Auditoria de certificació ISO 27001

PID_00239288

Rafael Estevan de Quesada

Temps mínim de dedicació recomanat: 5 hores

Universitat Oberta de Catalunya

Índex

Introducció

En el mòdul anterior d'introducció a l'auditoria informàtica, s'han presentat els principis generals del procés d'auditoria i les auditories sobre els sistemes d'informació, dins el context del bon govern TIC. Per a garantir el bon govern corporatiu, cada vegada més és necessari que també es garanteixi el bon govern o gestió dels sistemes d'informació o, de manera general, de la informació.

> El govern de les TIC és correcte quan la seva gestió es troba alineada amb els objectius de negoci, es coneixen els riscos que afecten els sistemes d'informació i es gestionen adequadament.

Les auditories internes són una eina per al govern de les TIC i serveixen perquè la mateixa direcció d'una organització conegui la manera com es gestionen els riscos, i per a demostrar a altres organitzacions la seva posició davant els riscos que afecten la informació. D'aquesta manera, en el mòdul anterior, s'han presentat dos grans tipus d'auditories relacionades amb la protecció de la informació: auditories tècniques de seguretat dels sistemes d'informació i auditories de certificació dels sistemes de gestió de la seguretat de la informació.

Tots dos tipus d'auditoria tenen per objecte final oferir al client de l'auditoria una visió de l'estat en què s'està gestionant la seguretat de la informació. No obstant això, aquesta visió s'ofereix des de punts de vista diferents. Les auditories tècniques de seguretat comproven aspectes concrets de la implementació dels controls aplicats, mentre que les auditories de certificació d'un sistema de gestió de la seguretat de la informació tenen un objectiu més genèric: comprovar si el procés de gestió s'està duent a terme d'acord amb certs requisits. Aquests requisits han estat recollits en la Norma ISO/IEC 27001 (l'última versió d'aquest material era de 2013, amb correccions realitzades el 2014 i el 2015. En un futur, es pot preveure que serà actualitzada de nou per mantenir-la alineada tant amb la tecnologia com amb l'entorn de risc tecnològic i les activitats de l'ISO, la qual cosa en part va ser la raó que va impulsar la modificació entre la versió de 2005 i 2013).

Per tant, podem observar que el primer tipus d'auditoria s'integra en el mateix esquema de govern de les TIC, i acostumen a ser auditories de primera part. També poden existir com de segona part, en circumstàncies en què el client de l'auditoria vol comprovar la manera com l'auditat gestiona la seva informació. En aquest cas, el client de l'auditoria tècnica de seguretat té un interès legítim a garantir la seguretat de la informació gestionada per l'auditat. Per exemple, l'auditat pot estar tractant informació pertanyent al client de l'auditoria en el marc d'un contracte.

D'altra banda, les auditories de certificacions són purament de tercera part, i a més tenen un objecte més general. No es tracta de comprovar la implementació de controls concrets, sinó que se centren en la verificació del mateix esquema de gestió amb el qual s'estiguin controlant els riscos. És a dir, les auditories de certificació inclouen la comprovació dels mecanismes de gestió dels riscos, i les auditories internes són un més d'aquests mecanismes. Per tant, davant el resultat d'una auditoria de certificació (és a dir, mitjançant el certificat emès per l'organització auditora), una organització externa pot estar segura, en certa manera, que s'estan fent auditories internes i que aquestes són adequades amb vista a gestionar els riscos sobre la informació.

En aquest mòdul, ens centrarem en els aspectes que fan de l'auditoria de certificació una eina interessant per a les organitzacions i, posteriorment, en la manera com aquestes es duen a terme.

1. Sistemes de gestió de la seguretat de la informació

En l'actualitat, es reconeix que la manera més eficaç de controlar els riscos que amenacen la informació, i per tant el negoci, és mitjançant la implantació d'un sistema de controls interns en l'organització per a gestionar el risc.

La gestió del risc ha estat tradicionalment associada a la gestió de riscos financers. No obstant això, tal com s'ha dit anteriorment, la importància que han anat adquirint els sistemes d'informació ha arribat fins al punt que els riscos que es gestionen en una organització ja no són principalment financers, sinó que es complementen amb els riscos als quals està sotmesa la informació. Això és a causa de l'elevada integració entre l'estat financer d'una organització i els actius d'informació. Els riscos en la confidencialitat, integritat o disponibilitat d'un determinat actiu d'informació poden repercutir directament en els aspectes financers. La primera causa d'això és la dependència dels processos organitzatius en els sistemes d'informació, i la segona és l'aportació que fa la informació a la generació de valor en l'organització.

Aquest nou escenari ha fet que, actualment, les organitzacions prestin una atenció creixent a gestionar els riscos que amenacen la seva informació i els sistemes TIC que la tracten. La manera com es tracten aquests riscos, com veurem a continuació, també ha variat.

1.1. Gestió dels riscos de la informació

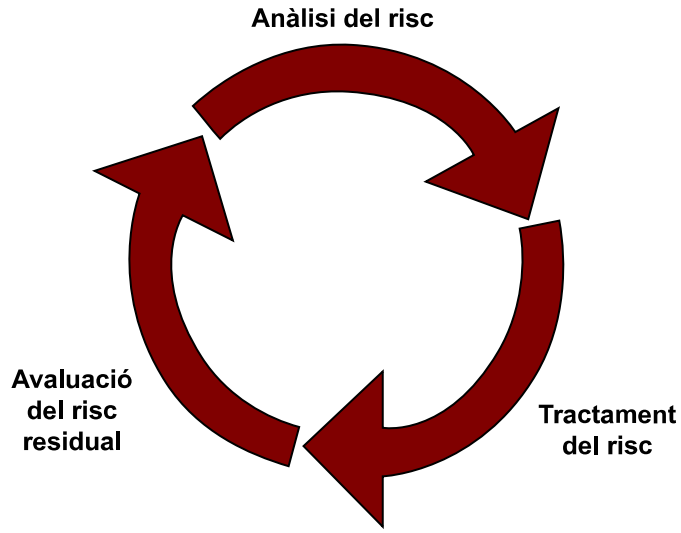
Una visió molt estesa de la manera de gestionar els riscos relacionats amb la informació, i especialment els sistemes d'informació, ha estat la visió ascendent (*bottom-up*). Segons aquesta visió, les accions sobre els controls que s'han d'implantar es decideixen des del punt de vista tàctic, tenint en compte la tecnologia disponible. Són accions d'ordre més precís, ajustades a una situació concreta i preses sobre el terreny. De vegades, les decisions es prenen d'acord amb la percepció directa del risc i, en certs casos, fins i tot quan el risc en si ja s'ha materialitzat. Per això, aquestes accions no es prenen en l'àmbit d'una decisió estratègica de la direcció de l'organització, sinó sempre tenint en compte les circumstàncies concretes de la realitat. D'aquesta manera, el resultat tendeix a ser un simple agregat de controls, al qual li falta una visió de conjunt i coherència.

D'aquesta visió reactiva de la gestió de la seguretat s'ha passat a un enfocament holístic de la seguretat de la informació. Amb aquest nou enfocament, la seguretat de la informació es gestiona no solament quan la informació és tractada pels sistemes TIC, sinó que es gestiona durant tot el seu cicle de vida: des del moment en què la informació entra en l'organització, fins que desapareix. Per

tant, els controls necessaris per a gestionar el risc hauran de tenir en compte no solament els sistemes informàtics i les xarxes de comunicacions, sinó també les persones i els processos que aquestes executen.

D'altra banda, per a abordar aquest enfocament es necessiten unes eines per a comprendre els riscos, prendre decisions i mesurar els resultats que se n'han obtingut. Per tant, és necessari que es faci un procés de gestió dels riscos més metòdic.

D'aquesta manera, podem representar el procés de gestió del risc mitjançant el diagrama següent:



Procés de gestió contínua del risc

Aquest procés de gestió del risc empra les seves pròpies tècniques, metodologies i eines, les quals serien matèria per a un altre curs com aquest. No obstant això, podem resumir les tasques que comporten els sistemes de gestió de la seguretat de la informació de la manera següent:

- Anàlisi del risc
  - Establir el context en què s'analitzarà el risc, tant pel que fa als mateixos actius d'informació que s'hi ha d'analitzar com a les amenaces que s'hi han de considerar.
  - Identificar amenaces potencials i vulnerabilitats en els actius que podrien ser explotades.
  - Avaluar el risc mitjançant l'estimació de la probabilitat que s'esdevinguin l'amenaça i l'impacte.

  Tractament del risc. Segons els diferents nivells de risc determinats, s'ofereixen tres alternatives:
  - Mitigar el risc. S'hi apliquen controls que poden tenir com a objectiu la reducció de la probabilitat d'esdeveniment, la reducció de l'impacte

o, més directament, la reducció de la importància de l'actiu amenaçat. A partir d'aquestes mesures, el nivell de risc és inferior que si no hi ha control de seguretat. El grau màxim de reducció, difícilment assolible, serà el punt en què el risc pugui ser eliminat.

– Acceptar el risc. Ja sigui perquè el cost o la complexitat d'implementar el control ho fa inviable o extremament costós, l'organització decideix acceptar un nivell de risc determinat.
Aquesta opció s'ha de prendre amb molta cura, i només si abans s'han avaluat tots els possibles controls que mitiguin el risc (encara que només sigui parcialment). Es diu llavors que hi ha un risc residual que no pot ser controlat i que s'ha d'acceptar.

– Transferir el risc. Amb l'objecte de tenir absolutament controlats tots els riscos, hi ha la possibilitat de transferir el risc financer que se'n deriva mitjançant una pòlissa d'assegurança. Aquesta opció sol ser tinguda en compte en escenaris madurs de gestió del risc, ja que les primes d'aquestes assegurances poden ser molt elevades si l'organització no demostra que tots els riscos són gestionats fins a un bon nivell.

- Avaluació del risc residual i replantejament de l'escenari de risc. Una vegada fet l'exercici anterior d'anàlisi i tractament, el risc s'ha de gestionar contínuament, ja que canvia la naturalesa dels riscos antics i sorgeixen riscos nous: les tecnologies evolucionen, la importància dels actius d'informació canvia, nous actius apareixen i altres desapareixen, etc. Això implica la necessitat de revisar, periòdicament, la manera com ha canviat l'exposició al risc i la manera com els controls existents també han de canviar. Aquest procés de revisió provoca al seu torn que es reinicií el procés de gestió del risc.

És interessant destacar que, amb l'objectiu d'aplicar les millors pràctiques que hi hagi en el sector, les organitzacions tenen a la seva disposició diferents tipus de catàlegs de controls de seguretat. Els més estesos actualment, sobretot per la seva amplitud i cobertura de més tipus de risc, són l'estàndard ISO/IEC 27001 i el catàleg COBIT d'ISACA (n'hi ha altres com NIST SP 800-53 Controls de seguretat i privadesa per a sistemes d'informació i organitzacions federals dels EUA, Criteris de Seguretat del Ministeri de les Administracions Públiques del Govern d'Espanya, i molts altres sorgits en els àmbits governamentals). Aquests catàlegs són àmpliament emprats com a referència per les organitzacions a l'hora d'implementar els controls de seguretat.

És interessant en aquest punt, i per a la resta d'aquest mòdul, introduir la família de normes ISO/IEC 31000. Aquest conjunt de normes de creació bastant recent (totes publicades com a primera versió el 2009) es va crear per, de manera general, donar un marc genèric per a la gestió del risc a les organitzacions que estiguin preocupades per gestionar un procés sobre la base de riscos, amb independència del seu sector. L'estàndard descriu un procés complet de gestió

del risc, basat en un cicle de millora continuada. És a dir, ho afronta des de la seva definició, el seu disseny, la seva implementació, el seu control i la seva millora. També introdueix un canvi en el concepte de risc. Les principals normes que s'han publicat són:

a) ISO 31000:2009 - *Risk management - Principles and guidelines*, que bàsicament defineix:

- Principis:
  - Ha d'aportar valor a l'organització.
  - Ha de ser una part integrada en els processos organitzatius.
  - Ha d'incorporar-se als processos de presa de decisions.
  - Ha de tenir en compte explícitament les incerteses que hi pugui haver en l'entorn.
  - Ha de ser un procés que ha de basar les seves conclusions en la millor informació disponible en el moment.
  - Ha d'executar-se seguint mètodes sistemàtics, estructurats i en un marc temporal precís, però adequat al context de l'organització així com a factors humans i culturals.
  - El procés ha de ser dinàmic, iteratiu i capaç d'adaptar-se al canvi per permetre que l'organització pugui millorar de manera continuada.
- Marc de referència per a un procés de gestió del risc que, més que trobar-se de manera autònoma en l'organització, s'integri en el procés de gestió al qual ha d'aportar valor. Per tant, el procés de gestió del risc segueix un model de millora contínua PDCA (més endavant en aquest mòdul s'aprofundeix en aquest concepte) que, a partir d'un mandat de l'organització i una assignació de responsabilitats, defineix un procés iteratiu amb unes fases generals de:
  - Disseny del marc de procés de gestió de riscos (delimitar el context, la política de gestió de riscos, les responsabilitats, els recursos, la integració amb altres processos organitzatius, els mecanismes per a la comunicació i la comunicació dels resultats).
  - Implementació de la gestió del risc, fase en la qual de manera efectiva es realitza l'exercici de percepció del risc (en anglès *risk assessment*).
  - Monitoratge i millora del marc del procés de gestió del risc per a obtenir millors resultats en successives iteracions.

- Finalment, defineix les fases que s'han de seguir en l'exercici de percepció del risc, que són:
  - Establir el context (ve de fases anteriors).
  - Identificar riscos. Definir els escenaris de risc, és a dir, què pot passar, quan, on, de quina manera, per quines raons.
  - Analitzar els riscos. Determinar amb quina probabilitat es pot donar un determinat escenari, identificar quins controls existeixen ja i determinar les conseqüències que poden produir-se per tal de poder donar un nivell a aquest risc.
  - Avaluar els riscos. Aquesta fase ha de prendre del context els nivells de risc que són acceptables per a l'organització, els quals poden anar variant al llarg de l'execució continuada del procés de gestió de riscos, i que ajudaran a prioritzar els riscos en la fase de tractament.
  - Tractar els riscos. Seleccionar les diferents opcions de tractament del risc (vistes anteriorment), i preparar i implementar els plans per al tractament del risc.

Aquestes són les tres grans parts d'aquest marc.

b) ISO *Guide 73:2009 - Risk Management - Vocabulary*. Aquest document dóna les definicions i és interessant ja que matisa i defineix conceptes amb precisió, com ara el del mateix risc. El risc ja no es percep com un aspecte negatiu en el sentit de "possibilitat de pèrdua", sinó simplement com l'efecte de la incertesa en la consecució dels objectius. Com es pot observar, ja no es parla de pèrdua, sinó d'incertesa, i això es pot considerar com una oportunitat, tant en negatiu com en positiu. Però de totes maneres, es continua veient el risc com la combinació de les conseqüències d'un esdeveniment i la seva probabilitat d'ocurrència.

c) ISO/IEC 31010:2009 - *Risk Management - Risk assessment techniques*. Aquest document dóna més detalls sobre la fase concreta de l'exercici de percepció del risc (*risk assessment*) introduït en la norma ISO 31000.

En si mateixes, cap d'aquestes normes de la família ISO/IEC 31000 és certificable, però sí que tenen un gran impacte sobre la certificació de sistemes de gestió. Respecte a aquest nou marc, s'estan modificant els estàndards que defineixen els requeriments dels sistemes de gestió normalitzats per l'ISO/IEC, així com els de qualitat, gestió mediambiental i, també, el que més ens ocupa en aquest curs de gestió, la seguretat de la informació. Tots estan basats en la gestió del risc i en el procés de control per mitjà del cicle de millora. En tenir diversos punts en comú, més enllà de la seva especificitat, l'ISO/IEC ha decidit definir-los tots de manera coherent i igual. Això s'ha reflectit en un document general, denominat Directives - Part 1, el qual descriu la manera

de funcionament de l'ISO/IEC en el seu dia a dia per al desenvolupament de normes ISO. A part de descriure la manera de funcionament de tots els seus comitès, en els annexos es donen detalls concrets sobre la forma de treballar, les fases i, en el seu annex SL, es donen les indicacions sobre el mètode a seguir per desenvolupar nous estàndards per a sistemes de gestió. En el seu apartat SL.9, es defineix clarament l'estructura que tots els estàndards de sistemes de gestió hauran de seguir i, en l'apèndix 2, dóna els punts concrets que ha de tenir el text d'una norma d'aquest tipus. L'ISO/IEC27001, en la seva versió de 2013, va ser la primera a adoptar aquesta estructuració, en la qual es pot observar que la base de tots els sistemes de gestió ha d'estar en la identificació de riscos i oportunitats. Es basa en la manera de concebre el risc descrit en la Guia 73 esmentada anteriorment i, per tant, les organitzacions poden prendre la norma ISO/IEC 31010 com la manera d'aproximar-se a la tasca d'identificar i gestionar els riscos.

1.2. Sistemes de gestió

El procés descrit en el punt anterior pot ser institucionalitzat. És a dir, pot ser descrit, documentat i, finalment, implementat a partir dels elements següents: primer, un conjunt coherent i organitzat de controls de seguretat; segon, uns processos per a gestionar i revisar aquests controls; tercer, unes persones encarregades de fer aquests processos, i quart, uns recursos amb un component més o menys tècnic que permeten implementar els controls i gestionar-los. El més destacat d'aquest procés és que serà cíclic. El procés contindrà mecanismes que permeten l'anàlisi de la manera com s'està duent a terme i, segons les conclusions, es reajustarà el procés. D'aquesta manera, s'anirà millorant contínuament i gradualment l'eficàcia dels controls de seguretat.

Quan aquest tipus de processos s'estableix en una organització, es diu que hi ha un sistema de gestió. El sistema de gestió, en aquest cas, té per objecte garantir la seguretat (confidencialitat, disponibilitat i integritat) de la informació, i es denomina *sistema de gestió de la seguretat de la informació* (SGSI).

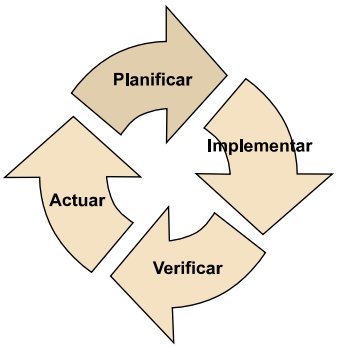
De manera general, s'entén per un *sistema de gestió* el conjunt de persones, processos i tecnologies d'una organització que treballen, conjuntament, per a gestionar i controlar unes determinades activitats de l'organització. Quan aquestes activitats són les necessàries per a garantir la seguretat (confidencialitat, disponibilitat i integritat) de la informació d'una organització, som davant un sistema de gestió de la seguretat d'informació, SGSI. Dins d'aquest sistema, per tant, es trobarà la gestió dels sistemes d'informació, ja que són els principals elements que emmagatzemen i tracten la informació.

Cada organització té els seus propis objectius, cultura i mitjans per a implementar un SGSI. No obstant això, amb independència de les seves característiques pròpies, tots els sistemes de gestió (qualitat, mediambiental, etc.) tenen certs punts en comú, ja que es basen en la implementació d'un cicle de millora per a controlar i millorar l'activitat. Hi ha diversos models (com els propo-

sats per Six-Sigma), però el més conegut, el que n'ha inspirat d'altres, i que és emprat en el context dels SGSI històricament, és l'anomenat *cicle de Deming* encara que tal com es va fer en la revisió de la norma ISO/IEC 27001 duta a terme el 2013, es va flexibilitzar la definició de requeriments i ja es defineix completament alineat amb aquest model PDCA el qual, no obstant això, és vàlid per a entendre què és un procés de gestió continuada d'una activitat.

1.3. Processos de millora continuada

Hi ha diverses formes de dissenyar un sistema per a la gestió de la seguretat de la informació i, en general, qualsevol procés que requereixi un control i un ajust continuats. Històricament, i en el context del control de qualitat de processos industrials, va sorgir el model de Deming de millora continuada conegut per les seves inicials en anglès PDCA (*pla*, *do*, *check*, *act*; en català, *planificar*, *implementar*, *verificar*, *actuar*), que es va estendre a molts altres àmbits.



Model de sistema PDCA

El model PDCA va ser popularitzat per Edward Deming, encara que ell mateix reconeixia que el model ja havia estat plantejat per Walter A. Shewhart, tots dos científics americans dedicats a l'estudi de les matemàtiques estadístiques i al control de processos i qualitat. El procés es pot aplicar a la resolució de qualsevol tipus de problema mitjançant un mètode d'aproximació progressiva. Pel que ens concerneix, l'objectiu que es vol aconseguir és una utopia, per exemple la qualitat total o la seguretat completa de la informació d'una organització. El procés pretén avançar cap a aquest objectiu inassolible en si mateix. No obstant això, la mera execució del procés permet anar millorant de manera contínua i contrastada l'eficàcia i l'eficiència del procés.

Aquest model de millora s'ha pres, des de l'inici de la labor d'estandardització de l'ISO, com a referència a l'hora d'estandarditzar sistemes de gestió com ara els de qualitat (ISO9001), gestió mediambiental (ISO14001) i, més recentment, gestió de la seguretat de la informació (ISO/IEC 27001).

Un sistema de gestió de la seguretat de la informació, per tant, serà un procés amb les característiques següents:

- Basat en un model iteratiu de millora.
- Integrat tant per persones com per processos i tecnologia.
- Amb mecanismes per a la presa de decisions basats en una anàlisi de riscos metòdica.
- Amb mecanismes de control de riscos recollits en un conjunt de bones pràctiques i reconeguts per l'entorn en què es trobi l'organització.

Hi ha diverses maneres de dissenyar un sistema per a la gestió de la seguretat. No obstant això, si ens atenim al que actualment està reconegut i estandarditzat internacionalment, l'opció més estesa és la implementació d'un SGSI basat en la Norma ISO/IEC 27001, que pren els seus controls de seguretat de la Norma ISO/IEC 27002, però altres models serien vàlids (CoBIT, per exemple).

Tal com hem comentat, el model PDCA és un dels més estesos i coneguts i, fins a la revisió de la norma ISO/IEC 27001 realitzada per l'ISO el 2013, es requeria que el model de l'SGSI estigués totalment alineat amb ell. Però a partir de la revisió de les directrius generals de l'ISO i la inclusió de l'annex SL, en l'apèndix 2 d'aquest annex es dóna una definició més flexible dels requeriments que ha de seguir el model de gestió per a tots els sistemes de gestió estandarditzats per l'ISO i, en la pràctica, es va eliminar aquesta referència directa al model PDCA. Aquesta nova especificació és més genèrica i pot adaptar-se a altres metodologies, algunes molt populars com per exemple SIX-SIGMA, encara que no per això s'ha eliminat el concepte de millora continuada basada en la planificació, implementació i correcció, ja que tots els models de millora estan inspirats d'alguna manera en aquest model. No obstant això, segons la norma ISO/IEC 27002, els requeriments per als sistemes de gestió ja no imposen un determinat model, però sí que inclouen tots uns requisits determinats que poden ser ajustats i alineats amb les fases del model PDCA.

1.4. Retorn sobre la inversió d'un SGSI

Quan una organització implanta un SGSI seguint les directrius d'un estàndard (estigui posteriorment certificat o no), obté una sèrie d'avantatges que han de ser els motivadors màxims per a la direcció. La motivació més important seran els beneficis econòmics.

La implantació d'un SGSI no reporta uns beneficis econòmics directes (augments directes de la xifra de negoci). Si més no, és molt complex i discutible trobar generació de recursos com a conseqüència de la implantació de controls de seguretat. Per tant, és difícil calcular el seu retorn sobre la inversió (ROI: *return over investment*) o, més concretament, el seu retorn sobre la inversió en seguretat (ROSI: *return over security investment*). Això és motivat per la dificultat de trobar uns beneficis que es puguin relacionar amb la inversió feta.

És més habitual expressar el ROI de seguretat en termes dels estalvis o recursos que es deixarien de perdre en cas que s'esdevingués un incident. És obvi que una despesa que es deixa de fer és un benefici indirecte. El problema és que aquest benefici només s'obté en cas de materialització de l'amenaça, i això és precisament el que es vol evitar. Per tant, la manera com es calcula el ROI és purament teòrica[1], ja que el benefici no s'està obtenint realment. Malgrat això, és possible avaluar aquest benefici mitjançant una anàlisi de riscos detallada i quantitativa en termes monetaris.

(1)És interessant contrastar amb diversos exemples que es donen en el web següent: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/677-bsi.html

Una de les maneres més habituals de calcular el ROI d'un SGSI és suposar que es materialitzen les amenaces, i avaluar els costos de recuperar la situació de normalitat amb els controls de seguretat i sense.

- Csin_ctrl: cost de recuperar la situació de normalitat en cas que es materialitzin unes determinades amenaces sense que hi hagi els controls que estan sota estudi.

- Ccon_ctrl: cost de recuperar la situació de normalitat en cas que es materialitzin unes determinades amenaces amb els controls que s'estan avaluant.

La diferència entre totes dues és el benefici de tenir implementats els controls de seguretat. No obstant això, no és realista pressuposar que aquest és el benefici real que es tindrà, ja que no es farà sempre, sinó només si les amenaces es materialitzen. Així, com que les amenaces es materialitzen amb una certa probabilitat anual, és possible multiplicar el benefici per aquesta probabilitat i tindrem l'estimació del benefici anual esperat.

B anualitzat_esperat = (Csin_ctrl - Ccon_ctrl) * *P* escenari_incidents

D'altra banda, tindrem el cost d'implantar els controls i l'SGSI en si mateix (Cctrl). La divisió del marge (benefici anual esperat menys el cost dels controls) entre el cost ens donarà el ROI.

ROI = (*B* anualitzat_esperat - Cctrl) / Cctrl

El càlcul és teòricament simple de fer, però en la pràctica ens trobem amb moltes dificultats: hi ha moltes variables a l'hora de calcular els costos, és difícil predir tots els costos de recuperació i és especialment complex i arriscat donar unes xifres de probabilitat de materialització. És possible plantejar el càlcul per a la presa de decisió sobre un control concret (o conjunt de controls), però és complex plantejar-ho per a la presa de decisió d'implantar tot un SGSI. Per tant, la direcció haurà de considerar una altra sèrie de beneficis menys tangibles i mesurables.

1.5. Beneficis generals dels SGSI

A part d'aquests beneficis econòmics indiscutibles, però de difícil quantificació, la implantació d'un SGSI comporta també els avantatges següents. Aquests són fàcilment transmissibles a la direcció d'una organització, a l'hora d'aconseguir el seu compromís i suport per a abordar les tasques d'implantar un SGSI i, molt especialment, efectuar-ho de manera efectiva:

- L'SGSI permet conèixer i analitzar els riscos que afecten la informació. S'identifiquen amenaces i vulnerabilitats, de manera que se'n pot avaluar

l'impacte en l'activitat empresarial, almenys de manera qualitativa i prioritzada.

- D'una manera prioritzada, coherent i organitzada, es pot prevenir, eliminar o reduir eficaçment el nivell de risc. Això s'aconsegueix mitjançant la implantació dels controls adequats, preparant el negoci davant possibles emergències i garantint-ne la continuïtat.

- El coneixement dels riscos assegura el compromís de l'organització amb el compliment de la legislació vigent. Per tant, assegura el compliment de la normativa de protecció de dades de caràcter personal, serveis de la societat de la informació, comerç electrònic, propietat intel·lectual i, en general, la relacionada amb la seguretat de la informació. Al seu torn, assegura la consideració dels marcs normatius de gestió del risc (per exemple, Sarbanes-Oxley) que hi siguin aplicables.

- L'execució del cicle de Deming permet planificar, organitzar i estructurar els recursos assignats a la seguretat de la informació.

- El procés d'anàlisi i de gestió de riscos permet definir objectius i metes amb què augmentar el grau de confiança en la seguretat.

- L'SGSI permet establir processos i activitats de revisió, millora contínua i auditoria de la gestió i tractament de la informació. Tot això facilita l'aproximació progressiva a un estat òptim d'ús de recursos i nivell de seguretat.

- L'SGSI definit en la Norma ISO/IEC 27001 està basat en un model de gestió comuna a altres sistemes de gestió que, habitualment, ja es troben en l'organització. Per tant, hi ha la possibilitat d'integrar la gestió de la seguretat de la informació amb la resta de sistemes de gestió implantats. Així, es poden aconseguir sinergies i estalvis de costos en alguns aspectes, com ara els processos de certificacions i les auditories de primera part del sistema de gestió.

- Garantir el tractament segur i correcte de la informació mitjançant el control d'un SGSI aporta un valor afegit de confiança en la protecció de la informació. D'aquesta manera, permet millorar la imatge de l'organització amb vista a altres empreses i es converteix en un factor de distinció davant la competència. De vegades, aquesta demostració pot arribar a ser una exigència contractual. No serà estrany que, en un futur, les organitzacions que externalitzin algun tractament de la seva informació sol·licitin als seus contractistes la certificació del seu SGSI, per a demostrar la gestió segura de la informació.

- Avui en dia, per l'auge del tractament de la informació amb tecnologies TIC, la implantació d'un SGSI afectarà directament les àrees TIC de

l'organització. Per tant, la seva implantació assegurarà que la gestió de les TIC està correctament alineada amb els objectius de negoci.

- Finalment, l'existència d'un SGSI assegura que es té garantida la continuïtat dels sistemes d'informació en cas d'incidents greus, almenys per als processos que es troben sota l'abast de l'SGSI. Això és especialment important, i pot ser pres com a element clau, a l'hora de determinar l'abast de l'SGSI. L'organització ha de determinar i conèixer quins processos són els crítics per a la supervivència de l'organització, quins escenaris de desastre la poden afectar negativament, quins es controlaran, i de quina manera s'actuarà. