El delito informático

JOSÉ A. SOLER DE ARESPACOCHAGA

CONFEDERACIÓN ESPAÑOLA DE CAJAS DE AHORROS

En un gran número de delitos informáticos se realizan una o varias actuaciones técnicas seguidas de la conversión de los resultados en beneficios. En otros casos, como el sabotaje físico, no es necesaria ninguna conversión para obtener «otro tipo» de beneficios. De cualquier modo, y por definición todos los delitos informáticos tienen una connotación tecnológica.

Hoy se puede asegurar que la informática es una necesidad impuesta a toda entidad o empresa de cualquier rango. La evolución de las tecnologías, de los servicios y de los entornos empresariales en general, han hecho que la «Información» y su ágil tratamiento sean, quizás, de los primeros patrimonios de las empresas.

Esta misma evolución fuerza a la adaptación de normas y de procedimientos de seguridad, que protejan al patrimonio aludido. En tiempos atrás la protección física de las instalaciones contra las agresiones internas, externas, naturales, etc... era suficiente para salvaguardar de una forma eficaz las diferentes propiedades de la época. La proliferación de los terminales en lugares remotos, con toda la diversidad conocida de servicios y sobre todo con una ingente cantidad de usuarios, provocó la alarma respecto a la adopción de una seguridad diferente, no necesaria hasta ese momento.

No se concibe en nuestra sociedad empresarial una seguridad integral que no esté formada por una seguridad física y una seguridad lógica. Mucho se ha escrito sobre la seguridad física, de su transformación y de sus contrastes mejoras; pero si hacemos una reflexión veremos que esas mejoras, espectaculares incluso, pasan por la utilización de sistemas de control informatizados. La informática ha propiciado este avance notable, pero a su vez incrementa las medidas de protección a tomar para su propia seguridad.

A mediados de la década de los 40, se produce la aparición de uno de los inventos que sin lugar a dudas cambiaría de una manera radical, en los siguientes años, las estructuras de toda la sociedad y del mundo laboral. Dicha máquina es la que por su idiosincrasia se la denominó en un principio como el «Cerebro electrónico».

Como todas las primeras apariciones, estaba llena de problemas y con una limitada utilidad, pero de cualquier forma no se podía bajo ningún concepto prever lo que supondría para el desarrollo del entorno empresarial y científico.

El primer problema que se les planteó a Eckert y Mauchly con la creación de dicha máquina, fue el calor que esta generaba, aunque con el pasar el tiempo, dejaría de tener importancia lo que en esos momentos era un problema.

A lo largo de los años siguientes los sucesivos descubrimientos fueron minimizando el problema comentado, influyendo en todos los aspectos de la concepción de los ordenadores. Solamente recordar la evolución desde la válvula o lámpara hasta los circuitos integrados y microchips, pasando por los transitores y la memoria de burbujas, nos da una ligera visión de lo que ha supuesto, en cuanto a la generación de calor o al tamaño de estos aparatos, el pasar de los años.

En definitiva, la aparición de esta nueva tecnología traería consigo el almacenamiento masivo de datos y con ello la incorporación al mundo de los riesgos de una de las más graves amenazas contra la seguridad de los bienes y de la información.

La mentalidad en los años 50 y 60 de los responsables de márketing de las primeras instalaciones con servicio a grandes compañías, hace que prioricen la publicidad a la seguridad. Se instalan los Centros de Proceso de Datos en lugares con visión directa desde las zonas públicas (calles, patios de operaciones, etc...) sin duda los más vulnerables, dando sus diferentes configuraciones la impresión de potencia empresarial, dejando el aspecto de seguridad relegado a un segundo término.

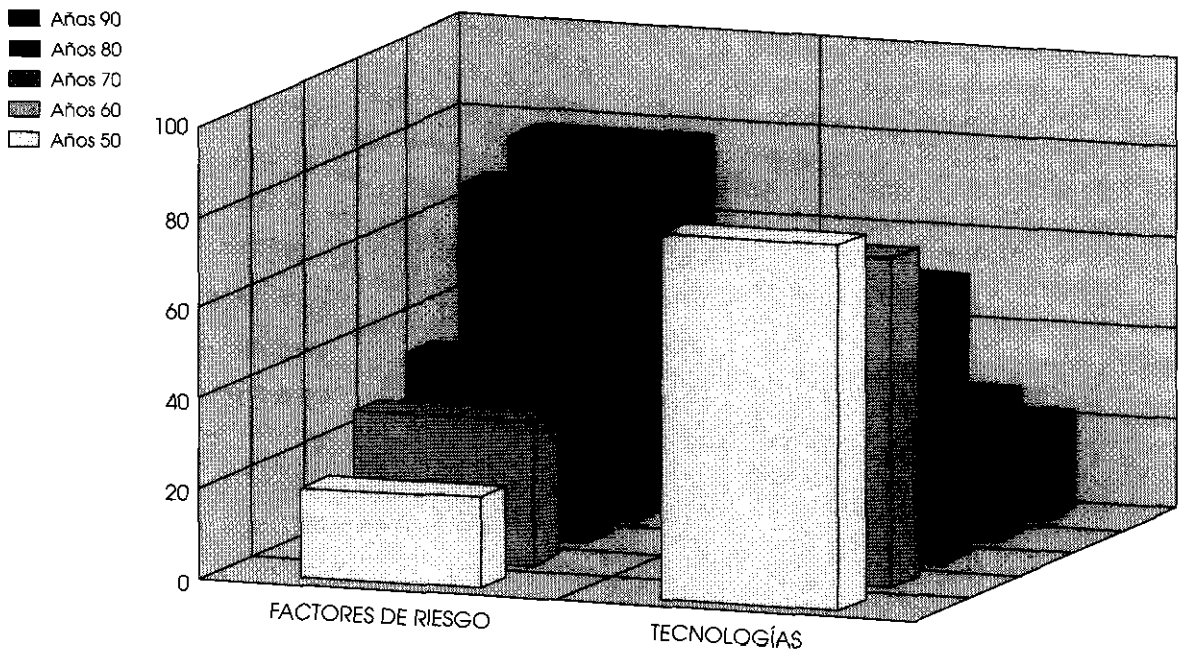
Al principio de la década de los setenta, comienza una cierta inquietud ante la posibilidad de que los Centros de Proceso de Datos, fueran objeto de agresiones delictivas. Al comienzo de la guerra del Vietnam se produjo la destrucción de algunas unidades informáticas del Gobierno Federal Norteamericano, lo que supuso un resorte de alerta para la protección de este tipo de bienes.

