ASPECTOS TÉCNICOS DE LA SEGURIDAD EN LA INFORMACIÓN SANITARIA

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

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

INTRODUCCIÓN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

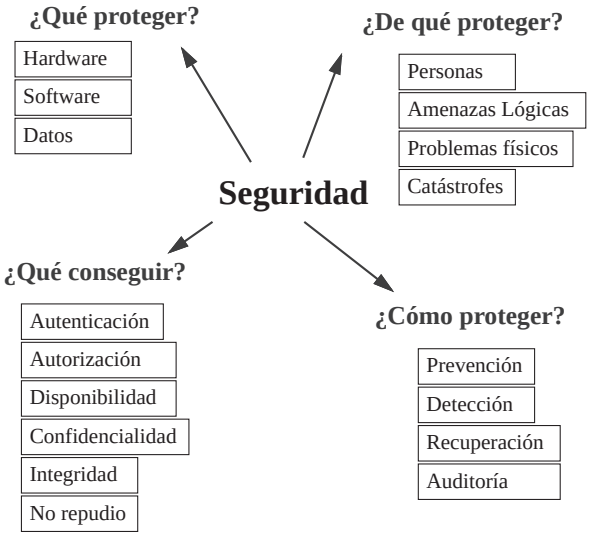
En este trabajo vamos a detallar las tecnologías que integran las TIC_S, haciendo más hincapié en aquellas que han surgido para dar respuesta a los sistemas distribuidos tanto por la red privada como por la red pública.

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

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

DEFINICIÓN

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



¿QUÉ PROTEGER?

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

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

¿DE QUÉ PROTEGERNOS?

a) Personas

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

b) Amenazas lógicas

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

c) Problemas físicos

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

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

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

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

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

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

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

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

d) Catástrofes

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

¿QUÉ CONSEGUIR?

a) Autentificación

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

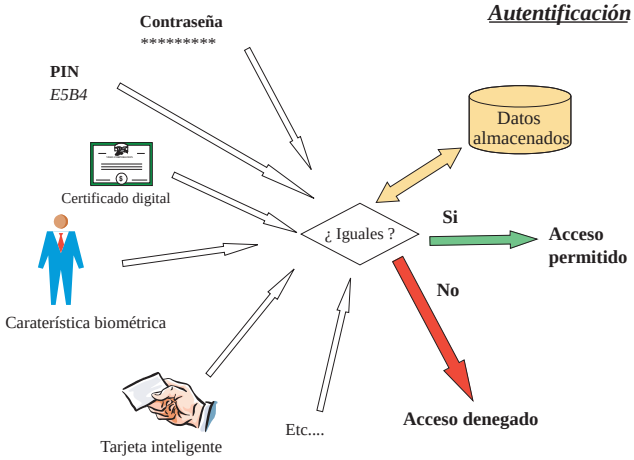
–Contraseñas

–Certificados

–Tarjetas Inteligentes (Smart card)

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

–Firma digital...



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

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

b) Autorización

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

c) Disponibilidad

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

d) Confidencialidad

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

e) Integridad de la información

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

f) No repudio

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

¿CÓMO PROTEGERNOS?

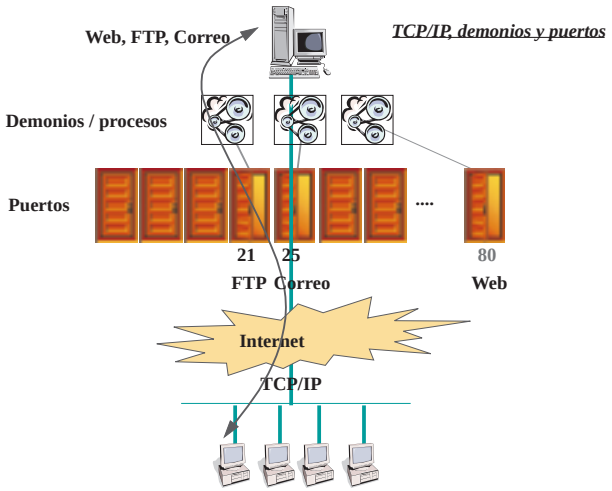
Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia. Partiendo de este análisis diseñaremos una política de seguridad que incluya responsabilidades y reglas para evitar tales amenazas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

