explican los aspectos de operación y nivel de servicio que permiten mantener operativo un sistema de información.

MECANISMOS DE SEGURIDAD

La seguridad en un sistema de información debe contemplar todas las posibles amenazas que se identifiquen sobre todos los elementos del sistema de información: máquinas, programas, datos, redes y electrónica de red. Entre las amenazas se

encuentran las personas, tanto con carácter voluntario como involuntario, y las catástrofes, como los incendios e inundaciones.

La Tabla 1 muestra los objetivos de seguridad y las medidas o mecanismos de seguridad que existen para garantizar su cumplimiento. Los dos mecanismos básicos de seguridad son las claves públicas y privadas, y los algoritmos de resumen de una dirección. Estos son los fundamentos para la construcción del resto de mecanismos de seguridad. Mediante la combinación de todos ellos se consigue proteger los sistemas de información mediante el cifrado o encriptación, la firma y los certificados digitales. Estos son los mecanismos técnicos de protección de la información.

Los mecanismos básicos y técnicos se complementan con los de organización de autorización y auditoría, así como con los de operación y de nivel de servicio.

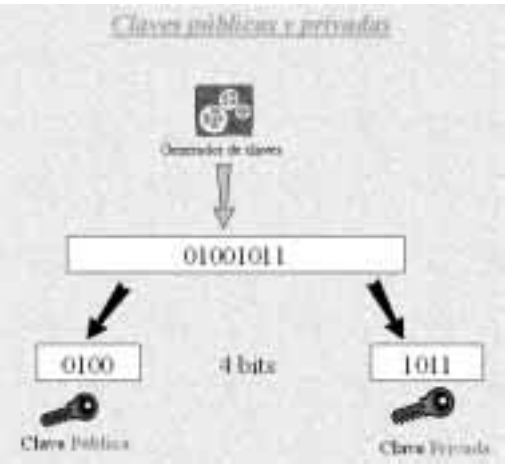
Tabla 1. Objetivos y medidas de seguridad

OBJETIVO	DESCRIPCIÓN	MEDIDAS
1. Identificación (Autentificación)	Es el proceso de identificar al cliente de la aplicación o servicio. No olvidar que los clientes pueden ser tanto personas, como otros servicios, procesos y otros ordenadores.	Certificados digitales.
2. Confidencialidad	Consiste en asegurar que a la información solo accede quien está autorizado para ello.	Cifrado, encriptación.
3. Integridad	Conjunto de acciones que garantizan que la información no se ha transformado durante su procesado, transporte o almacenamiento.	Firma digital.
4. No repudio	Procedimientos para asegurar que ninguna de las partes implicadas ya identificadas (autentificadas) puede negar haber participado en una determinada transacción.	Firma digital, auditoría.
5. Autorización	Determinar a qué información puede acceder y qué tareas puede acometer, un cliente autentificado, por lo tanto identificado con certeza. Este proceso determina los privilegios asociados a un perfil de usuario.	Cuestión organizativa que debe diseñar cada organización y llevar a cabo en sus sistemas particulares.
6. Auditoría	Es la posibilidad de poder rastrear los accesos realizados a la información y las operaciones hechas sobre ella por cada usuario y las circunstancias en que las hizo.	Registros de acceso y operaciones efectuadas sobre la información.
7. Disponibilidad	Forma parte de la seguridad el poder disponer de la información cuando se necesite. Por ello se deben proteger los sistemas de forma que se mantengan en funcionamiento y se pueda acceder a la información en cualquier momento.	Operación y nivel de servicio adecuados sobre los sistemas.

Claves públicas y privadas

Como ya se ha indicado, son mecanismos básicos de seguridad. Consisten en generar pares de claves, cada uno de los cuales está compuesto por la clave privada, conocida solamente por el propietario del par de claves, y la clave pública, que el propietario puede enviar a quien desee (Figura 1).

Figura 1. Claves públicas y privadas



Estos pares tienen las siguientes características:

– Están relacionadas pues la correspondencia entre ellas es única.

– No se puede deducir una a partir de la otra.

– La clave privada solo es conocida por su propietario y nunca se comparte.

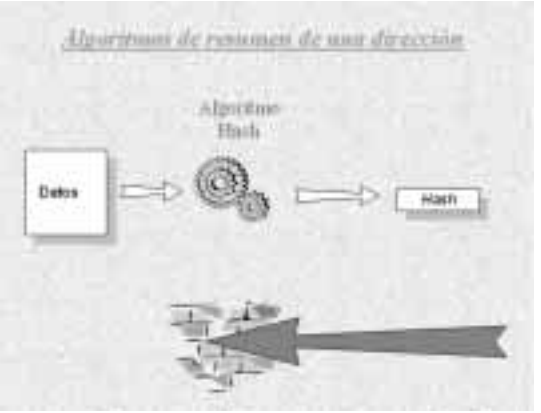
– La clave pública se distribuye y puede ser conocida por cualquiera que intervenga en una operación en la que se utilice estos mecanismos.

Las claves se generan mediante algoritmos matemáticos u otros dispositivos o técnicas, como tarjetas generadoras de claves.

Algoritmos de resumen de una dirección

Mediante un algoritmo matemático (hash) se genera un resumen de los datos (Figura 2).

Figura 2. Algoritmos de resumen de una dirección



Este resumen tiene dos características:

– Es imposible obtener el original a partir del resumen

– Es único, a partir de unos datos siempre se obtiene un resumen y solo ese resumen.

Como ejemplos de estos algoritmos se pueden citar:

– MD4 y MD5 (*Message Digest*) de 128 bits.

– SHA (*Secure Hash Algorithm*) de 160 bits.

También se puede obtener el resumen aplicando el algoritmo hash al conjunto formado por los datos originales más una clave. Un algoritmo de este tipo es el *MAC (Message Authentication Code)*.

Cifrado o encriptación

El cifrado o encriptación consiste en la transformación de una información de forma que solamente la entiendan el emisor y el receptor. Este se puede aplicar a cualquier tipo de información, como documentos, correo y formularios electrónicos entre otros.

Se distinguen dos tipos de cifrado:

Cifrado privado

El cifrado privado es el que se utiliza para la firma digital. En este proceso se encripta la información de forma que cualquiera que la reciba sea capaz de entenderla, pero lo que se asegura es que el emisor de la información es quien dice ser. Es decir, se garantiza el emisor de la información. Proporciona los mecanismos para que cualquiera pueda entender la información y comprobar que esta fue enviada realmente por quien dice ser el emisor.

En el punto correspondiente a la firma digital se describen en detalle los mecanismos de cifrado privado.

