Introducció a l'auditoria TIC i de seguretat TIC

PID_00239291

Rafael Estevan de Quesada

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Índex

1. Definició d'*auditoria*

Actualment, la gestió moderna dels negocis, i especialment en organitzacions de gran dimensió o activitat o que simplement siguin madures quant a la professionalització de la seva gerència, fa que existeixi cada vegada més una necessitat de comprovar que els processos de negoci operen seguint l'estratègia de governança establerta per l'alta direcció, així com de conèixer totes les influències externes que puguin afectar l'àrea de negoci del procés:

- Marcs regulatoris generals: tot el marc legal que apliqui per a l'àmbit geopolític on s'executi el procés de negoci.

- Marcs regulatoris generals per a tots els negocis, però específics en un àmbit concret, com per exemple, tota la normativa de regulació del control de l'activitat financera i comptable, les lleis referents a privadesa i protecció de dades de caràcter personal (LOPD), la llei de serveis de la societat de la informació i el comerç electrònic (LSSI-CE), la llei sobre signatura electrònica, etc.

- Marcs regulatoris del sector en què es desenvolupa l'activitat de negoci, com per exemple, el mercat de les assegurances i els serveis financers.

- Termes i condicions concretades en les relacions contractuals entre client i proveïdor, acords de col·laboració entre diferents entitats d'un grup empresarial o codis deontològics entre organitzacions d'un sector econòmic.

- Bones pràctiques de la indústria.

- Etc.

En aquest context, és legítim considerar que, per iniciativa pròpia o per necessitat imposada externament, la direcció de l'empresa necessita verificar aquest compliment d'una manera o una altra i d'aquí sorgeix la necessitat de realitzar auditories.

De manera molt informal, quan es parla d'*auditoria* es pensa en una eina a disposició de la gerència per al control d'algun procés de negoci. Aquesta activitat s'entén que ha d'involucrar una metodologia per a establir els criteris que ajudaran a mesurar l'eficiència, l'eficàcia i les possibles desviacions dels objectius donats a un procés concret. Però aquesta no és més que una idea general i poc precisa. L'objecte d'aquest mòdul és entrar amb més detall en la definició i les característiques que té el procés d'auditoria.

Definició d'*auditoria*

Una auditoria, des d'un punt de vista molt general, és un **procés** executat per un auditor, que té la característica de **ser sistemàtic, independent i documentat**, i que busca obtenir a partir de la **realització de proves d'auditoria** registres, declaracions de fets o una altra informació coneguda com a ***proves d'auditoria***. Les proves d'auditoria han de ser **verificables**, **pertinents i avaluables** de manera objectiva per tal de determinar, d'acord amb aquestes, la mesura en què el fet auditat compleix uns **criteris d'auditoria**. Aquests criteris estan determinats per un conjunt de polítiques, procediments o requisits i són usats com a referència contra la qual es compara la realitat. Les proves d'aquestes diferències entre la realitat i la referència són el que s'entén com a *constatacions d'auditoria*. Finalment, el procés conclou amb l'anàlisi d'aquestes troballes per poder **emetre unes conclusions de l'auditoria**.

Per tant, podem concloure que el procés d'auditoria pretén poder objectivitzar el que, d'una altra manera, seria més correcte de qualificar com *l'opinió d'un expert*.

S'entén per *prova d'auditoria* el conjunt de registres, declaracions d'un fet o altra informació que es reculli durant el procés d'auditoria, que sigui verificable i pertinent per a ser contrastat amb els criteris d'auditoria. Per *criteri d'auditoria* s'entén el conjunt de polítiques, procediments o requisits usats com a referència en l'auditoria i que solen tenir com a objectiu el control d'algun aspecte de l'activitat de l'auditat. És per això que de vegades s'empra com a sinònim de ***controls***.

És important entendre que segons l'àmbit de coneixement o d'organització, es parla de diferents tipus d'auditories, encara que totes tenen un patró comú. Les més comunes són les següents:

- Auditories financeres, amb moltes distincions (auditories de compte, valoració d'empreses, etc.) i tradicionalment és el tipus més conegut, regulat i àmpliament aplicat per les organitzacions per les obligacions legals i implicacions amb vista al mercat.

- Auditories a processos productius o de qualitat, no solament relacionades amb l'ISO 9001 sinó també amb altres esquemes de gestió de la qualitat total com Six Sigma.

- Auditories al procés de gestió de recursos humans.

- Auditories de compliment legal.

Exemple

Auditories del marc legal de protecció de dades de caràcter personal a Espanya. El reglament de desenvolupament de la LOPD, aprovat pel Reial decret 1702 de 2007, en el seu article 96 estableix aquesta obligació a partir de la implantació de mesures de seguretat de nivell mitjà.

- Auditories a la gestió mediambiental.

- Auditories als sistemes d'informació i en general a la manera en què és tractada i gestionada la seguretat de la informació digital d'una organització.

- Etc.

Convé destacar que ens ocuparem de les auditories a sistemes de gestió de la seguretat de la informació. En tot cas, les auditories pretenen comprovar si l'auditat està exercint prou control sobre algun dels aspectes d'un o diversos dels seus processos de negoci. Des d'aquest punt de vista comú, explicarem en aquest mòdul els aspectes que són independents del fet que s'estigui auditant.

1.1. Principis d'auditoria

Sigui quin sigui el tipus d'auditoria i el fet auditat, l'auditoria sempre s'hauria de guiar per uns principis que garanteixin que el treball fet correspon a alguna cosa més que l'opinió d'un expert i que es pot considerar com una auditoria, és a dir, una anàlisi sistèmica. L'adhesió a aquests principis és necessària perquè les conclusions de l'auditoria siguin pertinents i suficients, i per a assegurar que els auditors que treballen independentment entre ells arribin a conclusions similars en circumstàncies similars.

Podem afirmar que si l'auditoria es regeix pels principis següents serà prou objectiva. Els principis que a continuació presentem poden considerar-se àmpliament reconeguts i estan basats en la norma ISO/IEC 19011 Directrius per a l'auditoria de sistemes de gestió.

Els principis d'auditoria afecten tant el comportament i les característiques de l'auditor com el procés d'auditoria en si mateix. Els següents estan relacionats amb la manera de comportar-se dels mateixos auditors:

- **Integritat / Conducta ètica**. Fonament del professionalisme. En una assignació d'auditoria és essencial que s'estableixin relacions de confiança entre l'auditat i l'auditor. Per a això, és necessari que l'auditor actuï amb un grau elevat d'integritat, confidencialitat i discreció. Es diu que l'auditor s'ha de regir per un codi de conducta estricte. Aquest codi pot estar explicitat o no. És habitual que diverses associacions o entitats que emeten certificats d'auditor publiquin els seus propis codis, encara que tots responen a les característiques que hem enunciat.

- **Presentació justa i imparcialitat**. L'obligació d'informar veraçment i amb exactitud. Les constatacions fetes, les conclusions extretes i els reports de l'auditoria que s'emetin han de reflectir, amb veracitat i exactitud, les activitats de l'auditoria. En tot moment, l'auditor i l'auditat han de tenir constància de tots els obstacles significatius oposats durant l'auditoria, els aspectes no resolts o no tractats, juntament amb les raons que ho van provocar, o qualsevol opinió divergent entre l'auditor i l'auditat.

- **Atenció professional adequada**. L'aplicació de diligència i judici en l'auditoria. Els auditors procedeixen amb tota la cura i la professionalitat requerida d'acord amb la importància de la tasca que duen a terme i la confiança dipositada pels clients de l'auditoria i les parts interessades en ells. Un prerequisit per a gaudir d'aquest reconeixement, per part de l'auditat i del client, és tenir la competència professional i tècnica necessària, i potser acreditar-la mitjançant certificats professionals, títols acadèmics, anys d'experiència o similars.

D'altra banda, altres principis d'auditoria s'apliquen al mateix procés de l'auditoria. Per definició, una auditoria és independent i sistemàtica, i aquestes característiques estan estretament relacionades amb els principis d'auditoria següents (que d'altra banda també han de regir la labor tant de l'auditor com de l'organització a la qual pertanyen):

- **Independència**. És la base de la imparcialitat i objectivitat de les conclusions de l'auditoria. Els auditors haurien de ser, per definició de l'auditoria, independents de l'activitat auditada. Això no implica que no puguin pertànyer a l'organització, sinó que no han d'estar influenciats d'alguna manera per l'activitat que han d'auditar. Això implica que, per descomptat, un auditor que hagi participat d'alguna manera en la implantació dels controls que s'han d'auditar, directament o indirectament (perquè ha assessorat en alguna decisió, per exemple), no hauria de participar en una auditoria ni emetre un judici d'auditoria, perquè està influenciat. Aquesta influència sobre l'auditor és la que fa que, no solament els casos com l'anterior siguin els que inhabilitarien un auditor, sinó que també els conflictes d'interessos s'haurien de tenir en compte a l'hora d'acceptar o no un auditor en un equip o en una assignació.
  Els auditors han de mantenir un estat mental objectiu durant tot el procés d'auditoria, per a assegurar que les constatacions i conclusions es basaran solament en proves.

- **Enfocament basat en la prova**. La base racional per a arribar a conclusions d'auditoria confiables i reproduïbles en un procés d'auditoria sistemàtic.
  L'auditoria es basa principalment en un cicle d'obtenció de proves, anàlisi d'aquestes proves i confrontació amb els criteris d'auditoria per a determinar la presència o no d'una constatació d'auditoria, que serà el suport per a la conclusió. Per tant, l'obtenció de la prova de l'auditoria és crucial, ja que ha de suportar la seva posada en dubte i, per tant, s'ha de derivar de

fets verificables. La prova s'ha de basar en mostres d'informació disponible. L'ús apropiat del mostreig està molt relacionat amb la confiança que es pot tenir en les conclusions de les auditories.

- **Confidencialitat**. Finalment, les parts implicades en l'auditoria (client i auditat) han de poder confiar plenament en la discreció i professionalitat de l'entitat auditora (i, per tant, dels auditors assignats) a l'hora de tractar amb la informació que és necessari comunicar per poder realitzar les proves d'auditoria. Totes les parts han de confiar que l'organització auditora o els auditors mai no faran un mal ús de la informació que obtinguin en una assignació d'auditoria.

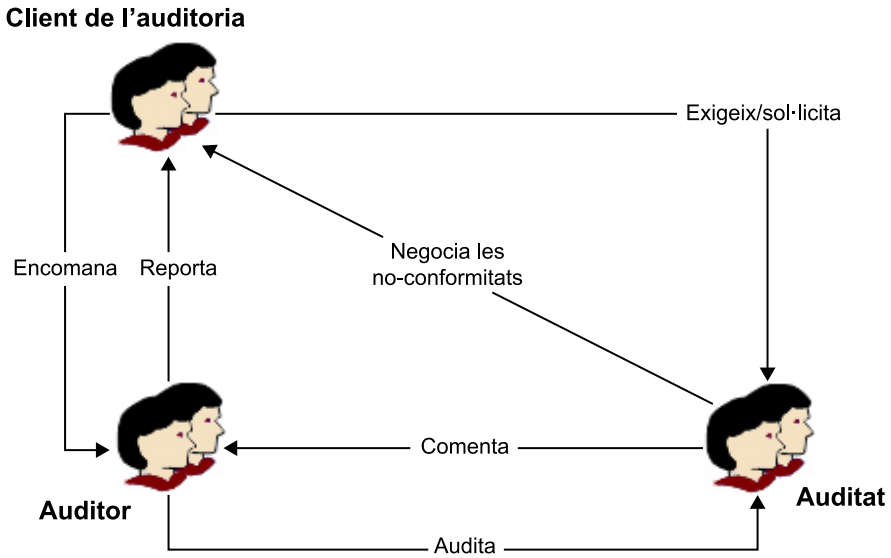
Si un auditor se cenyeix als principis descrits, el resultat del seu treball serà sòlid i podrà suportar la seva posada en dubte.

2. Components d'una auditoria

Hi ha diversos elements que defineixen una auditoria. De l'anàlisi d'aquests elements podrem anar aprofundint en els detalls generals i comuns a tot tipus d'auditoria.

2.1. Tipus genèrics d'auditories

En el procés d'auditoria apareixen tres actors principals que estan íntimament relacionats entre ells i que sempre apareixen en una auditoria:



Relacions entre els actors d'una auditoria

- L'auditor, o millor dit, l'equip auditor: és el grup de persones (o una de sola) que han estat designats per a executar l'auditoria en l'interès del client de l'auditoria.

- L'auditat: és l'organització (o podria també ser la persona, encara que això és menys comú que es doni) responsable del fet que s'audita.

- El client de l'auditoria: és la persona o l'organització interessada a conèixer la conclusió de l'auditoria.

De l'existència o no dels tres actors d'una auditoria, la relació que tinguin entre ells, l'organització a la qual pertanyi l'equip auditor, i la motivació que hi hagi en l'assignació, es deriven els tres tipus genèrics de tipus d'auditories, que són les següents:

- Auditories internes o de primera part.
- Auditories de segona part.

- Auditories de tercera part.

2.1.1. Auditories internes o de primera part

En aquest cas, les auditories són executades per un equip auditor que pot ser propi de l'organització responsable del fet auditat, o bé extern, però designat per l'organització auditada. En aquestes situacions, el destinatari final dels resultats del treball és la mateixa organització.

Aquest treball, en certes ocasions, és utilitzat per les organitzacions per a fer una autoavaluació prèvia a altres tipus d'auditoria. També pot tenir altres objectius més pràctics, com detectar punts de millora en el fet auditat. En tot cas, l'interessat en l'auditoria és directament el mateix auditat.

