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

Juan Antonio Pérez-Campanero Atanasio

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

INTRODUCCIÓN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

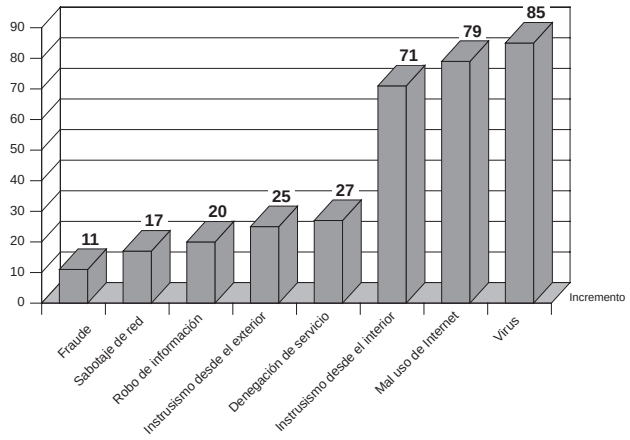

Figura 1. Ataques a un sistema de información (Fuente FBI/CSI)

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

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

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

REQUISITOS DE SEGURIDAD

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

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

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

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

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

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

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

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

–Seguridad externa o física.

–Seguridad interna o lógica.

–Seguridad funcional.

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

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

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

SEGURIDAD EXTERNA

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

Seguridad física

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

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

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

Seguridad de personal

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

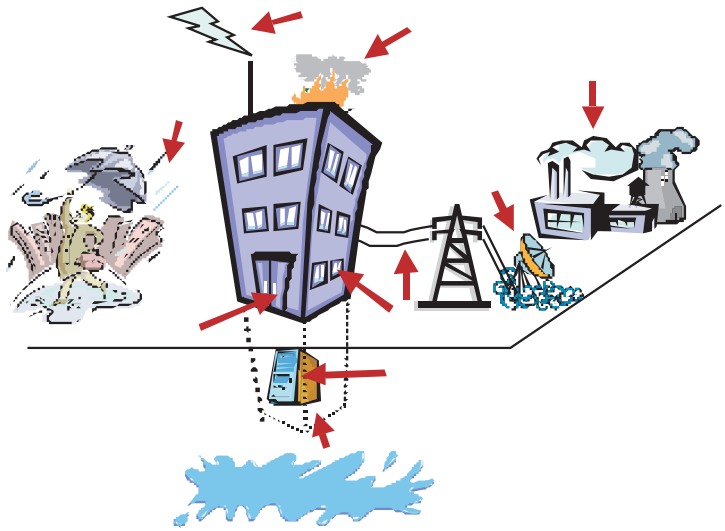

Figura 2. Seguridad externa

SEGURIDAD INTERNA

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

Administración de usuarios

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

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

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

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

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

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

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

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

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

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

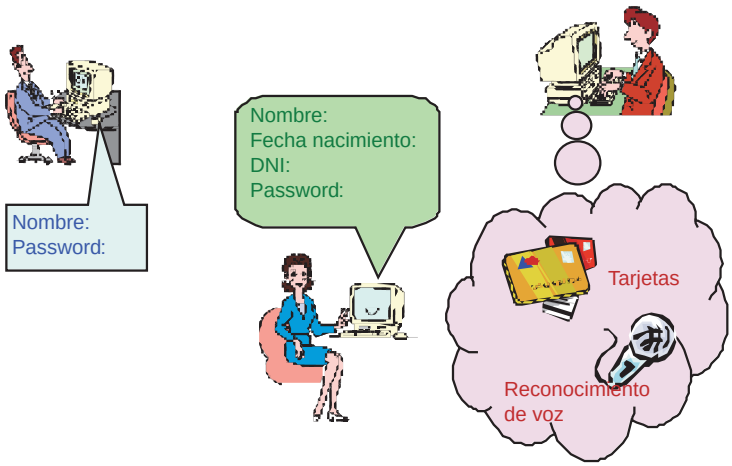

Figura 3. Tipos de protección de acceso de los usuarios

Seguridad en los ficheros

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

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

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

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

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

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

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

Disponibilidad de los ficheros

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

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

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

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

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

Privacidad de los ficheros

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

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

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

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

SEGURIDAD FUNCIONAL

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

Seguridad en la transmisión de datos

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

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

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

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

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

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

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

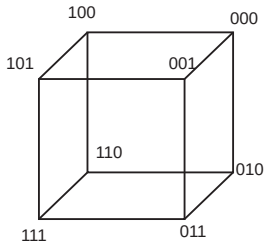

Figura 4. Cubo de Hamming

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sistemas tolerantes a fallos

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

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

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

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

–Problemas en los discos magnéticos.

–Errores de instalación de los discos.

–Errores de paridad en la memoria.