Cifrado público

El cifrado público es el cifrado clásico utilizado para enviar información cifrada entre dos extremos de forma que solamente estos extremos son capaces de entenderla. En este proceso se encripta la información para un destinatario concreto, asegurando que solo él podrá comprenderla. Lo que se asegura es que solo un destinatario, y exclusivamente ese destinatario, recibirá el mensaje de forma correcta. Por lo tanto, se asegura al destinatario de la información.

El detalle el proceso de cifrado público de la información es el siguiente:

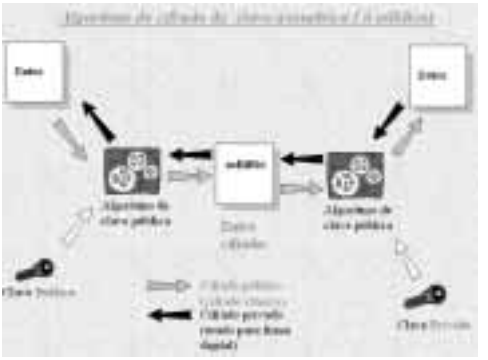
1. Para el envío del mensaje, el emisor cifra el mensaje utilizando la clave pública del receptor. Lo hace aplicando un algoritmo de clave pública a los datos y esta clave.
2. De esta forma se obtienen los datos cifrados, es decir, ininteligibles para cualquiera excepto los dos extremos de la comunicación.
3. En la recepción el receptor necesita descifrar el mensaje para entenderlo.
4. Para ello aplica un algoritmo de clave pública al conjunto de los datos cifrados y su clave privada (del receptor).

Es decir, que solo podrá descifrar este mensaje el receptor al que iba dirigido, pues solo él posee la clave privada necesaria para hacerlo.

Como ejemplos de algoritmos de clave pública se pueden citar RSA (Rivest-Shamir-Adleman [*public key encryption technology*]) y Diffie-Hellman.

En la Figura 3 se superponen los dos tipos de cifrado, el público y el privado para hacer más evidentes las diferencias y similitudes entre ambos.

Figura 3. Algoritmo de cifrado de clave asimétrica (o pública)



Algoritmos de clave privada o simétricos

También existen algoritmos de clave privada o simétricos, en los cuales el proceso de encriptación se realiza de la misma manera, pero utilizando solamente la clave privada del emisor. El receptor descifra la información utilizando también la clave privada del emisor, la cual le ha sido enviada previamente de alguna forma, es decir, existe solamente una clave que conocen ambos extremos de la conversación y que se utiliza tanto para cifrar como para descifrar.

Estos algoritmos se utilizan en circunstancias que requieran unos requisitos de seguridad no muy exigentes, ya que el envío de la clave requerida para el descifrado hace que las garantías de seguridad desciendan mucho. La única ventaja de este mecanismo es su velocidad, ya que al ser más simple se ejecuta con mucha más rapidez.

Ejemplos de este tipo de algoritmos son DES (*Data Encryption Standard*) y triple DES, IDEA (*Internacional Data Encryption Algorithm*), RC2 (*Ron's Code 2 - RSA Variable-Key-Size Encryption Algorithm Designed by Ron Rivest*), RC4, y SkipJack.

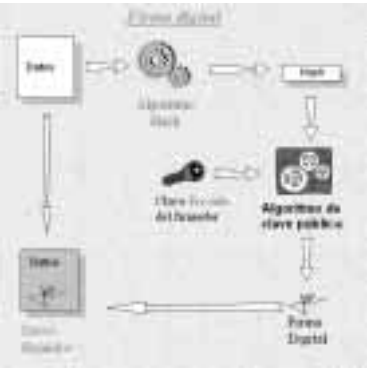
Firma digital

Para el proceso de firma digital se utiliza el cifrado privado de la información, cuyo mecanismo básico se ha explicado antes. Mediante el mecanismo de firma digital no solo se asegura la autenticidad de la identidad del emisor de la información, si no que se asegura también que los datos no han sido manipulados durante el envío.

Proceso de firma

El proceso necesario para realizar la firma digital de una información (Figura 4) es el siguiente:

Figura 4. Firma digital



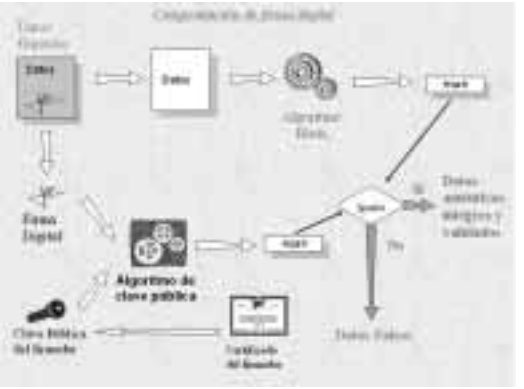
1. Se obtiene un resumen (hash) de los datos a firmar mediante un algoritmo hash.
2. Este resumen se encripta con la clave privada del emisor mediante un algoritmo de clave pública. Al producto de la encriptación del resumen se le llama la firma digital del documento.
3. Esta firma digital se adjunta al documento original de forma que cualquiera pueda comprobar su autenticidad.

Obsérvese que solo el emisor conoce su clave privada, por lo que solo él puede encriptar la información con esa clave. De esta manera se asegura la autenticidad del emisor de la información.

Comprobación de la firma

El proceso contrario, la comprobación de la firma digital de una información, consiste en comprobar que realmente ese documento lo envió quien dice que lo envió, y también en asegurarse que los datos no han sido manipulados durante el envío. Consta de los siguientes pasos (Figura 5):

Figura 5. Comprobación de firma digital



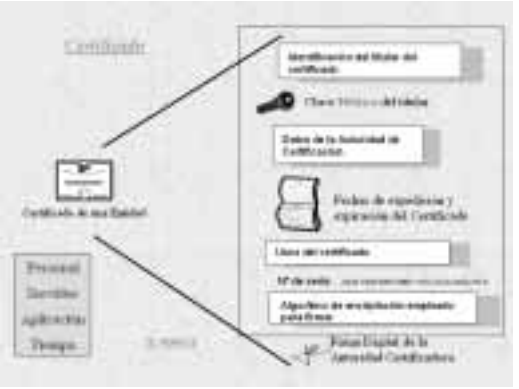
1. Se toman los datos firmados tanto los originales como la firma digital y se separan ambos componentes.
2. Por un lado se toman los datos y se genera, igual que en el firmado, el resumen o hash (debe recordarse la correspondencia única entre los datos y su resumen).
3. Por otro lado se toma la firma digital, que es el resumen encriptado con la clave privada del emisor, y se le aplica un algoritmo de clave pública con la clave pública del emisor, que se obtiene del certificado del emisor, para obtener el hash o resumen original.
4. Finalmente se compara el hash calculado a partir de los datos, con el hash obtenido de descifrar la firma digital adjunta al documento y se obtiene la validez o no de los datos:
   - Si son iguales, los datos son auténticos, íntegros y validados.
   - Si no son iguales, los datos son falsos, bien porque el emisor no es cierto, o bien porque sí lo es pero los datos han sido manipulados durante su envío.

