HERRAMIENTAS DE AUDITORIA

El fraude informático

Eulàlia Manero Font
Departamento de Informática de la Sindicatura de Comptes de Catalunya

La función informática de una organización es la que se dedica a coordinar la utilización de los recursos informáticos: materiales, financieros y humanos de la misma. De una forma más general se puede hablar de aquella función encargada de la adquisición, tratamiento, almacenamiento y difusión de las informaciones de la organización, dentro y fuera de ésta.

La función informática de una organización es cada vez más importante. La informática se ha implantado de forma masiva en los últimos años y a veces ha faltado la adaptación del mundo a la invasión de los ordenadores. El mundo significa aquí las leyes, los usuarios, las empresas... De hecho, aún existe la creencia de la infalibilidad de la informática, pero se debe tener muy claro que es una fuente muy importante de riesgos. Para una entidad, y más aún si se trata de una entidad financiera, los sistemas que integran la función informática son básicos ya que en ellos se encuentra toda la información.

Delitos informáticos : tipos y definiciones

Un delito informático es aquel que está relacionado directamente o indirectamente con un medio informático. Como medio informático nos referimos al *hardware* (ordenadores, redes de comunicación, dispositivos de entrada y salida de datos...), al *software* (tratamiento de textos, programas, sistemas operativos...), y a los datos que se generan y almacenan.

Delito significa, *«un acto deliberado realizado con la intención específica de perjudicar a una persona u organización y, a veces, proporcionar un beneficio ilegítimo a quien lo realiza»*.

El concepto de *delito informático* es ambiguo ya que se puede referir a:

- Delitos que recaen sobre objetos pertenecientes al mundo de la informática: destrucción o substracción de programas o material; alteración, destrucción o reproducción de datos almacenados; utilización indebida de los ordenadores.
- Delitos más variados y tradicionales en los cuales la informática no es el objeto sino el medio para cometerlos: delitos contra la intimidad, contra el patrimonio, contra la administración pública, contra la seguridad nacional.

Algunos ejemplos de delitos son:

Fraude informático: Delito informático realizado con intención de engañar o perjudicar a una persona u organización y proporcionar un beneficio ilegítimo a quien lo realiza.

Hacking: Significa *Intrusión* en inglés. Acceso no autorizado a un sistema informático. Puede ser que no pretenda perjudicar sino, tan solo, que se haga como hobby. Un *hacker* es un fanático de la informática a menudo equipado con un PC y un módem, que tiene como objetivo entrar en los sistemas informáticos saltándose las medidas de seguridad establecidas y leer la información confidencial o substraerla.

Sabotaje: Se refiere a cualquier tipo de acción que perjudique el funcionamiento normal de la empresa. Por ejemplo, destruir datos en soportes magnéticos con imanes o causar cualquier daño a los sistemas informáticos.

Virus informáticos: Programa usualmente diseñado para copiarse de un sistema a otro y situarse en el ordenador de manera que sea posible modificar o destruir los programas y los ficheros de datos.

El fraude informático

Características del fraude

Las características intrínsecas de todo tipo de fraude son las siguientes:

- El fraude es una acción deliberada de manipulación de datos: en la entrada, en el programa o en la salida de datos.
- El fraude puede producirse en cualquiera de las fases de tratamiento o procesamiento informático de los datos.
- El objetivo es obtener un beneficio económico.
- El fraude se realiza contra una organización o persona.
- El medio informático está involucrado directa o indirectamente.

La Informática no es infalible y sí una fuente importante de riesgos

Entorno propicio al fraude

Los tres elementos más importantes que se presentan en un entorno propicio al fraude, bien en el potencial perpetrador o en la organización donde se comete, son los siguientes:

Deshonestidad: Refiriéndose a la deshonestidad del potencial perpetrador de un fraude.

Motivación: Generalmente son dos tipos de necesidades que presenta el que realiza el fraude:

- Necesidad económica
- Necesidad psicológica: desafío, venganza, vanidad...

