

## AUDITORIA:

*Segons l'Enciclopedia Catalana* : **1** Càrrec d'auditor. **2** Despatx de l'auditor. **3** Examen de la situació econòmica d'una societat feta per auditors, a fi de donar a conèixer l'estat patrimonial o financer i per la qual hom pot detectar si una empresa es troba en situació de suspensió de pagaments o fallida o si hi ha irregularitat o frau en els llibres de comerç.

AUDITOR: **1 a** Assessor, relator, prop de certs tribunals superiors. **b** Jurista que exerceix funcions públiques d'assessor prop dels tribunals integrats per jutges no togats. **c** Instructor d'una causa eclesiàstica nomenat pel bisbe. **d** Oficial del cos jurídic militar a qui pertoca de donar judici en tots els casos d'interpretació o d'aplicació de les lleis. **2** Persona que realitza una auditoria.

*Segons el Diccionario de la Lengua española*: Empleo de auditor.|| Tribunal o despacho del auditor.

AUDITOR: Oyente.|| – **de guerra**. Funcionario del cuerpo jurídico militar que informa sobre la interpretación o aplicación de las leyes y propone la resolución correspondiente en los procedimientos judiciales instruidos por el fuero militar. || - **de la nunciatura**. Asesor del nuncio en España. || - **de la Rota**. Cada uno de los doce preladados del tribunal romano de la Rota. || - **de marina**. Juez letrado que entiende en las causas del fuero marítimo.

*Segons la Llei de protecció de dades amb el reglament que la desenvolupa: Real decreto 994/1999 de 11 de juny:*

### **Artículo 17.- Auditoría.**

1.- Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2.- El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3.- Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

*Segons The Encyclopaedia Britannica*: Examination of the records and reports of an enterprise by accounting specialists other than those responsible for their preparation. Public auditing by independent accountants has acquired professional status and become increasingly common with the rise of large business units and the separation of ownership from control. The public accountant performs tests to determine whether the management's statements were prepared in accord with acceptable accounting principles and fairly present the firm's financial position and operating results; such independent evaluations of management reports are of interest to actual and prospective shareholders, bankers, suppliers, lessors, and government agencies.

In English-speaking countries, public auditors are usually certified, and high standards are encouraged by professional societies. Most European and Commonwealth nations follow the example of the United Kingdom, where government-chartered organizations of accountants have developed their own admission standards. Other countries follow the pattern in the United States, where the states have set legal requirements for licensing. Most countries have specific agencies or departments charged with the auditing of their public accounts (*e.g.*, the General Accounting Office in the United States and the Cour des Comptes in France).

Internal auditing, designed to evaluate the effectiveness of a business' accounting system, is relatively new. Perhaps the most familiar type of auditing is the administrative audit, or pre-audit, in which individual vouchers, invoices, or other documents are investigated for accuracy and proper authorization before they are paid or entered in the books.

#### INFORMATION SYSTEMS AUDIT:

The effectiveness of an information system's controls is evaluated through an information systems audit. It is a part of a more general financial audit that verifies an organization's accounting records and financial statements. Information systems are designed so that every financial transaction can be traced. In other words, an audit trail must exist that can establish where each transaction originated and how it was processed. Aside from financial audits, operational audits are used to evaluate the effectiveness and efficiency of information systems operations.

Per desgracia a l'únic lloc on surt l'auditoria de sistemes d'informació es a la Britannica, al nostre país encara no està reconegut la professió d'auditor de sistemes.

Dons bé intentarem que amb el temps sortim amb algú dels nostres diccionaris i enciclopèdies, mentrestant ho intentarem explicar una mica.

#### AUDITORIA:

Procés sistemàtic pel qual una persona competent i independent obté i avalua objectivament evidències respecte a afirmacions sobre una entitat econòmica a fi de formar-se una opinió sobre ella i fer un informe sobre el grau en que dita afirmació s'ajusta a un conjunt determinat d'estandars.