Como existe correspondencia entre la clave pública y la clave privada, unos datos que han sido encriptados con una clave privada, solo podrán desencriptarse con la clave pública correspondiente a esa clave privada.

Certificado digital

El certificado digital es el mecanismo que permite garantizar que una clave pública enviada por un interlocutor es verdadera. El certificado digital contiene todos los datos que el usuario expone al exterior y que permite comprobar que la clave pública es válida y es además de quien dice ser (Figura 6).

Figura 6. Contenido de un certificado electrónico



El contenido mínimo de un certificado consiste en los siguientes elementos:

– Datos de identificación del titular del certificado.

– Clave pública del titular.

– Datos de la autoridad de certificación que lo emitió.

– Fechas de expedición y expiración de la validez del certificado.

– Usos para los que está autorizado este certificado.

– Número de serie.

– Algoritmo de encriptación utilizado para firmar.

– Firma digital de la autoridad certificadora (firma del resto del contenido del certificado de forma que se pueda consultar su validez).

Dependiendo del tipo de certificado, la entidad que lo emite o su uso, el certificado puede contener además otra información, como otras entidades en las que confía, o los datos de representación si se trata de certificados de empresas.

El elemento fundamental que asegura la validez del contenido de un certificado es la entidad certificadora, que asegura la validez del contenido del certificado firmando digitalmente este contenido. Esta firma se realiza mediante los mecanismos vistos anteriormente, y su validez se comprueba también mediante los mismos mecanismos.

La entidad certificadora tiene también como misión generar y mantener las listas de certificados revocados (CRL) para que se publiquen en un repositorio público en el que consta su número de serie, de forma que se pueda consultar si un determinado certificado continúa vigente en el momento de su uso. La entidad certificadora también mantiene una relación de los certificados con las claves emitidas asociadas a estos certificados.

En la figura 7 se observa que el proceso de comprobación de la autenticidad de un certificado se practica de la misma forma que el de cualquier otra información, considerando que los datos del certificado son los firmados por la entidad de certificación.

Figura 7. Comprobación de la autenticidad de un certificado

El proceso se realiza en dos pasos:

1. *Comprobar que el certificado es auténtico y no ha sido manipulado*. Esa comprobación es exactamente igual que la de cualquier otro tipo de información firmada digitalmente:
   - Separar la información de la firma.
   - Volver a generar el hash.
   - Obtener el hash original aplicando un algoritmo de clave pública a los datos firmados, más la clave pública de la entidad de certificación

– Comparar finalmente los dos hash obtenidos por ambos medios para comprobar si son iguales.

2. *Comprobar que el certificado no ha sido revocado*. Es decir comprobar que el certificado no está entre los expuestos en la lista de certificados revocados de la entidad que lo emitió. Para ello se utilizan unos servicios de consulta a través del web que las entidades certificadoras ponen a disposición de los clientes.

Mecanismos organizativos de autorización y auditoría

Asignación de perfiles y roles

Antes de implantar un sistema de información clínico se debe definir quién puede acceder a qué contenidos de la información y qué acciones se pueden llevar a cabo sobre ella. Es decir, se debe definir qué perfiles de usuario existen para el sistema, indicando a qué información pueden acceder estos perfiles, qué operaciones o roles pueden realizar sobre esta información y en qué medida pueden ejercer estos roles.

Una organización típica de esta definición de perfiles es la siguiente:

– Se ordenan desde el nivel más restrictivo, con acceso en lectura a ciertos aspectos de la información, hasta el nivel máximo o de administrador, que tiene control total y posibilidades de acceso, modificación y borrado de toda la información.

– Se definen los roles o papeles a desarrollar por estos perfiles de la organización. Son unidades de trabajo o responsabilidad mínimas que cada elemento o perfil de la organización puede o no ejercer.

– Se define la escala en que los perfiles pueden ejercer un determinado rol. Por ejemplo, un perfil médico puede ejercer el rol de modificar una ficha de información clínica; pero lo puede hacer de diferente forma según la ficha haya sido creada por él, si ha sido creada por otro médico de su servicio, o si ha sido creada por otro médico de diferente servicio. En este último caso, probablemente no podrá modificarla sino simplemente leerla.

La Tabla 2 muestra un ejemplo de una organización en la que se han definido perfiles y roles. En cada casilla se indica en qué medida puede ejercerse cada perfil y cada rol. Lo normal es que estos sean acumulativos, partiendo de los perfiles más bajos que solo tendrán acceso en lectura a cierta información, a los administradores que tendrán control total sobre toda la información.

Tabla 2. Ejemplo de definición de perfiles, roles y asignación de escala de permisos en un Servicio de Radiología

PERFIL/ROL	DEMOGRÁFICOS	LECTURA DATOS CLÍNICOS	MODIFICACIÓN DATOS CLÍNICOS	BORRADO DATOS	EXPLOTACIÓN
Administrativo Admisión Citación	Actualizar	No	No	No	No
TER	Leer	Solo los suyos	Solo los suyos	No	No
Enfermera	Leer	Los del Servicio	Solo los suyos	No	Los suyos
Médico	Leer	Todo	Los del servicio	Solo los suyos	Los suyos
Jefe médico o administrativo del Servicio	Leer	Todo	Los del Servicio	Los del servicio	Los del servicio
Administrativos de la unidad de informes	Leer	Todo	Los del servicio	Los del servicio	No
Administrador	Actualizar	Todo	Todo	Todo	Todo

Aunque llamen la atención los privilegios de los administrativos de la unidad de informes, se ha puesto un ejemplo de servicio en el que, en muchos casos, ellos son los únicos que modifican la historia clínica, pues transcriben la información que reciben a través de un dictáfono. Debe tenerse en cuenta también que el borrado es "borrado lógico", es decir, que la ficha se marca como borrada y no aparece en pantalla, pero no se borra físicamente de la base de datos, con lo que luego se puede consultar esta información en caso de duda. Este ejemplo de definición de perfiles y roles también pone de manifiesto que el deber de guardar secreto se extiende a todo el personal, tanto sanitario como no sanitario, que accede a la información clínica.