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

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

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

Criptografía

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

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

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

Figura 5. Proceso de cifrado y descifrado

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

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

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

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

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

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

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

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

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

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

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

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

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

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

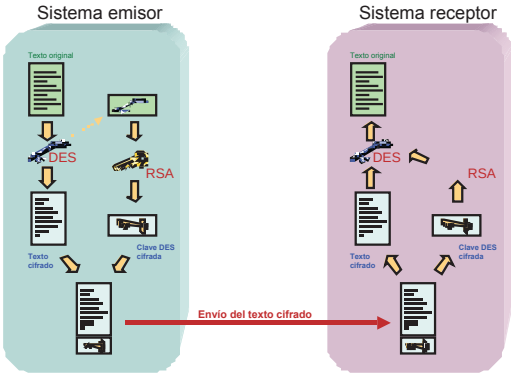

Figura 6. Algoritmo RSA de encriptación

PKI (Public Key Infraestructure)

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

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

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

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

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

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

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

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

Certificados digitales

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

Los certificados digitales tienen dos misiones:

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

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

Hay dos tipos de certificados digitales:

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

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

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

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

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

3. El nombre de la Autoridad de Certificación.

4. El periodo de validez del certificado.

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

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

Autoridad de certificación

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

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

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

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

Estándares de seguridad

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

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

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

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

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

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

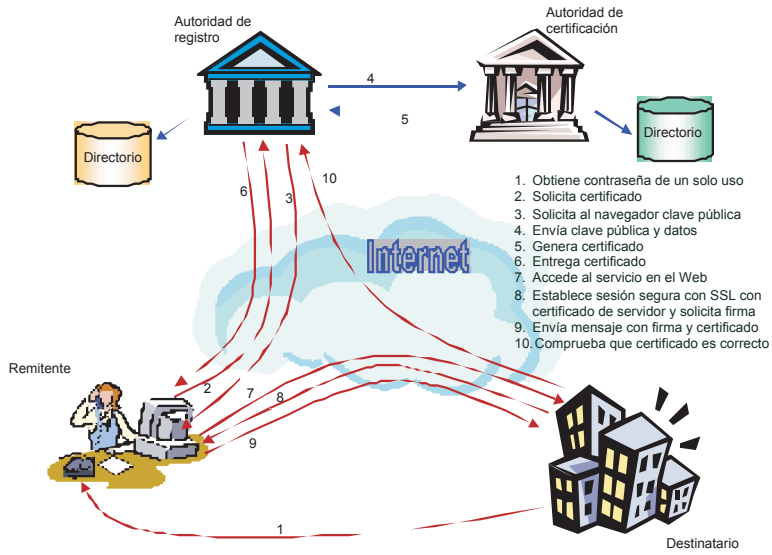

Figura 7. Proceso de transferencia de mensajes con PKI

Cortafuegos

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

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

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

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

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

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

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

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

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

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

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

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

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

Virus

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GESTIÓN DE LA SEGURIDAD

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

Organización

La organización general

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

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

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

El control

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

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

La auditoría

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

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

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

El entorno físico

El edificio

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

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

Las salas de ordenadores

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

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

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

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

El plan informático

El plan informático general

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

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

El control

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

El plan de seguridad

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

I. Identificación y evaluación de los riesgos.

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

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

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

V. Valoración del presupuesto necesario.

VI. Organización y responsabilidades.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Plan de migración

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

Plan de contingencia

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

TENDENCIAS ACTUALES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

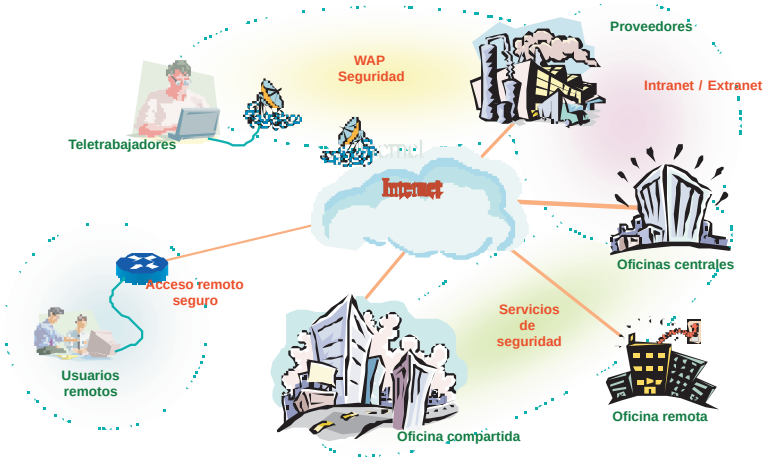

Figura 8. Servicios de "túnel"

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

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

Figura 9. Problemática de la situación actual

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

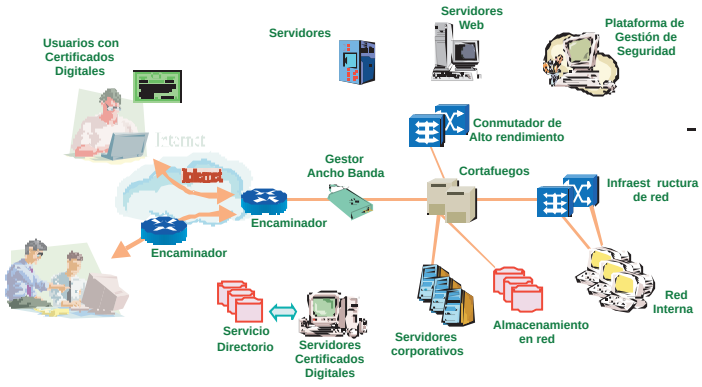

Figura 10. Infraestructura de conectividad

BIBLIOGRAFÍA

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