Las medidas de seguridad de la época inciden de una forma directa en las utilizadas sobre los ordenadores. Se basan esencialmente en puertas acorazadas y muros aislantes de hormigón por una parte, y vigilancia activa y sistemas de circuito cerrado de televisión por otra. Como complemento a las anteriores hay que añadir las medidas contra incendios que constituyen un conjunto idóneo para la informática de esos años, en la que todo el entorno era local y dentro del Centro de Proceso de Datos no llegando nunca al usuario.

En ningún momento se pensaba en riesgos que no fueran exclusivamente físicos. Su gran activo, su verdadero patrimonio que era la información no entraba en los cálculos de protección. ¿Quién sería capaz de entender de estos complicados aparatos, como para poner en peligro la integridad de los datos? Eran técnicas en poder de unos cuantos avanzados, todos ellos de gran confianza para las organizaciones, «no había peligro», el lenguaje empleado, las expresiones utilizadas y el misterio, rodeaba los comienzos de la Informática.

Los avances, como se menciona anteriormente, en el campo de los componentes electrónicos, comienza a abaratar los costes de las máquinas y a considerar la instalación en lugares remotos de terminales en comunicación con su Centro. Este tipo de proceso en «on line» y el tiempo real, deja desfasadas las medidas tomadas en años anteriores, pues la información deja de ser local para convertirse en impulsos que viajan por las líneas, debiendo

Figura 1. Tecnologías y riesgos (evolución)



abordar con urgencia la protección de dichos elementos. Además, al diversificar los accesos a los datos fuera del entorno local, aumenta el número de personas, que para mayor gravedad, pueden entrar dentro de la información. Lo que al principio era patrimonio de unos pocos pasa a ser poco a poco de comienzo generalizado.

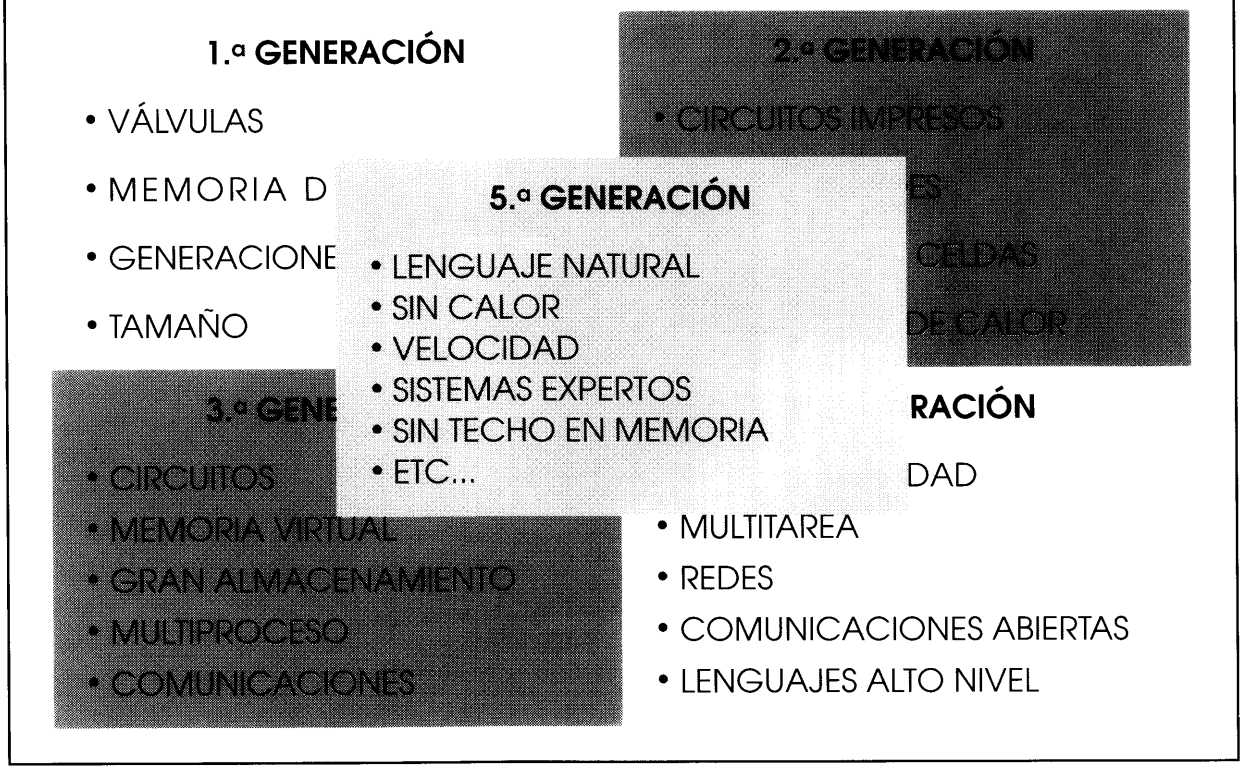
En esos años se empieza a tomar conciencia de los riesgos que se están asumiendo y se inician las primeras protecciones. Se crean las «password's» o palabras clave, con el fin de salvaguardar los accesos no deseados a las bases de datos.

Los problemas de seguridad aumentan en la década siguiente, en la que se generaliza el uso de grandes instalaciones de ordenador central a la que se unen usuarios remotos, prestándose un número cada vez mayor de servicios a través de las líneas de comunicaciones. Esta diversidad de servicios sobre usuarios fijos al sistema y ocasionales complica más y más la seguridad de las instalaciones.

Lo que se conseguía con el control de los accesos no era válido de cara a los mensajes que recorrían las líneas de datos, pues su vulnerabilidad era doble, en primer lugar cualquier intervención en la comunicación, dejaba a disposición del intruso el contenido del mensaje y lo que es peor su posible modificación con fines fraudulentos.

Este aumento de problemas se generaliza en los años ochenta y noventa, pues no solo es inevitable esta forma de trabajo sino que es necesaria como elemento incuestionable para la supervivencia económica de los países desarrollados.