a) Mecanismos de prevención

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

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

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



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

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

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

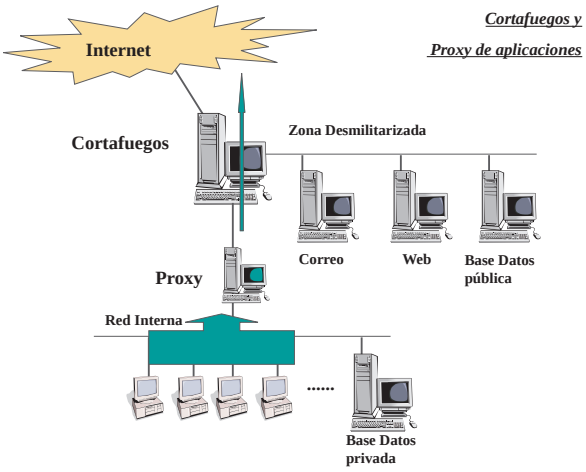


tabla de condiciones y acciones, reglas que efectúan un filtrado de paquetes basándose en el origen y destino del paquete, así como el servicio TCP/IP que utiliza (Web, correo...).

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

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

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

b) Mecanismos de detección

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

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

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

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

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

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

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

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

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

c) De recuperación

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

d) De auditoría

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

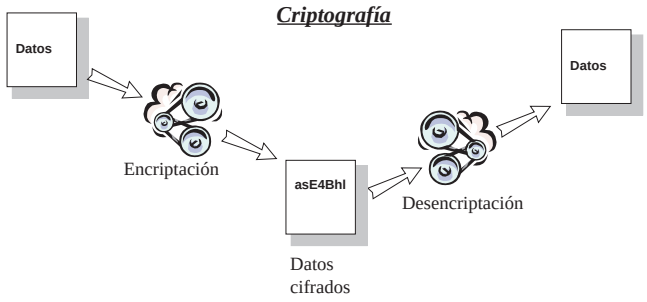
CRIPTOGRAFÍA

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

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

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

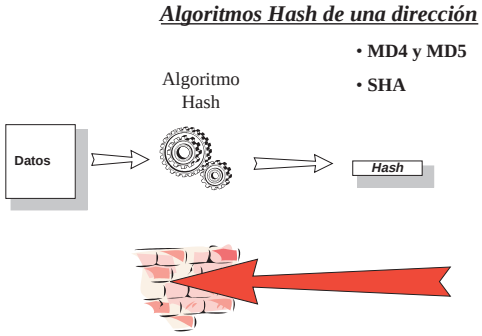
Vamos a describir los principales tipos de tecnologías empleados para cifrar información y sus diversas implementaciones.



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

a) Algoritmos hash de una dirección

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



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

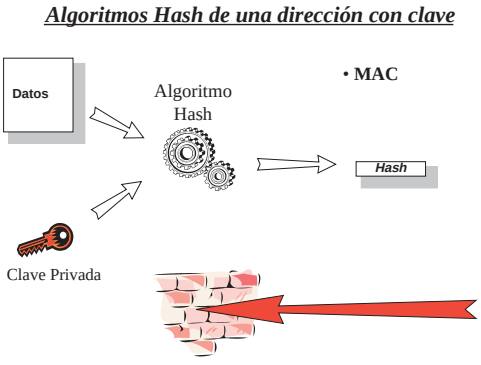
Ejemplos de algoritmos:

–MD4 y MD5 (Message Digest) 128 bits.

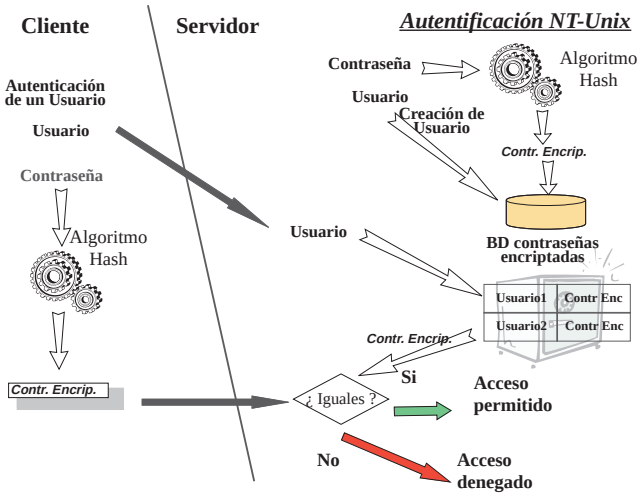
–SHA (Secure Hash Algorithm) 160 bits.