Oportunidad: Se refiere a la oportunidad que la organización presenta al potencial perpetrador a través de controles y medidas preventivas inadecuadas.

Contra la oportunidad, la organización puede tomar medidas. A más seguridad de los sistemas, menos oportunidad habrá para cometer fraudes. En cambio, contra la motivación se puede hacer muy poco desde el punto de vista informático.

Fuentes de fraudes

En la siguiente figura podemos ver la procedencia de las personas que realizan un fraude:

Fraude interno: Originado por componentes de la propia organización. Puede ser muy grave ya que es realizado por personas que conocen muy bien la función informática.

Fraude por colusión: Originado por personas de la organización y personas externas, en asociación.

Fraude externo: Originado por personas no pertenecientes a la organización.

Los fraudes más comunes son los de tipo interno. Por esta razón es muy importante que el personal sea cuidadosamente elegido

Tipología del fraude

Tipos según el objeto del fraude

En esta sección se hace una clasificación de los fraudes. Esta no será una lista cerrada, sino una relación de los fraudes más comunes agrupados por el objeto del fraude, es decir, según el bien que se pretende obtener ilegalmente.

(1) Movimiento: Cambio en un fichero. Puede ser una modificación, un alta o una baja de un registro.

(2) Transacción: Cada una de las operaciones de entrada, normalmente hechas desde el terminal o estación de trabajo y, a menudo, de forma interactiva por medio de las cuales un usuario comunica al sistema los datos de un movimiento.

Sustracción de dinero o documentos que lo sustituyen: Aquí se incluiría la apropiación de dinero, cheques auténticos emitidos por el ordenador, emisión de cheques ficticios y apropiación de cheques recibidos de clientes.

Sustracción de mercancías: Uno de los casos más frecuentes es la manipulación de sistemas mecanizados de control de inventarios para hacer desaparecer mercancías mediante la introducción de movimientos [1] de salida falsos o de no registro de los movimientos de entrada. Esto es muy sencillo dejando que la conciliación de facturas de proveedores o la facturación de clientes están mecanizadas. También puede darse el caso de un fraude de este tipo por colusión de personal de la organización con proveedores o con clientes.

Sustracción de valores negociables o documentos que sirvan de soporte para el intercambio de mercancías o de dinero: Ejemplos: Apropiación de acciones, valores, participación en fondos de inversión, de pensiones o bien de albaranes de mercancías.

Sustracción de servicios: Este fraude acostumbra a darse en compañías suministradoras de servicios (agua, gas, teléfono, electricidad). El fraude se realiza mediante la manipulación de los sistemas de medición, registros, facturación y seguimiento de cobros. También se encuentra en este grupo la utilización de los dispositivos informáticos de una empresa en provecho de los trabajadores.

Sustracción de software: Más conocido como *piratear software*.

Sustracción de información: Sería, por ejemplo, sustraer información confidencial sobre productos, tecnología, clientes... De este tipo de fraude se dan cada vez más casos.

