DATOS INFORMATICOS: RIESGOS Y PREVENCION

JOSÉ MANUEL MORÁN VIÑE*

El autor de este trabajo deja a un lado todo lo relativo a los equipos (Hardware) para centrarse en los datos informáticos (Software) haciendo un recorrido por los distintos riesgos que pueden afectarlos y recomendando algunas acciones para minimizar sus consecuencias.

La exposición se divide en dos grupos: a) *riesgos físicos que pueden afectar a los datos por destrucción o deterioro de los portadores externos, y* b) *aquellas alteraciones que pueden realizarse en el Software por manipulación fraudulenta a través de terminales.*

La creciente mecanización que se ha producido en los distintos sectores económicos en los últimos años ha generado una gran influencia en la economía de la empresa de aquellos riesgos que afectan a sus medios informáticos.

Si bien la destrucción o paralización del Centro de Procesos puede llegar a causar una interrupción en la marcha normal del negocio, que produzca importantes pérdidas económicas, no es menos cierto que la manipulación o destrucción de los datos pueden causar no solamnete el mismo efecto sino también conllevar una responsabilidad civil de la empresa por violación de la privacidad de terceras personas.

Este artículo se centra en los riesgos que afectan a los datos *(software)* y su prevención, tanto en lo que se refiere a los daños físicos que puedan sufrir los portadores externos como a los que se pueda causar a la información contenida en ellos por manipulaciones fraudulentas.

En este aspecto, tres grandes grupos recogen la clasificación de los daños que puede sufrir la información:

Destrucción.
- Divulgación.
- Modificación.

Existe un matiz importante a tener en cuenta: mientras la destrucción se presenta como un hecho visible que lleva inmediatamente a tomar medidas de reconstrucción a partir de duplicados, en los dos segundos casos, el fichero aparece in-

* Licenciado en Ciencias Económicas y Actuario. En la actualidad, desempeña las funciones de gerente de riesgos y seguros de IBM en España.

tacto y puede pasar un largo período de tiempo antes de que se detecte que la información registrada es errónea o que la misma se ha facilitado a terceras personas.

RIESGOS DE DAÑOS MATERIALES EN DATOS INFORMATICOS

Localización del almacen de portadores externos

Por motivos operativos, el almacén de portadores suele ser contiguo al Centro de Procesos, por lo que las recomendaciones sobre su situación física serán las mismas que para éste.

El criterio más difundido es que el Centro de Procesos debe situarse en un edificio separado, dado que las operaciones que se realizan en él tienen un menor peligro potencial que las del resto de la industria y permite un mejor control de entrada.

En sentido contrario, hay que señalar, no obstante, que la localización en un edificio aislado hace al Centro de Procesos más vulnerable a ataques deliberados, ya que es más fácil identificar los accesos y las líneas de fuerza y telecomunicación.

La decisión sobre la situación del Centro de Procesos deberá basarse en un detallado estudio de los riesgos potenciales y medidas de seguridad. Es posible que la baja peligrosidad de las actividades de la empresa y los medios de prevención ya existentes en el momento de la instalación del Centro de Procesos no hagan aconsejable la elección de un edificio aislado.

Una localización en el centro del edificio es más segura que la situada con muros al exterior. Hasta hace relativamente poco era costumbre bastante difundida situar el Centro hacia el exterior, cerrándolo con cristales que permitieran su visibilidad, consiguiendo así un escaparate anunciador de la actividad informática realizada. Esto es una clara invitación a la ejecución de actos dolosos; si no es posible sustituir los cristales por muro de obra, éstos deberán ser antigolpes y se colocarán paneles interiores que impidan la visión.

Intrusismo

Es importante que el acceso al Centro de Procesos esté limitado a las personas que trabajan en su interior o a aquéllas con suficiente autorización. Es recomendable la habilitación de dos entradas, una para personal y otra para proveedores. Las salidas de emergencia deberán abrirse sólo desde el interior y estar provistas de una alarma que actúe cuando se abran aquéllas.

Existen diferentes métodos de control de la entrada: cerraduras especiales, tarjetas magnéticas, doble puerta controlada por circuito de televisión, etc. Es conveniente que la puerta esté provista de un sistema de alarma que actúe cuando aquélla permanezca abierta más tiempo del necesario para el paso de personas.

Se deberá registrar en un libro al efecto la entrada de toda persona no perteneciente al Centro de Procesos indicando motivo y duración de la estancia. Cada persona presente en el recinto deberá llevar su identificador claramente visible que indique su condición de:

— Empleado.
— Visitante.
— Proveedor.

