Facultad de Informática
Universidad de A Coruña

Auditoría Informática

Apuntes de la Asignatura

Serafín Caridad Simón

Temas 1 al 3 adaptados de EDP Auditing: Conceptual Foundations and Practice. Ron Weber, 1982.

Indice

Tema 3 El Marco de Control de Aplicación

Tema 5 Recuperación de Sistemas Informáticos en Situaciones de Desastre

Tema 6 Sistemas de Gestión de Problemas

TEMA 1: INTRODUCCION

Propósito de Auditoría Informática (AI)

La función de AI es garantizar que los sistemas de ordenador:

- Salvaguardan los "bienes" de la organización
- Mantienen la integridad de los datos.
- Alcanzan los objetivos de la empresa de un modo eficaz y efectivo

En los siguientes puntos se introducirá la función de AI, su necesidad y motivaciones, sus objetivos y se dará un vistazo general al proceso de AI y como se debe de implantar en una organización.

1.1 Visión General de AI

Hace 40 años, la mayoría del proceso de datos era manual. Incluso operaciones como la contabilidad de las empresas se realizaban de forma manual. Hoy, los ordenadores hacen la mayor parte del proceso en los sectores tanto público como privado.

Uno de los problemas que han surgido con el uso generalizado de los ordenadores es la necesidad de mantener la integridad de los datos. A medida que los ordenadores toman mayor control de los datos, la carencia de un control directo sobre los mismos se vuelve cada vez mayor y esto proporciona una inquietud creciente en las empresas.

Esto es debido a que en un sistema manual las operaciones están completamente delimitadas y se sabe como funcionan, pero cuando pasamos a un sistema informático, el control que tenemos sobre los datos y cómo se procesan disminuye. Por ejemplo: de estadísticas realizadas en Estados Unidos, sobre bancos de tamaño medio, se concluye que, si éstos perdieran sus datos, al cuarto día su volumen de negocio disminuiría en un 50% y la quiebra se produciría aproximadamente en 10 días.

Debido a esto tenemos que considerar:

- Implicación: Estamos en manos de la Informática. Por ejemplo, ningún banco, sin importar su tamaño, sería capaz de realizar su trabajo sin ayuda de la informática

- Cuestión: ¿Quién garantiza que los procesos informáticos son correctos? ¿Quién garantiza a un usuario que la liquidación periódica de su cuenta corriente es correcta, por ejemplo?

Estas conclusiones aplicadas al sector bancario son perfectamente extrapolables a la gran mayoría de las empresas, hoy en día.

1.1.1 Necesidad de Control y AI

Estando en un medio informático en el que el ordenador realiza de forma automática las tareas tendremos que controlar si lo que hace es lo que realmente queremos que haga.

Los ordenadores juegan un papel muy importante al ayudarnos en el proceso de datos, por lo que hay que controlar su uso, ya que en el procesamiento de datos es uno de los puntos donde se puede producir el fraude con mayor facilidad.

Estos controles son necesarios ya que los medios abusan de la capacidad del proceso de datos, dando lugar a intercambio de datos privados entre empresas o fraudes por falta de controles en los sistemas, por ejemplo.

Además con el aumento de la potencia de los ordenadores se puede ver incrementado el denominado "abuso informático". Definiremos el abuso informático un poco más adelante, en este mismo tema.

Por todo ello, es necesario establecer mecanismo de Control y Auditoría de Ordenadores en las organizaciones.

1.1.1.1 Coste de la pérdida de datos en las organizaciones

En la actualidad, los datos son recursos críticos para la continuidad de las funciones de cualquier empresa, y su importancia dependerá de lo vital que sean para la organización.

Para poder proteger estos recursos será necesario establecer una política a nivel organización, de copias de seguridad y recuperación. Por su importancia, se estudiarán estos temas con más profundidad más adelante.

1.1.1.2 Toma de decisiones incorrecta

Los datos nos van a permitir entre otras cosas realizar tomas de decisión. Pero para que las decisiones tomadas a partir de los datos sean correctas, tendremos que garantizar que los datos que nos son suministrados son asimismo correctos.

La importancia de la veracidad de los datos viene dada por el tipo de decisiones que se toman a partir de ellos. Por ejemplo:

- En planes estratégicos a largo plazo: Los datos que facilitan la toma de decisiones pueden ser "algo" imprecisos, puesto que el resultado es global, genérico. Se pueden utilizar "grandes números", es decir, cantidades brutas aproximadas, sin importar el detalle.

- En cambio, en control de operaciones y en control de gestión se necesitan datos totalmente precisos.

1.1.1.3 Abuso Informático o Abuso del Ordenador

"Cualquier incidente asociado con la tecnología de ordenadores en el cual una víctima sufrió o pudo haber sufrido pérdidas, y el que lo ocasiona tuvo o pudo haber tenido beneficios" [Parker, 1976]

Dada la definición, se podría pensar que el abuso informático constituye la causa principal de la necesidad de AI. No obstante, tras estudios intensivos se ha llegado a la conclusión de que existen otras dos causas de problemas, que son aún más importantes que el abuso informático:

1) Errores y omisiones que originan pérdidas: frecuentemente, son el motivo de toma de decisiones erróneas. Por ejemplo: un simple error en el inventario que indique que existen 500 unidades de un determinado producto, cuando en realidad hay 5.000, puede inducir a realizar un nuevo pedido, con el consiguiente coste de adquisición, almacenamiento o pérdidas si el producto es perecedero.

2) Destrucción de datos ocasionada por desastres naturales (agua, fuego, y fallos de energía)

Esto nos obliga a plantear soluciones para estas dos causas en primer lugar, antes incluso que al abuso informático.

De todos modos, no podemos dejar de establecer controles para evitar el abuso informático, dado que los costes derivados de éste suelen ser muy superiores a los producidos por el abuso "manual", o a los derivados de las dos causas anteriormente citadas. En general, los fraudes que se pueden realizar con los ordenadores producen más pérdidas que los que se realizan con sistemas manuales.

1.1.1.4 Privacidad de los datos

Desde siempre se han recogido datos de personas para su uso comercial: datos personales, médicos, de impuestos, etc. Pero desde la llegada de los ordenadores la difusión "incontrolada" de estos datos se ha convertido en un serio problema, principalmente debido a que crear, actualizar y difundir una base de datos con datos personales de posibles clientes es mucho más fácil ahora que cuando los sistemas eran manuales.

En muchos países, la privacidad de los datos es un derecho. En nuestro país, la Ley de Protección de Datos de Carácter Personal asegura la confidencialidad de los datos y protege a los propietarios de los mismos del uso ilegítimo de ellos por terceras personas.

No obstante, en la sociedad actual existe un sentimiento general de que en alguna parte hay una enorme base de datos, donde todos estamos incluidos, y de que "alguien" la controla.

Lo que tenemos es que garantizar de que esto no ocurra, y que los datos sólo se utilizan con el propósito para el que fueron dados por su propietario, fin último de la Auditoría Informática.

1.1.1.5 Evolución controlada del uso del ordenador

La tecnología en general es neutral: es decir, no es buena ni es mala. Lo que realmente puede ocasionar problemas es su uso incorrecto.

Para garantizar que esto no ocurra, hay que tomar decisiones importantes sobre como se deben usar los ordenadores en la sociedad. Por ejemplo: ¿Hasta qué punto se debe permitir que el uso de ordenadores elimine puestos de trabajo?

Es función del gobierno, de las sociedades profesionales y de los distintos grupos de presión (sindicatos, asociaciones para la defensa de los consumidores, etc.) el evaluar el uso "racional" de la tecnología. No obstante estas organizaciones también necesitan utilizar ordenadores, por lo que su actuación se puede ver condicionada por este hecho.

1.1.2 Definición de AI: Estudio pormenorizado

"AI es el proceso de recoger evidencias para determinar si un Sistema Informático (SI) salvaguarda los bienes, mantiene la integridad de los datos, alcanza los objetivos de la empresa de un modo efectivo y consume los recursos con eficacia."

Vamos a distinguir entre dos tipos de Auditoria:

Auditoria externa: que se centra en objetivos de seguridad: salvaguarda de bienes e integridad de datos, principalmente.

Auditoria interna: que, además de en los objetivos anteriores, se centra en objetivos de gestión, es decir garantizar que las tareas se realicen en unos grados adecuados de efectividad y eficacia.

1.1.2.1 Objetivos de salvaguarda de bienes

Consideraremos como "bienes" de un Centro de Proceso de Datos (CPD) el hardware, software, personas, datos (ficheros, bases de datos, etc.), documentación, suministros, etc. El hardware puede ser dañado por accidente o malintencionadamente; el software, al igual que los datos, puede ser robado o destruido; los suministros pueden ser usados con fines ajenos a los de la empresa, etc.

Además, estos bienes se concentran todos en un mismo sitio, el ámbito físico del CPD, por lo que deben de ser especialmente protegidos por un sistema de control interno, y su protección debe de ser un objetivo importante.

1.1.2.2 Objetivos de integridad de datos

Ya hemos visto que uno de los aspectos que debemos cuidar especialmente es la integridad de los datos, pero realizar esta tarea nos va a suponer un coste frente a los beneficios esperados al implantar unas medias de seguridad. Desde de un punto de vista puramente empresarial, estos beneficios deben de superar los costes de implantación,

para que sea rentable su utilización. No obstante, disposiciones legales pueden obligar a establecer controles, al margen de su rentabilidad.

Para determinar los costes y beneficios, estudiaremos dos factores que afectan al valor de un dato para la empresa:

El valor de la información que proporciona el dato. Este valor depende de la capacidad que ésta tenga para reducir la ambigüedad en una toma de decisiones. Es decir, los datos que influyen directamente en las tomas de decisiones serán los más importantes y deberán de ser especialmente protegidos.

Las veces en que el dato es usado por personas que toman decisiones. Si el dato es compartido, su falta de integridad afectará a todos los usuarios, por lo que en un entorno compartido es vital mantener esta integridad.

1.1.2.3 Objetivos de efectividad del sistema

Para ver si un SPD (Sistema de Proceso de Datos) es efectivo hay que conocer las características del usuario y el tipo de decisiones que se van a tomar. No se debe de evaluar de igual manera la efectividad de un SPD de una gran empresa que la de un pequeño comercio, por ejemplo.

Para saber si el sistema está trabajando correctamente, y para poder medir su efectividad, es necesario esperar a que el sistema lleve funcionando un cierto tiempo, tras el cual, normalmente la gerencia solicita una auditoría para saber si el sistema alcanza los objetivos que se había planteado.

Como resultado de la auditoria se sabrá si hay que descartar el SPD, modificarlo, o si se debe de dejar como está. Téngase en cuenta que esta auditoría también se puede hacer durante la fase del Diseño del Sistema. Además, es posible que la gerencia solicite una auditoría independiente.

1.1.2.4 Objetivos de eficiencia del sistema

Un SPD eficiente es el que utiliza el mínimo de recursos (tiempo de máquina, periféricos, canales, software de sistemas, mano de obra, etc.) para alcanzar sus objetivos.

En cualquier sistema los recursos son escasos y hay que compartirlos, por lo que saber si se están utilizando los recursos de forma eficiente no siempre es fácil. Además, no se puede considerar la eficiencia de un sistema por sí solo, sino en conjunto con los demás sistemas dentro de la organización.