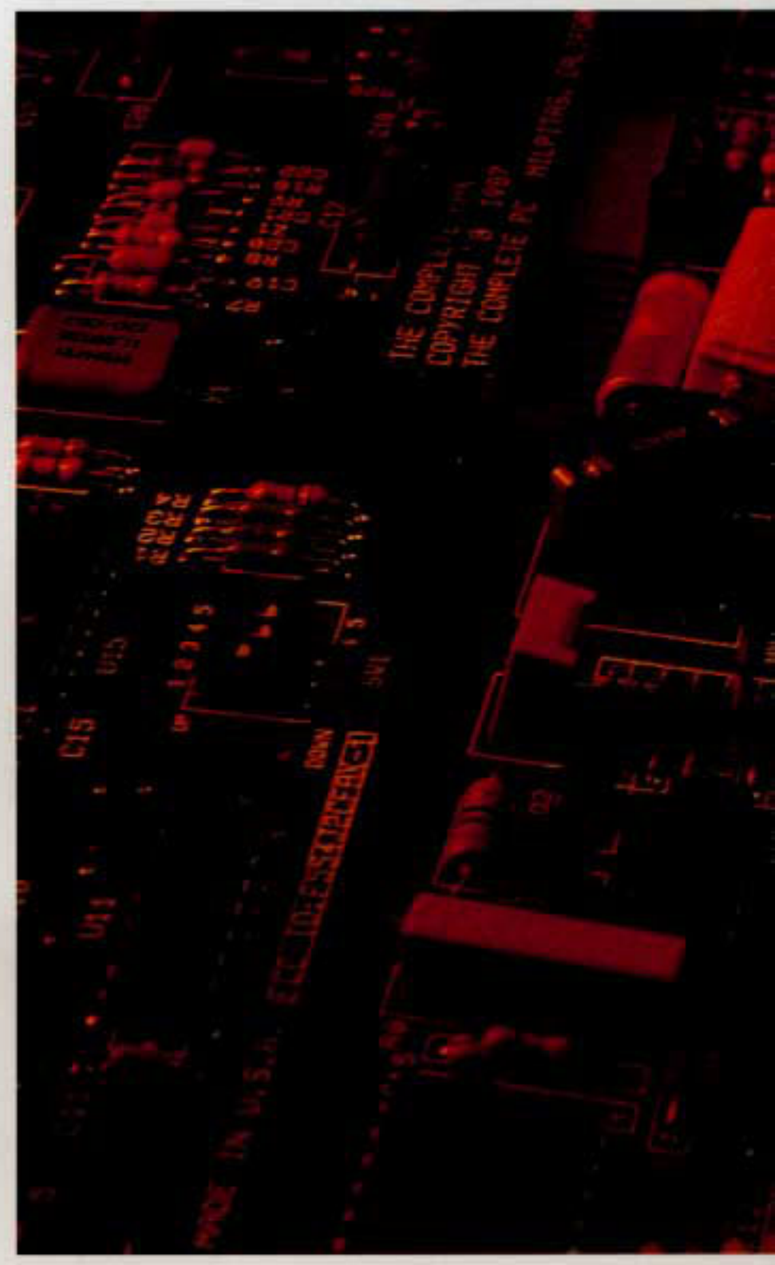
Tipos según las técnicas utilizadas

Las técnicas para realizar fraudes servirán para alcanzar uno o más de uno de los objetivos citados anteriormente. Existirá también un objetivo común: la manipulación de la información y de los programas.

Procedimientos habituales:

Introducción de datos falsos: En inglés, *Data Diddling*. Es el más común y más sencillo de llevar a cabo. Consiste en manipular las transacciones [2] de entrada para introducir movimientos falsos o eliminar transacciones que se deberían haber introducido.

Caballo de Troya: En inglés, *Trojan Horse*. Introducir en un programa un conjunto de instrucciones



o rutina no autorizada para que dicho programa actúe de una forma distinta a la prevista en determinados casos.

Ejemplo: realizar un cálculo erróneo de una nómina aumentando el importe.

Salami: En inglés, *Rounding Down*. Manipulación de un gran número de pequeños importes. Se denomina salami ya que el fraude se realiza en pequeños cortes. Un ejemplo en una entidad bancaria sería añadir unas líneas adicionales de código en un programa de cálculo de intereses para redondearlos, desviando la cifra redondeada a una cuenta controlada por la persona que efectúa el fraude.

Recogida de información desechada: En inglés, *Scavenging*. La información que se tira a la papelera por contener errores o ser obsoleta puede contener datos confidenciales de interés para empresas competidoras. El fraude consiste en recoger estos datos confidenciales y venderlos. Jurídicamente se plantea el problema de establecer la propiedad de estos datos ya que la empresa, en un principio propietaria, los ha desechado.

Superzapping: Se refiere a utilidades que permiten modificar archivos y bases de datos sin acceder a ellos por el programa que los gestiona. El peligro surge cuando estas utilidades están al alcance de todo el mundo y su utilización no está controlada. Un ejemplo: alterar el saldo de una cuenta modificando este dato directamente en el archivo donde se encuentra.