El sistema de información tendrá la capacidad de asignar los usuarios a cada uno de los roles y por supuesto, de limitar a cada usuario a que solo ejerza los privilegios asociados a su perfil, impidiendo que se efectúe cualquier otra acción indebida.

Auditoría

Con independencia de con qué perfil se acceda y las acciones que se lleven a cabo, se establecerán los mecanismos que permitan registrar y dejar un rastro de todas las operaciones que se han hecho con la información. Se registrará toda la información necesaria para que luego se puedan hacer auditorías, en las que se determine si el acceso a la información estaba o no justificado.

El conjunto mínimo de información que se debería registrar para cumplir con este objetivo sería el siguiente:

– Usuario.

– Unidad.

– Estación de trabajo o dirección IP.

– Fecha y hora en la que se accede.

– Perfil con el que accede y nivel de privilegio asociado.

– Información a la que accede y operación que efectúa.

Se debe alcanzar un compromiso entre el registro de la información necesaria para luego poder auditar el sistema y que el funcionamiento sea operativo. Si se pretende registrar con máximo detalle todo lo que ocurre, se alcanzará un mecanismo de auditoría perfecto, pero el sistema puede emplear más recursos en registrar accesos que en hacer su trabajo propiamente dicho, con lo cual su operatividad se resentirá.

Se deberán facilitar las herramientas necesarias para realizar estas auditorías, así como personal encargado de realizar esta labor. Existen dos tipos distintos de auditoría.

– Las "de oficio" que se realizan al azar, con carácter periódico, con el fin de controlar que el acceso a la información se realiza en general de forma correcta.

– Específicas sobre un paciente, en las que se comprueba si los accesos a la información sobre ese paciente están justificados y son adecuados. Estas auditorías se llevan a cabo sobre pacientes sobre los que se considera que existe un mayor riesgo para su confidencialidad, o sobre pacientes que por cualquier motivo solicitan su práctica.

La labor de registro de accesos y auditoría posterior se simplifica si se dispone de la posibilidad de acceder a la información de los pacientes a través de listas de trabajo, que consiste en integrar el sistema clínico con los sistemas administrativos de citación de consultas, gestión de ingresados o de urgencias. De esta forma al usuario se le restringe el acceso a los pacientes que aparecen en su lista de trabajo: los citados en su consulta, los ingresados en su planta, los atendidos en urgencias, los correspondientes a su cupo de atención primaria.

MECANISMOS DE DISPONIBILIDAD

Además de garantizar la confidencialidad e integridad de la información sanitaria, se hace necesario que esté accesible para las personas autorizadas y que éstas puedan llevar a cabo sus transacciones cuando lo necesiten. Las catástrofes en materia de protección de datos no siempre son por accesos indebidos o por pérdida de la información, también lo son por no poder acceder, disponer, de la información cuando ésta es necesaria (9).

En este apartado se revisa el concepto de nivel de servicio, cómo alcanzar un compromiso sobre el nivel de servicio requerido y cómo garantizar el cumplimiento de ese compromiso (10, 11).

Nivel de servicio

Un servicio es un conjunto de sistemas de Tecnologías de la Información (TI) que soportan un proceso de negocio. Con esta definición se puede considerar servicios las aplicaciones de línea de negocio como la historia clínica informatizada, el sistema de información clínico-administrativa, o los servicios de infraestructura tecnológica, como el correo electrónico, y los servidores de bases de datos.

El nivel de servicio de un sistema de información depende de los elementos que lo componen (programas, servicios, datos y software de plataforma), de la infraestructura tecnológica, el hardware, los equipos de red y comunicaciones, y de las funciones de operación y gestión de servicio. El diseño del sistema de información deberá incluir aquellos elementos, tanto tecnológicos como de procedimiento, que permitan ofrecer el nivel de servicio adecuado.

Acuerdo de nivel de servicio

La organización de TI y los usuarios del servicio deben alcanzar un acuerdo que defina las responsabilidades de todos los participantes, usuarios finales, gestores y miembros de la organización de TI; que obligue a la gestión de TI a proporcionar el servicio con unas características determinadas de calidad y cantidad, y que a su vez limite las expectativas y requerimientos de los usuarios a los límites establecidos en el acuerdo.

Con ese acuerdo, por lo tanto, se trata de definir qué servicio, cómo se utiliza ese servicio y cuánto se utiliza el servicio. No es lo mismo el nivel de servicio que debe tener una aplicación administrativa de utilización exclusiva por personal funcionario en horas de oficina, que la misma aplicación con acceso a través de Internet por los ciudadanos, que esa misma aplicación si los ciudadanos no sólo

acceden por Internet, sino que además hacen transacciones. Tampoco es lo mismo esa aplicación, que la historia clínica, que debe prever posibles accesos y transacciones desde varios servicios y centros sanitarios, en ocasiones de forma concurrente, con el máximo nivel de seguridad y confidencialidad.

Como se ha indicado, los objetivos y compromisos del acuerdo de nivel de servicio debe ser cuantificados. Por ejemplo, el Departamento de Operación de TI podría acordar proporcionar una disponibilidad del servicio del 99,99% a determinadas unidades de negocio, o responder las llamadas de petición de soporte por parte de los usuarios a los 15 minutos de producirse.

Etapas del compromiso de nivel de servicio

Para garantizar el nivel de servicio de una solución deben seguirse los siguientes pasos:

1. El análisis de los requerimientos de la solución, que incluirá los requerimientos específicos de nivel de servicio de modo que sean considerados desde el principio en la arquitectura y el diseño de la solución.
2. Las directrices de gestión del nivel de servicio, que están orientadas a incrementar la calidad de la solución que se diseña, asegurando que están presentes todos los elementos necesarios para permitir ofrecer el nivel de servicio adecuado.
3. La revisión relativa del nivel de servicio, que permitirá valorar el diseño y el uso de la tecnología en los elementos de la solución y los procedimientos de gestión de servicio definidos.
4. Las pruebas de nivel de servicio, que permitirán comprobar el comportamiento de la solución y la respuesta del sistema ante situaciones que podrían influir en el nivel de servicio.

Análisis de los requerimientos de la solución

Dentro del análisis de requerimientos tanto funcionales como técnicos de la solución, se considerarán aquellos que tengan impacto en el nivel de servicio, bien sea porque influyen en la forma en que se alcanzará este nivel de servicio, o bien sea porque son requisitos propios o exclusivos del nivel de servicio. Por ejemplo, un requerimiento funcional es que la historia clínica esté integrada con el laboratorio, que son dos sistemas distintos, lo que supone que debe mantenerse el servicio tanto de los dos sistemas como de la conexión entre ellos. Un requisito propio del

nivel de servicio es que el laboratorio de análisis clínicos funcione 24 horas al día, lo que supone una disponibilidad de servicio del 99% del tiempo.