Suboptimización: Se produce cuando un sistema se optimiza a expensas de otros. Ejemplo: Dedicar exclusivamente un recurso a un sistema (que no lo utiliza a tiempo completo) penalizará a otros sistemas que necesiten el recurso.

La eficiencia se vuelve crítica cuando el ordenador comienza a estar escaso de recursos (escasez de capacidad de almacenamiento en discos, de memoria, de procesador, etc.),

por lo que, si además los recursos son caros, hay que saber si se agotaron porque las aplicaciones son ineficientes, porque existen cuellos de botella, o simplemente porque el crecimiento natural de las aplicaciones ha reducido dichos recursos.

Una vez mas, el trabajo de un auditor independiente puede ser necesario para determinar este tipo de cuestiones.

1.1.3 Efectos de AI en el Control Interno

Los beneficios de AI solo se alcanzan si la gerencia organiza un sistema de control interno.

En la Auditoría tradicional, las características de dicho control interno son:

1. Separación de tareas
2. Delegación clara de autoridad y responsabilidad
3. Contratación y entrenamiento de personal altamente cualificado
4. Supervisión de la gerencia
5. Sistema de autorizaciones
6. Acceso limitado a bienes
7. Comparación de bienes con registros contables

En AI también existen estos controles, aunque su implementación es diferente, como se verá a continuación.

1.1.3.1 Separación de Tareas

Como su nombre indica, la idea fundamental de la separación de tareas es tener distintas personas para realizar distintas tareas o partes de una tarea, y poder así establecer controles cruzados. Por ejemplo, en un sistema manual, la iniciación y grabación de transacciones y la custodia de bienes deben de ser realizados por personas distintas, para garantizar una cierta integridad, y detectar errores y posibles fraudes.

En un SPD esta separación de tareas no siempre existe. Un único programa puede "casar" una factura con un pedido y emitir un cheque. Todas las tareas las hace el mismo programa. No obstante, una vez desarrollado, el programa puede ser probado por diferentes personas, para asegurar su correcto funcionamiento, y asimismo se puede separar la capacidad de ejecutarlo en un entorno de pruebas y en un entorno real de producción.

En un ordenador personal, esta separación de tareas aún es más difícil de conseguir. En este entorno cualquiera puede modificar o ejecutar un programa, ya que no existe un nivel de seguridad tan alto en los sistemas operativos de los ordenadores personales como en los de los grandes sistemas. Por eso, una de las funciones de AI es garantizar que sólo se compren ordenadores que proporcionen una capacidad de control básica, sobre todo si estos se van a usar en aplicaciones financieras.

1.1.3.2 Acceso a bienes

Un CPD es un caso único en cuanto a la concentración de bienes en un mismo sitio. Además de daños al hardware, es posible modificar programas para cometer fraude o acceder a datos confidenciales para beneficio propio, etc. Debido a esto, los bienes de un CPD se deberán de proteger de un modo especial.

Comparado con otros departamentos, el CPD es el de mayor riesgo en la mayoría de los casos.

1.1.3.3 Tipos de controles internos

Los objetivos básicos de control interno no cambian en un CPD; lo que sí cambia es la tecnología empleada para alcanzar esos objetivos. Asegurarse de que un disco funcione bien implica un conjunto de controles que no existirían si el proceso fuera manual; asimismo, los procedimientos de prueba de programas no son aplicables en un sistema manual.

1.1.3.4 Las Pistas de Auditoría / Gestión

Las Pistas de Auditoria proporcionan un registro de todo lo que ocurre en un SPD. Normalmente pueden ser pequeños módulos que se insertan en las aplicaciones para controlar que todo funciona correctamente, o incluso constituir programas completos al margen de la aplicación, y su conservación depende de un buen diseño de las aplicaciones.

Estas pistas, constituidas por Log's, diarios, etc., no se deben de perder y es necesario incluirlas siempre en todas las operaciones que se realizan.

El uso creciente de PC's puede poner en peligro la adecuación de las Pistas de Auditoria, ya que cuando trabajamos sobre estos sistemas los aspectos de seguridad son escasos, como ya se explicó anteriormente. Si esto se combina con el aumento creciente de la posibilidad de separar tareas... nos vamos a encontrar con serios problemas.

1.1.3.5 Comparación de bienes con registros contables

El ejemplo típico de este control puede ser un inventario, un balance, un cuadre de cuentas, etc. Este control hay que hacerlo periódicamente para detectar inconsistencias. Si se trata de un SPD, habrá que desarrollar los programas necesarios para llevarlo a cabo.

1.1.3.6 Consecuencias de los errores

"Las consecuencias de los errores en un SPD son casi siempre mas graves que las de un sistema manual" [Boritz, 1979]

Los errores en sistemas manuales tienden a ocurrir estocásticamente. Cada cierto tiempo alguien se equivoca, mientras que en un SPD los errores tienden a ser determinísticos (un programa erróneo siempre se ejecuta erróneamente), se producen muy deprisa y el coste de corrección es alto.

Implicación: Los controles internos que garanticen una alta calidad de los Sistemas de Proceso de Datos, en lo tocante a diseño e implementación, son siempre controles críticos.

1.1.4 Bases de AI

Auditoria Informática no es solo una prolongación de la auditoría tradicional, sino que es un aspecto importante en la seguridad y buen funcionamiento de la empresa.

El reconocimiento de la necesidad de AI es debido a:

- Los auditores comprobaron que los SPD's cambiaron su capacidad de auditar sistemas, ya que no es lo mismo auditar un sistema manual que uno informático.

- La gerencia considera que los ordenadores son recursos valiosos que deben de ser controlados como cualquier otro recurso.

Se puede considerar AI como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática.

Fig. 1.0 A.I. como intersección de otras disciplinas

1.1.4.1 Auditoria Tradicional

Proporciona conocimiento y experiencia en Técnicas de Control Interno. Es decir, aspectos sobre cómo controlar las actividades de la empresa.

Un SPD tiene componentes manuales y mecanizados, que serán objeto de control.

- Los manuales están sujetos a los principios de Control Interno de la auditoria tradicional: separación de tareas, personal fiable, definición clara de responsabilidades, etc.

- Los mecanizados pueden utilizar controles "clásicos", desde el punto de vista informático: totales de control, cuadres, balances, etc.

Otra aportación de la auditoría tradicional la constituyen las metodologías de recogida y evaluación de evidencias, aunque el aspecto más importante es que la auditoria tradicional proporciona un "saber hacer", un "modus operandi", para examinar los datos y procesos con mente crítica, cuestionando la capacidad de un SPD de salvaguardar los bienes, y de mantener la integridad de los datos de un modo eficaz y eficiente.

1.1.4.2 Gestión de Sistemas de Información

En los comienzos de la era informática hubo grandes fracasos al implementar Sistemas de Proceso de Datos por no disponer de técnicas y herramientas adecuadas. Por desgracia, esto a veces sigue ocurriendo en nuestros días... por no utilizarlas.

Hoy en día disponemos de mejores técnicas: Programación Estructurada, Estándares de Gestión de Proyectos, Equipos de Trabajo, Metodologías de Análisis y Desarrollo, etc. La causa final de la existencia de estas técnicas es la de simplificar el mantenimiento de los SPD's. Todos estos avances tienen un impacto en AI porque afectan directamente a las funciones de AI.

1.1.4.3 Ciencias del comportamiento

"La razón principal del fallo de los SPD's es el desconocimiento de los problemas del comportamiento organizativo en el diseño e implantación de los Sistemas de Información". [Lucas, 1975]

El auditor debe de conocer las condiciones que originan problemas de comportamiento y que pueden causar fallos en el Sistema. Es decir, es necesario conocer los problemas de las personas en las organizaciones.

Algunos investigadores están aplicando la Teoría de las Organizaciones al desarrollo e implantación de los Sistemas de Información. Es decir, se debe de considerar, de modo concurrente, el impacto de un SPD tanto en:

- El cumplimiento de las tareas (que se haga lo que se espera)
- El sistema técnico (que tengamos recursos técnicos para realizar las tareas)
- El sistema social (la calidad de trabajo de las personas; que haya un buen ambiente de trabajo)

1.1.4.4 Informática

La última de las disciplinas base de AI es la Informática. Los informáticos también están fuertemente involucrados en las funciones de AI.

En Ingeniería del Software se han desarrollado investigaciones sobre:

- Como desarrollar software con “cero errores”
- Como mantener la integridad global del hardware y el software: Programación Estructurada, Teoría de Fiabilidad, Teoría de Control, etc.

Y estas disciplinas se han incorporado en AI, ya que deben de ser conocidas por el auditor informático. No obstante, este conocimiento tecnológico de alto nivel ocasiona beneficios y desventajas a AI, ya que:

- Permite al auditor despreocuparse acerca de la fiabilidad de algunos componentes del Sistema, ya que supone que funcionarán correctamente.

- Si hay “abuso” será muy difícil de detectar. Ya que no tiene los conocimientos necesarios para detectarlos.

- El fraude perpetrado por un programador altamente cualificado será muy difícil de detectar por un auditor que no tenga ese alto grado de conocimiento técnico.

1.1.5 Resumen

AI es una función organizativa que evalúa la salvaguarda de bienes, la integridad de datos, la efectividad y la eficacia de los Sistemas de Procesos de Datos.
Existen cinco motivos importantes para tener AI en una organización:

- Las consecuencias de una posible pérdida de recursos de datos

- La posibilidad de utilizar mal los recursos por decisiones tomadas erróneamente debido a datos incorrectos

- La posibilidad de fraude o desfalco si no se controlan los SPD’s

- La necesidad de mantener la privacidad de los datos

- La necesidad de controlar el uso evolutivo de los ordenadores

Las funciones de AI solo se alcanzan si existe algún tipo de Control Interno

El uso de ordenadores no afecta a los objetivos básicos del Control Interno, pero sí a como éstos se consiguen.

AI obtiene la mayor parte de su teoría y metodología de otras áreas: Auditoria Tradicional, Gestión de Sistema Informáticos, Ciencias del Comportamiento e Informática.

1.1.6 Ejercicios y Casos

1.1.6.1 Equity Funding Corporation

En 1973 se descubrió en California el mayor fraude conocido que involucraba a una única empresa. El colapso de la Equity Funding Corporation of America se debió a un fraude de aproximadamente dos billones de dólares. El caso es sumamente complejo y las investigaciones duraron varios años. A continuación se recogen algunos de los resultados obtenidos de los informes de la comisión investigadora.

La Equity Funding era una institución financiera dedicada primordialmente a los seguros de vida. En 1964, la gerencia general comenzó a perpetrar un fraude que tardaría casi 10 años en ser descubierto. El fraude consistía en inflar los ingresos de modo que la gerencia se pudiera beneficiar negociando sus fianzas a un alto precio.

El fraude fue pasando por tres etapas principales: la “fase de inflar los ingresos”, la “fase extranjera” y la “fase de seguros”. La primera fase consistió en inflar los ingresos por medio de comisiones falsas, supuestamente obtenidas a través de los préstamos que se hacían a los clientes. La Equity Funding disponía de un programa de fondos de seguros de vida por el que los clientes que compraban acciones de fondos de la mutualidad podían obtener un préstamo de la empresa para pagar las primas en una póliza de seguro de vida. Después de algunos años, el cliente podría vender las acciones para pagar el préstamo, y se esperaba que para entonces las acciones se hubiesen revalorizado lo suficiente como para que no hiciera falta venderlas todas, y obtener así beneficios. De esta manera, los beneficios del cliente serían el valor de la póliza de seguros y el resto de las acciones que no tendría que vender.