Figura 2. Evolución de los sistemas informáticos



La alarma sobre la posible fragilidad de la Seguridad de los sistemas, es la puesta en marcha de ambiciosos planes de Seguridad Informática, en previsión de todo tipo de incidentes. Estos planes comenzaron unos años antes en Estados Unidos que en Europa, consistentes en la prevención de amenazas resultantes de los análisis básicos de riesgos que comienzan a efectuarse sobre este tipo de entornos lógicos contrastando con el desinterés que se mostraba anteriormente a este respecto.

El rumor público se hace eco, cada vez hay más pérdidas resultantes de fraudes o accidentes cuyo objetivo son los sistemas informáticos. Los hechos y las cifras proporcionadas, no permiten en absoluto dar una imagen precisa del fenómeno por la falta de denuncias, pero demuestran de una manera indudable su realidad y su agravamiento constante. Las nuevas tecnologías están dando vida a tipos de medios y servicios tales como el videotex, el correo electrónico, la banca a domicilio, la «telecompra»; que conlleva graves problemas de seguridad y de garantía jurídica de las transacciones que permiten efectuar.

La proliferación de microordenadores en las empresas constituye otra causa de agravamiento del riesgo, en la medida en que los equipos informáticos han sido adquiridos y se encuentran utilizados bajo control de la dirección informática o la dirección general, por personal poco o mal formado en su uso, y generalmente no advertido de los riesgos resultantes.

La consecuencia en ese dominio es muy a menudo una falta total de las más elementales preocupaciones, que en cambio son comunes en el

mundo informático tradicional, tales como la salvaguardia de ficheros, la utilización y gestión de palabras clave, la alimentación eléctrica estabilizada e ininterrumpida, etc. que facilita en gran medida el fraude informático.

Puntos críticos de seguridad en los sistemas lógicos

En un gran número de delitos informáticos, se realizan una o varias actuaciones técnicas seguidas de la conversión de los resultados en beneficios. En otros casos, como el sabotaje físico, no es necesaria ninguna conversión para obtener «otro tipo» de beneficios. De cualquier modo, y por definición todos los delitos informáticos tienen una connotación tecnológica.

Los posibles actos técnicos se reducen a modificar, destruir, revelar, utilizar o impedir la utilización de los datos.

Partiendo de este planteamiento se expone seguidamente que la criptografía proporciona el medio más seguro, por el momento, de protección de un sistema formado por el ordenador y las redes de información. Sin embargo, su eficacia depende de su correcta aplicación. Por supuesto que una implementación incorrecta deja expuesto, al sistema informático supuestamente protegido, a multitud de riesgos.

Por sí sola la Criptografía no lo es todo a la hora de incrementar la seguridad. Los sistemas informáticos se ven comprometidos de muchas formas. La principal garantía viene dada por un correcto control en el acceso a la información, preservando de este modo la confidencialidad y la integridad de los ficheros y bases de datos.

En contra de las primeras creencias, la mayor parte de los fraudes relacionados con los Centros de Proceso de Datos, tienen como autores al propio personal informático. En este caso se cumplen las premisas de cualquier acto delictivo, la *capacidad* de efectuarlo, al ser personal formado en las técnicas informáticas, la *oportunidad* de realizarlo al ser su elemento de trabajo el propio ordenador y el *motivo* que viene dado en cada caso por diferentes connotaciones del propio individuo. Por consiguiente se deduce que el diseño de protección y seguridad se debe concebir bajo el prisma del riesgo de un ataque interno.

En consecuencia, un sistema de seguridad criptográfico debe tener una serie de bloques básicos para su implementación de una forma eficaz. Esta teoría mantenida por la mayoría de los profesionales en seguridad informática, se basa en:

a) La identificación del usuario/terminal, orientado a la intrusión no deseada en el acceso a los datos.

b) La autentificación del mensaje, orientado a la protección de integridad del mensaje y no manipulación o alteración del mismo.

c) El encriptado, orientado a la protección sobre la privacidad de los mensajes.

d) Por último, la gestión de claves, orientado a la seguridad del sistema en sí mismo. No cabe la menor duda que es la parte del diseño de seguridad informática más difícil y la que destaca como su aspecto más importante.

Seguridad de accesos

La identificación del usuario/terminal, es la protección de las redes de información ante la intrusión no deseada en nuestros ficheros y bases de datos.

La intrusión electrónica se puede hacer sobre un sistema en tiempo real, donde los usuarios tienen terminales y donde su identidad es verificada automáticamente por el sistema. Cuando un terminal se pone en funcionamiento, el ordenador autoriza el acceso, habitualmente después de la recepción de una señal enviada por el giro de una llave, introduciendo una contraseña o mediante un procedimiento similar, previamente definido.