El alcance de los requisitos o sus características pueden variar en función del nivel de servicio que se les quiere proporcionar. Por ejemplo, si se quiere garantizar la conexión entre dos centros remotos al 99% podría ser necesario duplicar las líneas de comunicaciones, lo cual implica variar los requisitos técnicos de comunicaciones. En ocasiones, proporcionar unos requerimientos con el nivel de servicio que se está pensando en ofrecer supone costes que la organización no puede asumir, por lo que habrá que matizar o suavizar unos u otros hasta encontrar una solución posible de alcanzar con un coste razonable.

Directrices de gestión de nivel de servicio

La capacidad de proporcionar un nivel de servicio adecuado se basa en la gestión de una serie de aspectos o áreas que hacen posible mantener el servicio operativo en las condiciones pactadas en los acuerdos.

El compromiso sobre nivel de servicio debe tener en cuenta la capacidad, la disponibilidad, las contingencias o desastres que puedan producirse, la gestión de los cambios que se deban introducir, la gestión de los cambios en la configuración y la gestión de los problemas.

Los servicios requieren cambios periódicos, por ejemplo, porque varían los requerimientos de los usuarios o porque se renueva el hardware. Por ello debe estar previsto cómo se introducen esos cambios de forma que no se produzcan trastornos en el funcionamiento de la solución. También debe tenerse en cuenta que, por mucho que se invierta en seguridad y disponibilidad, pueden producirse contingencias o desastres y la organización debe estar preparada para hacerles frente.

1.- Gestión de la capacidad de la solución

La gestión de la capacidad es el proceso de planificar, dimensionar y controlar la capacidad de servicio de la solución, de manera que se satisfagan las condiciones establecidas en los acuerdos de nivel de servicio. Este proceso exigirá que la solución diseñada proporcione información relativa a los escenarios y patrones de uso, datos sobre la carga y parámetros de rendimiento, de manera que se disponga de información suficiente para determinar cuándo es necesario ampliar la capacidad.

La solución debería ofrecer mecanismos de monitorización para, al menos, las siguientes métricas:

– Utilización de la solución: peticiones por unidad de tiempo, tiempos de respuesta, franjas horarias y estacionalidad de uso entre otros.

– Utilización de recursos físicos como procesador, red y memoria.

– Entrada y salida de información, páginas, acceso a datos, transacciones y accesos a disco.

– Información sobre los usuarios: cantidad e intensidad de utilización.

– Límites de capacidad del sistema.

– Datos de disponibilidad de los servicios y de los componentes de la solución.

2.- Gestión de la disponibilidad de la solución

El objetivo es asegurar que los usuarios podrán utilizar los servicios siempre que lo necesiten. Cada uno de los servicios ofrecidos dentro de la solución tendrá unos requerimientos de nivel de servicio distintos. Por ejemplo, por encima del 99%, lo que significa asegurar que los cortes de servicio no exceden de 90 horas al año.

En concreto se revisarán los siguientes aspectos:

– Puntos únicos de fallo.

– Tolerancia a fallo de los sistemas hardware, las aplicaciones y componentes de software de la solución, la plataforma de software y la red.

– Redundancia de elementos críticos.

– Mecanismos para incrementar la disponibilidad de la solución mediante cambios en la plataforma hardware o software, sin requerir cambios en los componentes de software desarrollados.

3.- Gestión de contingencias de la solución

Hay dos aspectos fundamentales en la gestión de las contingencias, prevenir las paradas de servicio y su recuperación; tanto en el caso de desastres como en el de otras incidencias que afecten al nivel de servicio. Tan peligroso es tener un desastre como no saber cómo gestionar su solución, o aunque se sepa, no hacerlo.

Como parte de la solución deberán evaluarse los principales riesgos de parada de servicio, incluyendo la probabilidad de que ocurran, el impacto y los planes de contingencia y recuperación para cada uno de ellos, de forma que se minimice el efecto sobre el nivel de servicio en el caso de que ocurran. Los planes de contingencia y recuperación incluirán tanto la documentación sobre identificación de las

causas de la parada, como el procedimiento a seguir para cada una de ellas, las herramientas que se deben utilizar y la información de soporte de los distintos proveedores de la solución.

En concreto, se deberán considerar los siguientes aspectos:

– Procedimientos de actuación en caso de caída de servicio.

– Recuperación de datos a partir de copias de seguridad.

– Reinstalación completa de la infraestructura, la plataforma y los componentes de la solución.

– Procedimientos para poner en marcha medidas alternativas manualmente en caso necesario.

Durante la revisión del diseño de la solución se revisarán los planes de contingencia, incluyendo alcance, objetivos, políticas y procedimientos, para determinar si se han incluido todos los planes necesarios y validar la adecuación del contenido planificado de cada uno de ellos.

4.- Gestión de cambios de la solución

La gestión de cambios de la solución deberá proporcionar los procedimientos adecuados para salvaguardar los servicios existentes y permitir la introducción de nuevos, garantizando el nivel de servicio. Esos procedimientos deberán asegurar la disponibilidad de la solución reduciendo el número de cambios innecesarios y asegurando que los cambios efectuados en la plataforma base o los componentes no deterioran el nivel de servicio.

Los procedimientos de gestión de cambios afectarán al hardware, los equipos de red, el software de sistemas, el software de aplicación, los datos, los procedimientos y la documentación que formen parte de la solución y que sean relevantes para la operación, el soporte y la gestión de la solución. Es decir, cualquier elemento de la solución necesario para asegurar el nivel de servicio de la solución desarrollada deberá estar bajo control de cambios.

La gestión de cambio deberá incluir al menos los siguientes procedimientos:

– Control de cambios, de manera que se incluya la información relativa a la complejidad, el coste, el riesgo y el impacto del cambio, y que obtenga las aprobaciones correspondientes del personal autorizado de la organización antes de realizar cualquier cambio a los sistemas en producción.

– Petición de cambio, que formalicen la comunicación al personal de la organización de la descripción del cambio que se va a realizar, los componentes afectados, los motivos del cambio, los requerimientos de recursos humanos y técnicos, y la aprobación correspondiente.

– Cambios urgentes, que establezca el mecanismo para realizar cambios urgentes al sistema de manera muy rápida cuando ello sea necesario para no afectar al nivel de servicio.