Los ingresos obtenidos de estas comisiones falsas se anotaban manualmente en los libros de la empresa, y aunque no había ninguna documentación de estas anotaciones, de alguna manera se evitó que los auditores de la empresa se dieran cuenta del fraude. Sin embargo, estos supuestos ingresos no producían dinero real, y la empresa sufrió fuertes faltas de liquidez por culpa de operaciones reales que produjeron pérdidas.

Para remediar esta falta de liquidez, la gerencia decidió entrar en la segunda fase del fraude, llamada la “fase extranjera”. La empresa adquirió otras empresas subsidiarias en el extranjero y las utilizó para hacer complejas transferencias de bienes. Se enviaron fondos a las empresas subsidiarias para reducir la cuenta de préstamos de fondos y simular así que los clientes realizaban los pagos de sus préstamos. Sin embargo, este planteamiento tampoco funcionó como se esperaba.

Entonces la gerencia decidió entrar en la tercera fase, la llamada “fase de seguros”, que consistía en revender las pólizas de seguros a otras compañías aseguradoras. Esta es una práctica normal en el ámbito de los seguros, cuando una empresa necesita fondos urgentemente y la otra dispone de ellos. La Equity Funding creó pólizas falsas para venderlas a otra compañía y resolver así su problema de falta de liquidez a corto plazo. Sin embargo, a largo plazo, la compañía que compraba las pólizas esperaría obtener los ingresos correspondientes a las primas de esas pólizas, y dado que éstas eran falsas, la Equity Funding tendría que disponer de dinero al contado para pagarlas. De este modo, el que el fraude se descubriese se convirtió en una simple cuestión de tiempo.

Curiosamente, el fraude salió a la luz porque un empleado que conocía las actividades fraudulentas de la gerencia fue despedido y reveló los hechos.

El ordenador no se utilizó en el fraude hasta la "fase de seguros", porque el crear las pólizas falsas era una tarea tan grande que no podía realizarse a mano. Por ello, se escribió un programa que generaba las pólizas, las que se codificaban con la ahora tristemente conocida "Clase 99".

El informe de la comisión investigadora revela dos conclusiones claras. En primer lugar, el fraude era muy poco sofisticado y estaba condenado al fracaso, y en segundo lugar, los auditores de la Equity Funding fueron completamente negligentes. No se aplicaron los principios fundamentales de una buena auditoría.

Este fraude causó la ruina de muchas familias.

Se pide:

Escribir un breve informe sobre algunos procedimientos de auditoría tradicional que hubieran detectado el fraude y explicar por qué estos procedimientos hubieran tenido éxito.

1.1.6.2 Jerry Schneider

Uno de los casos más famosos de abuso de ordenador fue el de un joven llamado Jerry Schneider. Schneider siempre tuvo una habilidad especial para la electrónica y cuando dejó la universidad ya había creado su propia empresa para comercializar sus circuitos. Además, su empresa se dedicaba a mejorar y vender equipo telefónico de la Western Electric. En 1970, se le ocurrió una manera de obtener equipo telefónico de la Pacific Telephone en Los Angeles… ¡completamente gratis!

La Pacific Telephone utilizaba un sistema de pedidos de equipos por ordenador, con el cual sus diferentes almacenes podían pedir equipos utilizando un marcador telefónico de tarjeta del tipo Touch-Tone. Los pedidos posteriormente se perforaban en tarjetas y el ordenador actualizaba los ficheros maestros de inventario e imprimía los pedidos, los cuales eran enviados a una oficina de transportes, que se encargaba de su distribución.

Schneider trató de conseguir acceso al sistema de pedidos para hacer que la Pacific Telephone se los enviara a él y pensara que se los había enviado a sus correspondientes almacenes.

Para ello, utilizó una gran cantidad de argucias para descubrir cómo funcionaba el sistema y romper su seguridad. Rebuscó en los contenedores de basura de la Pacific Telephone y encontró listados con información sobre el sistema de pedidos. Se hizo pasar por escritor de una revista y entrevistó a algunas personas de la Pacific Telephone que le proporcionaron información valiosa. Para camuflar sus actividades, compró una furgoneta de la Pacific Telephone en una subasta, "adquirió" la clave maestra de las direcciones de envío de suministros en el área de Los Angeles y compró un marcador

telefónico de tarjeta del tipo Touch-Tone, con un juego de tarjetas similares a las que utilizaban los almacenes para hacer los pedidos.

Schneider se aprovechó del sistema de presupuestos que empleaban los almacenes para hacer los pedidos. Normalmente, los almacenes tenían un adjudicado presupuesto para materiales superior a lo que realmente necesitaban, y mientras no se superase ese presupuesto, no se hacían averiguaciones sobre los pedidos realizados. Schneider se las arregló para acceder al sistema on-line de presupuestos para averiguar cual era el límite de cada almacén y poder hacer pedidos sin despertar sospechas.

Durante siete meses, la Pacific Telephone le envió equipos, pensando que lo hacía a sus almacenes, material que él vendía a sus clientes ¡y a la propia Pacific Telephone! Llevaba el control del stock de los diferentes inventarios, rebajaba esos inventarios con sus pedidos y luego le vendía de nuevo los equipos a la Pacific Telephone, para que completasen el stock.

Schneider fue descubierto cuando reveló sus actividades a un empleado suyo. Llegó un momento en que no pudo mantener sus actividades por si mismo y pidió la colaboración de un empleado de su confianza. Cuando el empleado le pidió un aumento de sueldo, Schneider lo despidió, y entonces el empleado le contó el fraude a la Pacific Telephone.

Los investigadores no se pusieron de acuerdo sobre la cantidad que Schneider defraudó a la Pacific Telephone. Donn B. Parker [1976] estima, en su libro “Crime by Computer”, que Schneider consiguió equipo por valor de varios millones de dólares.

Por el fraude, Schneider fue condenado a dos meses de cárcel, seguidos de tres años de libertad condicional.

Curiosamente, cuando a los dos meses salió de la cárcel, creó una empresa especializada en seguridad de ordenadores.

Se pide:

Escribir un breve informe sobre algunos procedimientos básicos de control interno que, de haberse aplicado, hubieran evitado o detectado el fraude y explicar por qué estos procedimientos hubieran tenido éxito.

1.1.6.3 Union Dime Savings Bank

Los bancos suelen ser entidades propensas al abuso de ordenador. Roswell Steffen utilizó un ordenador para defraudar 1,5 millones de dólares del Union Dime Savings Bank en Nueva York. En una entrevista con Miller [1973] después de haber sido descubierto, afirmó: “Cualquiera que tenga una cabeza sobre sus hombros puede defraudar dinero de un banco con éxito. Y la mayoría lo hacen.”

Steffen era un jugador empedernido. El fraude lo empezó cuando tomo “prestados” $5000 de la caja para hacer frente a sus apuestas, con la intención de devolverlos con los beneficios de las mismas. Desafortunadamente, perdió los $5000 y pasó los tres años

y medio siguientes intentando devolverlos, utilizando el mismo sistema de tomar "prestado" el dinero para gastarlo (y perderlo) en las carreras.

Como cajero principal del Union Dime, Steffen tenía un terminal desde el que podía acceder en modo supervisor al sistema on-line del banco, para labores administrativas diversas. Steffen cogía el dinero de la caja y utilizaba su terminal para manipular los saldos de las cuentas de los clientes para esconder el desfalco, y para que éste no apareciese reflejado en las Hojas de Fondo diarias.

Steffen empleaba técnicas diversas para obtener dinero. Al principio, se concentró en cuentas con un saldo superior a $100.000 y que tuviesen pocos movimientos, y en aquellas en las que sus intereses se pagaran trimestralmente, utilizando su terminal para rebajar los saldos de las cuentas. De vez en cuando, un cliente llamaba protestando, y entonces Steffen simulaba una llamada al Centro de Proceso de Datos para averiguar lo que había ocurrido, e informaba al cliente que había sido un simple error; luego corregía el saldo del cliente y lo cargaba en otra cuenta.

Otra fuente de ingresos lo constituían las cuentas de plazo a dos años y las cuentas de nueva apertura. Con las primeras, Steffen preparaba la documentación necesaria pero no la registraba en los ficheros den banco. De esta manera disponía de dos años para corregir la situación, pero las cosas se complicaron cuando el banco comenzó a pagar los intereses a esas cuentas trimestralmente. Con las cuentas nuevas, utilizaba dos libretas nuevas, procedentes del stock de libretas numeradas del banco, utilizaba el número de cuenta de la primera libreta para registrar el alta de la cuenta, pero la registraba en la segunda, y a continuación destruía la primera.

Con el tiempo, el fraude se volvió mas y más complejo y Steffen cometió muchos errores. No obstante, el sistema de control interno del banco y las técnicas de auditoría eran lo suficientemente "pobres" que siempre pudo explicar las diferencias y seguir adelante.

Steffen fue descubierto porque la policía se dio cuenta de que las apuestas que hacía no se podían sostener con el simple sueldo de un cajero.

Se pide:

Escribir un breve informe indicando algunos procedimientos básicos de control interno que, de haberse aplicado, hubieran evitado o detectado el fraude y explicar por qué estos procedimientos hubieran tenido éxito.

1.2 Enfoque General de AI

"Estar a cargo de AI en una instalación con varios cientos de programadores y analistas, un Host monstruo y miles de bases de datos y ficheros es una experiencia irrepetible"

Problema: Solo en las instalaciones más pequeñas puede un auditor llevar a cabo una comprobación detallada de todos los procesos que se realizan. Estar al frente de

auditoría informática en una instalación muy grande es completamente distinto a la auditoría que se puede realizar en una instalación pequeña o mediana.

Implicación: ¿Cómo garantizar que AI alcanza sus objetivos?

En este punto se verá un enfoque general para llevar a cabo una AI y algunas técnicas para simplificar la labor del auditor, y se discutirán algunas de las decisiones más importantes de un auditor cuando planifica una auditoria.

1.2.1 El sistema de Controles Internos y el enfoque de auditoría.

Una forma de comprobar que AI alcanza sus objetivos es examinar directamente los resultados de las aplicaciones:

- Los datos obtenidos
- Su utilización por los que toman decisiones.
- Los recursos consumidos por los sistemas.

No obstante, esto no es posible excepto en instalaciones muy pequeñas. Sin embargo, el auditor si puede examinar el Sistema de Controles Internos establecido por la gerencia.

El sistema de controles proporciona una forma de determinar si las cosas están funcionando correctamente. Si el sistema está correcto, el auditor puede estar más tranquilo con respecto a la calidad de las aplicaciones, y siempre podrá realizar comprobaciones “selectivas” de los resultados de las aplicaciones.

Por ejemplo, si la gerencia exige a los analistas y programadores el uso de una determinada metodología, es probable que el auditor no tenga necesidad de comprobar cada programa desarrollado, ya que existe una exigencia (control) por parte de la gerencia y se supone que los empleados la van a cumplir.