Bomba lógica: En inglés, *Logic Bomb*. Rutina no autorizada de un programa que produce consecuencias destructivas en una fecha, tiempo o evento predeterminados. Un ejemplo sería que un empleado que fuera despedido, incluyera en un programa una de estas rutinas para que se ejecutase cuando él ya no estuviese en la organización.

Puertas Falsas: En inglés, *Trap Doors*. Cuando un programador elabora un programa, normalmente introduce puntos de control para comprobar que los resultados intermedios son correctos. Estas son las puertas falsas. Cuando la aplicación ha finalizado y entra en proceso normal, estas puertas deberían eliminarse, cosa que a menudo no se realiza por olvido. Como consecuencia, las aplicaciones se quedan con unas puertas de entrada que no están documentadas ya que no formaban parte de las especificaciones.

Fuga de información: En inglés, *Data Leakage*. Se trata de la divulgación no autorizada de datos reservados. Es lo que tradicionalmente se ha denominado como espionaje industrial. La sustracción de información confidencial es uno de los principales peligros que corren los sistemas informáticos. En muchas instalaciones es muy sencillo realizar una copia de un fichero con datos privados.

Acceso no autorizado: En inglés, *Piggybacking*. Significa acceder a áreas restringidas, ya sean físicas (salas de ordenadores) como dentro del ordenador (dispositivos, discos ...).

Pinchazo de líneas: En inglés, *Wiretapping*. Se trata del pinchazo de todo tipo de líneas de comunicación, ya sean telefónicas o de datos.

La seguridad informática puede evitar la comisión del fraude

Simulación y modelación: En inglés, *Simulation and Modeling*. Sería utilizar un ordenador para planificar y simular un delito. Por ejemplo sería hacer un estudio sobre las repercusiones que tendría realizar asientos contables falsos utilizando una copia de la contabilidad de la empresa.

Prevención y detección de fraudes

La *oportunidad* ha sido nombrada como uno de los elementos del fraude. Las oportunidades para cometer fraudes existen, en diferentes grados, en casi todas las organizaciones que utilizan la informática y que presentan deficiencias en diferentes aspectos que influyen directa o indirectamente sobre la función informática. Estos aspectos son:

- Políticas de la dirección
- Controles administrativos
- Control de personal
- Control interno
- Seguridad

Políticas de la dirección

Uno de los factores que se puede considerar a la hora de valorar las oportunidades para realizar un fraude es la ética o los estándares de conducta que sigue la organización. La política y la conducta fijada por la dirección establecen el ambiente en el que se trabaja.

Controles administrativos

Aunque los controles administrativos deben establecerse en el mar-

HERRAMIENTAS DE AUDITORIA

co de las políticas de la dirección, inciden más específicamente en las reglas del «día a día» de los departamentos. Estas reglas tratan, preferentemente, de los procedimientos a seguir en la manipulación de los datos.

Control del personal

Como ya se ha mencionado al hablar de las fuentes del fraude, la mayoría son originados por personal interno de la organización. Por este motivo, debe ponerse especial énfasis en los controles de personal refiriéndonos tanto a las políticas de selección de nuevo personal como al seguimiento del ya existente.