5.- Gestión de la configuración de la solución

El objetivo fundamental de la gestión de la configuración es la identificación, el inventario y el seguimiento de los elementos que componen la solución o elementos de la configuración. La información que deberá recogerse dependerá de cada elemento de la configuración en concreto, pero deberá incluir la descripción, la versión, los componentes, la relación con otros elementos de la configuración, su ubicación y el estado actual. Los elementos de la configuración serán los mismos que están sujetos a la gestión de cambios.

La solución deberá incluir una base de datos con la información de los elementos de la configuración. Los procedimientos de instalación del software de aplicación desarrollado deberán actualizar esa base de datos siempre que sea posible. La base de datos deberá reflejar todos los cambios realizados a los elementos de la configuración. Existirá una biblioteca de software que incluirá todo el necesario para instalar los elementos de configuración de acuerdo con la base de datos de la configuración y se considerará la ubicación oficial del software de sistemas y de aplicación de la solución. Esa biblioteca de software será utilizada además en caso de recuperación de desastres.

Por lo tanto, para cada cambio realizado a la configuración, deberá seguirse el procedimiento de gestión de cambios y actualizarse la base de datos de configuración y la biblioteca de software.

Las actividades de la gestión de configuración que deberán incluirse en la solución serán:

– Planificación de la gestión de la configuración. Definición del alcance, objetivos, políticas y procedimientos, que serán revisados junto al diseño global de la solución.

– Identificación de los elementos de la configuración. Estructura de la base de datos de configuración, identificadores y versiones, y relaciones entre elementos de configuración.

– Control de la configuración. Asegurar que no se añade, modifica, elimina o sustituye ningún elemento de la configuración sin seguir el procedimiento de control de cambios y actualizar la base de datos de la configuración.

– Verificación de la configuración. La solución deberá incluir un procedimiento o mecanismo para obtener información sobre los elementos de la configuración de la solución en producción, para poder comparar con la base de datos de la configuración.

6.- Gestión de problemas de la solución

El objetivo de la gestión de problemas de la solución es definir los procedimientos para:

– Interpretar los mensajes de error.

– Identificar y localizar a las personas de contacto.

– Informar del problema existente.

– Analizar las causas.

– Escalar (hacer llegar el problema a quien lo puede resolver) y resolver los incidentes.

– Informar de la causa y las medidas necesarias para la resolución.

– Incorporar esa información a la base de conocimientos de problemas de la solución.

– Iniciar el proceso de cambios correspondiente para la resolución del problema.

La solución deberá incluir medios para la identificación de errores y para la detección de circunstancias que puedan amenazar o afectar al nivel de servicio. Esos medios podrán ser documentos o herramientas.

Revisión relativa al nivel de servicio

En la fase de diseño de una solución deben comprobarse las funciones de gestión y los elementos de la configuración como son los servidores, los sistemas de comunicaciones, las bases de datos y demás elementos de la solución. También debe comprobarse si se cumplen los criterios que se han fijado en el acuerdo de nivel de servicio. La Tabla 3 muestra la lista de los elementos que deben comprobarse.

Tabla 3. Revisión de diseño relativa al nivel de servicio

Revisión de funciones de gestión del nivel de servicio
Revisión de los planes de gestión de nivel de servicio Despliegue de los elementos de la solución Contingencia y copias de seguridad Gestión de la solución
Revisión de los elementos de configuración de la solución
Red y comunicaciones Servidores de archivos e impresión Bases de datos Web Mensajería y notificación Servicios de seguridad
Criterios de evaluación de la revisión de nivel de servicio
Escalabilidad: Incremento de la capacidad con elementos de configuración. Planificación del crecimiento. *Disponibilidad:* Puntos únicos de fallo, redundancia de elementos, especialización de elementos. *Seguridad:* Medidas de protección de los datos, los componentes y el nivel de servicio. *Gestión y administración:* Facilidad de despliegue, configuración, monitorización y detección de fallos. *Soportabilidad:* Existencia de procedimientos y herramientas para que los incidentes se resuelvan en tiempos adecuados. *Rendimiento:* Adecuación de los tiempos de respuesta y la concurrencia a la demanda estimada. *Estándares:* Utilización de estándares de interoperabilidad e integración

Pruebas de nivel de servicio

En la fase de pruebas se deben llevar a cabo las siguientes pruebas para asegurarse de que se cumplen todos los requisitos de nivel de servicio:

1.- Pruebas de instalación y configuración

El objetivo de estas pruebas es comprobar que la documentación de instalación y configuración incluye todo lo necesario para que el sistema funcione correctamente. Esta prueba debería ser la primera del conjunto de pruebas relativas al nivel de servicio para asegurar que se ejecutaron sobre un sistema configurado de acuerdo a la documentación.

2.- Pruebas funcionales

Se debe comprobar que todos los servicios funcionan adecuadamente: servicios de red, servicios de datos y servicios de web. Así como que las aplicaciones responden adecuadamente a los requerimientos.

3.- Pruebas de disponibilidad

Comprobación de que los mecanismos de tolerancia a fallos tanto físicos (tarjetas y dispositivos de red, fuentes de alimentación, controladoras, discos duros y otros dispositivos hardware) como servicios de balanceo de red o de clustering, funcionan adecuadamente en las diferentes condiciones de error, comprobando que los componentes redundantes o alternativos responden sin interrupciones de servicio inesperadas. Estas pruebas deberán ejecutarse primero sin simulación de carga y posteriormente con cargas de saturación o cercanas a la saturación.

4.- Pruebas de gestión del sistema

Tienen como objetivo la comprobación de los mecanismos de monitorización y alertas y de las funciones de administración remota. Deberán definirse la lista de casos de pruebas a partir de los requerimientos del sistema.

5.- Pruebas de rendimiento

Se debe conocer la capacidad del sistema en diferentes situaciones de carga y los límites operativos. Para ello se prueba la capacidad individual de cada servicio y del sistema completo, de modo que se disponga de esa información para que puedan tomarse decisiones de diseño en caso de necesitar aumentar la capacidad del sistema.

6.- Pruebas de escalabilidad

El objetivo es medir la dificultad de expandir la infraestructura para incrementar la capacidad del sistema y analizar la linealidad del aumento de capacidad de la solución respecto al incremento de capacidad de los elementos de infraestructura. Por lo tanto, se busca que los procesos necesarios para expandir la infraestructura y dotarla de más capacidad sean previsibles, no sujetos a cambios bruscos en la relación infraestructura/capacidad, y se sepa de antemano con certeza como responderá la capacidad del sistema ante aumentos en la infraestructura tecnológica.

7.- Pruebas de seguridad

Comprobar que solo los usuarios autorizados pueden acceder a servicios y datos. Existen distintas aproximaciones, pero las más efectivas son las auditorías de seguridad o las pruebas de intrusión.