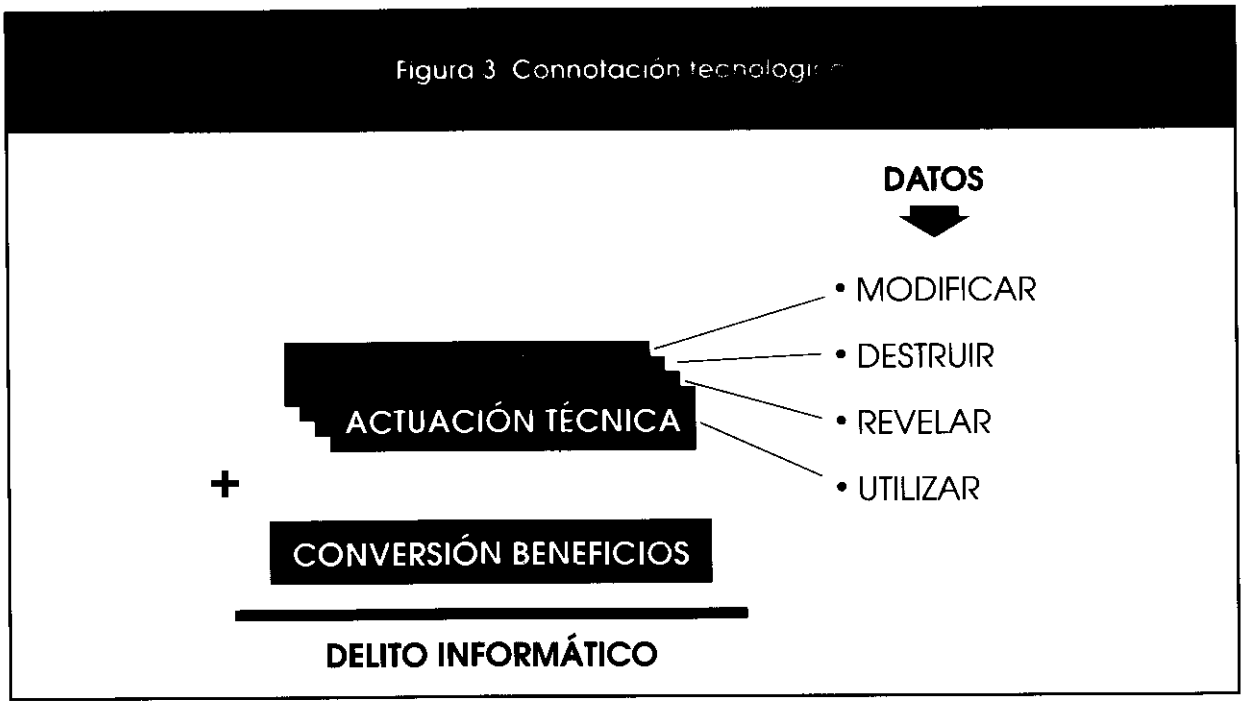
Si se conecta un terminal a la línea después de la identificación del mismo, podría accederse a la información sin que el ordenador sea capaz de reconocer ambos terminales. La intrusión puede igualmente producirse cuando un usuario se desconecta de forma incorrecta, dejando el terminal en estado de funcionamiento o dejando al ordenador en un estado tal, que funciona como si estuviese todavía conectado.

El control de accesos es una característica esencial en la mayor parte de los sistemas de seguridad. La capacidad real de identificación de un usuario es vital de cara al éxito del sistema en el control de acceso.

Un sistema informático, dotado de un mecanismo de palabras clave razonablemente seguro como control de accesos, debe poseer las características siguientes:

- Las palabras claves deben ser suficientemente largas, para resistir una investigación exhaustiva de todas las combinaciones.
- Deben estar compuestas por caracteres elegidos al azar.
- No deben ser visibles para otras personas cuando se teclea en el terminal.
- No deberían aparecer en claro en el ordenador o durante la transmisión. En caso de existir un fichero de palabras clave, éstas deben estar cifradas.
- Descubrir las palabras clave mediante ensayos debe ser difícil. No deberán permitirse más de tres reintentos de introducción del número secreto.
- El ordenador debe registrar y memorizar las informaciones que en cada tentativa de acceso se acompañen, con fines de auditoría. Debe inmediatamente dispararse una alarma e imprimirse un informe cuando se produzca una actividad no habitual, que podría indicar una tentativa de abuso del sistema informático.
- Los sistemas informáticos de alto riesgo, para los cuales sea necesario una gran seguridad, deberían estar equipados con una alarma que se dispare en caso de violencia. Si un usuario es obligado por la fuerza a acceder al sistema, debería ser capaz de introducir discre-

Figura 3 Connotación tecnológi



tamente un código en el terminal que alertase al operador del ordenador.

- Debe existir un plan de acción de salvaguardia cuando las palabras clave sean violadas.
- La gestión de las palabras clave debe ser confiada únicamente utilizando medidas de protección y reglas muy estrictas.
- Las palabras clave deben ser cambiadas periódicamente sobre todo si hay alguna posibilidad de que el sistema pueda ser violado.
- Los usuarios de palabras clave deben ser periódicamente alertados, sensibilizándose en los problemas de seguridad, y deben estar advertidos sobre las penalizaciones si no respetan las reglas, siendo los primeros en cumplir las normas de seguridad.
- El procedimiento de entrada de las palabras clave y la respuesta del ordenador no debe ser tedioso y frustrante, que haga que los usuarios intenten descubrir procedimientos alternativos.

La concepción de los procedimientos de conexión y de gestión de las palabras clave, es compleja, por lo que debe ser realizada con una gran minuciosidad y teniendo en cuenta el comportamiento humano y en particular los problemas de interacción hombre-máquina.

La solución de cifrado para la identificación del usuario, consiste en la utilización de una palabra de paso o clave de acceso dinámica. El principio en el que se basa esta solución radica en que antes del acceso, el usuario debe responder correctamente a una pregunta no repetitiva. Para cada tentativa de acceso se utiliza una respuesta diferente proporcionada por una máquina auxiliar con cifrado, con ello el conocimiento de respuestas anteriores no sirve para nada.

Lógicamente la identificación no sólo debe hacerse sobre el usuario, un sistema de identificación de accesos también asegurará que la conexión del terminal se realiza con el ordenador central deseado, como ejemplo comentar que un cajero automático debe asegurar que la respuesta de autorización a una operación se la está dando su Centro de Cálculo o autorizador de la operación y no de un elemento introducido de forma fraudulenta en la línea de conexión con el mismo.

Este sistema es una alternativa o complemento a la seguridad en los accesos, pudiéndose implementar un control de identificación de elementos; el cual consiste en el reconocimiento de las diferentes partes físicas que intervienen en un sistema.

Se lograría con mensajes cifrados en los que el terminal que desea acceder al ordenador tenga una identificación fija, procedente de un elemento hardware o una identificación asignada según su ubicación dentro de la red. En las redes de comunicaciones públicas (RETD, X25, etc.) cada mensaje va precedido de una cabecera en la que identifica que elemento emite el mensaje, de igual forma en una red privada (punto a punto, etc.) se puede implementar una gestión de identificaciones que redundaría en la seguridad de la red en general y al control de la intrusión no deseada a la misma.

La identificación de mensajes

Como veremos en el apartado de encriptación o de criptografía, ésta no garantiza necesariamente la integridad o no alteración del contenido de un mensaje. A menudo, cuando se produce una alteración de los datos, las consecuencias son más graves que cuando simplemente se produce una lectura de los mismos. Por consiguiente se puede afirmar que la protección de la integridad de un mensaje puede ser más importante que la protección de su confidencialidad.