1.2.2 Controles y Potencial de Pérdidas.

La gerencia debe de establecer un Sistema de Controles Internos para minimizar el potencial de pérdidas. El “valor” de estos controles se puede medir en términos de su coste y comprobando como pueden reducir dicho potencial de pérdidas.

Por otra parte, se tendrá que comprobar si el coste de implantación de los controles es menor que los beneficios esperados. No se pueden poner controles indiscriminadamente sin saber si el beneficio que obtendremos al ponerlos va a ser menor que los gastos de implantación. Por ello, es necesario determinar el conjunto mínimo de controles que hacen máximo el beneficio.

Existen dos maneras de reducir el potencial de pérdidas:

- Reduciendo la probabilidad de que ocurran las pérdidas
- Reduciendo la cantidad perdida, si es que finalmente ocurren

El Control reduce las pérdidas esperadas actuando sobre las "causas" que lo originan. Si hay una pérdida, tiene que haber una causa de la pérdida, y los controles deben de actuar sobre dichas causas. No obstante, esta puede ser una labor compleja, porque los controles y las causas se entremezclan e interactúan, haciendo muy complicada la evaluación global de los sistemas de control interno.

Por ejemplo, una toma de decisiones errónea puede ser debida a que los datos sean imprecisos y/o incompletos, y esta imprecisión ser causada por errores cometidos durante su captura, a su vez causados por… Existe una jerarquía de pérdidas y sus causas, y el auditor debe de comprobar lo bien que actúan los controles sobre dichas causas.

El problema es que entre controles y causas no existe siempre una relación 1:1, como tampoco existe entre las causas de alto nivel y de bajo nivel. Por el contrario, existen relaciones múltiples (relaciones funcionales) entre los controles y las causas, y el auditor debe de conocer muy bien la empresa y el negocio de la empresa para poder determinar y comprender estas relaciones.

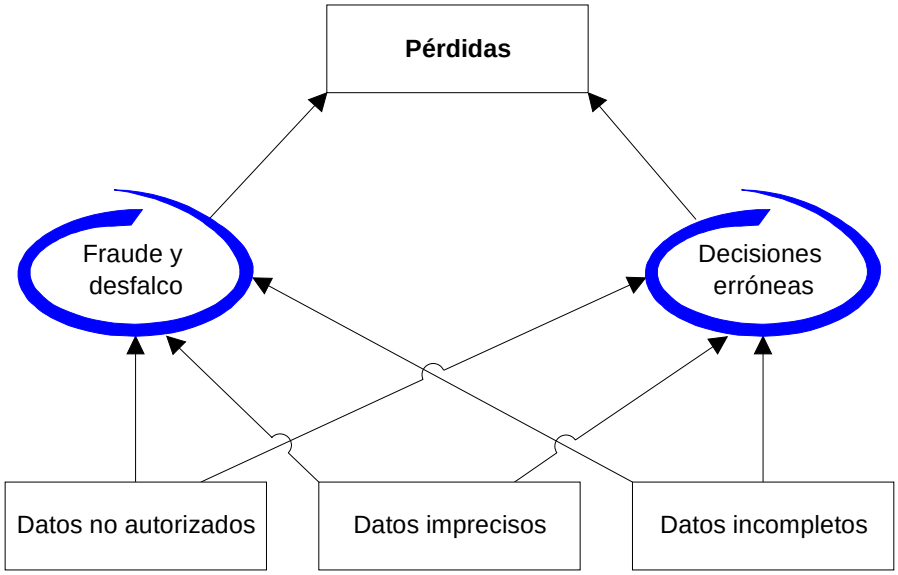


Fig. 1.1 Jerarquía de las pérdidas y sus causas

1.2.3 La Naturaleza de los Controles del Ordenador

Estableceremos en este punto una clasificación de los controles de internos, ya que esta clasificación va a facilitar la labor del auditor.

Estableceremos dos categorías principales:

- Según el tipo de control: Controles de Gerencia y de Aplicación
- Según el momento en que se realizan: Controles Preventivos, de Detección y Correctores

1.2.3.1 Controles según el tipo de control: Controles de Gerencia y Controles de Aplicación

Clasificar los controles en Controles de Gerencia y Controles de Aplicación es útil por varias razones:

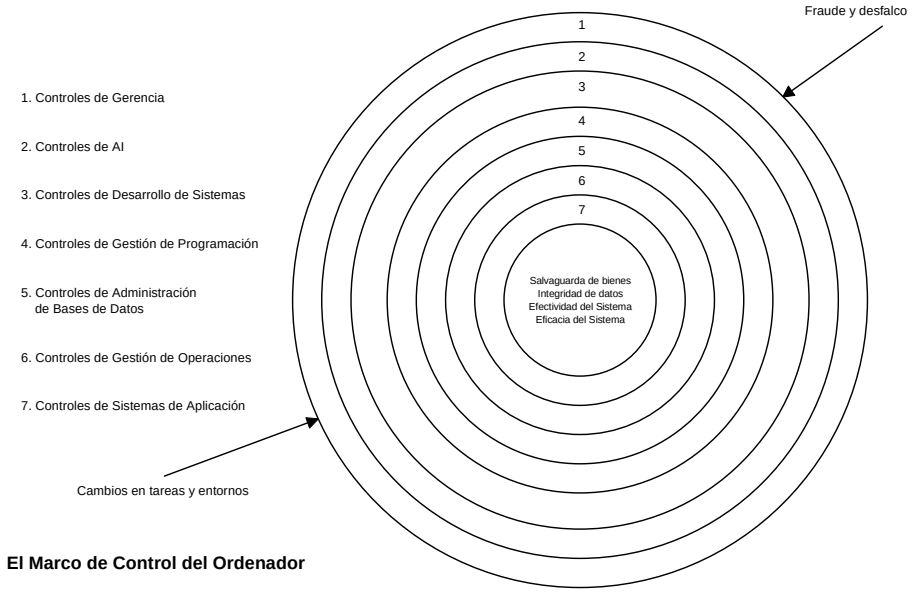


Fig. 1.2 El Marco de Control del Ordenador

- En primer lugar, casi siempre es mejor para el auditor el evaluar en primer lugar los Controles de Gerencia, por lo que está clasificación proporciona un orden adecuado para conducir la auditoría.

- Parece conveniente presentar, conceptualmente, los controles en un CPD por capas. De esta manera, cualquier intento de violación de los controles tendrá que atravesar todas esas capas, por lo que, si las exteriores están intactas, es muy probable que las interiores también lo estén.

1.2.3.1.1 El Marco de Control de Gerencia.

Estos controles intentan garantizar que el desarrollo, implementación y operación de los Sistemas de Información se efectúan de un modo controlado y planificado.

Distinguiremos 6 niveles de controles.

1. Gerencia General

La gerencia general debe garantizar que la instalación esté bien gestionada. Es responsable principalmente de establecer políticas a largo plazo sobre cómo se deben de utilizar los ordenadores de la empresa.

2. Gerencia de AI

Es responsable de planificar y controlar las actividades del ordenador. Obtiene datos que sirven a la gerencia para su toma de decisiones a largo plazo y convierte estas políticas a largo plazo en objetivos a corto plazo.

3. Gerencia de Desarrollo de Sistemas

Responsable del diseño, implementación y mantenimiento de todas las aplicaciones.

4. Gerencia de Programación

Responsable de programar nuevos sistemas, mantener los existentes y del soporte software general de sistemas.

5. Administración de Bases de Datos

Responsable del uso y control de las bases de datos de la instalación o de las librerías de ficheros del sistema.

6. Gerencia de Operaciones

Responsable del día a día de la instalación: preparación de datos, flujo de datos en la instalación, ejecución de los sistemas de producción, mantenimiento del hardware y, en ocasiones, mantenimiento de librerías de programas y ficheros, facilidades de librerías y seguridad de la instalación.

Estos controles se aplican a todos los Sistemas de Información de la instalación. Su ausencia sería un serio inconveniente para un auditor ya que tendría que verificar todas las actividades. Por el contrario, si existen estos controles, puede estar más seguro, ya que se da por hecho que los empleados seguirán las normas de la gerencia.

Por otra parte, es conveniente evaluar estos controles en primer lugar y una sola vez, ya que son comunes a todas las aplicaciones, e incluso puede no ser aconsejable auditar los Controles de Aplicación si los de Gerencia son “débiles”. Más aún, es posible no continuar con la auditoría cuando se compruebe que no hay existen suficientes garantías del cumplimiento de los controles de gerencia.

1.2.3.1.2 El marco de Control de Aplicación.

Estos controles intentan garantizar que las aplicaciones individuales cumplan los requisitos AI. Se dividen en 9 capas o niveles.

1. Controles de Captura de datos

Garantizan que se registran todas las transacciones y que éstas están autorizadas y son completas y precisas. También garantizan que los datos de origen se envían a donde son preparados para su entrada en el ordenador, y que posteriormente se devuelven a su lugar de origen y archivan. Ejemplo: Captura de datos de cheques que llegan a una entidad bancaria, para su tratamiento informático y posterior archivo de los cheques.

2. Controles de Preparación de Datos

Garantizan la conversión de todos los datos a un formato entendible por el ordenador, y que todo dato es completo, autorizado y preciso. Garantizan además que los datos de entrada lleguen al ordenador o a un dispositivo de entrada, y que además se devuelven a su origen y se archivan.

Estas dos primeras categorías en la actualidad se pueden refundir en una sola.

3. Controles de Acceso

Garantizan que solo el personal autorizado tenga acceso a los recursos del ordenador, tales como ficheros y programas. Ejemplo: Sistema de Gestión de Control y Acceso de Recursos.

4. Controles de entrada

Garantizan que todo dato que entre en el ordenador esté autorizado, sea preciso y esté completo. Garantizan también que los errores que se detecten sean corregidos y se vuelvan a introducir para ser procesados. Ejemplo: Controles en las altas de nuevos datos en cualquier aplicación.

5. Controles de Transmisión

Garantizan que la transmisión de datos entre dos puntos sea precisa, completa y esté autorizada. Ejemplos: En la actualidad, los protocolos de transmisión de datos ya incorporan medidas de seguridad, tales como indicar si la transmisión fue completa, realizar reintentos de transmisión frente a cortes en la transmisión, etc. Temas relacionados: Encriptación de datos.

6. Controles de proceso

Garantizan que los programas procesan todos los datos que entran y que ese proceso está autorizado, es preciso y está completo. Ejemplo: Control del número de registros procesados para verificar que se han procesado todos, control de procesos que pueden acceder a toda la memoria del sistema, control de procesos protegidos con palabras de paso, autorización para ejecutar determinados procesos, etc.

7. Controles de salida

Garantizan que la salida está autorizada, es precisa y está completa; que se entrega al personal responsable de ella y es adecuadamente archivada. Ejemplo: Controles para verificar que la información impresa sólo la puede ver la persona o personas autorizadas, destrucción de documentos confidenciales, etc.

8. Controles de pistas de auditoria

Garantizan que los datos pueden ser seguidos a través del sistema, desde su origen hasta su destino final y que se puede restaurar su integridad si se corrompen durante su camino. Ejemplo: Control de transacciones por medio de logs, procedimientos de rollback y recovery, etc.

9. Controles de Copias de Seguridad y Recuperación

Estos controles garantizan que los datos físicos se puedan recuperar en caso de pérdida o de daños en su integridad. Ejemplo: Uso de copias de seguridad, centros de backup, etc.

1.2.3.2 Controles según el momento en que se realizan.

Distinguiremos tres tipos:

- Controles Preventivos
- Controles Detectores
- Controles Correctores.

Esta clasificación es útil porque indica cuando hay que utilizarlos.

1. Controles Preventivos

Intentan evitar que ocurra el error. Se utilizan en las primeras etapas del flujo de datos de un sistema. Por ejemplo: el tener buenos formularios de entrada de datos ayuda a evitar que se produzcan errores en la captura.

Son controles generales. Este hecho les hace inmunes a los cambios, pero posibilita la aparición de errores de muchas clases. Por ejemplo: la separación de tareas no cambia aunque las tareas se realicen de diferente manera, pero no garantiza que las tareas estén bien ejecutadas. El hecho de tener buenos formularios no impide que se cometan errores en la captura.

2. Controles detectores

Identifican los errores después de que éstos ocurran. Tienden a ser controles específicos, utilizados en una fase posterior en el tiempo a los controles preventivos. El hecho de ser específicos hace que sean dependientes de los cambios. Ejemplo: programas de validación de entrada de datos.

3. Controles Correctores

Tratan de garantizar que se corrigen los errores detectados. Por ejemplo: Listar los errores de una actualización y grabarlos en un fichero donde se corrigen, para posteriormente utilizarlos como nueva entrada de datos, repitiéndose el proceso hasta que no se detecten nuevos errores.

1.2.4 Visión General de los pasos de una Auditoria Informática.

En este punto se describirá brevemente cada uno de los pasos a realizar durante una Auditoria Informática. Este esquema, que se muestra en la figura siguiente, ha sido desarrollado por el American Institute of Certified Public Consultants, y es el comúnmente aceptado por la mayoría de las empresas de auditoría.

Aunque los pasos indican una progresión secuencial, algunos de ellos se pueden simultanear. Por ejemplo, por efectividad, los datos necesarios para la revisión preliminar y para la revisión detallada se pueden recoger al mismo tiempo.

1.2.4.1 Fase I: Revisión Preliminar

El objetivo de esta fase es revisar la instalación para obtener información sobre cómo llevar a cabo la auditoría. Al finalizarla, el auditor puede proceder de tres maneras:

- No continuar con la auditoría. Por ejemplo por problemas de independencia, si el auditor no tuviera capacidad técnica para realizar la auditoría y necesitara ayuda del propio auditado.

- Pasar a la Fase II para realizar la revisión detallada de los controles internos, esperando poder confiar en ellos, y reducir así los Tests de Apoyo.

- Pasar directamente a la Fase IV. Si no se confía en los controles internos, puede ser menos costoso realizar directamente los Test de Apoyo. También puede ocurrir que los controles de AI sean iguales que los controles del usuario, en cuyo caso puede ser mejor revisar estos últimos.

1.2.4.2 Fase II: Revisión Detallada

El objetivo de esta fase es obtener la información necesaria para tener un conocimiento detallado (profundo) de los controles utilizados en la instalación. Al finalizarla, el auditor puede tomar una de las siguientes decisiones:

- No continuar con la auditoria

- Pasar a la Fase III, esperando poder confiar en los controles internos

- Pasar directamente a la Fase IV

En esta segunda fase se revisan de nuevo los controles de Gerencia y de Aplicación, se identifican las causas de las pérdidas y los controles para reducirlas y al final de la fase, se decide si estos controles reducen las causas de las pérdidas a un nivel aceptable.

Dado que aún no se sabe lo bien que funcionan dichos controles, se asume que lo harán bien, a menos que se tenga evidencia que demuestre lo contrario.

En esta fase pueden existir diferencias en el modo de conducir la auditoría, dependiendo de quién la esté realizando. En el caso de ser un auditor interno, éste buscará causas que afecten principalmente a la eficiencia y a la efectividad del sistema, y tratará de que no se produzca un control excesivo del mismo, buscando el juego de controles mínimo necesario. Si se trata de un auditor externo, lo más probable es que busque controles para garantizar la salvaguarda de bienes y la integridad de los datos, principalmente.

1.2.4.3 Fase III: Pruebas de Comportamiento

El objetivo de esta fase es comprobar que los controles internos funcionan como lo deben de hacer; es decir, que los controles que se suponía que existían, existen realmente y funcionan bien. Las técnicas utilizadas, además de la recogida manual de evidencias ya descrita, contemplan el uso del ordenador para verificar los controles.

- Al final de la fase, el auditor puede decidir evaluar de nuevo el sistema de controles internos, de acuerdo con la fiabilidad que han mostrado los controles individuales.

- El procedimiento de evaluación y la elección de nuevos procedimientos de auditoria son los mismos que los de las fases anteriores.

1.2.4.4 Prueba y evaluación de los Controles del Usuario (Controles de Compensación)

El auditor puede decidir que no hace falta confiar en los controles internos porque existen controles del usuario que los sustituyen o compensan. Para un auditor externo, revisar estos controles del usuario puede resultar más costoso que revisar los controles internos. Para un auditor interno, es importante hacerlo para eliminar posibles controles duplicados, bien internos o bien del usuario, para evitar la redundancia.

1.2.4.5 Fase IV: Pruebas de Apoyo.

El objetivo de esta fase es obtener evidencias suficientes para tomar la decisión final sobre si pueden ocurrir o no pérdidas materiales durante el procesamiento de los datos.

Por ejemplo, un auditor externo podrá formarse una opinión sobre si existen o no discrepancias sobre el estado de cuentas de la empresa, mientras que un auditor interno deberá de tener una perspectiva más amplia y se cuestionará si se está de acuerdo o no con los controles internos, si han ocurrido pérdidas o pueden ocurrir en el futuro, etc.

De acuerdo con [Davis et al, 1981], existen cinco tipos de pruebas de apoyo:

1. Para identificar procesos erróneos
2. Para garantizar la calidad de los datos
3. Para identificar datos inconsistentes
4. Para comparar datos y cuentas físicas
5. De confirmación de datos con fuentes externas

En todas estas pruebas, se puede utilizar el ordenador como herramienta de apoyo.

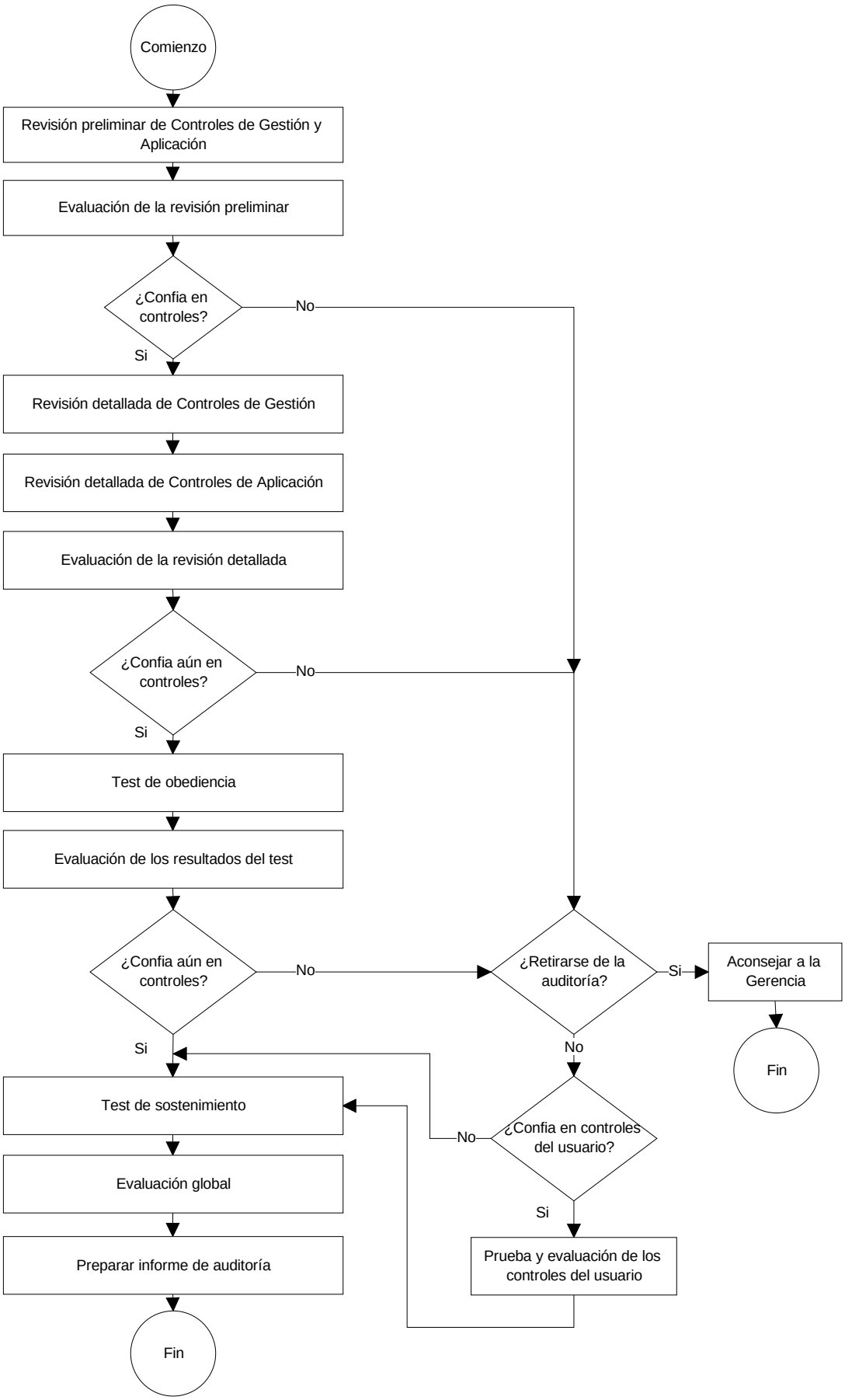


Fig. 1.3 Pasos de una Auditoría Informática

1.2.5 Algunas decisiones importantes de Auditoria.

En los puntos siguientes se estudiará la naturaleza de las decisiones a tomar así como algunas consideraciones sobre cómo se toman.

1.2.5.1 El Criterio de Evaluación

Se hace al final de cada fase y es la decisión más difícil, ya que es una cuestión de criterio y no existe un único método aceptado para tomar la decisión. Se decide si:

- Se continúa o no con la auditoria
- Los controles internos son fiables o no
- Qué controles son críticos y cómo se deben de probar
- Qué y cuántos tests de apoyo hay que realizar
- La aplicación pasa o no la auditoria

Como ejemplo, en la tabla siguiente se muestra una representación conceptual de los criterios a considerar en un proceso de captura de datos.

Control/Causa de la Pérdida	Reconocimiento o medida imprecisa	Reconocimiento o medida incompleta	Evento no reconocible o no medido	Reconocimiento o medida no autorizada
Contratar personal de alta calidad	√	√	√	√
Asegurarse de que el personal está entrenado	√	√	√	
Asegurarse de que hay separación e tareas	√	√	√	√
Procedimientos bien distribuidos	√	√	√	
Procedimientos bien documentados	√	√	√	
Supervisar el personal adecuadamente	√	√	√	√
Tareas bien diseñadas	√	√	√	
Entorno de trabajo agradable	√	√	√	
Restringir acceso físico				√

Fig. 1.4 Matriz de Criterios de Evaluación en un Proceso de Captura de Datos

En las columnas se indican las posibles causas de las pérdidas, es decir, aquellas circunstancias que originarían una pérdida si sucedieran durante el proceso de captura de datos. En las filas figuran los controles necesarios para minimizar dichas pérdidas.

Asimismo, en la tabla podría figurar alguna ratio de efectividad, que indicase cuán efectivo es el control.

A partir de esta tabla, se realizarán tres tipos de evaluaciones:

- De columnas: Responden a la pregunta: "Para una causa dada, ¿los controles reducen las pérdidas a un nivel aceptable?" El auditor deberá de evaluarlo antes y después de verificar los controles.

- De filas: ¿Los beneficios que proporciona un control exceden el coste de su implantación? Para facilitar la respuesta, los elementos de la matriz deberán de tener el beneficio marginal neto (beneficio – coste) de cada control, con respecto a cada causa de pérdidas.

- Global: ¿Cuál es el juego de controles óptimo para la empresa? Implica la evaluación conjunta de filas y columnas.

Al revisar los controles se tendrá en cuenta que, aunque desde un punto de vista de columnas pueda no ser interesante implantar un determinado control, desde el punto de vista de las filas puede ocurrir que los beneficios que proporciona el control, al ser ejecutado sobre todas las causas, sea superior al coste de implantación de dicho control.

Otros factores a considerar a la hora de especificar controles pueden ser los siguientes:

- Los costes y beneficios pueden ser "condicionales". Es posible que algunos de los controles que se desee poner ya se estén utilizando, por lo que su coste de implantación es cero.

- Si ya hay muchos controles implantados, el añadir uno más puede ocasionar que se disparen los costes.

La Matriz de Criterios de Evaluación sirve también para ilustrar las diferencias entre Auditoría externa e interna:

- Auditor externo: Considerará principalmente la evaluación de columnas, centrándose en aspectos tales como la salvaguardia de bienes y la integridad de datos. Es decir, se centrará en intentar reducir las pérdidas a un nivel satisfactorio, y el hecho de que la elección de controles sea óptima, desde un punto de vista global, será para él una cuestión secundaria.

- Auditor interno: Aunque se centrará en la efectividad y eficiencia del sistema, realizará los tres tipos de evaluación, de filas (costes marginales), columnas (efectividad y eficacia) y global (juego óptimo de controles)

El cómo llevar a cabo la evaluación, sea del tipo que sea, aún es un área de investigación, aunque existen unos estándares mínimos para la evaluación de columnas. [Canadian, 1970] [EDP, 1977]

1.2.5.2 Planificación de los Procedimientos de AI

Existen diferentes criterios para determinar cómo y cuándo se deben planificar los procedimientos de AI. Algunos auditores opinan que debe de haber pocas diferencias con respecto a la auditoria tradicional, y que es necesario intervenir al comienzo del proyecto, en el medio del proyecto y al final del proyecto, realizando luego una fase de seguimiento una vez que el proyecto ha terminado, si bien reconocen que AI necesita una fase de preparación previa.

Sin embargo, otros auditores estiman que existen diferencias fundamentales entre las dos auditorias, y sostienen que AI debe de participar en la fase de diseño, en la fase de operaciones y en la fase de post-auditoría.

La razón esgrimida es que cambiar los controles después del diseño es muy caro, y además, conocer el sistema si no se ha participado en su diseño es casi imposible.

Como mínimo, tanto los auditores internos como los externos deben de revisar y evaluar el diseño de los controles de ordenador en varios “checkpoints” durante el ciclo de vida del desarrollo del software.

El posible inconveniente de este enfoque es que al involucrarse el auditor con los diseñadores puede perder su independencia, como se ha confirmado en algunas encuestas [Rittemberg, 1977] No obstante, existen modos de paliar esta pérdida de independencia. Entre otros podemos citar:

- Aumentar el conocimiento informático del auditor
- Poner auditores diferentes en la Fase de Diseño y en la de Post-implementación
- Crear una sección de auditoria especializada en AI
- Conseguir auditores con experiencia en Informática
- Obtener mayor apoyo de la Dirección

En principio, y de acuerdo con encuestas realizadas, los dos primeros métodos parecen ser los más recomendables y los que proporcionan mejores resultados.

1.2.5.3 Uso del Ordenador en AI

Una de las cuestiones que se ha debatido constantemente es decidir si se debe de usar el ordenador como ayuda a la auditoría, y si se decide hacerlo, cómo puede beneficiarse la auditoría con su uso. Estudiaremos en esta apartado las dos posibilidades.

<u>Auditoría sin ordenador</u>

Si no se utiliza el ordenados, el sistema a auditar se verá como una caja negra. Será necesario examinar el sistema de controles internos y examinar entradas y salidas, pero sin examinar los procesos, ya que sería imposible hacerlo “a mano”.

Esta opción es válida si el sistema a auditar es batch puro y es simple, o bien si el sistema usa software genérico bien conocido y probado (por ejemplo, si se ha comprado la aplicación y no se dispone de los programas fuente)

Entendemos por un sistema batch puro aquel sistema donde la lógica es "directa". Es decir, no existen rutinas especiales y las transacciones de entrada se procesan en batch y se pueden controlar por métodos tradicionales. Además, los procesos consisten principalmente en clasificar datos de entrada y en actualizar ficheros maestros secuencialmente.

Para dicho sistema, existen pistas de auditoria claras e informes detallados en puntos clave del proceso, y el entorno de tareas es relativamente constante y generalmente existe software comercial ya probado. En este caso, el auditor debe de comprobar que no se hayan hecho modificaciones a los paquetes originales, y que existan controles sobre el código fuente, sobre el código objeto y sobre la documentación, para evitar modificaciones no autorizadas.

En algunas ocasiones, los proveedores facilitan módulos genéricos que se deben de combinar, por medio de programas de control, para obtener los resultados deseados. En estos casos, es labor del auditor el comprobar dichos programas de control para garantizar su correcto funcionamiento.

Las ventajas de la auditoría sin ordenador podrían ser la simplicidad, la falta de necesidad de conocimiento informático de algunos auditores, aunque éstos deban de ser controlados por un auditor especialista en informática.

El principal inconveniente de este enfoque es que los sistemas de este tipo son escasos, y el auditor no puede determinar muy bien la probabilidad de que el sistema se degrade si el entorno cambia, ya que se está trabajando con paquetes cerrados sobre los que no se tiene control de sus procedimientos internos.

Auditoría con ordenador

Esta es la opción normal en la gran mayoría de los casos. Se debe de usar el ordenador para probar la lógica y los controles existentes en el sistema auditado y los resultados obtenidos por el sistema.

El ordenador se debe de emplear cuando el sistema procesa grandes cantidades de datos de entrada y salida, cuando una parte significativa de los controles internos está embebida en los programas o cuando la lógica es compleja.

Las ventajas de esta opción residen principalmente en la capacidad de proceso que proporciona el ordenador para hacer las pruebas, mientras que el mayor inconveniente es la necesidad de un amplio conocimiento informático por parte del auditor.

1.2.5.4 Aplicaciones candidatas para AI

En general, deberán de pasar una auditoría todas aquellas aplicaciones críticas para el negocio de la empresa.

Entre otras, las aplicaciones candidatas a ser auditadas serán aquellas que produzcan errores (para descubrirlas se deberá de hacer una auditoría de usuarios para determinar qué problemas producen y la importancia de los mismos), las "incómodas de manejar" y que por tanto afectan al entorno de trabajo (aplicaciones antiguas, aplicaciones con interfases poco amigables, etc.), las que sean más sensibles a posibles fraudes o las que interactúen con otros sistemas.

1.2.6 Resumen

Los pasos a dar en AI son similares a los dados en una auditoria clásica.

- El auditor hace una revisión preliminar para conocer el funcionamiento del Sistema
- Si cree que puede confiar en los controles internos, realiza una revisión detallada
- El auditor verifica los controles
- Realiza un "Test de Apoyo"
- Emite su opinión final sobre el Sistema.

El auditor debe de tomar varias decisiones importantes a lo largo del proceso de AI, ya que tiene que decidir si debe de fiarse de los controles, si continúa o no con la auditoría, si participará o no en el diseño y si utiliza o no el ordenador para conducir la auditoria.

1.2.7 Ejercicios y Casos

1.2.7.1 Independencia del Auditor

Eres un miembro del staff de una empresa de Auditoría Externa que está contratada para realizar una auditoría a una empresa financiera de tamaño pequeño - medio. Un día, recibes un comunicado para el Jefe de Auditoría, en el que se indica que el cliente está pensando reemplazar su ordenador central y reemplazarlo con 20 PC's, y convertir las aplicaciones existentes para que puedan ser ejecutadas en los PC's.

Alarmado por este cambio tan radical, y por las implicaciones de auditoría que representa, le pides permiso al Jefe de Auditoría para investigar el porqué de esos cambios y para proponer algunas alternativas de diseño, si fuera necesario.

El Jefe no está muy conforme con tu petición, y piensa que no te deberías involucrar tan pronto porque eso podría afectar a la independencia de la empresa. No obstante, está de acuerdo en que este cambio puede producir problemas y te pide un informe completo de tu posible actuación.

Se pide:

Escribir un informe para el Jefe de Auditoría indicando algunos de los problemas de control y de auditoría que pueden surgir por culpa del cambio propuesto, y justificar por qué deberías de involucrarte inmediatamente en el tema.

1.2.7.2 Causas de Pérdidas y Potencial de Pérdidas

El Departamento de Contabilidad de una pequeña empresa es responsable del pago a proveedores. Recibe una copia de cada orden de compra emitida, un albarán cuando se recibe la mercancía y finalmente la factura del proveedor.

Todos los documentos tienen estampada la fecha de recepción y se archivan en una caja fuerte. Cuando se recibe la factura del proveedor, un administrativo comprueba que la mercancía recibida coincide con la indicada en el albarán y en la factura y se asegura así de que la factura es correcta. Un segundo administrativo prepara la orden de pago y el correspondiente cheque y entrega toda la documentación y el cheque al Jefe del Departamento, quien la examina antes de firmarlo.

Se pide:

Relación de objetivos de control para toda la operativa indicada. Preparar una matriz de control en la que las columnas indiquen las causas de las pérdidas y las filas los controles para reducir las pérdidas potenciales. Los elementos de la matriz deben de indicar qué controles actúan sobre qué causas de pérdidas. Indicar en qué medida el sistema de controles internos permite alcanzar los objetivos de control.

1.2.7.3 Auditoría con Ordenador o sin Ordenador

Eres un miembro del staff de Auditoría Informática de una empresa pública de cuentas. La empresa acaba de conseguir un nuevo cliente, una pequeña empresa de manufactura, que utiliza un mini-ordenador para su proceso de datos.

Todos las aplicaciones del cliente son batch con entradas y salidas bien definidas. Sin embargo, el cliente utiliza un Sistema de Gestión de Bases de Datos que se compró en principio para su aplicación de Almacén, pero que en la actualidad es utilizado por todas las demás aplicaciones.

Estas a punto de realizar la primera auditoría del nuevo cliente, y el Jefe de Auditoría te pide tu opinión sobre si utilizar o no el ordenador en la auditoría.

Se pide:

Escribir un breve informe con tus recomendaciones y las razones de las mismas.

1.3 Organización y Gestión de la Función de AI

Por la literatura existente, se podría llegar a pensar que AI es una función separada de la auditoría tradicional. No obstante esto no es así, ya que AI es una parte integral de la totalidad de la función de auditoría que trata con la calidad de los sistemas por ordenador. Precisamente por esto, surge de inmediato la cuestión de cómo integrar AI dentro de la función de auditoría.

En este punto se estudiarán diversos problemas y controversias sobre la función de AI desde el punto de vista de organización y gestión.

1.3.1 Necesidad de una Función de AI independiente

La cuestión a plantearse es: ¿es necesario tener un grupo aparte de especialistas en AI? ¿se necesitan especialistas en AI? Y si es así, ¿dónde se ubican en la empresa?

1.3.1.1 La necesidad de especialistas en AI

La necesidad de especialistas en AI viene dada por tres razones principales: se necesita "suficiencia técnica", se necesita independencia y se necesita facilitar las comunicaciones con analistas y programadores.

De inmediato se plantean las siguientes preguntas: ¿cuánto conocimiento informático necesita un auditor para tener suficiencia técnica? ¿Puede el auditor ser experto en informática y en AI? ¿Cuáles son las responsabilidades de un auditor?

Como siempre, existen varios puntos de vista dependiendo del tipo de auditor de que se trate.

Para los Auditores externos:

- Punto de vista 1: El auditor externo necesita la experiencia mínima en informática para entenderse con los analistas. El auditor sólo revisa controles de gestión. Si es necesario, se busca un experto para hacer las pruebas.

- Punto de vista 2: Debe de existir diferencia en los conocimientos necesarios para ser auditor general y para ser auditor especialista en AI. El auditor de AI debe de tener los conocimientos para hacer una auditoria de un sistema batch. Si hay que profundizar más, se necesita un especialista en informática.

Para los Auditores internos:

- Especialización: Los auditores internos tienen que estar altamente especializados en Informática y deben ser un grupo aparte del resto de auditoria tradicional.

- Independencia: Es totalmente necesaria, y ésta aumenta si existe un grupo separado; pero lo importante es la independencia en "actitud", ya que el auditor tiene siempre que confiar en otros que lo ayuden.

- Relación con el CPD: Se necesita facilitar las comunicaciones con informática. Si el auditor tiene conocimientos informáticos fuertes, el entendimiento será mucho mejor.

1.3.1.2 Ubicación de AI en la empresa

Existen dos tendencias: AI como "Staff" y AI como "Línea"

AI realiza una función de "staff". Los auditores están asignados a grupos externos de auditoría. Su labor es asistir, aconsejar, etc., en los temas relacionados con proceso de datos.

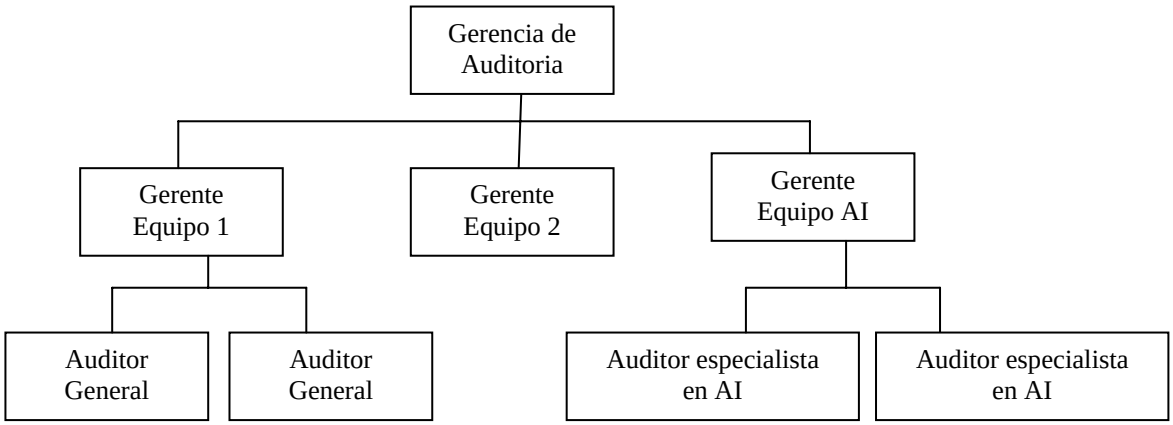


Fig. 1.5 AI como función de staff en la Empresa

Ventajas:

- Mejor uso de los recursos de AI, ya que no necesitan especializarse.
- No necesitan estar al día en los cambios tecnológicos en auditoria y en AI, puesto que sólo se ocupan de AI.
- Mejor considerado por la gerencia, ya que también forma parte de ella.
- Mejor coordinación y control, ya que tienen su propio gerente
- Permite especialización en tareas concretas

AI realiza una función de "línea". Los auditores están asignados a grupos internos de auditoria, formando parte de cada equipo de auditoria.

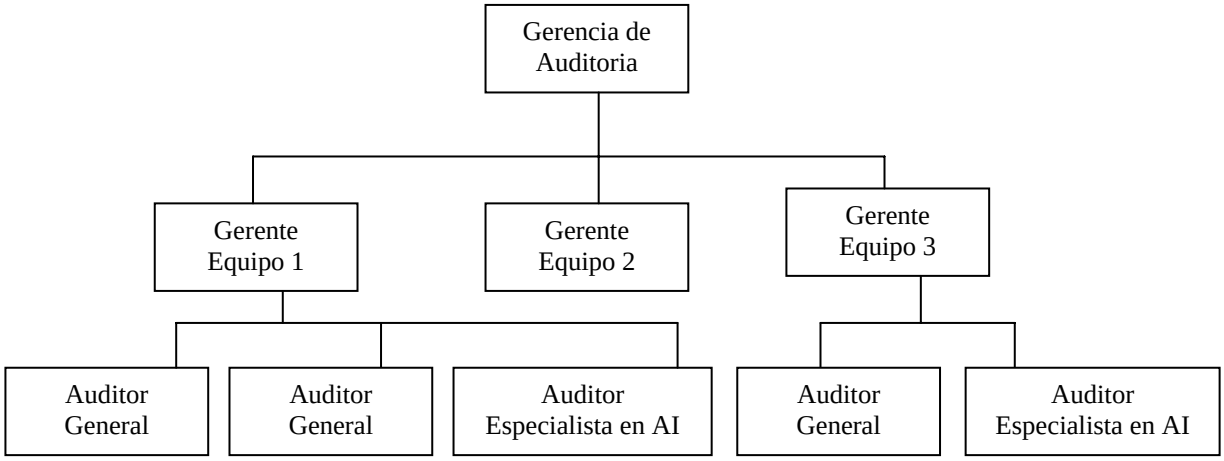


Fig. 1.6 AI como función de "línea" en la empresa

Ventajas:

- Al tener responsabilidades concretas para realizar la auditoria, habrá un mejor entendimiento de los objetivos.
- Mejores comunicaciones con el Equipo de Trabajo.
- Mejora la experiencia informática del auditor.

1.3.2 Centralización / Descentralización de la función de AI

Otra de las cuestiones a considerar es cómo se debe de implantar la función de Auditoría Informática. Como siempre, no hay una única solución, por lo que daremos algunos factores que influyen en la decisión.

Centralizar: Si hay pocos expertos en AI, si los auditores generales tienen un conocimiento básico de informática (situar AI como staff), si es difícil implementar técnicas asistidas por ordenador para recogida de evidencias en ubicaciones dispersas o si los grupos son de reciente creación.

Descentralizar**:** Si AI se realiza en ubicaciones dispersas geográficamente o si los grupos están "maduros", es decir, si tienen la suficiente experiencia.

1.3.3 La función de AI como staff: características principales

Para completar la creación del grupo de AI es necesario saber cuántos auditores informáticos son necesarios, y con qué especialistas se debe de formar el grupo de AI.

1.3.3.1 Número de auditores necesarios

[Weiss, 1977], tras un estudio en diversas empresas, concluye que se necesita un auditor informático por cada 16,5 analistas y programadores por término medio.

Además, es necesario considerar otros factores que influyen en el tamaño del grupo de AI, tales como el tamaño de la empresa, el negocio al que se dedica, el poco o mucho uso de los datos, el tipo de ordenador del que se disponga, la estabilidad del entorno, etc.

1.3.3.2 Origen de los Auditores Informáticos

Dado que hay pocos expertos tanto en auditoría tradicional como en auditoría informática, al crear un grupo de AI casi siempre es necesario formar nuevos auditores.

La cuestión que se plantea es: ¿es mejor dar formación de auditoria general a expertos en informática o de informática a auditores generales expertos en el negocio? En la práctica parece ser que la primera opción es la más aceptada.

1.3.4 Formación de AI

Según algunos autores, debería de ser suficiente con unas 3 semanas al año para mantener a los auditores al día en los cambios tecnológicos. No obstante, en algunas organizaciones esta formación alcanza fácilmente los 60 o más días al año.

Existen diversos factores que influyen en la decisión, tales como el nivel tecnológico existente, el nivel de cambios en la empresa, la madurez del grupo de AI, etc.

De acuerdo con [Perry, 1977], existen tres tipos de auditores informáticos: de nivel básico, de nivel intermedio y de nivel avanzado, y la formación a recibir varía dependiendo del grupo de que se trate.

Las diferentes técnicas de auditoría que necesita conocer cada grupo se indican en la tabla siguiente.

Técnica de auditoría	Básico		Intermedio		Avanzado	
	D&I	U	D&I	U	D&I	U
Puntuación (scoring)	4	4	4	4	4	4
Método de Test de Datos	4	4	4	4	4	4
Representación (mapping) asistida por ordenador	4	4	4	4	4	4
Guía de Auditoría	4	4	4	4	4	4
Registros extendidos	4	4	4	4	4	4
Rastreo manual y representación	4	4	4	4	4	4
Centro de competencia	4	4	4	4	4	4
Utilidad de Test Integrado	4	4	4	4	4	4
Test de Desastre	4	4	4	4	4	4
Selección de transacciones		4	4	4	4	4
Selección de área de auditoría		4	4	4	4	4
Recogida de datos embebidos		4	4	4	4	4
Instantánea (Snapshot)		4	4	4	4	4
Auditoría de software distribuido		4		4	4	4
Evaluación de sistemas base			4	4	4	4
Software de auditoría general			4	4	4	4
Software de auditoría terminal			4	4	4	4
Procedimientos de auditoría de post-instalación			4	4	4	4
Análisis de datos de procesos contables			4	4	4	4
Comparación de código			4	4	4	4
Diagramación asistida por ordenador			4	4	4	4
Simulación / Modelización					4	4
Operación en paralelo					4	4
Simulación en paralelo					4	4
Programas de auditoría de propósito especial					4	4
Rastreo asistido por ordenador					4	4
Ciclo de vida de desarrollo de sistemas					4	4
Guías de control de desarrollo de sistemas					4	4
Grupo de control de aceptación de sistemas					4	4

Fig. 1.7 Nivel necesario para el desarrollo, implementación y utilización de las técnicas de AI. Adaptado de Instituto de Auditores Internos. [Perry, 1977]
D&I: Desarrollo e Implementación; U: Uso

1.3.5 Relaciones entre AI y la gerencia y entre AI y otros grupos en la empresa.

Para que la tarea de auditoria en la empresa no resulte conflictiva, es imprescindible mantener buenas relaciones, tanto con la Gerencia de Desarrollo, como con los distintos Equipos de Trabajo y demás grupos del Centro de Proceso de Datos, ya que al haber un buen ambiente se facilita la realización del trabajo, y porque se necesita un fuerte apoyo de la gerencia, para poder realizar los controles de auditoria.

No obstante, durante el normal desarrollo de la función de auditoría van a aparecer una serie de problemas, de los que es necesario conocer sus causas, para intentar evitarlos o al menos minimizarlos.

1.3.5.1 Problemas conocidos

Los problemas al realizar una auditoria pueden deberse, entre otras cosas a:

1) Prisas por terminar la auditoría: Si hay posibilidad de fraude la gerencia quiere saberlo cuanto antes. Por lo tanto es necesario trabajar deprisa, lo que puede conducir a un abandono de los estándares, dejando la documentación para más tarde, por ejemplo.

2) Problemas de comunicación con la gerencia de Proceso de Datos: Entre los distintos grupos de proceso de datos y AI pueden producirse problemas debido al desconocimiento de la función de auditoria: Si los grupos desconocen los objetivos de AI, pueden pensar que la auditoría no va a aportar nada mas que trabajo extra durante el desarrollo, y considerar a los auditores como un "estorbo".

3) Fricciones con otros grupos: Con los grupos de desarrollo, porque los equipos de trabajo ven "supervisado" sus desarrollos por parte de AI, o incluso con los propios auditores generales, ya que éstos pueden sentir "celos" de AI.

1.3.5.2 Métodos para mejorar las relaciones

Para minimizar estos problemas e intentar mejorar las relaciones entre los distintos grupos y el equipo de auditoria se debe:

- Promover "comunicaciones abiertas", es decir, comunicar claramente los objetivos para que los distintos grupos sepan cómo van a ser auditados.

- Auditar solo dentro de las capacidades técnicas de AI. Es decir, auditar sólo sobre aspectos sobre los que los auditores tengan un amplio conocimiento. Esto debe ser así, sobre todo cuando el grupo de AI no es muy experto.

- Asignar prioridades a las tareas. Es decir, no pretender auditarlo todo, sino determinar qué tareas se deben de auditar y en qué orden, y hacerlo por consenso de todas las partes implicadas.

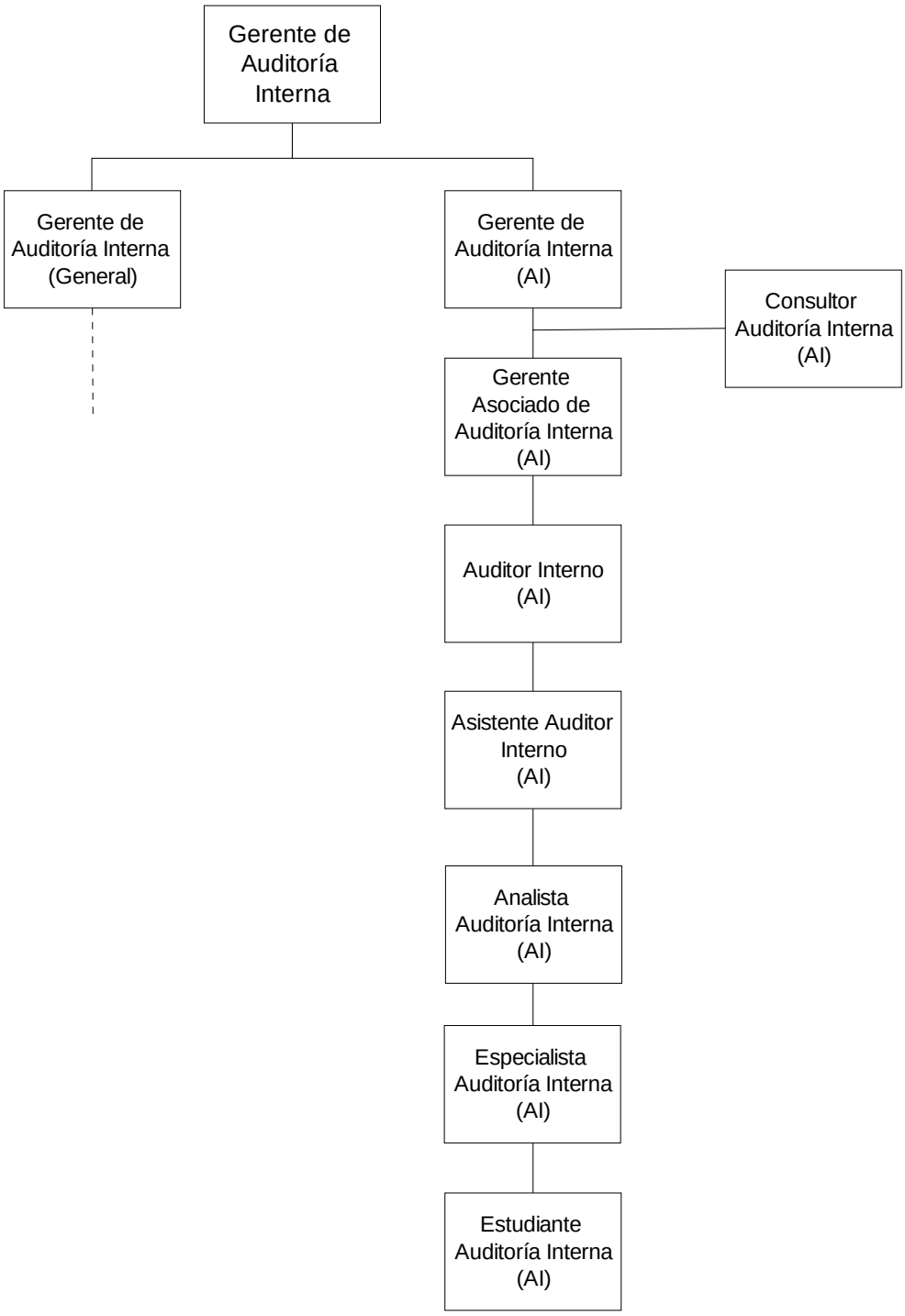
- Gestionar bien la función de AI. La impresión que el equipo de AI dé al resto de grupos de trabajo va a ser muy importante ya que si los demás grupos ven una auditoria sería tenderán a cooperar; pero si los grupos ven que los resultados de AI "no van a ninguna parte", pueden llegar a pensar que la auditoria no sirve para nada, que los auditores sólo sirven para "incordiar", que los únicos que hacen una labor constructiva son ellos, etc., etc.

1.3.6 Posibilidades de promoción para un auditor informático

Para finalizar este punto, se muestran a continuación algunas de las posibilidades de promoción de un auditor informático. Para un auditor externo, las posibilidades de

promoción pueden ser a Administración de Bases de datos, a Consultor de Proceso de Datos y a Gerente de Proceso de Datos, entre otras.

Para un auditor interno, éstas posibilidades vienen dadas por el propio Ciclo de Vida del grupo de AI, como se muestra en la figura del punto siguiente.



1.3.7 Ciclo de Vida del grupo de AI

Fig. 1.8 Jerarquía del Departamento de Auditoría Interna. Instituto de Auditores Internos, 1974.

1.3.8 Resumen.

En este punto hemos estudiado el debate sobre cómo formar los distintos grupos de AI, la conveniencia de realizar una centralización o descentralización de la función de auditoría, así como el número de auditores necesarios y la formación y procedencia de los auditores informáticos.

Para finalizar, se estudiaron los problemas de la función de AI y los distintos medios para minimizarlos, y el Ciclo de Vida del grupo de AI.

1.3.9 Ejercicios y Casos

1.3.9.1 Escasez de personal de AI

Eres el director de Auditoría Interna de una empresa grande. Un día el presidente te pregunta por las razones por las que el personal de AI dura tan poco tiempo en el departamento. Ha notado que, por término medio, un licenciado recién contratado para AI dura un año antes de cambiar de empresa y está preocupado por la pérdida de capital humano que eso representa. Le respondes que hay mucha demanda de auditores y que esa es la causa del problema. No conforme con esto, el presidente te pide que elabores un informe sobre la situación y sobre cómo corregirla.

Se pide:

Preparar un informe con diferentes estrategias para disminuir la pérdida de personal en AI, discutiendo los puntos fuertes y los puntos débiles de cada estrategia y haciendo una recomendación final sobre cuál adoptar.

1.3.9.2 Cambio de Infraestructura Hardware

Eres el gerente de AI en el departamento de Auditoría Interna de una cadena de tiendas. En la actualidad, tienes seis equipos de AI a tus órdenes, que realizan funciones de staff en el departamento.

La gerencia ha decidido cambiar el modo de operar entre las distintas tiendas de la cadena, pasando del sistema actual centralizado, donde cada tienda tiene varios terminales conectados con el ordenador central, a un sistema descentralizado, con ordenadores personales en cada tienda, donde se hará el proceso de datos propio de la tienda, y, en general, solo se enviará un resumen de operaciones a la sede central, utilizando una red de comunicaciones. Asimismo, las comunicaciones entre tiendas se harán a través del ordenador central.

El personal de proceso de datos para soportar la nueva red se mantendrá centralizado en la sede central, y se utilizarán aplicaciones estándar en cada tienda, aunque para su implementación, cada tienda mantendrá su propio programador / analista de sistemas.

Se pide:

Supervisar y aconsejar sobre el impacto de esos cambios en la empresa y en la gerencia de AI. Preparar un informe subrayando los cambios que consideras necesarios, con la justificación de cada uno de ellos.

1.3.9.3 Selección de Personal

Eres el gerente de Auditoría Interna de una empresa pequeña – mediana, que ha desarrollado sistemas batch para un gran número de aplicaciones. En vista de los recientes casos de fraude, la gerencia te ha encargado contratar a una persona para AI (la primera en la empresa), de la cual serás el jefe directo.

Recibes dos solicitudes para el cargo. La primera es de una persona perteneciente al staff de Auditoría Interna, un licenciado contratado hace seis años por la empresa, que trabajó al principio como gestor de cuentas en la empresa y que por sus méritos fue posteriormente asignado a Auditoría Interna. Esta persona no tiene experiencia con ordenadores, con la excepción de un curso para usuarios que recibió en la facultad. Sin embargo, es una persona brillante y posee un buen conocimiento del sistema contable de la empresa, por lo que piensas que su capacidad de aprendizaje sobre temas informáticos será bastante grande.

El segundo solicitante es licenciado en matemáticas, analista / programador de una conocida empresa. Aunque ha estado involucrado en el diseño e implementación de sistemas contables, no ha recibido una formación formal en gestión de cuentas. Después de mantener una entrevista con él, y después de sondear a un conocido tuyo que trabaja en su empresa, piensas que se trata de una persona muy capaz.

Se pide:

Preparar un breve informe para la gerencia indicando a qué persona has elegido para el cargo, proporcionando las explicaciones necesarias para justificar la decisión tomada. Indicar qué trabajos piensas abordar en AI contando con esta persona.