Control interno

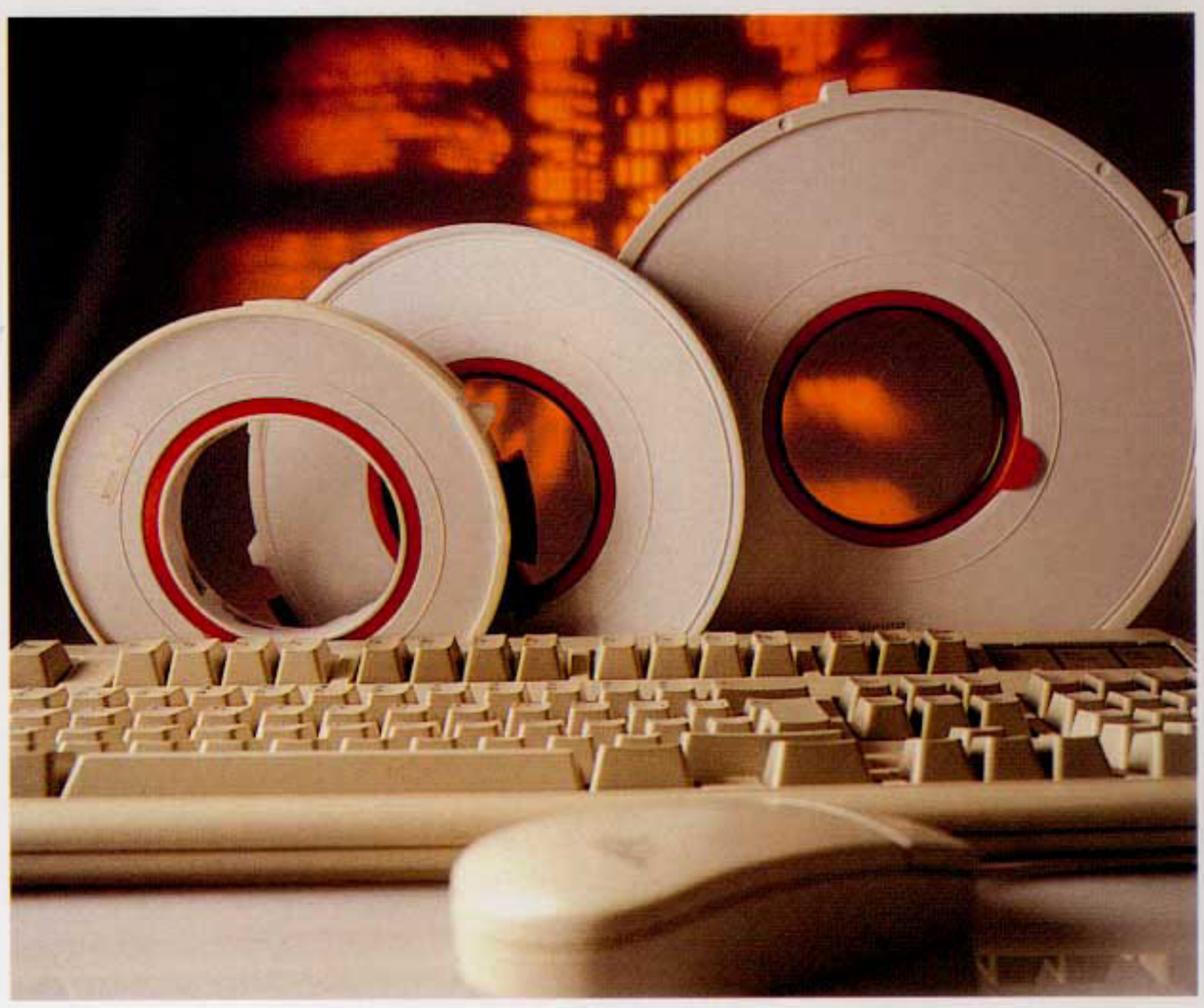
El control interno comprende el plan de la organización y el conjunto de métodos y procedimientos que aseguran el buen funcionamiento de la función informática. Se puede afirmar que los fraudes se realizan cuando los controles internos no existen, son débiles o son esquivados. Los controles pueden ser específicos de una aplicación, de un aspecto o generales de toda la función informática.

Seguridad informática

Tener un sistema completamente seguro es casi imposible. Algunas razones por las que los sistemas en los que se ha establecido un plan de seguridad continúan siendo, en mayor o menor grado, vulnerables son:

- La implantación de medidas de seguridad excesivas pueden llegar a dificultar la operativa de la empresa.

- Pueden existir brechas en la seguridad que no se habían previsto.



- La empresa puede tener dificultades para afrontar el coste de las medidas de seguridad.