En el caso de visitantes y proveedores, mientras dure su permanencia, deberán estar constantemente acompañados de un empleado.

Interrupción en el suministro de energía eléctrica

Un corte de energía eléctrica puede producir una pérdida de datos en el sistema. Si la información se almacena en cintas, discos, etc., los únicos datos que se perderán serán los que se encuentran en proceso en el momento del corte y podrán ser reconstruidos a partir de los ficheros. En caso de procesos de larga duración, se utiliza el sistema de etapas *(check points)*. Una vez que se procesa una etapa, se almacena la información de la misma. De esta manera, en caso de fallo en el suministro eléctrico la información perdida será solamente la de la última etapa y no será necesario rehacer el proceso entero.

En cualquier caso, es aconsejable disponer de generadores a gas-oil o baterías que entren en fun-

cionamiento automáticamente en caso de corte de corriente.

Daños por agua

Los portadores de datos no son dañados por el agua. De hecho, ésta se utiliza en algunas ocasiones para limpiar las cintas.

Si bien los datos no son destruidos por el agua, es recomendable su limpieza y secado a la mayor brevedad.

Fuego

Los daños a cintas magnéticas comienzan a temperatura de aproximadamente 38 °C, si bien pueden, en general, ser reparados satisfactoriamente los ocurridos hasta los 49 °C. A partir de este punto, las posibilidades de reconstrucción decrecen rápidamente con el aumento de temperatura.

En lo que a discos se refiere, los daños comienzan a partir de unos 66 °C con más rápido incremento del deterioro al elevarse la temperatura.

No hay que olvidar que aunque el portador de datos no sufra la acción directa del calor, las partículas desprendidas en la combustión pueden depositarse en su superficie haciendo ilegibles los datos registrados.

La experiencia muestra que la mayor parte de los casos de daños producidos por fuego en Centros de Proceso de Datos son consecuencia de incendios provenientes del exterior.

Para proteger la librería de datos de fuegos exteriores, las paredes, techos, suelos y puertas del recinto deben tener una resistencia al fuego de al menos 2 horas. En la actualidad existen en el mercado cámaras prefabricadas especialmente diseñadas como almacenes de portadores de datos, con diferentes formas de resistencia al fuego.

Se pueden adquirir igualmente contenedores para cintas y discos que mantienen en su interior una temperatura máxima de aproximadamente 43 °C y una humedad relativa del 85%.

Como primera línea de defensa contra incendios pueden utilizarse extintores de agua o mangueras, debiéndose entrenar a los operadores adecuadamente sobre su uso.

El sistema de alarma deberá ser por detectores de humo, que se colocarán en el recinto, en los falsos techos, si existen, y en el conducto de retorno del aire acondicionado. La situación de los detectores dentro de la sala se efectuará teniendo en cuenta el flujo del aire y manteniendo una densidad de un detector por cada 23 m^2.

Dado que, como se ha mencionado anteriormente, el agua no daña a los portadores de datos, resulta eficaz la utilización de *sprinklers*. Puede ocurrir que, cuando la temperatura del local alcance el techo donde están instaladas las cabezas, los daños causados hayan sido ya considerables, por lo que es recomendable el uso de sprinklers tarados a más baja temperatura de la normal de actuación o conectar la red con el sistema de detección.

Magnetismo

Un campo magnético permanente no produce efectos apreciables en una cinta o disco a más de 52 cm. A una distancia de 21 cm puede causar errores y hacer ilegibles los datos. Sólo a una distancia de 8 cm el efecto de un potente campo magnético puede borrar los registros.

En estas circunstancias, es prácticamente imposible que un campo magnético generado fuera del edificio pueda causar efectos en los ficheros situados en su interior. Una simple medida de protección sería separar los portadores de datos a una distancia de 52 cm del límite exterior del edificio. Si la librería se encuentra en una zona con paredes al exterior, se puede disponer de un corredor alrededor del perímetro para conseguir esta distancia.

Radar

Para que una señal de radar pueda interferir en operaciones de procesos de datos, la señal de llegada al equipo debería ser al menos 5 voltios por metro. Esto sucede solamente si la antena emisora puede verse desde una ventana y está apuntada directamente a la misma.

Las paredes por sí mismas reflejan la señal y es protección suficiente para las ventanas la instalación de una rejilla de aluminio.

Radiación

La radiación y partículas radiactivas no constituyen una amenaza para las instalaciones de proceso de datos. La energía de los campos magnéticos relacionada con radiaciones atómicas o rayos X es insignificante para poder modificar los registros contenidos en un portador de datos.