8.- Pruebas de copias de seguridad y contingencia

El objetivo de estas pruebas es comprobar que se dispone de procedimientos adecuados de contingencia y recuperación de desastres, de acuerdo a lo establecido en el apartado "Gestión de contingencia".

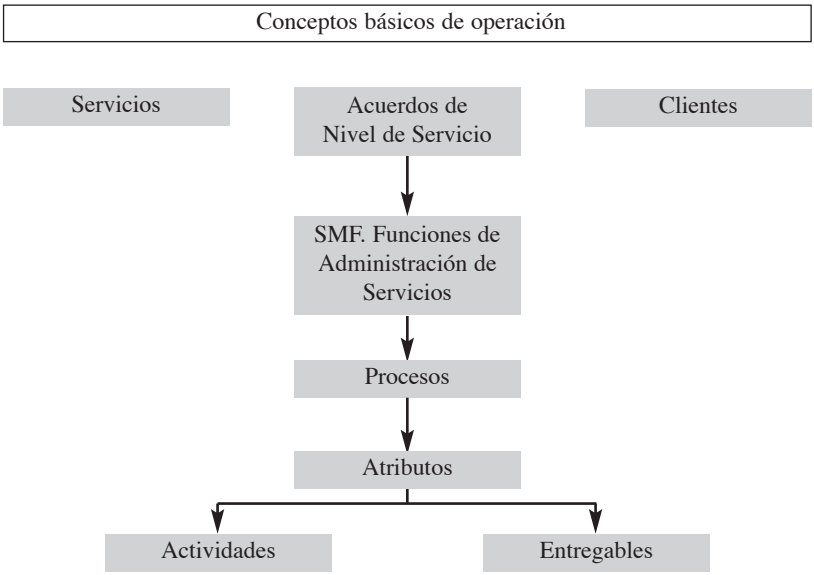
9.- Pruebas de estabilidad

El objetivo de estas pruebas es asegurar que el sistema se mantiene estable después de ejecutar pruebas de carga durante un período de tiempo continuado, y que no aparecen condiciones de errores acumulativos como pérdidas de memoria o degradación del rendimiento.

Operación de los Sistemas de Información

Como se ha indicado antes, para alcanzar la calidad en el servicio deseada se precisa un acuerdo entre la organización de TI y los usuarios del servicio que defina las responsabilidades de todos los participantes y que fija las especificaciones de calidad de servicio. Para dar cumplimiento a ese acuerdo existen unos mecanismos, que son los que se indican a continuación (12) (Figura 8).

Figura 8. Conceptos básicos de operación



Existen una serie de funciones que se necesitan para mantener operativo un servicio, las llamadas funciones de administración de servicios, que describen una serie de procesos, actividades y entregables. Estas funciones se pueden aplicar a todo el conjunto de servicios que se encuentran en los entornos actuales de TI y son necesarias para mantener un entorno de operaciones estable, confiable y disponible.

Son funciones de administración de servicios el soporte técnico, la gestión de problemas, la gestión de la configuración, del cambio y la administración de sistemas. Cada una de estas funciones debe tener asignado un responsable, que será un experto en los procesos de operación y que debe conocer tanto las actividades como el entorno de las operaciones.

Cada Función consta de procesos que tienen atributos (indicadores de la realización de los procesos) que describen aquellos criterios significativos que aseguran la realización óptima de dicha Función.

Se definen como atributos de los procesos:

– Las **actividades** de cada proceso: tareas que se ejecutan durante el proceso. Las actividades facilitan la gestión de los procesos aumentando el grado de efectividad en su ejecución.

– Los **entregables**: Son las entradas y salidas de los procesos, y que sirven como elementos de control de la ejecución de las actividades de un proceso.

Así pues, las Funciones de Administración de Servicios se soportan con la realización de las actividades y en la gestión de los entregables.

Es necesario definir los roles y responsabilidades para la correcta operación, soporte y mantenimiento del servicio.

Cada servicio debe tener asignado un administrador que será el responsable de garantizar los niveles de servicio. Entre sus tareas están definir cómo se ejecutan las tareas de administración y operación, y coordinar con los responsables de las funciones de administración de servicios la ejecución de sus actividades. También será el gestor de versiones en los cambios que afecten al servicio.

ALGUNAS DIRECTRICES PARA DISPONER DE UN SISTEMA SEGURO

La adecuación de un sistema a los requisitos de seguridad puede venir en dos momentos, durante el diseño y construcción de un nuevo sistema o en un sistema que ya existía con anterioridad.

Durante el diseño y construcción de un nuevo sistema

En primer lugar deben identificarse los riesgos y amenazas. Por lo tanto, en la fase de diseño de la solución es esencial la identificación de áreas vulnerables en las que alguien de forma involuntaria, o intencionada, pueda comprometer la seguridad del sistema.

En la fase de desarrollo se tendrán en cuenta las guías y buenas prácticas para la construcción de sistemas seguros (13). La implantación de la solución se hará sobre un entorno seguro. Como se ha indicado antes, la seguridad en un sistema de información consiste en proteger todos los elementos de ese sistema: máquinas, programas, datos e infraestructuras de comunicaciones (redes y electrónica de red), de todas las posibles amenazas que se identifiquen sobre estos elementos.

Para proteger cada uno de los elementos de un sistema de información se seguirán las siguientes directrices:

– *Infraestructuras de comunicaciones*. En el caso de cable, *routers, firewalls y switches*, se asegurará la integridad del tráfico que transporta la red, protegiéndolo frente a las amenazas que pudieran detectarse: como son los ataques basados en TCP/IP y *passwords*.

– *Máquinas*. En los servidores web, de datos y de aplicaciones, se deberían tener en cuenta aspectos como parches y actualizaciones, servicios, protocolos, cuentas de usuario, puertos de comunicaciones, ficheros y carpetas, entre otros.

– *Programas y datos*. Se deben tener en cuenta aspectos como validación de las entradas de datos por parte de los usuarios, gestión de perfiles de acceso, autorización a estos perfiles, configuración de las conexiones, encriptación, gestión de errores y auditoría.

Principios de seguridad

Los principios de seguridad que se deberían cumplir en cualquier caso y que han demostrado su validez con la experiencia (13) son:

– Sistema dividido en compartimentos: Se reduce la vulnerabilidad ante un ataque separando el sistema en áreas independientes para que estén a salvo de ataques a otras áreas.

– Utilización del mínimo privilegio necesario en cada ocasión: cuando se lleve a cabo cualquier tarea, se deben utilizar cuentas de usuario que tengan los privilegios indispensables para hacerlas.