- El coste de las medidas puede ser superior a las pérdidas potenciales que evitarían.

- La tecnología avanza más rápidamente que la evolución de la seguridad de una empresa.

Para implantar o renovar un sistema de seguridad se tendría que hacer lo siguiente:

Análisis del riesgo: Evaluar los riesgos de toda la instalación informática y de su emplazamiento físico.

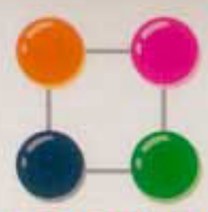
Definición de objetivos: Definir los objetivos que se quieren alcanzar. Las partes implicadas en este tema tienen que ser tanto la parte técnica como la parte organizativa, con el asesoramiento de expertos externos a la organización si hiciera falta.

Plan de seguridad:

Diseño: Cuando los objetivos están bien definidos se tiene que diseñar un plan de seguridad con la ayuda de expertos externos a la organización. El plan debe ser elaborado por el departamento de informática y sometido a la dirección para su aprobación.

Puesta en marcha: Se tiene que establecer qué personal se dedicará a la puesta en marcha, qué tipo de pruebas y evaluaciones se harán para ver si la implantación se cumple y si aumenta la cobertura frente a los riesgos enumerados en el plan.

El plan de seguridad debe contemplar tanto los aspectos de seguridad física como de seguridad lógica. La seguridad física engloba el conjunto de equipos, instalaciones y medios físicos. La seguridad lógica engloba la seguridad de las aplicaciones y programas, informaciones y ficheros, usuarios y personas implicadas.



Conclusión

Es muy importante que las organizaciones sean conscientes de que la informática no es infalible. Esta es una importante fuente de riesgos. Según el tipo de organización, la informática puede ser vital para el funcionamiento.

La seguridad informática es hoy en día una cuestión de suma importancia. A más seguridad de los sistemas, menos oportunidades habrá en la organización para cometer fraudes, pero con esto no será suficiente. Se tendrá que seguir una política de personal adecuada para que los empleados de la organización no piensen nunca que llevar a cabo un fraude es justificado. ■

Bibliografía

- Alonso Ribas, G. «*Auditoría Informática*». Ediciones Díaz de Santos S.A. Madrid, 1988.
- Bueno Arús, F. «*El delito informático*». ACTUALIDAD INFORMÁTICA ARANZADI, abril de 1994, nº 11.
- Camacho, Luis. «*El delito Informático*». Madrid, 1987.
- CIPFA. «*Computer Survival Guides*». Londres, octubre 1991.
- CIPFA. «*Computer Audit Guidelines*». Londres, 1994.
- Gutiérrez Francés, M. «*En torno a los fraudes informáticos en el derecho español*». ACTUALIDAD INFORMÁTICA ARANZADI, abril de 1994, nº 11.
- Jones, Peter. «*Combating Fraud and Corruption in the Public Sector*». Chapman & Hall. Londres, 1993.
- Lanza Suárez, P. «*Auditoría de Sistemas de la Información*». CUADERNOS DE ACTUALIDAD, 5/1994 año V.
- Pérez Gómez, J.M. «*Areas vulnerables en la empresa por los abusos informáticos*» TÉCNICA CONTABLE, abril 88, nº 472.
- Poveda Maestre, J.P. «*Auditoría de Cuentas y Auditoría Informática. Análisis de las normas básicas*». TÉCNICA CONTABLE, julio 94, nº 547.
- Poveda Maestre, J.P. «*Auditoría Informática: Controles de aplicaciones*». TÉCNICA CONTABLE, agostoseptiembre 94, nº 548-549.
- Sneyers, Alfredo. «*El fraude y otros delitos informáticos*». Tecnologías de Gerencia y Producción, S.A. Madrid, octubre 1990.
- Thomas A., J. y Douglas I. J. «*Auditoría Informática*». Paraninfo, Madrid, 1990.
- Thorin, M. «*La Auditoría Informática: Métodos, Reglas y Normas*». Masson, Barcelona, 1989.