Backup

En caso de información importante para la empresa se deben crear, con una frecuencia predeterminada, duplicados de los ficheros, que se guardarán en un lugar alejado del local principal para evitar que un mismo riesgo pueda destruir ambos.

En caso de tratarse de registros vitales, es usual la confección de dos copias del mismo fichero.

Hasta el momento, lo tratado se ha referido al riesgo de destrucción física del portador externo con la consiguiente pérdida de la información. Pero, tal como se ha expuesto al principio de este trabajo, los datos pueden ser modificados o destruidos por manipulación a distancia a través de terminales, riesgo que se acentúa en la actualidad con el creciente auge del teleproceso. A continuación se analizarán las posibles formas de protección de los datos.

RIESGOS DE DESTRUCCION DE DATOS POR MANIPULACION. MEDIDAS DE PROTECCION

Propietario

Se puede definir una *aplicación* como un conjunto de programas creados para resolver un determinado problema.

Antes del desarrollo de una *aplicación* se nombrará un *propietario* de la misma que deberá ser una personal íntimamente ligada al área que se va a mecanizar y tendrá la responsabilidad de la calidad y seguridad de los datos contenidos.

Entre los cometidos del *propietario,* se pueden destacar los siguientes, relativos a la seguridad:

a) Separación de tareas

De no existir suficientes medidas de seguridad, sería relativamente fácil para un programador realizar un acto fraudulento simplemente cambiando las instrucciones del programa.

En estas circunstancias, es aconsejable que las tareas de programación, autorización, modificación y proceso se distribuyan entre distintas personas.

b) Clasificación

El *propietario* debe analizar las características de la información contenida en la aplicación y clasificarla según las consecuencias que su divulgación o modificación pueden acarrear a la empresa.

Un posible cuadro de jerarquías sería:

— Sin clasificación.
— Uso interno.
— Confidencial.
— Restringuido.

c) Autorización

Se deben examinar las solicitudes de acceso a la *aplicación* de terceras personas en función de su relación con la misma y la necesidad de su uso. Una vez confirmada esta necesidad y aprobado el acceso, se establecerá el nivel de operatividad de la persona dentro de las siguientes categorías:

-- Lectura

Permite acceder a la información pero sin poder actuar sobre los registros.

— Escritura

Autoriza a añadir nuevos registros pero no a modificar los existentes.

— Modificación

Permite, además, la modificación de los registros del fichero.

Lógicamente cada una de las categorías contiene las atribuciones de las anteriores.

Una vez autorizado el acceso a una determinada persona, se le asigna un número de usuario *(user-id)* que constituirá su identificación.

d) Control

Deben establecerse controles para el mantenimiento de la seguridad de la información, pudiendo seguirse las siguientes etapas:

- Análisis de la posibilidad de manipulación fraudulenta de la *aplicación*.
- Determinación de los programas críticos dentro de la *aplicación*.
- Separación de las tareas de mantenimiento de estos procesos entre varias personas.
- Revisión y aprobación de nuevos programas o modificación de los existentes.
- Control de instalación de programas para evitar cambios.
- Comparación periódica de los datos almacenados en los portadores externos con una copia de control.
- Procedimientos de auditoría.

Todos estos controles deben ser informados oportunamente a todas las personas afectadas.

Acceso

Para poder acceder a una determinada *aplicación*, el usuario debe identificarse ante el sistema, pudiendo esta identificación ser de tres tipos:

- Identificación personal.
- Identificación por cerradura.
- Identificación por clave.

Dentro del primer grupo se encuentran características únicas de las personas, como huellas dactilares o la voz, por lo que es el sistema más seguro de los tres. No obstante, su difusión es un tanto limitada debido a su alto coste.

El segundo grupo engloba la utilización de llaves especiales y tarjetas que abren el acceso a través de terminal. Este sistema es el menos seguro por la posibilidad de extravío o realización de copias de las mismas.

Algunos tipos de tarjetas poseen una banda magnética grabada digitalmente que identifica al operador. Este código no es visible y su reproducción es sumamente compleja. Como precaución accesoria se deben cambiar estos códigos con cierta frecuencia.

Las tarjetas no deben dar ninguna indicación de su utilidad para evitar su mal uso en caso de extravío. Una medida de prevención contra el copiado puede ser recoger las tarjetas de los operadores después de terminada la jornada y guardarlas en lugar seguro.

Al tercer grupo, el más difundido, pertenecen las *passwords*. Una *password* es un conjunto de caracteres alfabéticos o numéricos ideados por el propio usuario y que constituyen su código de entrada al sistema.