#### CLASIFICACIONES:

- **Auditories Financeres:** Examen independent i emissió d'una opinió sobre la correcció dels estats o registres financers d'una organització. Es refereix a la integritat i fiabilitat de la informació.
- **Auditories Operatives:** Avaluar l'estructura dels controls interns en un procés o àrea determinada. Alguns exemples són les auditories de sistemes d'informació dels controls d'aplicació o dels sistemes lògics de seguretat.
- **Auditories Integrades:** Combina l'auditoria financera i l'operativa.
- **Auditories Administratives:** Orientades a analitzar aspectes relacionats amb l'eficiència de la productivitat operativa dins d'una organització.

- **Auditories de Qualitat:** Procés de revisió i emissió d'una opinió en referència al grau de compliment de les diferents normes ISO 9000.
- **Auditories de Riscos Laborals:** Avaluació sistemàtica, documentada i objectiva de l'eficàcia del sistema de prevenció de riscos laborals.
- **Auditories Mediambientals:** Procés de revisió i emissió d'una opinió en referència al grau de compliment de les diferents normes ISO 14000.
- **Auditories del Sistemes d'Informació:** Procés de recollir i avaluar evidències per a determinar si els sistemes d'informació i recursos relacionats, protegeixen adequadament els actius, mantenen la integritat de les dades i del sistema, donen informació fiable, aconsegueixen les metes de l'organització, consumeixen els recursos de manera eficient, i tenen actualitzats els controls interns que donen una garantia raonable que s'assoliran els objectius operatius i de control.

### **Segons la definició d'Auditoria Interna inclou l'anàlisi de riscos**

Indeed, the new definition of internal auditing, unanimously approved on June 26, 1999, by The IIA Board of Directors, includes "risk management".

(See <http://www.theiia.org/STANDARD/Newdef.htm>) It reads as follows:

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

## **PROCEDIMENTS GENERALS D'AUDITORIA**

1. Conèixer l'àrea objecte de l'auditoria.
2. Avaluació de riscos i planificació general de l'auditoria.
3. Planificació detallada de l'auditoria.
4. Revisió preliminar.
5. Avaluació.
6. Proves de compliment.
7. Proves substantives.
8. Informe.
9. Seguiment.

## **AUDITORIA BASADA EN RISC**

Cada cop més organitzacions estan anant a una auditoria basada en risc que permet desenvolupar i millorar el procés d'auditoria continua.

Les fases típiques serien:

- **Buscar informació i Planificar.**
  - Coneixement del negoci i de la indústria.

- Resultats de l'auditoria de l'any anterior.
- Informació financera recent.
- Lleis i normatives.
- Estimació de riscos inherents.
  
- **Comprendre el control intern.**
  - Ambient de control.
  - Procediments de control.
  - Determinació de la detecció del risc.
  - Determinació del control del risc.
  - Risc total.
  
- **Proves de compliment.**
  - Comprovar polítiques i procediments.
  - Comprovar la segregació de funcions.
  
- **Proves substantives.**
  - Procediments analítics.
  - Proves detallades.
  - Altres procediments substantius d'auditoria.
  
- **Tancar l'auditoria.**
  - Donar recomanacions.
  - Redactar l'informe d'auditoria.

### **RISCS D'AUDITORIA.**

- **Risc inherent.** El risc de que podria haver un error material, assumint que no hi ha controls relacionats per impedir o detectar l'error.
- **Risc de control.** El risc de que hi hagi un error material que no sigui previngut ni detectat pel sistema de control intern.
- **Risc de detecció.** El risc de que els errors o equivocacions materials que hagin ocorregut no hagin estat detectats per l'auditor.
- **Risc general d'auditoria.** El risc de que la informació o els informes financers puguin tenir errors materials o de que l'auditor pugui no detectar un error que hagi ocorregut.

### **ISACA (Information Systems Audit and Control Association)**

Es l'associació pel control i l'auditoria dels sistemes d'informació amb més de 28.000 associats a tot el món. Va néixer al 1969 als Estats Units amb el nom de EDPAA (Electronic Data Processing Auditors Association) més endavant al 1992 va canviar el nom a l'actual d'ISACA. Donat el caràcter altament especialitzat de l'auditoria dels sistemes d'Informació i les habilitats necessàries per dur a terme aquestes auditories es necessiten codis d'ètica professional i estandars aplicables globalment que s'adeqüin específicament a l'auditoria dels sistemes d'informació.