– Utilizar múltiples barreras de defensa.

– No confiar en las entradas de datos por parte del usuario, suele ser la principal fuente de ataques. Validar todas las entradas de datos asegurando que no tendrán consecuencias negativas en el sistema.

– Hacer las comprobaciones lo antes posible, no diferirlas, pues cuanto antes se detecte un ataque, menores serán sus consecuencias.

– Prever y tratar las caídas del sistema, dejando rastro del motivo de la caída, y sobre todo, no dejando los datos accesibles.

– Asegurar especialmente los elementos más débiles de la cadena. En el estado actual de la tecnología en el que un sistema de información está compuesto de múltiples piezas independientes entre sí, como diferentes servidores, máquinas, infraestructuras de red; es importante centrarse en proteger los más débiles, ya que los importantes suelen estar más protegidos, por ejemplo un servidor de base de datos.

– Reducir las posibilidades de ataque, es decir, eliminar del sistema todo lo que no sea imprescindible, pues puede ser una vía de entrada.

Adaptación de un sistema existente

Por desgracia, no todos los sistemas pueden ser diseñados desde el principio teniendo en cuenta que deben cumplir con un reglamento de medidas de seguridad, sino que en muchas ocasiones hay que adaptar sistemas existentes que presentan carencias en este sentido. IPS Certification Authority (14) propone un Plan de adaptación al reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que se compone de 5 fases:

– Análisis de seguridad.

– Elaboración de la normativa de seguridad.

– Puesta en funcionamiento de la normativa de seguridad.

– Formación a los responsables de seguridad y de los ficheros.

– Auditoría de seguridad

El plan de seguridad es un aspecto que se trata con amplitud en el Informe SEIS "La seguridad y confidencialidad de la información clínica"(8). La auditoría de seguridad se trata en otro apartado de este trabajo.

RESUMEN Y CONCLUSIONES

Los derechos de los pacientes, y de los ciudadanos en general, a la confidencialidad de la información sanitaria están reconocidos tanto en la normativa de protección de datos como en la sanitaria. Estos derechos generan en las instituciones la obligación de adoptar las medidas necesarias que garanticen esa confidencialidad.

Pero el derecho del paciente a una adecuada atención sanitaria también exige garantizar la disponibilidad de esa información, de forma que siempre que sea necesaria pueda accederse a la información, tratarla y modificarla en su caso.

Los objetivos que deben cumplirse para garantizar la seguridad, confidencialidad y disponibilidad de la información clínica son los de autentificación, confidencialidad, integridad, no repudio, autorización, auditoría y disponibilidad.

Las medidas que deben adoptarse para cumplir esos objetivos son los certificados digitales, el cifrado de la información, la firma digital, la gestión de las autorizaciones y privilegios, los registros de acceso y la gestión del nivel de servicio adecuado.

La historia clínica electrónica o informatizada, que forma parte de un sistema integrado de información clínica, que contiene información muy íntima de las personas, que puede ser accesible desde cualquier lugar que sea necesario para atender al paciente; es más segura que la historia tradicional en papel y custodiada en un archivo convencional. La disponibilidad de la historia clínica electrónica también es mayor que la de la historia convencional. Para garantizar la seguridad, confidencialidad y disponibilidad de la historia clínica se debe adoptar un plan de seguridad que cumpla al menos con las directrices que se indican en este trabajo y que se refieren a personas, máquinas, programas, datos e infraestructuras de comunicaciones.

Se debe alcanzar un equilibrio entre las medidas de seguridad y la disponibilidad. Un exceso en las medidas para garantizar la confidencialidad puede suponer colapsar los sistemas, con lo que no se garantiza la disponibilidad de la información.

La seguridad, confidencialidad y disponibilidad de la información clínica requieren, en primer lugar medidas organizativas, que afectan a todos los miembros de la institución, entre los que se encuentra la alta dirección, el personal sanitario y el personal de sistemas de información. La primera de esas medidas organizativas es conseguir que todos los implicados en el problema lo conozcan y sean sensibles a la importancia que tiene para las personas que atienden.

BIBLIOGRAFÍA

1 Rodríguez Sendín J. J. La pérdida del derecho a la intimidad. OMC 2003; 90: 5-6.

2 Sierra G. Confidencialidad, punto clave en la relación médico-paciente (Editorial). OMC 2003; 90: 3.

3 Carnicero J. La historia clínica en la era de la información. Dimens Hum 2002; 6 (4):167.

4 Mandl K. D., Szolovits, Kohane I. S. Public standars and patients'control: how to keep electronic medical records accesible but private. BMJ 2001; 322: 283-7.

5 Mc Donald R. Commentary: A patient's viewpoint. BMJ 2001; 322: 287.

6 Andérez A. Aspectos legales de la seguridad y confidencialidad en la información clínica. En: Carnicero J y Hualde S (Eds). La seguridad y confidencialidad de la información clínica. Informes SEIS (3). Pamplona: Sociedad Española de Informática de la Salud 2001. http://www.seis.es/informes/2001/default.htm.

7 Sanz J., Hualde S. Aspectos técnicos de la seguridad en la información sanitaria. En: Carnicero J. y Hualde S. (Eds). La seguridad y confidencialidad de la información clínica. Informes SEIS (3). Pamplona: Sociedad Española de Informática de la Salud 2001. http://www.seis.es/informes/2001/default.htm.

8 Pérez Campanero J. A. La gestión de la seguridad en los sistemas de información y de las comunicaciones. En: Carnicero J y Hualde S (Eds). La seguridad y confidencialidad de la información clínica. Informes SEIS (3). Pamplona: Sociedad Española de Informática de la Salud 2001. http://www.seis.es/informes/2001/default.htm.

9 Kilbridge P. Computer Crash - Lessons from a System Failure. N. Engl J. Med 2003; 348:881-882.

10 (*IT Infrastructure Library-ITIL*) Agencia Central de Informática y Telecomunicaciones (*Central Computer and Telecommunications Agency-CCTA*) del Reino Unido http://www.itil.co.uk.

11 NGA y Microsoft. Servicios Telemáticos para la Hacienda Tributaria de Navarra. Propuesta para diseño y construcción. 2003.

12 (*Microsoft Operations Framework-MOF*) http://www.microsoft.com/technet/itsolutions/tandp/opex/mofrl/mofeo.asp?frame=true.

13 Improving Web Application Security: Threats and Countermeasures: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp.

14 "La protección de los datos personales". Soluciones en entornos Microsoft. Microsoft. IPS Certification Authority SL. http://www.ipsca.com.