La eficacia de la *password* depende obviamente de su privacidad, motivo por el que no debe quedar reflejada en la pantalla cuando se teclea, evitando así observaciones dolosas.

La *password* debe ser fácil de memorizar, para que pueda recordarse sin necesidad de escribirla, pero nunca obvia, predecible o trivial. Para dificultar su descifrado, debe constar al menos de seis caracteres numéricos, cinco si son alfabéticos o cuatro en caso de alfanuméricos. Algunos sistemas contienen ficheros de palabras fácilmente deducibles (nombres, días, meses, etc.) y rechazan aquellas *passwords* que coinciden con los mismos.

Una práctica habitual para comprobar la idoneidad de una *password* es que el jefe de cada grupo requiera periódicamente a su personal que le informe de la elegida por cada uno, cambiando seguidamente todas ellas.

Este código debe ser cambiado periódicamente, sin que el sistema admita la repetición de la anterior. En circunstancias normales el plazo no debe ser superior a dos meses, reduciéndose a un mes en el caso de personas que tengan poder para manipular los datos (operadores, administradores, técnicos de sistemas, etc.), o en caso de que la información a la que se accede sea de carácter confidencial.

La identificación del usuario se realiza por comparación de la *password* recibida con la archivada en el fichero del sistema, lo que hace vital, para la utilización de este método de acceso, la protección del citado fichero.

Una primera medida es situar el fichero en el mismo recinto del Centro de Procesos, con lo que se beneficiaría de las medidas de seguridad de éste. Como protección complementaria puede cifrarse la *password* antes de su registro en el fichero. La criptografía puede igualmente utilizarse para evitar revelación de la *password* por conexión de terceros en la línea terminal del ordenador.

Esquema de acceso

Actualmente existen programas de protección, incluidos en los sistemas, que controlan el acceso a los diferentes ficheros. A continuación (figura 1) se observan las distintas etapas de uno de ellos (concretamente RACF):

- El operador teclea su número de usuario *(userid).*
- El sistema lo identifica comparando este número con los contenidos en un fichero de *userids.*
- El operador teclea la *password.*
- El sistema la valida efectuando una doble operación:
  - Compara la recibida con las recogidas en un fichero de *passwords* del sistema y paralelamente compara este fichero con el de *userids* para comprobar que efectivamente corresponde al usuario que solicita el acceso.
  - Como norma general, al tercer intento de acceso utilizando una *password* errónea, el sistema rechaza al usuario prohibiéndole la entrada.
- Un programa de selección de accesos determina para qué ficheros tiene autorización el usuario, facilitándole la entrada a los mismos y rechazando cualquier intento de consulta a los no autorizados.
- Este programa registra al mismo tiempo los intentos no autorizados de acceso a datos protegidos *(violaciones),* facilitando periódicamente al *propietario* de la *aplicación* un informe de éstos.

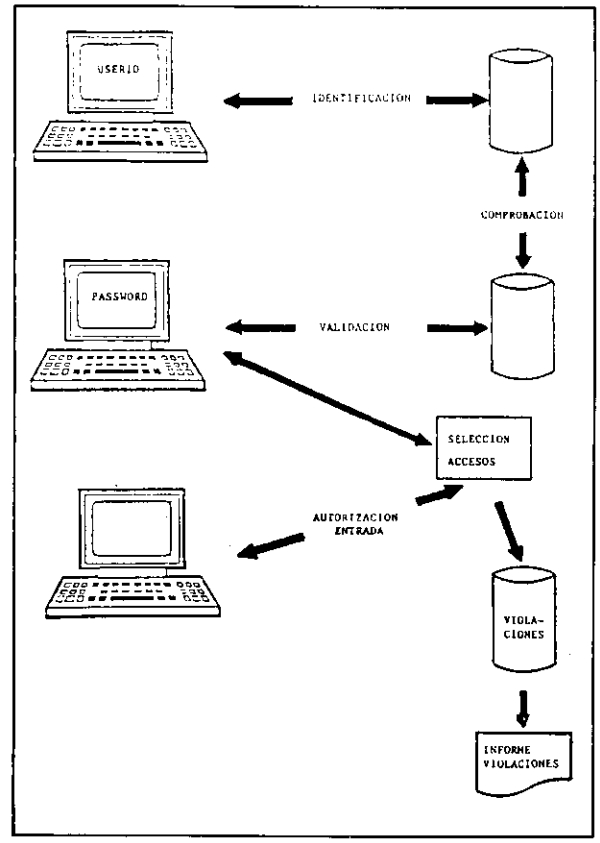

Figura 1. — Etapas del programa de protección de datos informáticos.

□