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

–MAC (Message Authentication Code).

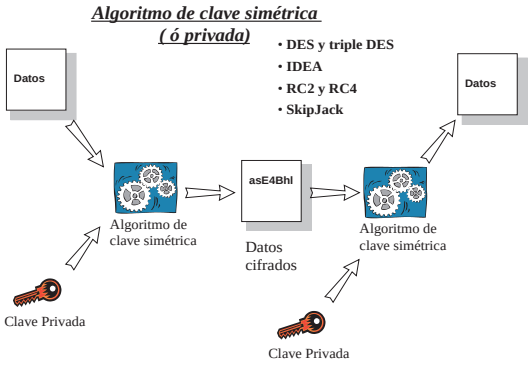


A modo de ejemplo describimos en esta imagen el proceso de Autentificación en un entorno NT ó UNIX tradicionales. La línea negra determina lo que viaja por la red. Claramente se observa que no viaja nunca la información de la contraseña. Además, el servidor no conoce la contraseña.



b) Algoritmos de clave privada (simétricos)

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



Ejemplos de algoritmos:

–DES y triple DES. –RC2 y RC4.

–IDEA. –SkipJack.

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

c) Algoritmos de clave pública (asimétricos)

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

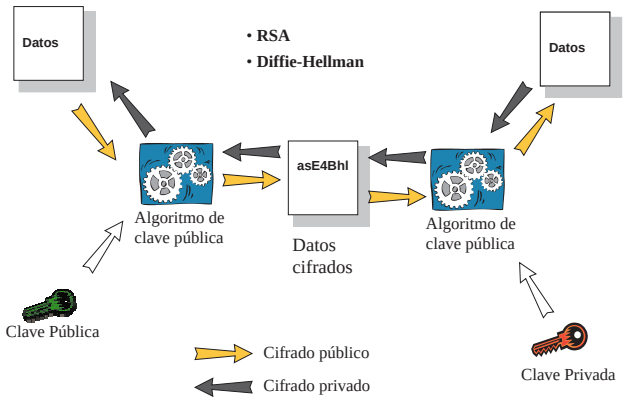
Funciona de este modo: el emisor introduce un documento en el algoritmo así como su clave privada, se obtiene el mismo documento pero cifrado, es decir, ininteligible. El receptor recoge el documento cifrado y lo introduce de nuevo en el algoritmo así como la clave pública del emisor, obteniendo el documento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

Ejemplos de algoritmos:

–RSA (Rivest-Shamir-Adleman).

–Diffie - Hellman.

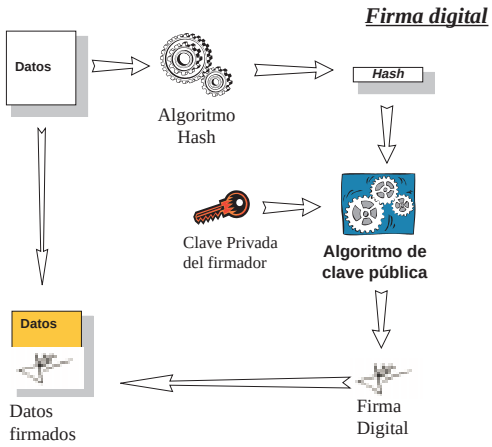
Algoritmo de clave asimétrica (ó pública)



USOS DE LAS TECNOLOGÍAS DE ENCRIPTACIÓN

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

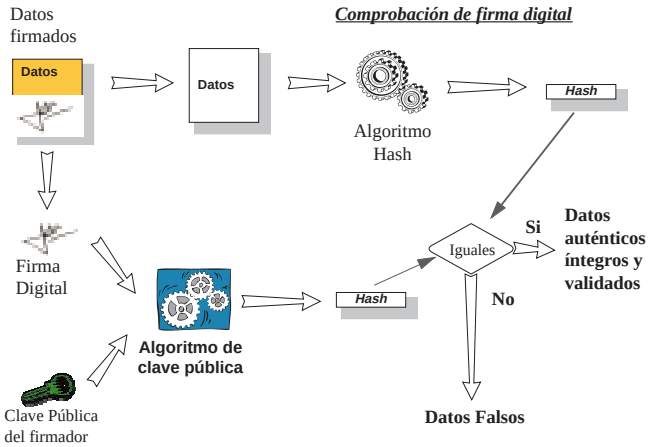
a) Firma digital



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

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

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



b) Certificados

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

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

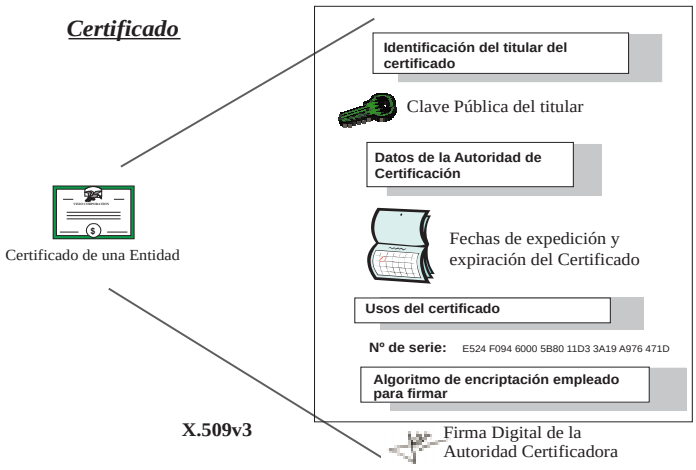
Tipos de certificados y su utilidad:

–Personales:

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

–De servidor

SSL
Time stamp
VPN's
...



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

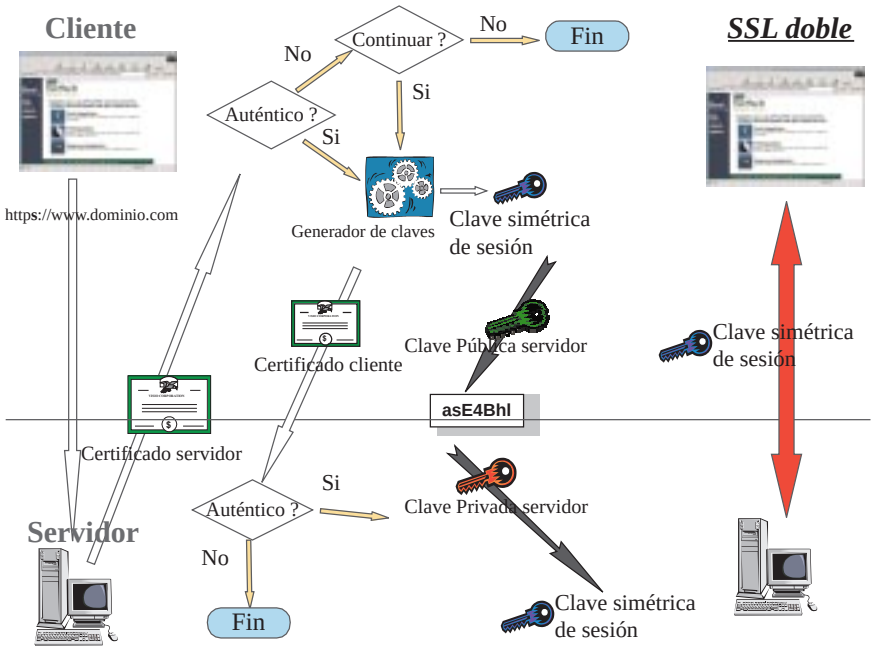
–Firma de código
Autenticidad del software

c) Comunicación segura con un servidor

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

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

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



d) Comunicación segura en sistemas financieros

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

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

e) Cifrado de correo y ficheros

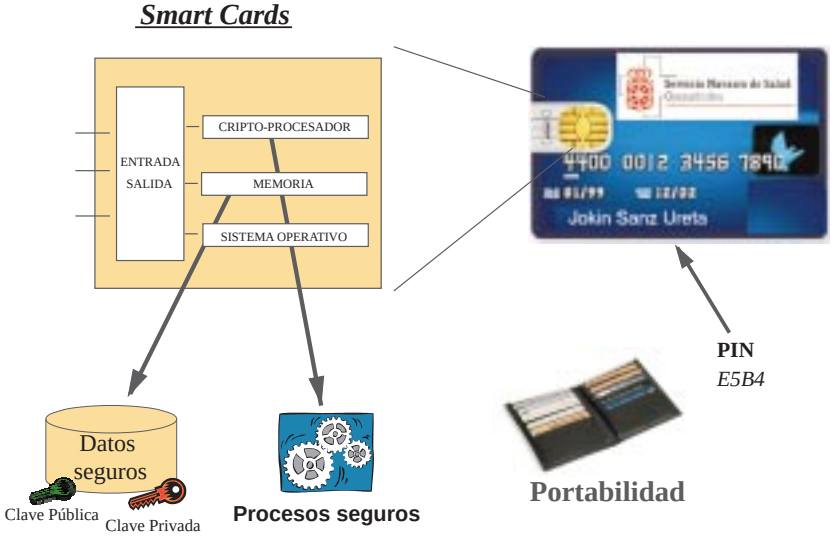
Dos entes especialmente sensibles son los ficheros y los correos electrónicos. Ambos son documentos con información que de algún modo debemos proteger.

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

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

f) Smart Cards (Tarjetas inteligentes)

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



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

Las tarjetas aportan las siguientes características de seguridad:

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

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

–Portabilidad de las credenciales digitales y otras informaciones.

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

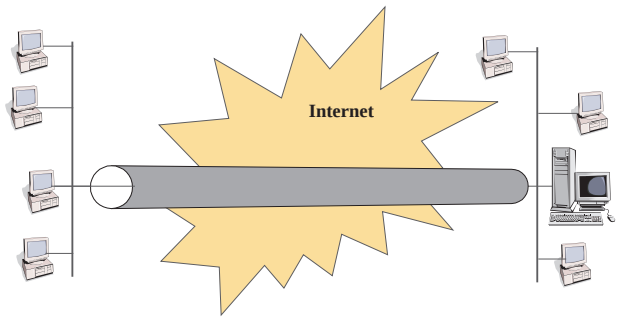
Su funcionalidad es la misma que aportan los certificados digitales, teniendo en cuenta que puede almacenar también la clave privada.

g) Redes privadas virtuales (VPN's)

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

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

VPN (Red Privada Virtual)



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

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

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

PKI

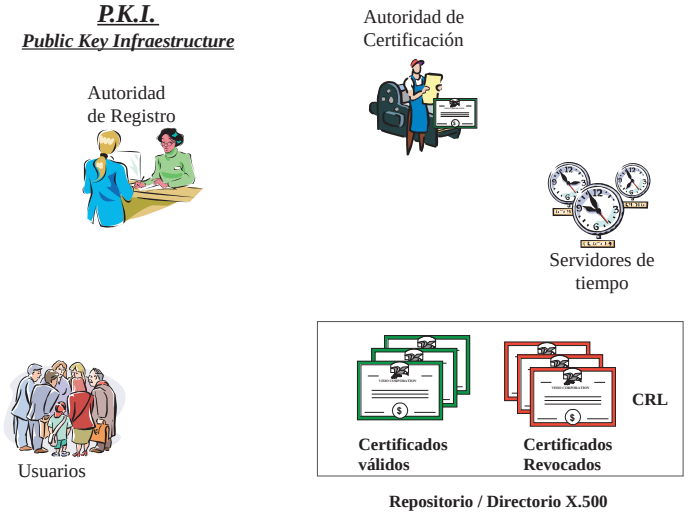
PKI (Public Key Infraestructure) es un conjunto de tecnologías que se aprovechan de los algoritmos de encriptación de clave pública, de clave privada y hash.

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

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

a) Autoridad de registro

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



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

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

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

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

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

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

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

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

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

b) Autoridad de certificación

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

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

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

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

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

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

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

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

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

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

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

c) Repositorio de información pública

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

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

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

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

d) Servidores de tiempo

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

e) Entidades de certificación

Españolas:

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

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

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

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

Internacionales:

–VeriSign

–SecureNet

–Entrust

–.....

CONCLUSIONES

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

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

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

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

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

RECURSOS Y BIBLIOGRAFÍA

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

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

   -PKCS#1: algoritmo RSA.

   -PKCS#3: algoritmo Diffie-Hellman.

   -PKCS#5: algoritmos basados en contraseña.

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

   -PKCS#9: atributos de los certificados extendidos.

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

   -PKCS#8: información de clave privada.

   -PKCS#10: petición de certificado.

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

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

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

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

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

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