A més a més l'ISACA dona el certificat del CISA (Certified Information Systems Auditor) previ pas d'un examen i l'acreditació de 5 anys d'experiència en auditoria de SI.

L'estructura d'ISACA es amb chapters locals dins dels diferents estats del món.

El de Catalunya i Balears ha estat el primer chapter amb estatuts democràtics de l'estat espanyol.

## **CODI D'ETICA PROFESSIONAL DE ISACA**

Els membres de ISACA i el CISAs:

- Donaran suport a la implementació i al compliment dels estandars apropiats dels procediments i dels controls per als sistemes d'informació.
- Serviran al interès de les parts rellevants d'una manera diligent, lleial i honesta i no seran part , amb coneixement, de cap activitat il·legal o indeguda.
- Mantindran la privacitat i confidencialitat de la informació obtinguda en el decurs de les seves funcions, a no ser que l'autoritat legal els hi demani la seva revelació. Aquesta informació no serà usada per a benefici personal ni donada a parts inapropiades.
- Realitzaran les seves funcions de manera independent i objectiva i evitaran activitats que perjudiquin, o sembli que perjudiquin, la seva independència i objectivitat.
- Mantindran la competència en els seus camps respectius d'auditoria i control dels sistemes d'informació.
- Acordaran emprendre tant sols les activitats que puguin raonablement esperar realitzar amb competència professional.
- Faran les seves activitats amb la deguda cura professional.
- Informaran a les parts apropiades sobre els resultats de l'auditoria dels sistemes d'informació i/o treballs de control realitzats, donant a conèixer tots els fets materials que coneguin, que si no fossin revelats podrien o bé distorsionar els informes d'operacions o bé amagar pràctiques il·lícites.
- Donaran suport l'educació de clients, col·legues, públic en general, gerència i juntes directives per augmentar la seva comprensió de l'auditoria i el control dels sistemes d'informació.
- Mantindran alts estàndards de conducta i caràcter i no participaran en actes que puguin desacreditar al professió.

El no compliment d'aquest codi d'ètica professional pot tenir com a conseqüència una investigació de la conducta del membre o del posseïdor del CISA i en darrera instància l'adopció de mesures disciplinaries.

Per altra banda i com diem abans a nivell estatal tenim ISACA-BARCELONA que es el capítol catalano-balear de la ISACA i el primer capítol creat el 2001 a l'estat espanyol amb estatuts plenament democràtics, després es van constituir el capítol de València i posteriorment el de Madrid.

Els objectius de ISACA-BARCELONA queden recollits amb la seva acta fundacional i en concret en el seu article 4 rt.

**ARTICLE 4.-** *Els objectius de ISACA-BARCELONA són els següents:*

4.1. *Promoure l'educació, el perfeccionament i el desenvolupament dels coneixements de les persones en l'àmbit de l'auditoria, la consultoria, la seguretat, la garantia de qualitat i el control dels sistemes d'informació i camps relacionats.*

4.2. *Promoure un intercanvi obert entre els membres sobre tècniques i enfocaments relacionats amb l'auditoria, la consultoria, la seguretat, la garantia de qualitat i el control dels sistemes d'informació, i la resolució de problemes relacionats amb aquests temes.*

4.3. *Impulsar una comunicació adequada que permeti als membres d'estar al dia de les innovacions en les especialitats de l'auditoria, la consultoria, la seguretat, la garantia de qualitat i el control dels sistemes d'informació, i que beneficïi tant aquests membres com aquells que els contractin.*

4.4. *Recolzar els empresaris, auditors, universitats, administració pública, i professionals dels sistemes d'informació en la identificació i avaluació dels riscos dels sistemes d'informació i en el disseny dels controls necessaris per assegurar la seva organització i utilització eficaç, eficient, legal i segura.*

4.5. *Donar suport a l'Administració Pública Catalana en el desenvolupament de legislació i organismes de supervisió i control sobre la seguretat, auditoria i el control dels sistemes d'informació.*