La alteración de los datos es la técnica más sencilla, segura y clásica de la criminalidad informática. Consiste en modificar los datos antes o durante su introducción en un sistema informático. Los cambios pueden ser hechos durante los procesos de creación, codificación, registro, transporte, verificación, conversión o transformación de datos destinados a ser intro-

ducidos en un ordenador. Podemos enumerar ejemplos de diferentes momentos como la falsificación de documentos, el reemplazamiento de bandas magnéticas, diskettes o discos por otros soportes preparados con anterioridad, la neutralización o la supresión de controles manuales. Es fácil, pues, ver porqué es la técnica más clásica empleada en los casos conocidos de criminalidad informática.

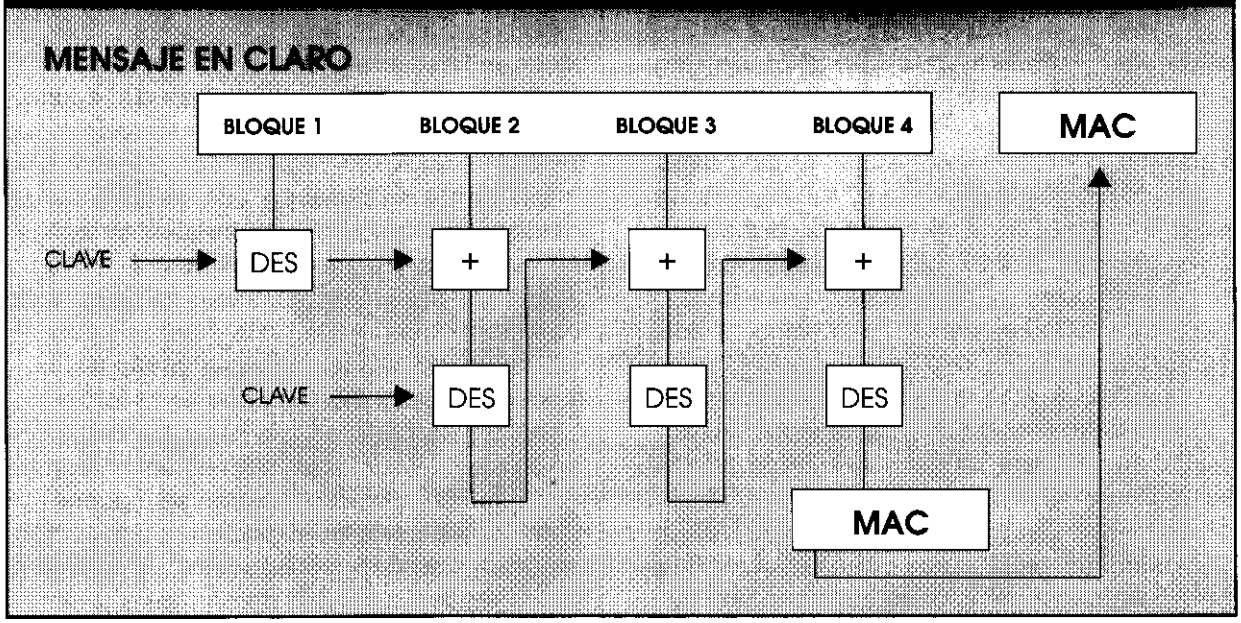
La protección, en materia de alteración de datos, requiere una seguridad considerable. La técnica criptográfica que garantiza que los datos no pueden ser alterados sin que sea detectado el hecho se denomina *Autentificación de mensajes*. Esta técnica implica el añadir a cada mensaje o registro de datos un campo de verificación criptográfica o autentificación del mensaje, el denominado MAC (Message Autentified Code) es uno de los más utilizados. El valor del MAC dependerá del contenido de cada mensaje o como mínimo del contenido de la parte que se necesita proteger.

El cálculo del MAC se efectúa partiendo de una clave secreta. Este secreto hace imposible para un agresor del sistema predecir cualquier cambio en el mensaje. Solo el conocedor de la clave puede calcular correctamente el contenido del MAC que se añadirá al mensaje. El receptor del mismo al ser conocedor de la clave secreta de cálculo, podrá calcular el contenido del MAC y al proceder a su comparación con el contenido recibido determinar que el mensaje en su recorrido por las líneas de comunicación no ha sido alterado.

Como ejemplo de cálculo de un MAC, veremos que la clave de cálculo secreta del mensaje puede incluso ser enviada dentro del propio mensaje encriptado y al proceder a su desencriptación en destino, proceder a su utilización para autentificar el mensaje por medio del contenido del MAC.

Esta técnica se puede complicar en la medida que se desee y estar, como se ha comentado anteriormente, pactada la fórmula secreta

Figura 4 Generación del código autentificador



de cálculo sin necesidad de variarla en cada transmisión.

Observando las diferentes protecciones sobre posibles riesgos en los entornos descritos, todo gira en torno a la criptografía.

La criptografía

La criptología es la ciencia que estudia las claves y escrituras secretas. La palabra criptografía proviene de los vocablos kriptos (oculto) y grafía (escritura) y la Real Academia de la Lengua Española la define como:

«Arte de escribir con clave secreta o de un modo enigmático.»

Se puede decir de una forma más amplia que es la metodología necesaria para convertir en incomprensible un determinado mensaje, salvo para quienes conozcan las claves o algoritmos necesarios para su descifrado. El objetivo, por tanto, es evitar la divulgación de la información mediante la transformación de algo legible en algo inteligible.

La escritura secreta se conoce desde tiempo remotos, su origen se encuentra en la antigüedad clásica. Los egipcios ya utilizaban tipos de escritura, como la hierática, para mantener en secreto rituales religiosos.

Julio Cesar cambiaba el orden de las letras para mandar mensajes secretos y en tiempos de Carlos V y Felipe II los barcos españoles utilizaban un código secreto para sus comunicaciones. Señalar que la criptología ha jugado un papel muy importante durante la historia y que gracias a ella se han podido ganar batallas, revelar secretos políticos, etc.

En nuestros días las técnicas de criptología ya no son de uso exclusivo de gobiernos y ejércitos pues han sido incorporadas a los ordenadores. Se han dado cuenta que la información contenida también debe ser protegida desde la almacenada en bancos de datos como la transferida a través de las líneas de comunicaciones.

Agresiones informáticas

Virus informáticos

Utilizando el mismo tratamiento que Juan Manuel Rodríguez Zarco, en su libro «Manual de prevención del fraude», se define el virus informático como el programa creado para infectar o pasar órdenes que son destructivas por medio de ordenadores, sistemas o programas. Los virus tienen la capacidad de borrrar, alterar o hacer inaccesibles las instrucciones contenidas en los soportes magnéticos quedando almacenados en la memoria del ordenador.

Los efectos negativos más generalizados que pueden producir los virus son:

- Actividad más lenta.
- Crecimiento incontrolado de los ficheros.
- Borrado de ficheros.
- Ataques a otros dispositivos.
- Imposibilidad de acceso.
- Molestias o daños.
- En cualquier caso interrupciones.

Todas estas consecuencias vienen provocadas principalmente cuando los virus atacan a:

- Registros de inicialización (boot).
- Programas Com.
- Programas Exe.
- Combinación de ellos.

En los años 70 se detectaron los primeros virus informáticos. No nació como un virus propiadamente dicho sino como un fraude informático, utilizado para desviar sumas de dinero en cuentas corrientes procesadas por ordenador.

La bomba lógica

Se denomina **bomba lógica**: «al conjunto de instrucciones, o rutinas, que, en un momento dado, obliga al programa a ejecutar acciones no previstas con el fin de ocasionar daños».

Son de fácil ejecución ya que no es más que la introducción de determinadas instrucciones en el programa deseado. Se ejecuta en unas condiciones muy determinadas. Estas pueden ser:

- Fijas (como el virus Viernes 13).
- Variables (cada «x» registros).
- Aleatorias (en función de la hora o de circunstancia prevista para desencadenar la acción).

Los efectos que este tipo de sabotaje producen son: Daños a ficheros, daños a registros, errores intermitentes, imposibilidad de acceso, fraudes, mala imagen, pérdida de tiempo, parada del proceso.

Todo esto indica que la persona o personas que se dedican a realizar este tipo de sabotaje tienen que ser conocedoras de la informática, como el caso planteado por comerciantes de software que introducen instrucciones de autodestrucción en los programas, con la finalidad de ejecutarlos si estos no eran abonados o eran copiados sin autorización.

«Superzapping»

Este nombre proviene del vocablo «superzap» o super llave. Se utiliza como una herramienta del sistema, la cual supera todo tipo de control con el fin de introducirse por motivos de emergencia en cualquier punto.

Esta técnica está destinada a: modificar, borrar, destruir, copiar, insertar o prohibir la utilización de datos memorizados en el ordenador o en los soportes del mismo con el fin de que no quede nunca constancia del trabajo realizado.

«Data diddling»

Es considerado un clásico dentro del género delictivo informático. Su significado es el de «entrampando datos» y consiste en la introducción de información falsa al ordenador o también la eliminación de datos reales cuyo destino fuera introducirlos en el ordenador.

Este delito es cometido durante los procesos de codificación, registro, transporte, conversión, modificación o en la verificación de datos. También se incluyen en estas actividades la sustitución de bandas magnéticas, discos o diskettes cuya prevención no es muy difícil pero si lo es la detección. Para ello sería necesario el realizar controles internos en las aplicaciones y además investigar a las personas que se encuentren relacionadas con el hecho.

«Trojan horse»

El «caballo de Troya» es asignado a la modificación de programas de uso habitual, de tal forma que en ciertos momentos actúe de forma contraria. Este nombre fue obtenido de la famosa historia «La Iliada» (Homero), ya que como en ella para conseguir el objetivo se emplearon medios que pasaran desapercibidos durante un tiempo.

Para la ejecución de este delito informático es necesario tener un nivel de conocimientos técnicos, conocer el acceso al programa o al ordenador. También debe disponerse de tiempo suficiente para realizar ensayos. La finalidad de este procedimiento es desviar las utilidades del programa para el aprovechamiento propio.

Las distintas opiniones sobre la posibilidad de prevenir los riesgos nos acerca a un dimensionamiento del problema que nos afecta. Desde la Dirección General de Policía, que asegura lo difícil y costoso de evitar, en su Seminario sobre «Fraude Informático». Hasta Luis Camacho que en su publicación «El delito informático», comenta como es un método muy difícil de detectar pero sencillo de prevenir ya que basta con realizar unos procedimientos de catalogación/descatalogación de programas en las librerías de tal forma que queden bloqueadas y no se pueda acceder a ellas más que con permisos.

«Rounding down»

Podemos traducirlo como «Redondeando abajo» pero lo llamaremos como se ha deno-

minado en España «La técnica del salami». Consiste en la introducción o modificación de algunas instrucciones en determinados programas (libretas de ahorro, cuentas corrientes, cálculos de intereses, etc.) con el fin de reducir de forma progresiva los saldos.

Las pérdidas, individualmente, son de escaso valor pero en conjunto suponen grandes cantidades de dinero. En esta actividad delictiva se hace muy necesario la realización de soluciones preventivas.

Podemos mencionar como vías de detección el procedimiento de verificar las instrucciones del programa y el recálculo después de la ejecución del mismo.

«Asynchronous attacks»

Este delito se desarrolla en los sistemas de explotación, ya que su funcionamiento es de forma asíncrona mientras que en los programas de aplicaciones no se podría producir porque funcionan de manera síncrona. Sus acciones son ejecutados con factores ajenos a él por lo que cabe la posibilidad de utilizarlos de tal manera que las condiciones de trabajo puedan ser modificadas y el sistema no lo registre, por lo tanto se estará trabajando en unas condiciones falsas. El período más propicio para una agresión de este tipo es el que se encuentra entre la creación y verificación de datos durante la explotación.

Contra este tipo de ataques se puede utilizar como medio de prevención el que los técnicos de sistemas no conozcan la estructura de la información ni el detalle de la aplicación.

«Scavenging»

Es la recogida, por un operador, de información residual de una cinta teóricamente obsoleta del fichero de clientes. Su intención es la de recuperar la información que en ella se contiene sobre el funcionamiento de las aplicaciones del sistema. Puede tener, esta información, un origen físico si procediera de material de desecho o electrónico, si su origen proviene de los residuos encontrados en la memoria del ordenador o en algún diskette.