2.1.2. Auditories de segona part

De vegades, una segona organització pot tenir un interès legítim per a fer una auditoria a l'organització. En aquest cas, aquesta "segona part" és la que designa el personal que fa l'auditoria, i és aquesta la destinatària final dels resultats del treball d'auditoria.

Hi ha múltiples situacions reals que exigeixen aquest tipus d'auditoria. La més habitual que se sol donar és l'encarregada per una organització client sobre el seu proveïdor, per això a vegades també es denominen *auditories de proveïdors*. Cada vegada més, les organitzacions externalitzen parts de la seva activitat, però se solen reservar el dret de fer auditories per a determinar el grau de compliment dels acords de nivell de servei. Altres situacions en què també es poden donar auditories de segona part són aquelles en què una empresa està en situació d'absorbir-ne una altra. Aquí és habitual trobar-nos amb encàrrecs d'auditories de comptes o de valoració de la prenedora de control sobre l'absorbida. En cas de fusions, com que hi ha més equilibri de forces, és possible que cada part encarregui una auditoria de segona part d'algun tipus sobre l'altra empresa. No obstant això, sol ser econòmicament més eficient, i per tant més comú, que l'auditoria la faci una tercera part acordada per totes dues empreses, la qual cosa ens introdueix el tipus següent.

2.1.3. Auditories de tercera part

Les auditories de tercera part són les dutes a terme per organitzacions auditores externes i independents de la part auditada i de l'interessat en el resultat de l'auditoria. Dins d'aquest tipus d'auditories, hi trobaríem les auditories de certificació de conformitat amb els requisits d'una norma.

En aquestes auditories, les tres parts (auditat, auditor i client) són absolutament independents entre elles. De vegades, en el moment de fer l'auditoria, pot ser que ni tan sols estigui definit qui n'és el client. L'auditor pot fer l'auditoria a petició de l'auditat perquè aquest últim vol que una part indepen-

dent certifiqui/auditi algun aspecte, en previsió que en un futur hi pugui haver un client d'auditoria interessat en el resultat de l'auditoria. També es pot donar el cas que l'auditat encarregui l'auditoria senzillament perquè hi ha un requisit (legal, regulador del mercat o contractual) que es disposi d'una auditoria feta per una part independent. Aquest tipus d'auditories també tenen lloc en casos en què el client de l'auditoria és molt genèric, com ara l'Administració pública. En aquests casos, el mercat marca els objectius de l'auditoria mitjançant reglaments, normes, contractes, etc. Les auditories de certificació contra una norma entren dins d'aquest tipus d'auditories de terceres parts. Les auditories de certificació permeten a l'auditat acreditar el compliment dels requisits de la norma davant una comunitat àmplia i *a priori* indeterminada, però potencialment interessada, com podrien ser, per exemple, els seus clients. Per a oferir la màxima objectivitat, es recorre a una entitat externa als interessats (l'auditat i la comunitat). Per això, aquesta auditoria és classificada com de tercera part.

Finalment, convé destacar que les entitats que fan aquest tipus d'auditories han de tenir reconegut el seu prestigi davant la comunitat, perquè els resultats de l'auditoria siguin considerats vàlids. Això comporta l'existència, de vegades i per a determinats sectors, de requisits que regulen les activitats dels auditors. Aquest és el cas, per exemple, dels auditors de comptes, dels auditors de certificació contra normes, i cada vegada més també dels auditors de sistemes, encara que en aquest sector la regulació l'està duent a terme el mateix mercat.

Resum dels tres tipus bàsics d'auditoria

	Relació		
Tipus	**Auditor enfront d'auditat**	**Client de l'auditoria enfront d'auditat**	**Client de l'auditoria enfront d'auditor**
De primera part	Poden pertànyer a la mateixa organització, sempre que hi hagi prou independència. Tampoc no és estrany que siguin diferents si en l'organització client no hi ha prou coneixement tècnic o els recursos disponibles.	Pertanyen a la mateixa organització.	Poden pertànyer a la mateixa organització sempre que hi hagi prou independència. Tampoc no és estrany que siguin diferents si en l'organització client no hi ha prou coneixement tècnic o els recursos disponibles.
De segona part	Pertanyen clarament a dues organitzacions diferents.	Hi ha una relació entre ells, que fa que el client tingui un interès legítim a exigir a l'auditat la realització de l'auditoria.	Solen pertànyer a la mateixa organització, encara que tampoc no és estrany que siguin diferents si en l'organització client no hi ha prou coneixement tècnic o els recursos disponibles.
De tercera part	Pertanyen clarament a dues organitzacions diferents.	El client no existeix *a priori* o és, de manera genèrica, el mercat o una comunitat d'interessats molt àmplia. Els interessos del client són representats per l'auditor.	Són diferents. En aquests casos, l'auditor representa el client de l'auditoria.

Convé destacar que només en entorns molt específics i coneixedors de la terminologia s'acostuma a emprar la distinció que hi hem exposat. El més comú és que es faci esment al concepte d'*auditoria interna* enfront del d'*auditoria externa*. Amb aquesta separació, simplement se sol descriure el fet que l'auditor pertany o no a l'organització auditada. No obstant això, i com hem vist en la definició anterior d'auditories, aquesta visió és simplista i només recull els aspectes econòmics. L'aspecte més determinant no és si l'auditor és o no intern

a l'organització, sinó més aviat si l'organització és la principal "consumidora" del treball d'auditoria, o bé si, per contra, ho és una organització externa. És a dir, si és la mateixa organització la que ha definit l'objectiu de l'auditoria, o bé ha estat una organització externa la que ha decidit. Els aspectes econòmics són complexos i s'hi poden donar tot tipus de situacions. Aquesta distinció és la que s'hi hauria de reflectir, i no l'aspecte econòmic.

Plan, do, check/study, act

De fet, en els sistemes de gestió que implementen el cicle de *plan*, *do*, *check/study*, *act*, l'auditoria interna és un element més per a la millora contínua d'algun aspecte de l'organització: la qualitat, l'impacte mediambiental de l'organització o la seguretat de la informació. Quan es determina que, en aquests tipus de sistemes de gestió, és necessari implementar la funció d'auditoria interna, es demana exactament que sigui la mateixa organització la que defineixi els objectius de l'auditoria i també un pla d'auditoria. Des d'aquest punt de vista, és irrellevant si l'organització implementa la funció d'auditoria amb recursos propis o si bé els externalitza. Les raons per a triar una opció o una altra són purament econòmiques, i no pròpies de l'auditoria, excepte pel fet que l'auditoria resultant ha de ser conforme als principis d'auditoria.

2.2. L'objectiu i criteris de l'auditoria

A part d'aquesta classificació fonamental i absolutament genèrica de les auditories, si ens fixem en el fet auditat, tenim tants tipus d'auditories com temes auditables hi ha. En el nostre cas, són especialment rellevants les auditories informàtiques, que són aquelles en què el fet auditat són els sistemes d'informació i més especialment al llarg del curs, les que es refereixen a la seguretat de la informació tractada per aquests sistemes. Aquest concepte és l'objectiu d'auditoria.

L'objectiu d'auditoria es refereix a les metes específiques que ha de complir l'auditoria. Els objectius d'auditoria, els determina el client de l'auditoria, i sovint se centren a validar si s'implementen certs controls definits per unes polítiques, normes i/o procediments. Aquestes polítiques, normes i/o procediments constitueixen els criteris d'auditoria contra els quals s'avaluaran les proves.

Els objectius poden incloure aspectes com comprovar el nivell de compliment de certs requisits legals, reguladors o contractuals (aquestes auditories són les que preveu el marc legal espanyol de protecció de dades de caràcter personal). També poden incloure l'avaluació dels controls implantats en una organització per a garantir la seguretat (confidencialitat, integritat i disponibilitat) de la informació tractada pels sistemes d'informació o, més genèricament, pels processos de negoci de l'organització. Per tant, els objectius són variats i és necessari que el client de l'auditoria (auditories) els defineixi.

Així, doncs, els objectius de l'auditoria defineixen què és el que s'aconseguirà durant aquesta. Els objectius d'una auditoria poden incloure un o diversos dels aspectes següents:

- Determinar el grau de conformitat del sistema de gestió de l'auditat, o part d'aquest, amb els criteris d'auditoria.
- Avaluar la capacitat dels sistemes de gestió per a assegurar el compliment amb requisits legals o contractuals.
- Avaluar l'eficàcia del sistema de gestió per a aconseguir els objectius especificats.
- Identificar àrees potencials de millora del sistema de gestió.

Posteriorment, és tasca de l'auditor traduir aquests objectius d'auditoria a punts específics de control que s'hauran de verificar. A partir d'aquests punts de control, s'aniran desgranant les comprovacions i proves que es planificaran i s'executaran.

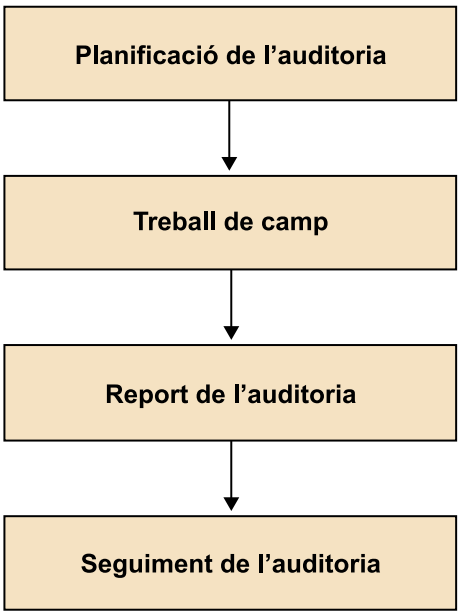
2.3. L'abast de l'auditoria

Les organitzacions auditades poden tenir múltiples processos associats, executats en una àrea geogràfica que pot ser molt àmplia, amb uns mitjans molt diversos i per personal també variat. Per tant, no solament s'haurà de definir l'objectiu de l'auditoria, sinó també quina part de l'organització comprèn, és a dir, quin en serà l'abast.

L'abast de l'auditoria descriu l'extensió i els límits de l'auditoria. Per exemple, les localitzacions físiques, les unitats organitzatives, les activitats o els processos que han de ser auditats en el període de temps cobert per l'auditoria. És a dir, tots els paràmetres que limiten físicament, temporalment i lògicament l'activitat de l'auditor dins de l'organització auditada.

3. Procés d'auditoria

Encara que cada projecte d'auditoria és específic en si mateix, fins i tot quan s'audita un mateix fet, però en diferents moments, podem afirmar que totes les assignacions d'auditoria es regeixen per un procés en quatre fases genèriques:



Fases generals d'una auditoria

- La fase de planificació hauria d'incloure totes les activitats necessàries per a dotar l'auditoria d'un marc de treball, els recursos necessaris i els objectius que s'han de complir. Per tant, ha d'incloure tasques com ara:
  - Designar l'equip auditor.
  - Definir l'abast, els objectius i els criteris generals de l'auditoria amb el client, tenint en compte les directrius estratègiques de l'organització en què s'enquadri la funció d'auditoria.
  - Recopilar el material necessari per al treball de camp i per a l'anàlisi posterior. Això pot implicar la preparació d'eines per a alguna tasca específica durant el treball de camp, o la identificació i l'estudi previ d'algun tipus de documentació.
  - Reunir-se amb l'auditat per a la reunió d'inici de l'auditoria.
  - Identificar els criteris d'auditoria, i elaborar un pla de l'auditoria que identifiqui el conjunt de proves que s'han de fer, de manera que els criteris estiguin alineats amb els objectius i l'abast de l'auditoria. Aquests

criteris seran la referència contra la qual l'auditor comparará els fets que constati durant el treball de camp.

- El treball de camp constitueix l'activitat principal d'una auditoria. Aquest treball consistirà en l'execució del pla d'auditoria fent les diverses proves d'auditoria que buscaran comprovar la manera en què se'n compleixen els criteris.

- Tot treball de camp ha de culminar en la transferència a l'auditat inicialment, i al client de l'auditoria finalment, dels resultats obtinguts. S'hauran d'analitzar les proves fetes i determinar si els resultats es poden catalogar com a proves d'auditoria, és a dir, si són rellevants per a determinar conclusions alineades amb l'objectiu de l'auditoria. Aquests resultats són contrastats primerament amb l'auditat, perquè pugui donar la seva opinió i aquesta es reflecteixi en les conclusions. Aquestes conclusions s'exposaran normalment en un document final denominat *informe d'auditoria*.

- Les conclusions de l'auditoria haurien de portar l'auditat a actuar d'alguna manera per a corregir els defectes que es van evidenciar durant l'auditoria. És recomanable que l'organització auditora ofereixi una revisió dels punts auditats i, arribat el cas, suggereixi de manera general propostes de solució a l'auditat. No obstant això, haurà de vigilar que aquestes recomanacions no comprometin la seva independència amb vista a la futura relació amb l'auditat i altres organitzacions. Sempre hi ha d'haver una separació clara entre el treball d'auditoria i el de consultoria, especialment en determinats tipus d'auditoria que identificarem més endavant.

Finalment, si ens centrem en la fase principal del procés d'auditoria, la realització pràctica d'una auditoria, s'ha de tenir sempre en compte que les proves hauran de ser rellevants per a l'objectiu de l'auditoria. S'hauran de seleccionar de la manera més adequada per a proporcionar la informació necessària a l'hora d'emetre una conclusió. L'experiència tècnica permetrà a un auditor escollir i fer les proves més adequades, i facilitar així la interpretació de resultats i l'obtenció de proves. L'elecció de proves útils en aquest sentit és el que marcarà, en certa manera, la perícia d'un auditor i el distingirà d'un altre. Aquest és el punt diferenciador que permetrà a un auditor ser més eficient en termes de costos i resultats. No oblidem que la funció d'auditoria també ret comptes econòmics en l'organització en què s'enquadri.