4.6 *Donar suport als òrgans judicials i de l'advocacia en matèria de Tecnologies de la Informació amb una qualificació i ètica garantida i en un format clar i exempt d'argot tècnic*

4.7. *Recolzar la certificació professional dels associats.*

## **ESTANDARS D'ISACA**

Tenim tres nivells:

- **Estàndards:** defineixen els requisits obligatoris per a l'auditoria i l'informe.
- **Directrius:** donen una guia per aplicar els estàndards.
- **Procediments:** donen exemples sobre la manera de complir amb els estàndards quan s'està fent una auditoria de SI però no fixen requisits.

A l'apèndix A-1 teniu els estàndars, directrius i procediments detallats, com a resum però:

### **010 Contracte d'auditoria**

#### **010.010 Responsabilitat i autoritat**

La responsabilitat i l'autoritat de les funcions d'auditoria dels sistemes d'informació han d'estar documentades d'una forma adient mitjançant un contracte o carta de compromís d'auditoria.

### **020 Independència**

#### **020.010 Independència professional**

En tots els assumptes relacionats amb l'auditoria, l'auditor de sistemes d'informació ha de ser independent de l'auditat tan en actitud com en aparença.

#### **020.020 Relació amb l'organització**

La funció d'auditoria de sistemes d'informació ha de ser lo suficient independent de l'àrea que està essent auditada per a poder permetre que s'assoleixin els objectius de l'auditoria.

### **030 Ètica professional i estàndards**

#### **030.010 Codi d'ètica professional**

L'auditor de sistemes d'informació ha d'acatar el codi d'ètica professional de l'associació.

#### **030.020 Deguda cura professional**

S'ha d'exercitar la deguda cura professional i s'han d'observar els estàndards aplicables d'auditoria professional en tots els aspectes del treball de l'auditor de sistemes d'informació.

### **040 Competència**

#### **040.010 Habilitats i coneixements**

L'auditor de sistemes d'informació ha de ser competent des de el punt de vista tècnic i ha de tenir les habilitats i coneixements necessaris per fer la seva tasca d'auditor.

#### **040.020 Educació professional continuada**

L'auditor de sistemes d'informació ha de mantenir la seva competència tècnica mitjançant una educació professional continuada.

### **050 Planificació**

#### **050.010 Planificació de l'auditoria**

L'auditor de sistemes d'informació ha de planificar el treball d'auditoria dels sistemes d'informació per aconseguir els objectius de l'auditoria y per a complir amb els estàndards aplicables d'auditoria professional.

## **060 Realització del treball d'auditoria**

### **060.010 Supervisió**

El personal d'auditoria de sistemes d'informació ha d'estar degudament supervisat per garantir que s'assoleixen els objectius de l'auditoria i que s'observen els estàndards aplicables d'auditoria professional.

### **060.020 Evidència**

En el decurs de l'auditoria, l'auditor de sistemes d'informació ha d'obtenir les evidències suficients, confiables, rellevants i útils per aconseguir els objectius d'una forma efectiva. Les troballes i les conclusions de l'auditoria han d'estar respaldats per anàlisis apropiats i per una interpretació correcta d'aquesta evidència.

## **070 Informe**

### **070.010 Contingut i forma de l'informe**

L'auditor de sistemes d'informació ha de donar un informe, de manera apropiada, als destinataris que correspongui al acabar el treball d'auditoria. L'informe d'auditoria ha d'establir l'abast, els objectius, el període comprés i la naturalesa i envergadura del treball d'auditoria que es va realitzar. L'informe ha de identificar l'organització, els destinataris i qualsevol restricció sobre la seva circulació. L'informe ha de contenir les troballes, les conclusions i les recomanacions, així com qualsevol reserva o qualificació segons l'opinió de l'auditor en relació a l'auditoria.

## **080 Seguiment de les activitats**

### **080.010 Seguiment**

L'auditor de sistemes d'informació ha de demanar i avaluar la informació pertinent sobre les troballes, conclusions i recomanacions anteriors que siguin rellevants per determinar si s'han implementat les mesures adients de manera oportuna.