Es muy fácil, regularmente, recoger material residual de los centros de proceso de datos y difícil incriminar al autor por lo que innumerables expertos ven la necesidad de potenciar en las siguientes facetas las normas de prevención:

- Custodia permanente a los listados de pruebas de programas, segundas copias de listados, listados de errores, etc., es decir todo el material de trabajo o de desecho.
- Destrucción metódica del material desechable.
- Como norma a cumplir se debe borrar las áreas de memoria utilizadas en un programa así como los directorios ya invalidados.
- Igualmente normatizar el borrado de las cintas magnéticas.

«Data leakage»

Es la divulgación de información confidencial por motivos tanto de orden económico (lucro) como ético (venganza personal). Este procedimiento es también conocido por espionaje industrial, el cual es muy temido por todo tipo de empresas. No se emplea medidas de control preventivo, y cuando se hace son muy escasas.

«Simulation and modeling»

Se utilizan las posibilidades del ordenador en simulación de situaciones para poder planificar el delito. Este no es un método muy común.

«Pygybacking and impersonation»

Estos dos métodos, de quienes intentan de forma ilícita acceder a la información, son el acceso indebido y la suplantación representadas en:

– El aprovechamiento de puntos débiles de la seguridad preventiva, lógica o tradicional que les permita acceder a las áreas restringidas y obtener información reservada.

– Suplantar la personalidad de otros empleados con el nivel de autorización suficiente que le permita acceder al lugar deseado.

Tanto uno como otro método son tradicionalmente perseguidos, ya que aunque se han aplicado soluciones en alguna ocasión se ha logrado un nivel alto de datos.

«Wiretapping»

Con este término se denomina el asalto de las líneas de transmisión de datos. Para paliar este método sería necesario criptografiar la información que se transmite por las líneas telefónicas, según se ha tratado anteriormente en este capítulo.

Para combatir el virus la mejor forma de hacerlo es con una vacuna. Denominamos VACUNA «al programa informático destinado a combatir los virus que han contaminado a los ordenadores ya sea por intercambio de disketes, interferencias telefónicas o accesos aleatorios con aparatos».

La primera vacuna fue la denominada TCELL creada por la empresa sueca de informática Sectra-Secure. La finalidad de esta vacuna es la de supervisar o revisar la red de sistemas de procesamiento de datos detectando los fallos en la marca electrónica de cada fichero. Más tarde otras empresas, como IBM; Data Hard; Esagei, etc., crearon vacunas para sistemas informáticos y ordenadores personales de sus usuarios.

Hoy día con la proliferación de los ordenadores personales, existen casas especializadas en crear vacunas específicas para los virus que de forma continua, aparecen en el mercado mundial.

Algunos casos significativos

Quizá el primer fraude informático conocido con resonancia fue el padecido por la «Equity Funding Life Company», ascendiendo a un total de 27.000 millones de pesetas (230 millones de dólares USA), lo que llevó a la quiebra a la mencionada entidad convirtiéndose en un clásico del género.

Consistía en la emisión fraudulenta de un gran número de pólizas de seguro de vida a nombre de personas inexistentes. Lógicamente como suele ser normal en el mercado asegurador, con el fin de dispensar los riesgos actuales y conseguir liquidez, las pólizas las comenzaron a vender a compañías reaseguradoras. Estas ventas les proporcionaban una entrada clara de dinero no ocasionando los gastos de formalización de las pólizas al ser de tipo fraudulento.

El inconveniente que se encontraron fue la legislación americana, pues exige que las compañías aseguradoras que emiten pólizas retornen el noventa por cien de las primas del primer año a los reaseguradores. Con esto después de este primer período tuvieron que hacer un fuerte desembolso, el cual lo cubrieron con la emisión de más y más pólizas fraudulentas. Al ver que las ganancias no eran del todo satisfactorias pensaron una segunda parte del fraude con unos beneficios más sabrosos, consistente en reclamar la cobertura de las pólizas a las compañías reaseguradoras ante la defunción de los suscriptores de las mismas. Sin duda el plan era alentador pues recogían las coberturas de las reaseguradoras sin tener que desembolsar, al no existir el fallecido. Naturalmente todo terminó con una denuncia de un empleado molesto que provocó la acción de una auditoría. Wall Street implacable ante comentarios o rumores sobre cualquier compañía se encontró con la bajada en picado de las

acciones de la Equity en la bolsa de Nueva York y el final de los hechos con la consiguiente sentencia de los tribunales sobre los artífices del fraude.

Todo ello fue posible al estar integrado en el ordenador los diferentes aplicativos de la compañía, una manipulación de los programas hacía aparentemente normal la operatoria fraudulentamente creada a una serie de pólizas.

A principios de 1990 se descubre uno de los más grandes fraudes informáticos. El artífice fue Michel Milken a quien le condenaron a pagar la cantidad de 70.000 millones de pesetas (600 millones de dólares) y una pena de cinco años de cárcel, sin lugar a dudas marcó el récord en este sentido.

Puede llevar a error el pensar en el volumen del fraude informático, pues se llegan a descubrir un bajo porcentaje de los mismos. Unas veces la falta de denuncia de los mismos hace difícil que trascienda a la opinión pública y a su conocimiento, se debe principalmente al daño intangible en la imagen de la compañía defraudada, lo que motiva esta falta de denuncias y este ocultismo sobre los fraudes.

En España, manejando alguno de los escasos datos fiables al respecto, nos alertan sobre la magnitud de estos delitos a pesar que en 1987 se promueve la legislación de normas protectoras del derecho de la propiedad intelectual del software, tipificando como delito la copia no autorizada de programas informáticos, las empresas del sector un año después hacen público un balance en el que la actividad fraudulenta había supuesto 56.000 millones de pesetas (500 millones de dólares UDSA) referida principalmente a la piratería del software en ordenadores personales.

Estando en plena vigencia la normativa, dos de cada tres equipos informáticos de éste tipo instalados en nuestro país utilizaban sistemas ilegales. El transcurrir de los años hasta el actual no ha visto variar sustancialmente esta situación, más bien ha empeorado.

Técnicas de investigación

El software de seguridad tiene como fin controlar el acceso, estado y fiabilidad de la información. El existente en el mercado es relativamente nuevo. Antes de que apareciera se utilizaban controles de acceso dentro de las aplicaciones.

También ocurre que no todos los sistemas operativos y aplicaciones pueden ser controlados por los productos que hay en el mercado y, en esos casos, es necesario desarrollar internamente mecanismos de protección.

El software de seguridad desde el punto de vista de adquisición se clasifica en: propio y paquetes de mercado.

Software de seguridad desarrollado por la empresa

Cuando no existen soluciones en el mercado que cubran las necesidades de la seguridad de la información debe ser la propia empresa quien desarrolle un sistema, aunque se deben tener en cuenta los siguientes aspectos negativos que presentan:

- Excesivo coste de desarrollo.
- Orientado a una aplicación cada vez.
- Los programas del sistema operativo se lo saltan.
- Dificultad de actualización.
- Mayor consumo de máquina.
- Basado en tablas o ficheros que hay que proteger.
- Dependencia de su creador.
- No resiste un ataque serio.
- Dificultad de acomodo a nuevos sistemas operativos.
- Etc.

Sólo es aconsejable la realización de un sistema de seguridad por parte de la propia empresa cuando esté apoyado por alguno estándard.

Paquetes existentes en el mercado

Los paquetes de Seguridad constan de una serie de programas que se incluyen en el sistema operativo de la máquina, además de unas tablas internas, en memoria, y de unos ficheros en donde se definen los perfiles y reglas de protección.

En el mercado existen varios paquetes de seguridad entre los que destacamos:

- RACF.
- TOP SECRET.
- OMNIGUARD.
- ACF2.
- SECURE.
- Etc.

El funcionamiento es similar, aunque su diferencia se encuentra en la potencia y sistemas operativos bajo los que pueden trabajar. La dinámica de investigación en todos ellos es igualmente similar, constando de las siguientes partes:

- **Control de incidencias**

Cuando un usuario quiere realizar algo distinto a lo que está autorizado el RACF responde de la siguiente forma:

- Impide el acceso al usuario y lo notifica con un mensaje.
- Graba lo sucedido anteriormente en el SMF (System Management File), con todos los datos de la anomalía.

*Además de esta misión el SMF graba en un fi*chero todo lo sucedido archivándolo por fechas y horas. De esta forma el administrador de seguridad, con ayuda de unas utilidades del SMF, podrá explorar todas las incidencias ocasionadas.

- **Clasificación de los recursos a proteger**

RACF protege distintos recursos, pero para ello los agrupa por clases. Va a ser en estas clases donde se definen los perfiles que antes hemos definido.

Clases principales:

- *Usuarios*

*El primer paso que se debe dar es el de identi*ficar a la persona o personas que vayan a utilizar el ordenador. Para ello será necesario incluir los datos del usuario/s (número de identificación, nombre, apellidos, contraseña, etc.). El único dato que no es conocido ni por el administrador de seguridad es la contraseña ya que es almacenada en lugar secreto y criptografiada.

Una vez que se conecta el ordenador el sistema operativo pasa información al RACF y este supervisa las características del usuario y la contraseña. Si el procedimiento es incorrecto no le permite pasar, le avisa del error cometido y registra lo sucedido. Si es correcto, le permite el acceso y que circule en el ámbito que tiene marcado de antemano.

Si el usuario intenta el acceso, sin conseguirlo, durante un número de veces prefijado el RACF tiene la posibilidad de revocarle y desactivarle. Para poder entrar se necesitará la intervención del administrador de seguridad.

- *Grupos*

Los grupos se forman para facilitar el trabajo al administrador y conceder los permisos a un número limitado de usuarios.

- *Dataset*

Esta clase se encarga de agrupar a todo tipo de ficheros en cintas, discos, librerías y bases de datos.

- Transacciones

Las transacciones interactivas son definidas por el RACF de tal forma que flexibiliza la seguridad y el control lo hace más grande y define por cada transacción la lista de usuarios que están autorizados. En el caso del IMS existen dos clases: TIMS para el real y el PIMS para las pruebas.

Figura 5. Software de seguridad

Planes de prevención

Selección de un paquete de seguridad

Antes de elegir un paquete de seguridad será necesario conocer una serie de criterios que ayuden a realizar la elección. No es un artículo común por lo que en la selección intervendrá un equipo formado por:

- El jefe de seguridad.
- El director de informática.
- El jefe de análisis/programación.
- El jefe de explotación.
- El administrador de seguridad.
- El auditor interno.
- El vendedor.

Será necesario disponer de una serie de **criterios funcionales** en un software de seguridad como pueden ser:

- Contabilidad
  - Controla a los individuos y acciones.
  - Estadísticas de acceso a recursos. Control de cómo se accede a los recursos.

- Auditoría
  - Debe llevar:
    - Log de accesos (quién)
    - Log de violación (quién y qué)
    - Log de modificaciones (quién y a qué)
- Integridad
  - Debe llegar al control de operaciones como:
    - *Allocate*
    - Open
    - Scratch
    - Rename
    - Catalog
    - Uncatalog
    - Recatalog
  - Debe llegar también a recursos varios como:
    - Terminales
    - Ficheros
    - Cpu
    - Comandos
    - Programas
    - Librerías
  - Debe alcanzar a los diversos subsistemas que haya:
    - Batch
    - Tso
    - Cics
    - Ims
- Uso/rentabilidad

Hay que tener en cuenta en una aplicación de este tipo la facilidad con que sean comprendidas las reglas por el personal y si el coste será provechoso con respecto al rendimiento.

Una vez expuestos los criterios funcionales serán objeto de consideración los siguientes aspectos que contemplan los **criterios técnicos**:

- Compatibilidad

Debe existir compatibilidad con el «hardware» existente, el «software» de sistemas y el «software» de aplicaciones.

- Impacto en la explotación
  Facilidad de instalación.
  Facilidad de implementación.
  Expandibilidad y compatibilidad.
- Documentación y soporte

La documentación existente debe ser amplia y de fácil comprensión mientras que el soporte será rápido y eficaz.

Con la aplicación de las medidas de seguridad en los puntos críticos de un sistema informático y la adecuación de normativa interna para el seguimiento y control de acceso y tráfico, en definitiva, de nuestros datos, se conseguirá minimizar el riesgo y estar en condiciones de conocer el fraude en los momentos en los que se pueden adoptar soluciones y acometer la estrategia específica sin producirse un deterioro importante del sistema. ■