3.1. Tipus de proves

L'auditor pot fer diferents tipus de proves basant-se en criteris tècnics respecte de la matèria que està auditant. No obstant això, des d'un punt de vista més teòric, és interessant destacar que a l'auditor se li planteja la possibilitat de dur a terme dos tipus de proves:

- Proves de compliment o de controls. Es tracta de procediments d'auditoria que es dissenyen amb la finalitat de comprovar l'efectivitat i el compliment de l'auditat amb la normativa que descriu el control sobre el procés que s'està auditant. És a dir, busquen obtenir proves que els controls interns estan funcionant.

- Proves substantives o de detalls. Tenen una finalitat més pràctica i solen ser necessàries quan no n'hi ha prou amb les proves de compliment. Aquestes proves busquen detectar de manera afirmativa febleses dels controls que estan materialitzades. És a dir, es busquen proves de com és fet el procés que es vol controlar, de la seva integritat i de la manera com els controls aconsegueixen realment els seus objectius. Amb aquest tipus de proves més concretes, s'obtenen no solament les proves del compliment dels controls, sinó també les proves de la seva eficàcia. Aquest tipus de proves són més costoses i difícils de realitzar, ja que poden implicar que l'auditor hagi de realitzar tasques que habitualment es duen a terme de manera automàtica i que tal vegada hagi de repetir verificacions o càlculs relatius a una mostra de dades o de registres per donar fe que els processos de control implantats coincideixen amb el que ell realitza fora del sistema de control.

És a dir, la prova de compliment busca comprovar si s'implementen els controls tal com es recull en la normativa de referència (pot ser interna a l'organització auditada, o bé externa, com una llei, un reglament, etc.). Si els resultats d'aquest tipus de proves són satisfactoris, pot caldre fer proves substantives, les quals són inherentment més costoses i complexes.

S'ha de tenir en compte, sobretot en les proves substantives, que pot ser poc pràctic o directament inabastable fer una comprovació exhaustiva o completa. En molts casos, s'imposa la necessitat de seleccionar només unes quantes comprovacions. Aquesta selecció és el que es denomina *mostreig*.

3.2. Mostreig

El mostreig s'usa quan les consideracions de temps i de cost impedeixen la verificació completa i total requerida per una prova substantiva. En algunes circumstàncies, en una prova de compliment també es pot imposar la necessitat de fer un mostreig. Aquest és necessari quan no es tenen prou recursos per a dur a terme les proves sobre tots els elements que s'haurien d'analitzar.

Quan ens referim a processos de mostreig, denominem *població* la totalitat dels elements que s'han d'examinar per a fer les proves. Qualsevol subconjunt d'aquesta població es denomina *mostra*. El mostreig és un procés estadístic conegut i usat per a inferir característiques d'una població d'acord amb l'observació d'un subconjunt representatiu i en el context de l'auditoria, seria igualment obtenir un subconjunt d'elements representatius que, en aplicar les

proves dissenyades per l'auditor, li permeti obtenir una conclusió amb un cert nivell de confiança en què els objectius de l'auditoria s'hagin aconseguit. Existeix, per tant, un risc inherent de l'auditoria pel fet de realitzar mostrejos.

El mostreig es pot afrontar de dues maneres:

- Mostreig estadístic. És l'enfocament més objectiu i més científic, i empra les tècniques de les matemàtiques estadístiques per a calcular la grandària de les mostres, seleccionar els objectes de la mostra, avaluar els resultats de la mostra, i decidir quantitativament (amb un percentatge d'error) el grau en què els resultats de la mostra representen la població total. Perquè un mostreig sigui estadístic, cadascun dels elements de la població ha de tenir la mateixa probabilitat de ser seleccionat per a formar part de la mostra. En els casos en què s'avaluïn aspectes quantificables, l'auditor haurà de dominar conceptes estadístics com ara:
  - Coeficient o nivell de confiança
  - Precisió
  - Taxa d'error esperat
  - Mitjana de la mostra
  - Desviació estàndard de la mostra
  - Taxa tolerable d'error
  - Desviació estàndard de la població

  Un paràmetre important a conèixer en el cas d'aplicar-se aquest tipus de mostreig és el *nivell de risc mostral* (o també es parla de *nivell de confiança acceptable*, que és 100 % menys el *nivell de risc mostral*) que l'auditor estarà disposat a acceptar. Aquest nivell de risc mostral és un percentatge que reflecteix el percentatge de mostres que no reflectirien els valors reals (per les raons que sigui) si s'examinés el 100 % de la població.
  A l'entorn de les auditories relacionades amb la informàtica, es donen amb relativa poca freqüència aquest tipus de mostrejos, a causa de les característiques de les proves que s'han de fer o de la dificultat extrema d'aplicar tècniques estadístiques.
- Mostreig no estadístic o també denominat *basat en un criteri*. En aquest cas, el mètode de mostreig, la grandària de la mostra i la selecció de la mostra queden a criteri de l'auditor, segons la seva experiència i el seu punt de vista subjectiu. Malgrat que és més subjectiu, és més pràctic.

En tot cas, el procés que ha de dur a terme l'auditor és:

- Determinar els objectius de la prova.
- Definir la població de la qual s'obtindrà la mostra.
- Determinar el mètode de mostreig.
- Calcular la grandària de la mostra.
- Seleccionar la mostra.
- Avaluar la mostra des de la perspectiva de l'auditoria.

Aquest procés pot comportar errors, ja que es traurà una conclusió d'acord amb una mostra. No obstant això, aquests errors són coneguts per l'auditor i, si la mostra s'ha fet estadísticament, poden ser fins i tot mesurats.

3.3. Proves d'auditoria

La prova és qualsevol informació usada per l'auditor per a determinar si algun aspecte del procés auditat compleix els criteris d'auditoria. Així mateix, la confrontació de les proves d'auditoria amb els criteris permet a l'auditor concloure si s'ha fet una constatació d'auditoria. Finalment, davant la totalitat de les constatacions fetes, l'auditor pot emetre un judici i donar una conclusió que doni resposta a l'objectiu d'auditoria.

Per tant, la importància de les proves és clara. Tot el procés d'auditoria es redueix a la realització de proves per a la recollida de proves.

Les proves seran quantitatives o qualitatives, i poden ser de molts tipus. Tot això dependrà, principalment, de la naturalesa del tema auditat, però les proves poden ser:

- Observacions de l'auditor realitzades durant una visita i es poden materialitzar mitjançant suport fotogràfic.

- Informació recollida en entrevistes i plasmada en actes d'entrevistes.

- Documentació (contractes, registres, formularis, etc.) que l'auditat facilita a l'auditor (perquè va ser identificada amb antelació a la realització de les visites o entrevistes, o bé perquè hagi estat identificada durant aquestes i es facilita amb posterioritat).

- Resultats de proves d'auditoria que poden tenir al seu torn formes molt variades, encara que cada vegada més tindran un suport informatitzat (arxius informàtics, resultats de l'execució d'algun programa informàtic que ajudi a l'auditoria).

Com hem vist, la prova és la pedra angular del treball de l'auditor i, per tant, ha de complir certes característiques:

- **Confiabilitat**. La confiança en la informació facilitada per una prova dependrà de la manera com s'obtingui. Per tant, perquè la confiabilitat en la prova sigui com més elevada millor, s'haurà d'avaluar:
  - La independència de la font que proporciona la prova. Es pot tractar d'una persona o bé d'un sistema d'informació. En tots dos casos, és lícit avaluar la independència de la persona segons les seves relacions amb l'auditat o, si és intern, amb l'àrea auditada. Quant a un siste-

ma d'informació, l'auditor haurà d'avaluar la possibilitat que hagi estat adulterat.

– L'objectivitat de la prova. Com menys interpretació requereixi una prova, més gran serà la seva confiabilitat.

– Temps de disponibilitat de la prova. L'auditor s'haurà d'assegurar que la prova estigui disponible per a futures comprovacions i, en cas que es pugui destruir, haurà de fer les còpies de manera confiable.

- **Rellevància**. L'auditor es trobarà davant diverses proves, però no totes seran igual de rellevants per a cobrir els objectius de l'auditoria. L'auditor únicament hauria de tenir en compte les que siguin rellevants, i descartar o no considerar de la mateixa manera les que siguin rellevants de manera tangencial.

- **Suficiència**. En certes proves que es basen en la quantitat (per exemple, nombre de registres no vàlids en una base de dades després d'haver fet una determinada prova), serà necessari disposar-ne d'una quantitat suficient per a poder determinar que s'ha fet una constatació. A més de disposar d'una quantitat suficient, la prova haurà d'estar basada en fets objectius i haurà de permetre a un observador correctament informat arribar a la mateixa conclusió que l'auditor. Només en aquest cas la prova es podrà considerar suficient. Com es veu, la suficiència no està exclusivament relacionada amb la quantitat, encara que pot ser necessari que la quantitat estigui present per a obtenir la suficiència.

- **Competència**. A més de suficiència, tota prova ha de tenir també la característica de competència. S'entén per *competència* la característica de qualitat de la prova, és a dir, la seva capacitat per a permetre a l'auditor determinar si ha fet o no una constatació d'auditoria. De vegades, es decideix que una prova és competent quan és vàlida, rellevant i confiable.

3.4. Constatació d'auditoria

Les proves que compleixin les característiques de suficiència i competència es confrontaran contra els criteris d'auditoria per a determinar si s'ha fet una constatació o no i de quin tipus. És important destacar que en aquest procés de confrontar evidències amb criteris.

Les constatacions, per tant, són el resultat de classificar les proves de la manera següent:

- No-conformitats (hi pot haver algun tipus de nivell de gradació, per exemple, en les auditories de certificació que es tractaran més endavant en el curs, es divideixen entre greus i menors) quan la troballa evidencia que en

el procés auditat no es compleix algun dels criteris de control de l'auditoria, sia perquè no hi ha control, no s'ha implementat conformement al criteri d'auditoria o no és eficaç.

- Observacions. Quan l'auditor té punts d'interès que vol presentar, però no prou evidència per emetre una no conformitat, pot presentar observacions.
- Possibilitats de millora. Pot ser que el control sobre el procés sigui eficaç, però no tan eficient com ho podria ser. En aquest cas, l'auditor podria facilitar alguna observació per millorar-lo, sempre parant molta atenció, sobretot en auditories de terceres parts o quan aquestes observacions no siguin una consulta o assessoria encoberta, la qual cosa afectaria la seva posterior independència.
- Conformitats. Confirmen que el criteri d'auditoria es compleix. En la pràctica no es presenten de manera detallada, sinó com a simples punts forts del sistema de control del procés auditat.

3.5. Risc d'auditoria

La tasca de determinar quan una o diverses proves confirmen una constatació (que portarà a unes conclusions d'auditoria) comporta un risc inherent d'error. És el risc que l'auditor conclogui de manera errònia, en qualsevol dels sentits, tant positiu que el criteri es respecta, com tot el contrari. L'auditor ha de conèixer aquest risc, denominat *risc d'auditoria*.

Hi intervenen molts factors que incideixen en aquest risc d'auditoria:

- **El mostreig**. Es tracta d'una activitat que es farà pràcticament en totes les assignacions d'auditoria a les quals s'enfronti un auditor en la seva carrera professional. El mostreig es pot deure a una planificació molt ajustada, a una falta de recursos o senzillament al fet d'enfrontar-se a un nombre total i potencial de proves a fer totalment desorbitat.

- **Avaluació errònia de la prova o les proves**. Ja sigui per falta d'experiència o perquè la prova no va resultar confiable, hi ha la possibilitat que l'auditor interpreti incorrectament la prova.

- **Falta de prou proves**.

En tots els casos, l'auditor haurà de ser conscient dels riscos i reconèixer que hi ha un risc d'error en emetre el seu judici d'auditoria. Però, de totes maneres, el fet de fer l'auditoria ajustant-se a plans de treball, seguint metodologies reconegudes i respectant els codis ètics de la professió, dóna garanties a l'auditor a l'hora de valorar les constatacions i emetre les conclusions. I a més, l'auditor ha de reconèixer aquesta possibilitat, especialment quan s'hagi realitzat un mostreig molt agressiu, i deixar-la reflectida en el seu informe final d'auditoria.

4. Programa d'auditoria

Fins ara hem estat parlant d'auditoria com una activitat aïllada que es fa una única vegada, o potser més vegades, però sense que hi hagi un objectiu estratègic per a l'activitat general d'auditoria ni unes relacions entre diverses auditories.

Sovint les organitzacions només es plantegen aquesta activitat d'auditoria en moments puntuals, sobretot quan es tracta d'auditories de segones o terceres parts. En aquestes situacions, el client encarrega l'auditoria en un moment donat i, una vegada executada, adopta les accions que tingui previstes i la relació amb l'auditor finalitza aquí o com a màxim hi ha una fase final de seguiment en la qual els auditors verifiquen si les no conformitats s'han resolt o no.

No obstant això, una organització obté les fortaleses i els beneficis més grans de la tasca d'auditoria quan aquestes se succeeixen en el temps de manera planificada, organitzades conformement a una estratègia general, i si té prou recursos amb un equip auditor propi (complet o externalitzat parcialment o total, però coordinat per algú intern). En aquestes situacions es diu que l'organització implanta la "funció d'auditoria" i que aquesta organitza la seva activitat conformement al que es denomina un programa d'auditoria. Els beneficis que es poden obtenir d'implantar un programa d'auditoria poden ser els següents (més endavant es detallen en un apartat específic):

- Els equips d'auditoria poden planificar millor l'esforç i l'assignació de recursos.

- Es facilita la consistència de les actuacions dels equips auditors, es refinen les seves tècniques i es millora així la seva capacitació. D'aquesta manera, s'augmenta la qualitat del treball, disminueixen els errors i s'optimitza el temps dedicat a la realització de proves.

- Es maximitzen els recursos i s'obtenen millors resultats.

- S'aconsegueix un seguiment correcte del nivell de millora contínua dels processos auditats.

Aquests programes solen sorgir en organitzacions en què els sistemes de gestió estan àmpliament implantats i entesos. Per tant, és molt habitual trobar-nos amb programes d'auditories tant de primera com de terceres parts en el context de sistemes de gestió de la qualitat, mediambiental, o també de seguretat de

la informació, encara que també podrien donar-se per realitzar auditories de segona part o de proveïdors si l'organització, de manera recurrent, avalua els seus proveïdors.

Existeix una relació entre els programes d'auditoria i els sistemes de gestió.

Els sistemes de gestió estan basats en la implantació d'un procés continu de millora, que sol ser conegut com a *cicle PDCA* (o *cicle de Deming* o *Shewhart*). El cicle PDCA està format per quatre processos que es van repetint de manera iterativa per al control d'un sistema: planificar, implementar (per a dur a terme el que s'ha planificat), comprovar (per a analitzar el funcionament del que s'ha implantat) i actuar (d'acord amb la revisió feta).

En aquest cicle, calen auditories de primera part en la fase de comprovació. D'altra banda, com que aquest cicle PDCA s'ha de fer contínuament per a garantir el control correcte del procés en qüestió, la realització d'auditories també és contínua. Aquestes auditories no es fan de manera independent les unes de les altres, sinó que més aviat són organitzades pels responsables de gestionar la funció d'auditoria en l'organització. És en aquest context en què es creen programes d'auditoria, que són el marc mitjançant el qual es gestiona la funció d'auditoria, d'una manera similar a qualsevol altre sistema de gestió, però amb un objectiu més concret. Encara que més endavant s'ampliarà en l'apartat d'implementació, de manera general aquest programa inclou:

- Els objectius generals del programa i de les principals accions d'auditoria, és a dir, què es pretén aconseguir amb el programa d'auditoria.

- La planificació de les auditories durant un període de temps. Malgrat que en conjunt tot té un objectiu general, la labor d'auditoria pot separar-se temporalment i cada auditoria planificada tindrà un objectiu específic o més.

- Els procediments per a dur a terme tots els aspectes del programa.

- Els criteris d'auditoria.

- Els mètodes i les tècniques d'auditoria.

- La gestió dels equips d'auditors (selecció i capacitació).

- La gestió dels aspectes logístics i pressupostaris.

En aquest punt és important no confondre el concepte de programa d'auditoria que aquí es descriu, alineat amb la concepció que se n'aplica en les entitats de certificació reflectida en la norma ISO/IEC 19011, amb el que s'entén per programa d'auditoria en altres ambients com ara l'ISACA. En aquest entorn, els programes d'auditoria són procediments més detallats per a

l'auditoria d'aspectes concrets de control d'algun tipus de procés. Mitjançant una consulta al website d'ISACA, en l'apartat d'"Audit/Assurance Programs" el lector podrà comprovar aquesta diferència de concepte.

4.1. Beneficis d'implementar un programa d'auditoria

Dins d'aquest context, els responsables d'auditoria tenen la possibilitat d'obtenir certs beneficis de desenvolupar aquest programa:

- Els programes d'auditoria poden assistir els gestors de la funció d'auditoria en la planificació de l'esforç i l'assignació de recursos. Per exemple, la gerència disposarà d'informació prèvia per a poder estimar l'esforç requerit per a dur a terme una auditoria basant-se en la quantitat de temps esmerçat en auditories anteriors. D'aquesta manera, l'organització podrà proveir partides pressupostàries realistes.

- Es promou la consistència en la manera d'actuar dels auditors i permet anar refinant les tècniques i anar millorant la capacitació del personal auditor, la qual cosa redunda en una millor qualitat del treball (menys errors d'auditoria, possibilitat de comparar resultats de diferents auditories en el temps). Durant la planificació i la preparació per a una auditoria, els materials (guies, llistes de comprovació, eines, equips específics, etc.) usats durant assignacions anteriors es poden emprar generalment com a base per als passos que es faran durant l'actual. Això no s'aplica, òbviament, en els casos en què s'auditi un procés que mai abans no s'ha revisat, o en els casos en què el procés ha canviat perceptiblement. En aquests casos, els materials s'han de crear des de zero.

- Es maximitzen els recursos d'auditoria i es permet obtenir millors resultats. Distribuint en el temps diferents auditories, es poden planificar millor els recursos. Per exemple, si parteix de les proves de determinades auditories del programa que es realitza comptant amb experts interns, el programa d'auditoria ajudarà a planificar-ne la disponibilitat, si és que aquests no desenvolupen permanentment la seva tasca professional en la funció d'auditoria.

Més enllà dels beneficis comentats, una organització que necessiti fer auditories contínues per a verificar els controls aplicats a un procés hauria d'implementar i gestionar un programa d'auditoria efectiu. El propòsit d'un programa és planejar el tipus i nombre d'auditories, i identificar i subministrar els recursos necessaris per a fer-les. El programa d'auditoria pot incloure auditories amb una gran varietat d'objectius, es pot establir més d'un programa d'auditoria, i el nombre d'auditories que contingui el programa dependrà molt de la grandària, naturalesa i complexitat de l'organització que s'ha d'auditar.

Programes d'auditoria per a mitjanes empreses

Per exemple, una organització d'una grandària mitjana (per sobre de les cent persones) que tingui implantat un sistema per a la gestió de la seguretat de la informació es podria plantejar els programes d'auditoria següents, per a revisar de manera contínua els principals punts del seu sistema:

- Verificació anual de la conformitat del sistema amb la Norma ISO27001:2005.
- Auditories trimestrals del funcionament dels controls de seguretat lògica.
- Auditoria anual de l'estat dels controls de seguretat física.
- Revisió anual del pla de continuïtat i de les seves proves.
- Auditoria biennal de protecció de dades de caràcter personal (a Espanya).

4.2. Establiment d'un programa d'auditoria

La forma d'implementar i gestionar un programa d'auditoria que hem repassat no difereix de la implantació de qualsevol altre sistema de gestió que pretengui controlar una activitat, en aquest cas l'activitat de la funció d'auditoria. El sistema ha de posar en valor tant les fases que es planifiquen i les que s'executen, com les posteriors fases de revisió de l'execució i extracció de conclusions. Implantar un programa d'auditoria no és més que aplicar un cicle de gestió PDCA (Deming) a la funció d'auditoria d'una organització, la qual cosa ens permet veure el procés de gestió del programa d'auditoria com un cicle que es reflecteix en el diagrama següent, inspirat en la descripció donada en la norma ISO/IEC 19011:2011.

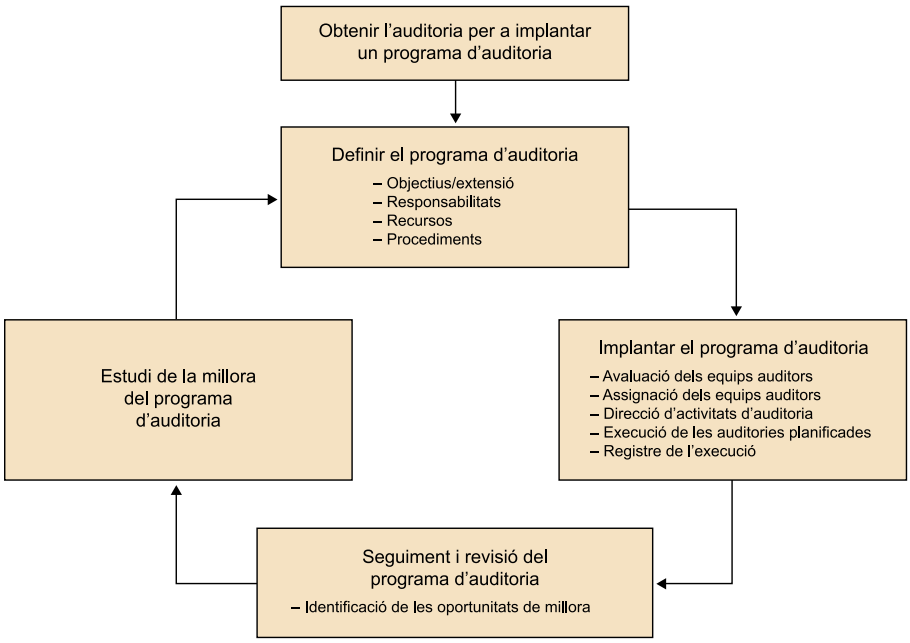


Diagrama general de la gestió d'un programa d'auditoria

Com es pot veure, la gestió d'un programa d'auditoria és un procés que va més enllà de simplement planificar les auditories que es faran al llarg d'una finestra de temps determinada. Es tracta, més aviat, d'un sistema de gestió que pretén controlar de manera contínua el procés d'auditoria. Per tant, seria lògic que s'integrés amb els processos que pretén verificar i que segueixen la mateixa filosofia de gestió, com ara la gestió de la qualitat, la gestió mediambiental, la gestió dels sistemes d'informació, o de la seguretat de la informació. Integrar l'auditoria amb els diferents sistemes de gestió d'una organització ajuda a in-

crementar-ne l'eficàcia i l'eficiència, ja que gran part del coneixement necessari (tot el relatiu a les generalitats de l'auditoria i de la gestió del programa) és comú i controlat per uns mateixos responsables. Això comporta la necessitat que aquests sistemes de gestió implementin una nova funció organitzativa: la d'auditoria (també se sol denominar *control intern*). Aquesta funció tindrà com a objectiu fer tots els processos que permetin comprovar que s'estan aplicant els controls interns sobre la resta dels processos de l'organització.

En cas que es decideixi crear una funció d'auditoria perquè gestioni un programa d'auditoria, la direcció de l'organització hauria d'oficialitzar aquesta funció i dotar-la d'autoritat per a dirigir el programa d'auditoria, i implementar un sistema que executi les fases descrites en el diagrama.

Els responsables del programa d'auditoria hauran de planificar i dirigir el procés d'auditoria contínua en l'organització. Per tant, hauran de fer el següent:

1) Establir els objectius i l'extensió del programa d'auditoria. Aquests objectius es poden basar en el següent:

- Estratègia i prioritats de la direcció.
- Requisits del sistema de gestió (si els controls que s'han d'auditar estan certificats).
- Requisits reglamentaris o contractuals.
- Necessitat d'avaluació de proveïdors.
- Requisits dels clients.
- Necessitats de les parts interessades.
- Riscos potencials per a l'organització.

L'extensió o l'abast d'un programa d'auditoria pot variar, tal com hem dit, per diversos factors:

- L'abast, l'objectiu i la durada de cada auditoria.
- La freqüència de les auditories.
- La grandària, la naturalesa i la complexitat de l'organització auditada.
- El nombre, la importància, la complexitat, la similitud i la ubicació de les activitats que s'han d'auditar.
- Normes, requisits reglamentaris i contractuals, i altres criteris d'auditoria.
- Necessitat d'acreditació o certificació/registre.
- Els resultats de les auditories prèvies o la revisió del programa d'auditoria previ.
- Aspectes lingüístics, culturals i socials.
- Preocupacions de les parts interessades.
- Canvis significatius per a una organització o les seves operacions.

Tots aquests factors poden variar fins i tot durant el període de temps en què s'està executant un programa, per la qual cosa és necessari que el programa sigui gestionat de manera contínua. Més endavant, veurem alguns aspectes relacionats amb la gestió contínua del programa.

2) Establir les responsabilitats. Les persones a les quals s'assigni la responsabilitat de dirigir el programa d'auditoria hauran de definir, implementar, revisar i millorar el programa d'auditoria, i també n'hauran de fer el seguiment. A més, des del punt de vista del dia a dia, hauran d'identificar i subministrar els recursos per al programa d'auditoria.

Per això la responsabilitat de la gestió d'un programa d'auditoria s'hauria d'assignar a una o més persones amb les característiques següents:

- Coneixements generals dels principis de l'auditoria.
- Coneixement de la competència dels auditors disponibles en els conceptes generals d'auditoria i en l'aplicació de tècniques d'auditoria, i també en els aspectes tècnics que hagin d'auditar.
- Habilitats per a la gestió.
- Coneixements tècnics i del negoci pertinents per a les activitats que s'han d'auditar.

3) Estimar i planificar els recursos necessaris. A l'hora de determinar els recursos necessaris per a la implementació del programa, els responsables haurien de considerar aspectes com els següents:

- Els recursos financers necessaris per al desenvolupament, la implementació, la gestió i la millora de les activitats d'auditoria. Per a pressupostar correctament el programa, és necessari disposar de coneixements sobre gestió de recursos i tota la informació de programes passats que hi pugui haver.
- Les tècniques d'auditoria que s'hi hauran d'aplicar, ja que pot ser que els auditors no disposin de la capacitació necessària i/o de les eines o tècniques necessàries.
- Els processos per a aconseguir i mantenir la competència dels auditors, i millorar-ne la qualitat i el rendiment del treball.
- La disponibilitat dels auditors i experts tècnics que tinguin la competència apropiada per als objectius del programa d'auditoria particular.
- La durada prevista de les auditories.

- Els temps de desplaçament, l'allotjament i altres necessitats logístiques durant l'auditoria.

4) Assegurar la implementació del programa d'auditoria. La implementació del programa d'auditoria va més enllà de la simple execució de les auditories que s'han programat. Aquestes tasques impliquen gestionar i controlar la funció d'auditoria fent les tasques següents:

- Comunicar el programa d'auditoria a les parts pertinents. Es tracta d'una tasca necessària de comunicació i divulgació a la direcció dels objectius generals del programa i dels específics de cadascuna de les auditories.

- Preparar material per facilitar la realització de les auditories (procediments, llistes de comprovacions, plantilles d'informes, procediments d'avaluació de la qualitat de la labor d'auditoria, plans de desenvolupament dels auditors, etc.).

- Coordinar i programar les auditories i altres activitats del programa d'auditoria. És a dir, controlar el procés d'execució de les diferents parts del programa:
  - Planificació i assignació dels recursos als diferents equips auditors.
  - Control d'execució d'acord amb els objectius del programa.
  - Avaluació de les auditories. Aquest aspecte seria com l'"auditoria" de l'execució de l'auditoria.
  - Revisió dels informes d'auditoria i comunicació als clients i a les parts interessades.
  - Assegurar que es fan les accions complementàries de l'auditoria, en cas que hi siguin aplicables (per exemple, revisions o noves auditories després de períodes de correcció de no-conformitats).

- Establir i mantenir un procés per a l'avaluació inicial i progressiva dels auditors. Aquest procés avaluarà les seves necessitats de formació i desenvolupament professional, de manera que siguin competents en la matèria i la seva capacitació es vagi adequant a les circumstàncies evolutives dels mercats.

Durant l'execució d'un programa d'auditoria, en una organització, hi ha la possibilitat que dues o més organitzacions auditores puguin cooperar en la realització d'una auditoria conjunta. En aquest cas, s'hauria de parar esment especial a la divisió de responsabilitats, el subministrament de recursos addi-

cionals, la competència addicional necessària en l'equip d'auditoria i els procediments apropiats. S'hauria d'arribar a un acord sobre aquests procediments i altres aspectes d'ordre pràctic abans de començar l'auditoria.

5) Fer seguiment, revisar i millorar el programa d'auditoria. El programa d'auditoria necessita un manteniment continu per a adequar-lo a canvis en l'organització, les tecnologies o, simplement, a les conclusions que es treguin respecte a com s'està duent a terme. Per tant, és recomanable que, a intervals apropiats, es faci una revisió del programa per a avaluar si els seus objectius s'han complert, i per a identificar oportunitats de millora.

Exemples de seguiment

Aquest seguiment es pot fer, per exemple, mesurant i revisant:

- La capacitació dels equips auditors per a implementar el pla d'auditoria. Per a això, s'haurà de tenir un control sobre la manera com han dut a terme les seves activitats, la seva formació actual i els canvis en l'entorn que no quedin coberts per les capacitats actuals dels auditors.
- La conformitat de l'execució de les auditories amb les previsions dels programes i cronogrames previstos per a cada auditoria.
- La satisfacció dels clients de l'auditoria, dels auditats i dels auditors.

Aquests indicadors han de servir per a identificar els punts de millora del programa d'auditoria i per a dissenyar les accions correctores que permetin alinear millor el programa d'auditoria amb les necessitats del client.

5. Estandardització de la tasca d'auditoria

Ja hem vist que una de les principals característiques del procés d'auditoria ha de ser l'objectivitat i la sistematització del procés. Això permet que les conclusions de l'auditoria siguin independents de la subjectivitat de l'auditor. Aquestes dues característiques fan que sigui possible plantejar-se descriure la tasca d'auditoria des d'un punt de vista teòric o independent de l'àmbit concret auditat. Per tant, és possible donar certs paràmetres, aspectes i elements que són comuns a qualsevol àmbit auditat, o almenys que ho són dins d'un cert àmbit molt general.

Aquesta possibilitat d'uniformitzar les característiques del procés d'auditoria es troba reflectida en el fet que existeixen estàndards l'objectiu dels quals és donar les guies de com s'ha de fer la tasca d'auditoria per a preservar les característiques d'objectivitat i sistematització del procés.

La realitat és que el conjunt d'estàndards és molt ampli. La tasca d'auditoria en un sector ha comportat gairebé sempre la publicació d'estàndards d'auditoria aplicables almenys en el seu sector, i de vegades extensibles a uns altres. Aquests estàndards són publicats per entitats amb més o menys prestigi en el seu sector i amb capacitat per a imposar els seus estàndards.

Podem destacar alguns dels organismes que més activitat normativa han fet en el tema de l'auditoria.

5.1. AICPA (American Institute of Certified Public Accountants)

L'AICPA és l'associació nord-americana dels auditors públics de comptes, encara que no tots els seus membres són auditors públics de comptes.

Encara que l'àmbit de l'auditoria de comptes no és el que ens ocupa, val la pena destacar l'activitat de l'AICPA, tant per la llarga història de tasca d'estandardització que ha fet com pel fet de ser la iniciadora, en part, de l'auditoria de sistemes d'informació.

La funció fonamental de l'AICPA és promoure la professió de l'auditoria de comptes. Per a aconseguir això, té una varietat de funcions, entre les quals ens interessa la d'elaboració d'estàndards professionals per a l'auditoria de l'estat de comptes i altres tipus d'auditories financeres o relacionades. Hi ha un gran nombre d'aquests estàndards. Es poden obtenir a la biblioteca electrònica de la Universitat de Mississipi, buscant pel títol "AICPA Professional Standards: U. S. Auditing Standards–AICPA" i, individualment, buscant per "Statement

on Auditing Standard". Entre els estàndards que podem trobar aquí, és interessant destacar els següents perquè tenen relació amb l'auditoria de sistemes d'informació:

- SAS55 (esmenat per SAS78) "Consideration of Internal Control in a Financial Statement Audit". Aquest estàndard requereix a l'auditor obtenir un coneixement i comprensió dels mecanismes de control intern d'una entitat que li permeti, primer, planificar una auditoria i, segon, identificar els controls més rellevants i avaluar-los posteriorment. En aquest context, s'ha de tenir en compte que la normativa financera exigeix que es facin certes provisions per a preveure riscos operacionals, entre els quals s'inclouen els riscos que introdueix el tractament de dades financeres mitjançant sistemes d'informació. Per tant, l'avaluació dels controls interns, per a garantir la correcció dels comptes i la inexistència d'errors o fraus, ha d'incloure per força l'auditoria dels sistemes d'informació.

- SAS70 (esmenat per SAS78) "Reports on the Processing of Transactions by Service Organizations" o també conegut com a "Service Organizations". S'entén com a *service organizations* organitzacions que presten un servei a l'auditat rellevant per al seu sistema de control intern. És a dir, es tracta d'organitzacions que ofereixen serveis (molt habitualment, els sistemes d'informació) externalitzats per altres organitzacions, els quals són rellevants per a l'exactitud dels comptes. Per tant, el SAS70 és aplicable en escenaris com ara: proveïdors de comunicacions, proveïdors d'aplicacions amb un servei totalment externalitzat (es coneix com a *mode ASP –application service provider–* o també com a *SaaS –software as a service–*), serveis de seguretat gestionada (tant lògica com física), etc.
  El SAS70 defineix els estàndards que ha de seguir un auditor per a la comprovació dels controls interns en una organització que presta serveis externalitzats per unes altres. Així mateix, defineix la forma que ha de complir l'informe d'auditoria que es generi perquè pugui ser utilitzat en una altra auditoria en l'organització que ha externalitzat el servei.
  La rellevància d'aquest estàndard prové de la necessitat de complir el SAS55 (i SAS78), que obliga que cada auditoria en una organització inclogui també una auditoria en les organitzacions on s'ha externalitzat un servei. El compliment d'aquest estàndard implicaria innombrables auditories en les organitzacions proveïdores de serveis. Per evitar això i reduir els costos de les auditories, el SAS70 dóna les directrius sobre la realització i el report de les auditories en organitzacions de serveis, perquè els seus resultats puguin ser comunicats i utilitzats per les organitzacions que externalitzen el servei.

- SAS94 "The effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit". Aquest estàndard obliga l'auditor a posar especial atenció en el paper que exerceixen els sistemes d'informació en el procés de control de l'estat financer d'una entitat.

Com es pot observar, el grau de detall que ofereixen els estàndards de l'AICPA és molt elevat. Arriba fins i tot a punts tan concrets com indicar quin tipus de contingut hi ha d'estar inclòs i en quins apartats específics d'un tipus d'informe particular (per exemple, un de SAS70).

A causa de la seva exhaustivitat i complexitat, aquests estàndards només han estat aplicats als Estats Units. Més concretament, s'han aplicat en l'àmbit d'auditories financeres i de compliment amb normativa legal també del sector, com per exemple la Sarbanes-Oxley Act. El seu ús no s'ha estès a Espanya.

5.2. ISO (International Organization for Standarization) i les entitats de certificació

Com ja hem comprovat en l'apartat anterior, hi ha organitzacions que tenen un gran control sobre el treball que es fa d'acord amb els seus estàndards. En l'altre extrem, hi ha organitzacions que donen guies, bones pràctiques i estàndards rellevants per al procés d'auditoria, però amb un afany de ser més universals. Entre aquestes, es troba l'ISO (Internacional Organization for Standarization), que ha desenvolupat sobre aquest tema certes normes que són del nostre interès.

Dins de l'àmbit de la certificació de sistemes de gestió de qualitat (ISO 9001) i mediambiental (ISO 14001), ISO ha fet un esforç extra per a sistematitzar-ne l'auditoria. Per això, s'ha definit un estàndard que dóna les directrius per a l'auditoria dels sistemes de gestió de la qualitat i ambiental, la Norma ISO 19011. Encara que aquesta norma s'ha desenvolupat inicialment per a l'auditoria d'aquests tipus de sistemes de gestió, les seves directrius es poden ampliar a les auditories d'altres tipus de sistemes de gestió i altres àmbits.

D'una banda, l'estàndard és fàcilment aplicable per a l'auditoria de qualsevol tipus de sistema de gestió basat en el cicle PDCA en els termes que ISO ha definit. En particular, l'estàndard és fàcilment aplicable als sistemes de gestió de la seguretat de la informació sense grans modificacions. A més, els termes que ISO ha definit es repeteixen en les normes ISO 9001, ISO 14001, ISO 27001, i futures relacionades amb la continuïtat de negoci ISO 25999, gestió de serveis TI, i família ISO 20000. Aquesta és la raó per la qual l'ISO 19011 està sent emprada per a l'elaboració de l'estàndard ISO/IEC 27007 (*Information Technology - Security Techniques - Guidelines for Information Security Management Systems Auditing*), el qual encara (en data del 2009) es troba en fase d'esborrany. Aquest estàndard s'engloba en la família de normes dedicades a la seguretat de la informació, i tindrà com a objecte definir i donar guies per a l'auditoria dels sistemes de gestió de la seguretat de la informació.

D'altra banda, si s'observa la Norma ISO 19011 des del punt de vista d'un auditor amb experiència, s'hi detecten elements generals i comuns a altres estàndards i codis professionals, la qual cosa ens confirma la seva capacitat de servir com a guia per a assumptes com l'auditoria de sistemes d'informació.

Respecte a l'auditoria de sistemes d'informació i de sistemes de gestió de la seguretat de la informació, convé destacar que tant la Norma ISO 19011 com la Norma més específica ISO/IEC 27007, són completament aplicables a qualsevol dels tipus d'auditoria descrits inicialment. És a dir, són aplicables a auditories de primera, segona i tercera parts. No obstant això, s'ha de destacar que les auditories de tercera part tenen un tractament especial per part d'ISO. Quan es parla d'auditories de tercera part d'un sistema de gestió, s'entén que els criteris d'auditoria són els que estan reflectits en algun tipus de norma o legislació. Pel que fa als sistemes de gestió que estan normalitzats per l'ISO, en cadascuna de les famílies de normes (ISO 9000, 14000 o 27000) hi ha una norma específica per a definir els requisits d'un sistema de gestió (les ISO 9001, ISO 14001 i ISO/IEC 27001). Les auditories que busquen comprovar el sistema de gestió implantat en una organització, per a controlar una activitat determinada, són denominades *auditories de certificació*, i les duen a terme organitzacions que estan fortament regulades: les entitats de certificació.

Aquestes entitats de certificació han de demostrar la seva vertadera independència perquè els dictàmens que facin (auditories de certificació) siguin presos en consideració pel mercat. És a dir, han de demostrar la seva independència perquè els resultats de les seves auditories siguin reconeguts per una organització diferent de l'auditat i l'auditor. Per tant, aquestes entitats hauran de gestionar els seus propis processos d'auditoria d'acord amb, no ja unes directrius o guies (que és el que són les normes ISO 19011 i ISO/IEC 27007), sinó amb una norma o un conjunt de requisits definits per un cos normatiu superior. Aquest cos normatiu superior pot ser, per exemple ISO, internacional, o també d'àmbit nacional, com AENOR a Espanya. Es parla, llavors, que l'entitat de certificació ha d'estar acreditada per una altra entitat, que es denomina *entitat d'acreditació*, per a fer auditories de certificació contra una norma.

Aquesta relació entitat de certificació / entitat d'acreditació cobreix una necessitat òbvia, que és: qui audita l'auditor? Com acabem de dir, aquest problema només està correctament resolt per uns quants tipus d'auditories, com les auditories de comptes o auditories de certificació. Aquestes auditories de certificació les duen a terme entitats de certificació que no són més que empreses (poques són organismes públics, encara que també ho podrien ser) que han passat un procés d'auditoria per una entitat d'acreditació. L'entitat d'acreditació certifica que l'empresa fa les assignacions d'auditoria d'acord amb certs estàndards, com la Norma ISO 17021, que especifica els requisits (en l'àmbit de les normes de la família ISO 27001, el complementaria la Norma ISO/IEC 27006). Aquest

procés es denomina *d'acreditació*, perquè acredita l'entitat de certificació a fer un cert treball i que les seves conclusions d'auditoria siguin reconegudes dins de l'àmbit de reconeixement que tingui l'entitat d'acreditació.

És interessant constatar que la Norma ISO 17021 és més estricta que la ISO 19011, i dóna els requisits perquè tant l'auditat com els potencials interessats en els resultats de l'auditoria puguin confiar en l'entitat de certificació. Aquesta confiança es garanteix mitjançant l'assegurament dels principis següents:

- Imparcialitat.
- Competència a l'hora de fer les auditories.
- Responsabilitat.
- Publicitat.
- Confidencialitat.
- Capacitat per a resoldre els conflictes amb els auditats.

Publicitat

En el sentit de fer pública la informació que es pugui revelar als interessats, com per exemple l'estatus d'un certificat emès per aquesta.

Els requisits que imposa són variats i amplis, com ara:

Aspectes organitzatius

Es refereix a estructures i dotació quant a recursos humans.

- Legals.
- Organitzatius.
- Gestió de la documentació (formats, registres, etc.) i informació (tipus d'informació que ha de ser revelada i tipus que ha de ser confidencial) relacionada amb l'auditoria de certificació.
- Manera com s'ha de fer l'auditoria de certificació i el programa d'auditoria que s'hi ha d'implantar.

Gràcies a aquests punts, el treball de l'entitat de certificació pot gaudir d'un reconeixement dins d'un àmbit que dependrà, en certa mesura, de l'entitat d'acreditació. Habitualment, les entitats d'acreditació són entitats públiques, per la qual cosa aquest reconeixement sol tenir sempre un caràcter nacional, dins d'un estat.

Atès que aquestes entitats d'acreditació tenen un àmbit d'actuació geogràfic, habitualment un estat, l'àmbit de reconeixement dels certificats emesos per entitats de certificació que s'hagin acreditat tindria un reconeixement limitat geogràficament a aquest àmbit. No obstant això, les organitzacions poden voler que els certificats tinguin un reconeixement internacional. Per a resoldre aquesta problemàtica, les diferents entitats d'acreditació s'agrupen i realitzen acords de reconeixement mutu dels esquemes d'acreditació. D'aquesta mane-

ra, s'amplia geogràficament l'àmbit de reconeixement d'una determinada certificació. Les organitzacions que desitgin cerfificar-se han de tenir en compte aquest punt a l'hora d'escollir l'entitat de certificació que hagi de realitzar l'auditoria de certificació, ja que, per necessitats de negoci, potser hi ha problemes de reconeixement del certificat obtingut.

Normalment, cada país té les seves pròpies entitats d'acreditació, i aquestes es reconeixen mútuament i s'agrupen en entitats supranacionals que "vigilen" aquestes entitats nacionals o més concretament estableixen criteris per a equiparar les formes de treballar de les entitats d'acreditació validant aquests acords mutus. L'organització que s'encarrega d'aquesta labor és l'International Accreditation Forum (http://www.iaf.nu/).

En definitiva, que l'auditoria realitzada per una entitat de certificació i posteriorment el certificat emès siguin reconeguts pel mercat es basa en aquesta cadena de confiança. No obstant això, a la pràctica, tampoc no aporta gaire certesa sobre la qualitat puntual d'un treball d'auditoria, però sí de manera general sobre el comportament i tractament professional de tots els elements de la cadena: entitat d'acreditació - entitats de certificació - auditat.

En un altre tipus d'auditories no relacionades amb certificacions, com auditories de primera part fetes per una organització externa (per falta de recursos o coneixements en l'organització auditada), no hi ha aquestes entitats de control. En aquest cas, per a garantir la qualitat del treball d'auditoria, no hi ha més recursos que confiar en les certificacions professionals de tercers. Aquestes certificacions professionals permeten tenir una opinió sobre la qualitat del treball que és capaç de fer un auditor a títol individual. De moment, no hi ha un esquema com l'acreditació que sigui aplicable en el sector de les auditories de primera part fetes per un extern.

En aquest últim cas, la fiabilitat i el grau de confiança que dóna una certificació professional els dóna el mercat. Actualment, en l'àmbit de la seguretat de la informació, hi ha dues certificacions destacables:

- CISA d'ISACA
- CISSP d'ISCC (Information Systems Security Certification Consortium, Inc.)

Aquestes certificacions s'obtenen en un moment donat i després la persona certificada ha de mantenir la certificació acreditant que es continua formant. Però aquestes entitats no responen de cap manera sobre el treball que fa un auditor, i no duen a terme controls sobre els treballs que aquests professionals facin, únicament garanteixen mitjançant els seus programes de renovació de les certificacions que el professional està capacitat per a executar labors d'auditoria.

A continuació, es facilita una llista de les entitats d'acreditació més rellevants en el nostre entorn:

Argentina Organismo Argentino de Acreditación (OAA)	**Luxemburg** Luxembourg Office of Accreditation (OLAS)
Àustria Federal Ministry for Economic Affairs and Labor (BMWA)	**Malàisia** Department of Standards Malaysia (DSM)
Austràlia i Nova Zelanda Joint Accreditation System of Australia and New Zealand (JAS-ANZ)	**Maurici** Mauritias Accreditation Service (MAURITAS)
Bèlgica Belgian Accreditation System for Bodies Operating Certification of Products, Quality Systems or Persons (BELCERT)	**Mèxic** Mexican Accreditation Entity (EMA)
Brasil General Coordination for Accreditation - Cgcre, of National Institute of Metrology, Standardization and Industrial Quality (INMETRO)	**Països Baixos** Dutch Accreditation Council (RvA)
Canadà Standards Council of Canada (SCC)	**Noruega** Norwegian Accreditation (NA)
Xile Instituto Nacional de Normalización (INN)	**Pakistan** Pakistan National Accreditation Council (PNAC)
República Txeca Czech Accreditation Institute (CAI)	**Filipines** Bureau of Product Standards Accreditation Scheme
Xina China National Accreditation Board for Certifiers (CNAB)	**Polònia** Polish Centre for Accreditation (PCA)
Dinamarca Danish Accreditation (DANAK)	**Romania** Romanian Accreditation Association (Asociatia de Acreditare din Romania (RENAR)
Finlàndia The Finnish Accreditation Service (FINAS)	**Singapur** Singapore Accreditation Council (SAC)
França Comite Français d'Accreditation (COFRAC)	**Eslovàquia** Slovak National Accreditation Service (SNAS)
Grècia Hellenic Accreditation System S. A. (ESYD)	**Eslovènia** Slovenska Akreditacija (S. A.)
Alemanya German Accreditation Council (DAR)	**Sud-àfrica** South African National Accreditation System (SANAS)
Hong Kong, Xina Hong Kong Accreditation Service (HKAS)	**Corea del Sud** Republic of Korea Accreditation System (KAS)
Índia National Accreditation Board for Certification Bodies (NABCB)	**Espanya** Entidad Nacional de Acreditación (ENAC)
Indonèsia Komite Akreditasi Nasional (KAN)	**Suècia** Swedish Board for Accreditation and Conformity Assessment (SWEDAC)
Iran Iran Accreditation System (IAS)	**Suïssa** Swiss Accreditation Service (SAS)
Irlanda The Irish National Accreditation Board (INAB)	**Taipei** Taiwan Accreditation Foundation (TAF)

Itàlia Sistema Nazionale di Accreditamento degli Organsimi di Certificazione e Ispezione - Italian Federation for Accreditation (SINCERT-FIDEA)	**Tailàndia** National Accreditation Council of Thailand (NAC)
Japó The Japan Accreditation Board for Conformity Assessment (JAB)	**Regne Unit** United Kingdom Accreditation Service (UKAS)
	Estats Units ANSI-ASQ National Accreditation Board (ANAB)

5.3. ISACA (Information Systems Audit and Control Association)

Un altre dels esforços que mereixen ser destacats és la tasca de la ISACA (Information Systems Audit and Control Association), encara que no es tractarà en aquest apartat perquè es desenvolupa més àmpliament en un altre mòdul d'aquest curs.

5.4. IRCA (International Register of Certificated Auditors)

IRCA és una organització actualment internacional, però d'origen britànic, que va sorgir promoguda pel govern britànic al mateix temps que UKAS (l'entitat d'acreditació del Regne Unit) i BSI (British Standards Institute), com a iniciativa per millorar la indústria i els negocis a través de la implementació de principis i millors pràctiques relacionades amb la qualitat.

Com a organització, l'IRCA està orientada a l'àmbit de l'auditoria de sistemes de gestió (és a dir, aspectes com les auditories de comptes queden fora del seu àmbit) i té per objectiu general promoure la professió d'auditor i proporcionar confiança en la qualitat del treball d'auditoria de sistemes de gestió mitjançant l'estandardització tant de la labor d'auditoria com de la formació dels auditors, la certificació de la qual figura entre les seves activitats. És a dir, l'IRCA és una organització que dóna garantia de la professionalitat i qualitat del treball realitzat per un auditor certificat per ella.

Això ho duu a terme recolzant-se en les entitats de certificació que realitzen formacions d'auditors d'acord amb paràmetres i mètodes acordats amb l'IRCA, de manera que un auditor format per una d'aquestes entitats pot acreditar-se davant l'IRCA i mostrar al mercat que la seva professionalitat està recolzada per una comunitat que estandarditza i controla la manera en què s'han de realitzar les auditories de sistemes de gestió.

En tractar-se de sistemes de gestió i també tenir una vocació internacional, les seves metodologies estan guiades en essència per normes internacionals ISO i, molt especialment, per les normes ISO 19011 i ISO 17021 comentades anteriorment.

6. Govern de les TIC

L'Organització de Cooperació i Desenvolupament Econòmic (OCDE), quan va emetre els seus *Principis del govern corporatiu* (1999), va definir el *govern corporatiu* com "el sistema pel qual les corporacions de negoci són dirigides i controlades". Cada país en l'OCDE està desenvolupant, a diferents velocitats, els seus propis esquemes per al control del govern corporatiu, reflectint la seva pròpia cultura i requisits. Dins del seu acostament al govern corporatiu, cada organització ha de determinar com manejarà la seva informació. Aquí la informació és entesa com la combinació tant dels actius de la informació base del seu model de negoci, com de la tecnologia d'informació que els tracta. Aquesta necessitat ha conduït a l'aparició del govern de les tecnologies de la informació i comunicacions (TIC) com a component específic, i cada vegada més important, de la cultura de govern d'una organització.

Habitualment, es defineix *govern* com "el marc per a la direcció (estructures organitzatives, i processos del negoci, estàndards i la conformitat pel que fa a aquests estàndards) que s'assegura que els sistemes d'informació i comunicacions de l'organització sostinguin i permetin l'assoliment de les seves estratègies i els seus objectius".

Una organització pot estar interessada a implantar estratègies per al govern TIC per diferents motius:

- Requisits legals, reguladors o sectorials.

  La Llei Sarbanes-Oxley per a les empreses cotitzades als Estats Units, o els acords de Basilea III en el marc europeu.

- Augment creixent del valor del capital intel·lectual d'una organització.

- Necessitat d'alinear l'evolució dels sistemes d'informació amb els objectius estratègics del negoci, i assegurar que proporcionen els beneficis planificats.

- Proliferació i complicació progressiva de les amenaces a la informació, amb el conseqüent impacte en la reputació, el benefici i la rendibilitat del negoci.

Hi ha dos factors fonamentals en la gestió efectiva dels riscos relacionats amb les TIC. El primer està relacionat amb el desplegament de les TIC de manera alineada amb els objectius de negoci. Els projectes TIC representen, sovint, una important inversió de recursos financers i humans. Per tant, els interessos dels propietaris del negoci s'haurien de defensar mitjançant mecanismes de control intern que garanteixin, de manera transparent i eficaç, que les TIC són

planificades, gestionades i monitoritzades adequadament. Això implica que els administradors del negoci han de tenir en compte els riscos que els puguin afectar i que puguin tenir impacte en el negoci. El segon factor és, en si mateix, com es gestionen aquests riscos.

És evident que la seguretat de la informació és un component dominant del govern TIC. Quan les TIC i la informació en si mateixa es converteixen en el factor determinant de l'estratègia de negoci, i en determinats casos en la mateixa pedra angular del model de negoci, la seva seguretat es converteix en una de les preocupacions bàsiques de les juntes de direcció de les organitzacions.

S'ha de destacar que l'auditoria de sistemes d'informació va néixer abans que es definís el concepte de *govern de les TIC*. Va sorgir com una necessitat durant el procés d'auditoria financera. Amb l'auge progressiu dels sistemes d'informació, els auditors de comptes havien de confiar cada vegada més en l'exactitud de les dades proporcionades pels sistemes, i cada vegada menys en el que es trobaven en suports tangibles (llibres de comptes, extractes, factures, albarans, etc.). Això era així sobretot per l'enorme volum de dades, i també per la seva desaparició progressiva a causa de l'increment de les transaccions purament electròniques. Per tant, va ser necessari des del primer moment comprovar si la informació d'aquests sistemes era correcta, i si no havia pogut ser manipulada. És en aquest context, per tant, que es va iniciar la disciplina de l'auditoria dels sistemes d'informació (i seguretat d'aquests), i va anar evolucionant i adquirint més protagonisme al mateix ritme que ho van fer els mateixos sistemes d'informació. Actualment, en tota auditoria financera hi ha un component d'auditoria dels sistemes d'informació, però hi ha transcendit i existeix per si mateixa en diferents contextos.

Per tant, des d'aquest punt de vista, per a garantir un bon govern TIC és essencial que hi hagi una revisió del govern TIC. Més específicament, és essencial que aquesta funció d'auditoria dels sistemes d'informació estigui integrada en els mecanismes de govern TIC. La funció d'auditoria ha de comprovar com s'estan gestionant els mecanismes de control implantats en les TIC per a garantir la seguretat.

De manera general, els objectius d'auditoria que persegueix una auditoria de sistemes d'informació són:

- Validar els aspectes organitzatius i administratius relatius al procés de gestió dels sistemes de seguretat, amb l'objectiu de garantir que no comporten un risc per a la seguretat de la informació.

- Validar els controls aplicats a la gestió del cicle de vida d'un sistema d'informació, especialment en les seves fases inicials de disseny, implementació i posada en producció.

- Validar el control d'accés físic a instal·lacions, terminals, biblioteques de cintes, etc.

- Automatitzar els controls d'auditoria integrats en els sistemes d'informació.

- Formar, capacitar i sensibilitzar els usuaris en general i, específicament, el personal dedicat a la gestió, a l'operació i al manteniment dels sistemes d'informació.

- Controlar el procés d'auditoria dels sistemes d'informació.

Aquests objectius que hem exposat corresponen tant a l'auditoria de sistemes d'informació com, en general, al procés de gestió de seguretat de la informació. Aquesta coincidència d'objectius és més destacable si el sistema de gestió de la seguretat de la informació (SGSI) està alineat amb la Norma ISO/IEC 27002, abans denominada *ISO/IEC 17799*, i més encara si l'SGSI està implementat complint els requisits de la Norma ISO/IEC 27001. És a dir, els objectius d'una auditoria de sistemes d'informació (SI) són els mateixos que busca un SGSI. Per tant, hi ha la possibilitat de fer dos tipus d'auditoria als sistemes d'informació:

- Auditoria de seguretat als sistemes d'informació.
- Auditoria de certificació del sistema de gestió de la seguretat de la informació.

S'ha de destacar que la certificació d'un SGSI assegura que l'entitat auditada gestiona d'acord amb l'estàndard i, per tant, haurà de fer auditories internes de seguretat als sistemes d'informació. Aquestes és el nexe comú entre tots dos tipus.

6.1. Auditoria dels sistemes d'informació

Aquest tipus d'auditoria s'incorpora directament al procés intern de gestió de la seguretat de la informació. La seva funció és comprovar que la implantació dels controls de seguretat compleix el que estableixen les diferents polítiques dictades per l'organització, i que aquests controls han estat implantats de manera tècnicament correcta. L'auditoria consisteix, per tant, en la revisió de les mesures de seguretat, sense cap més objectiu que dictaminar si la seguretat és correcta o si presenta deficiències. La revisió de les mesures de seguretat es fa davant una referència donada, que pot ser la mateixa política de seguretat de l'organització o una norma de referència com l'ISO/IEC 27002 o COBIT.

És important destacar que, com que es tracta d'un procés intern de l'SGSI, l'auditoria tindrà un abast que, com a màxim, serà el del mateix SGSI. No obstant això, l'auditoria també es podrà centrar en un abast més reduït com, per exemple, un tipus concret d'infraestructura, aplicació o procés de l'SGSI.

L'auditoria es pot centrar en el compliment d'algun aspecte legal relatiu a la privadesa, la protecció de dades personals o els processos relacionats amb la gestió del personal (processos de selecció, entrenament, terminació de contractes, etc.).

En tot cas, abans d'abordar un procés d'auditoria, és essencial definir tant l'abast com la referència contra la qual es vol auditar. En aquest sentit, hem de destacar que, més endavant, tractarem amb més detall els aspectes que intervenen en una auditoria de revisió d'implantació de controls. Per tant, ens interessarem en les revisions que s'han de fer en els controls tècnics de seguretat implantats en la infraestructura de xarxa, o els serveis que s'ofereixen sobre aquestes infraestructures.

Aquestes auditories tenen consideració d'auditoria de primera part i, per tant, les pot fer un grup intern o una entitat externa. No obstant això, en qualsevol dels dos casos, és important prou independència entre l'equip auditor i l'equip implantador i d'operacions, per a poder garantir la qualitat del resultat.

Les auditories internes es poden fer sempre que les organitzacions tinguin un grup d'auditoria independent de l'àrea que s'ha d'analitzar. Aquest grup independent haurà de tenir prou coneixements de seguretat per a dictaminar si les mesures de seguretat són suficients i si, alhora, estan configurades correctament.

Les auditories externes són les que duen a terme empreses externes que s'encarreguen de revisar les diferents mesures de seguretat. Aquestes empreses han de ser totalment independents de l'organització i tenir coneixements acreditats de seguretat.

En els dos casos, el resultat d'aquests processos d'auditoria consisteix en l'elaboració d'un informe en què es dictaminen les deficiències de seguretat que s'hi hagin pogut detectar, sempre dins de l'abast que s'hagi determinat per a l'auditoria. És important destacar que aquest informe ha de ser el més objectiu, clar, concís i directe possible. Molt probablement tindrà com a públic objectiu tant personal directiu d'alt nivell com comandaments intermedis i operatius, per la qual cosa s'haurà d'organitzar tenint en compte aquesta circumstància.

Més endavant, detallarem els aspectes més importants sobre les auditories de seguretat.

6.2. Certificació de seguretat

Per a la matèria que ens ocupa, el procés de certificació de seguretat el duu a terme una organització que ha implantat un sistema de gestió de la seguretat de la informació. Aquesta implantació s'ha fet d'acord amb la normativa ISO/IEC 27001. Per a obtenir la certificació de seguretat, l'organització consulta una entitat externa que està acreditada i que s'encarregarà de veure la implantació correcta d'aquesta normativa. L'objectiu de l'entitat externa és dictaminar si

la implantació és correcta i, una vegada finalitzada la seva revisió, elaborarà un informe. En cas que l'informe sigui favorable, es lliura a l'organització un segell que certifica el compliment i la implantació correcta de la normativa.

Aquestes certificacions de seguretat únicament les poden fer organitzacions degudament acreditades per organitzacions superiors, denominades *organismes d'acreditació*, com per exemple ENAC a Espanya. És a dir, la certificació únicament la poden atorgar les organitzacions que compleixen una sèrie de requisits comprovats (auditats) per un tercer de confiança (l'organisme d'acreditació). Un altre aspecte important que s'ha de destacar és que aquestes organitzacions de certificació són independents, és a dir, no ofereixen serveis de consultoria, sinó que són expressament auditores.

Algunes d'aquestes empreses són: AENOR, APPLUS, BSi (British Standard Institute), TüV, etc.

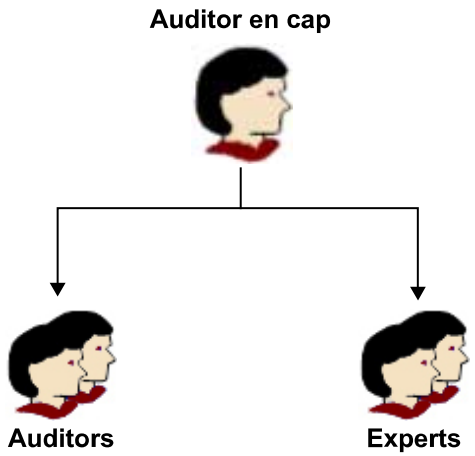
Quant a la l'auditoria i la certificació, sempre que sigui d'acord amb la normativa anterior, es fan de la mateixa manera i l'única diferència és el resultat final, que en el segon cas és únicament un informe de certificació.

7. Equip auditor

En aquesta secció, veurem els diferents aspectes que tenen relació amb els equips d'auditories que fan revisions dels sistemes de gestió de la seguretat de la informació. La descripció dels equips d'auditories que es proporcionarà és vàlida tant per a revisions amb vista a la certificació com per a revisions amb vista únicament a l'auditoria de sistemes d'informació.

Els aspectes que es descriuen en aquesta secció es corresponen amb els requisits imposats a les entitats de certificació (ISO 17021, ISO 27006 i també en part l'ISO 19011), per la qual cosa s'han de veure com un exercici de màxims. És a dir, aquests requisits són completament aplicables a entitats de certificació. Les organitzacions que, tot i no ser entitats de certificació, es dediquin a l'auditoria no estan obligades a complir la totalitat dels aspectes que aquí es descriuen. No obstant això, és recomanable que les organitzacions auditores tinguin en compte aquests requisits i els prenguin com una recomanació.

L'equip auditor és l'equip de persones que estarà encarregat d'executar el projecte d'auditoria, tant per a la revisió de les mesures de seguretat (auditoria de seguretat), com per a la revisió de la implantació correcta de la normativa ISO/IEC 27001 (en cas de recerca de l'obtenció de la certificació). Aquest equip estarà idealment compost per un grup d'auditors organitzat idealment de la manera següent:



Estructura bàsica d'un equip d'auditoria

L'equip auditor està compost, com a mínim, per un auditor en cap, que és el responsable final de l'assignació d'auditoria. El poden assistir un o diversos auditors i/o experts tècnics per a l'execució de les proves. Els experts tècnics treballaran en les proves en què els coneixements i l'experiència de l'auditor en cap o l'equip d'auditors siguin insuficients.

El nombre final de persones inclòs dependrà de les limitacions de temps/cost i l'abast de l'auditoria. D'altra banda, no és necessària la participació de tots els auditors i experts durant tot el marc temporal en què tingui lloc l'auditoria. No obstant això, aquest no és el cas de l'auditor en cap, que en tot moment hi participarà, atès que és el punt de contacte entre l'organització auditada i l'auditora, i és també el responsable últim del treball dut a terme.

Els requisits recomanables que es necessiten per a poder pertànyer a un equip d'auditoria, com també les seves responsabilitats, es descriuen a continuació. Aquests requisits són imposats de manera estricta quan l'equip ha de certificar un SGSI contra la Norma ISO/IEC 27001. En aquest cas, aquests requisits són imposats per l'organisme d'acreditació. En altres situacions, s'han de prendre com a recomanacions.

D'altra banda, l'equip auditor no és l'únic involucrat en la realització de l'auditoria i, per part de l'auditat, és necessària la participació de diversos interlocutors. Aquest punt es tractarà més endavant.

7.1. Auditor en cap

L'auditor en cap és designat per la direcció del programa d'auditoria en què s'enquadri l'auditoria o per la direcció de l'organització auditora. En cas que es facin auditories conjuntes (diverses entitats auditores), s'ha d'aclarir qui té la direcció de la tasca d'auditoria.

En definitiva, l'auditor cap és el responsable últim del resultat de l'auditoria, tant davant el client d'aquesta, com l'auditat i, en general, de cara a la direcció de l'organització a la qual pertany (per exemple, en el cas de les entitats de certificació o empreses que realitzen auditories més tècniques sobre sistemes d'informació). Aquesta responsabilitat inclou:

- Els objectius d'auditoria, l'abast, els criteris i la durada estimada de l'auditoria.

- La competència general de l'equip auditor necessària per a aconseguir els objectius de l'auditoria.

- Els requisits necessaris dels organismes d'acreditació/certificació, si hi són aplicables.

- La necessitat d'assegurar la independència de l'equip auditor de les activitats que s'han d'auditar, i evitar conflictes d'interessos.

- La capacitat dels membres de l'equip auditor per a interactuar eficaçment amb l'auditat i treballar-hi conjuntament.

- L'idioma de l'auditoria i la comprensió de les característiques socials i culturals de l'auditat, o bé per mitjà de les pròpies capacitats de l'auditor, o bé per mitjà del suport d'un expert tècnic.

- Liderar les reunions d'inici i tancament de les auditories (són reunions que sempre es realitzen).

- Controlar que l'auditoria s'estigui desenvolupant correctament, avançant d'acord amb el pla, i comprovar si els objectius de l'auditoria es podran aconseguir.

- Realitzar el seguiment de les evidències que es vagin trobant. És l'últim responsable de la categorització d'aquestes com a troballa, així com del seu nivell de classificació com a no conformitat.

- Donar suport a l'equip auditor si hi ha problemes, incidències o conflictes durant el desenvolupament de l'auditoria.

Des del punt de vista de les seves característiques, és recomanable que els auditors en cap tinguin coneixements i habilitats addicionals als de la resta dels auditors de l'equip. Aquestes habilitats addicionals són les de lideratge de l'auditoria, per a permetre a l'equip auditor dur a terme l'auditoria de manera eficient i eficaç. Els coneixements i les habilitats en aquesta àrea han de preveure:

- Planificació i gestió de recursos.

- Capacitat de comunicació amb el client de l'auditoria i l'auditat, per a representar i defensar l'equip auditor.

- Capacitat de lideratge de persones.

- Pou coneixements tècnics per a conduir l'equip auditor i aconseguir conclusions de l'auditoria. Per a això, se li exigirà la formació acadèmica que sigui rellevant en l'àrea que s'ha d'auditar.

- Capacitat de previsió i resolució de conflictes.

- Finalment, és recomanable (i necessari en auditoria de certificació) que l'auditor hagi participat, com a mínim, en tres auditories com a membre d'un equip auditor fent tasques d'auditor en cap sota la supervisió de l'auditor en cap.

7.2. Auditor

L'auditor (i també, per extensió, l'auditor en cap) ha d'acreditar la formació adequada que demostri els coneixements i les habilitats següents:

- Coneixements sobre els principis d'auditoria, procediments i tècniques que li permetin assegurar-se que les auditories es duen a terme de manera coherent i sistemàtica. Si ens fem càrrec d'entorns d'auditories de certificació de SGSI, aquest coneixement és recomanable que s'acrediti mitjançant formació específica en auditoria, i també mitjançant experiència. Aquesta experiència pot ser, per exemple, haver participat en quatre auditories i almenys en vint jornades completes duent a terme les activitats següents:
  – Revisió de la documentació de l'SGSI.
  – Revisió de l'anàlisi de riscos d'una organització.
  – Haver auditat la implantació d'un SGSI.
  – Haver elaborat els informes relatius a l'auditoria en què va participar.

  Aquesta experiència pot ser, per exemple, haver participat en quatre auditories i com a mínim en vint jornades completes desenvolupant les activitats següents:

- Coneixements específics en l'àmbit de l'activitat auditada. Això inclou: conèixer documents de referència i característiques dels sistemes de gestió i de control, conèixer aspectes tècnics que li permetin entendre l'abast de l'auditoria i aplicar-hi els criteris d'auditoria. Aquest requisit està molt relacionat amb la formació acadèmica que hagi rebut l'auditor. Respecte a la formació acadèmica, n'hi pot haver prou d'acreditar l'experiència professional equivalent. En el cas de l'auditoria de sistemes d'informació, se sol considerar que n'hi ha prou amb una experiència de quatre anys en l'àmbit de les tecnologies de la informació, i almenys de dos anys en seguretat de les tecnologies de la informació. També és necessari haver fet un curs de cinc dies d'auditoria.

- Capacitat per a entendre les situacions particulars i la idiosincràsia de l'organització auditada, que li permeti entendre el context de les operacions de l'organització. Això inclou entendre el model de negoci de l'auditat, el seu sector i les característiques socials d'aquest.

- Coneixement de la legislació aplicable, reglaments i altres requisits rellevants a la disciplina, que li permeti treballar-hi i ser conscient dels requisits aplicables a l'organització que s'està auditant.

A aquests requisits de coneixements i habilitats, d'ordre professional, cal afegir-hi certes capacitats i habilitats personals que garanteixin l'èxit del seu treball. Les qualitats personals que contribueixen al rendiment reeixit d'un auditor són:

- Ser ètic, imparcial, sincer, honest i discret.

- Tenir una actitud oberta i estar disposat a considerar idees o punts de vista alternatius.
- Mostrar-se diplomàtic i hàbil en les relacions amb la gent.
- Ser observador, constant i activament conscient dels entorns físics i les activitats.
- Ser perspicaç, instintivament conscient i capaç d'entendre i adaptar-se a les situacions.
- Ser versàtil, capaç d'adaptar-se a diferents situacions.
- Ser tenaç, persistent i orientat sobre la consecució dels objectius.
- Tenir poder de decisió i ser capaç d'aconseguir conclusions oportunes basades en el raonament lògic i l'anàlisi.
- Mostrar-se independent en les actuacions, relacionant-se al mateix temps amb uns altres de manera eficaç.

Per descomptat, totes les característiques exigibles a l'auditor també valen per a l'auditor en cap.

7.3. Expert tècnic

Les habilitats tècniques requerides per l'equip auditor dependran, exclusivament, de l'entorn que s'ha d'auditar. Si aquests coneixements i habilitats necessaris per a executar certes proves d'auditoria no els cobreix l'equip auditor, es poden satisfer incloent-hi experts tècnics. En qualsevol cas, els experts tècnics operen sempre sota la direcció d'un auditor i no han d'actuar com a auditors pròpiament dits emetent conclusions d'auditories derivades de l'execució de les tasques que se'ls hagi encomanat. L'equip auditor necessita, per tant, tenir un nivell de coneixement tecnològic ampli i, sobretot, ha de conèixer les interrelacions dels diferents àmbits de la seva especialitat, però no necessàriament aquest coneixement ha de ser exhaustiu en una àrea en particular.

Una altra circumstància en la qual pot ser necessària la participació d'un expert és quan hi pugui haver dificultats logístiques o fins i tot de comunicació per desconeixement d'un idioma comú entre auditor i auditat.

7.4. Independència d'auditoria

L'equip auditor, amb la finalitat de garantir la seva imparcialitat, no pot participar en l'elaboració de manuals, polítiques o procediments d'una organització. Tampoc no pot formar part del grup que pren decisions sobre l'estat del sistema de gestió de la seguretat de la informació, i tampoc no pot donar recomanacions específiques per al desenvolupament de l'SGSI. Una vegada finalitzada l'auditoria, sí que pot emetre les recomanacions que consideri oportunes.

Per contra, l'equip auditor sí que pot auditar, detectar les no-conformitats i fer el seguiment de les no-conformitats que s'hagin detectat, i de fet té l'obligació de fer-ho.

No-conformitat

És un error, en la creació de l'SGSI referent a la Normativa ISO/IEC 27001, o qualsevol altre marc que es prengui com a referència, contra el qual s'està auditant.

D'altra banda, un membre de l'equip auditor també té capacitat d'impartir formació genèrica sobre normatives o aspectes de seguretat, elaborar publicacions sobre interpretacions relatives a la normativa i, finalment, fer que es duguin a terme auditories prèvies a la certificació, per a verificar l'estat del sistema de gestió de la seguretat de la informació.

7.5. Codi de conducta de l'equip auditor

Especialment quan es tracta d'auditories de certificació, els membres de l'equip auditor tenen un codi de conducta que han de seguir, el qual assegura la realització correcta de les seves tasques. En aquest sentit, el seu codi de conducta és:

- Actuar de manera veraç i imparcial.
- Evitar qualsevol tipus d'assignació que pugui causar un conflicte d'interessos.
- No acceptar cap tipus d'incentiu, comissió, descompte o un altre tipus de profit per part de l'organització auditada.
- No revelar les observacions de les auditories a tercers.
- No actuar de manera que pugui perjudicar cap de les parts implicades en l'auditoria.

En cas d'incompliment d'aquest codi, es durà a terme una investigació en què l'equip auditor col·laborarà per tal d'aclarir-ho.

7.6. Distribució de funcions

Dins del procés d'auditoria, l'auditor en cap té les funcions següents:

- Planifica i gestiona totes les fases de l'auditoria.
- Dirigeix la primera fase.
- Col·labora en la selecció de l'equip d'auditors.
- Controla els conflictes i maneja les situacions difícils.
- Dirigeix les reunions amb l'equip auditor i el personal auditat.
- Pren decisions en matèria de l'auditoria i l'SGSI.

Les funcions que pertanyen als auditors de l'equip d'auditoria són:

- Donar suport a l'auditor cap.
- Documentar i fonamentar totes les constatacions.

- Fer el seguiment de les accions correctores per a corregir les no-conformitats oposades.

7.7. Relació amb l'auditat

Durant les auditories, hi poden participar més persones de les que s'han esmentat fins ara (auditor en cap, auditors i auditat).

El personal que pot intervenir en un procés d'auditoria és:

- **Equip auditor**
  - **Cap i membres de l'equip**. Normalment, es tracta d'una o més persones.
  - **Auditors en formació**. Personal en formació per a convertir-se en auditor.
  - **Observadors, auditor provisional**. Pot ser un observador de l'organisme d'acreditació (per exemple, ENAC) que supervisi l'auditoria. Però en cap cas podrà participar en cap de les activitats d'auditoria.
  - **Experts, personal assessor**. Personal que assessora l'auditor sobre temes tècnics o concrets del negoci o les tecnologies que s'han d'auditar, encara que no hagi d'actuar en cap prova d'auditoria, únicament dóna suport tècnic.
  - **Testimonis i convidats**.
- **Equip de l'auditat**. Habitualment es compta amb:
  - Representant de la direcció més en línia amb l'objectiu i l'abast de l'auditoria (per exemple, en una auditoria de certificació en la qual existeixen requeriments aplicables a l'alta direcció, s'haurà de comptar amb un representant màxim de la direcció; però en una auditoria tècnica sobre una infraestructura TI, podria tractar-se simplement del responsable de l'àrea d'infraestructures TI de l'organització auditada o bé el seu superior).
  - Persones auditades. És molt habitual que part de les proves d'auditoria requereixin la interlocució amb personal de l'auditat. Les àrees o grups de treball poden ser seleccionats per l'auditat, però és responsabilitat de l'auditor escollir les persones concretes finalment entrevistades.
  - Guia. És recomanable que l'auditat identifiqui una persona com a guia per a l'equip auditor que li permeti resoldre aspectes logístics, aportar

aclariments sobre respostes donades per persones que són entrevistades, facilitar documentació, etc.

– Observadors, personal en formació. Normalment, personal de l'empresa en formació per a esdevenir auditor intern.

– Consultors. Quan l'empresa contracta un consultor extern (per exemple, per assessorar-la en el desenvolupament de l'SGSI), aquest pot observar l'auditoria, però no ha d'intervenir-hi en cap moment.

8. El peritatge informàtic

De manera general, el peritatge, o més exactament la prova pericial, és un mitjà més de prova per a la resolució de conflictes. Aquesta prova l'aporta una persona amb coneixements tècnics especialitzats en el tema per a ajudar a interpretar els fets sota prova pericial i dirimir el conflicte.

Els tipus de peritatge són múltiples i gairebé tants com àrees del coneixement, encara que els més freqüents solen ser: cal·ligràfic, grafològic, documentoscòpic, immobiliari (taxació), falsificació de marques, reconstrucció d'accidents (laborals, de trànsit), peritatge d'incendis (valoració de danys, reconstruccions), sociolaborals, peritatge de joies, anàlisi de veus, medicina pericial, plagi textual, etc.

Amb la penetració creixent dels sistemes d'informació en la pràctica totalitat dels àmbits de la societat i de l'activitat humana duta a terme, els sistemes d'informació estan cada vegada més involucrats en situacions de conflicte que necessiten ser resoltes. Per tant, cada vegada és més freqüent que, en els conflictes entre persones o organitzacions, hi hagi elements relacionats o continguts en els sistemes d'informació. En aquest context, s'ha tornat cada vegada més freqüent la necessitat de disposar d'un peritatge informàtic, que sigui capaç d'analitzar una realitat amb totes les garanties legals, i que pugui donar una explicació basada en els fets i la lògica, seguint a més unes regles determinades.

Els casos que es poden peritar abracen un ampli ventall de possibilitats, i van des d'acomiadaments de personal per ús improcedent de l'equipament informàtic, demandes per incompliments de contracte en la creació d'aplicacions informàtiques, taxació de béns materials i immaterials, etc. Per tant, s'ha de trencar amb la idea que el peritatge informàtic està relacionat directament amb delictes informàtics. No és així. El peritatge informàtic té un camp d'aplicació molt més ampli, i pot estar present en pràcticament qualsevol conflicte en què els sistemes d'informació tinguin alguna funció.

Convé indicar que un tribunal no és l'únic demandant de perícies. També empreses i particulars poden necessitar, per diversos motius, una prova pericial informàtica en els seus equips. Per exemple: determinar on és la pèrdua de correus interns, anàlisi dels sistemes de seguretat per a detectar usos indeguts, etc.

És interessant destacar que hi ha una certa similitud entre l'auditoria de sistemes d'informació i la prova pericial informàtica.

En els peritatges, igual que en les auditories, la informació s'obté mitjançant un procés d'anàlisi sistemàtica, lògica, repetible i objectiva, ja que està absolutament basada en els fets i la realitat observable. No obstant això, hi ha diferències molt notables, la principal de les quals és que l'objectiu de tots dos processos és diferent. L'auditoria té per objectiu analitzar la realitat per a determinar si s'ajusta a unes normatives determinades (els criteris d'auditoria), mentre que el peritatge simplement analitza la realitat per a poder-la explicar i respondre als dubtes que un neòfit pugui tenir de la interpretació.

Una altra diferència important que s'ha de tenir sempre en compte és que el dictamen pericial (resultat d'efectuar la prova pericial) és una conclusió emesa per una persona individual, el perit, mentre que les conclusions d'auditoria són emeses per l'organització auditora. La diferència és subtil, ja que es pot pensar que és l'auditor en cap qui respon del resultat de l'auditoria, però això només és cert de manera interna a l'organització encarregada de fer l'auditoria. L'auditoria és un procés en què es relacionen organitzacions, l'auditor i l'auditat. Òbviament, pot ser que l'auditoria l'hagi fet una única persona, i que en el contracte d'auditoria assumeixi les responsabilitats de manera personal. No obstant això, en la prova pericial és el perit qui s'exposa i podria arribar a ser sancionat.

Finalment, és interessant destacar la relació que hi ha entre la informàtica forense i el peritatge informàtic. La informàtica forense és una de les activitats que poden estar involucrades en una prova pericial. És a dir, no totes les proves pericials comporten necessàriament activitats forenses. La informàtica forense consisteix en una sèrie de tècniques i procediments metodològics que permeten capturar proves contingudes en equipaments computacionals i dispositius digitals, les quals es poden presentar com a prova.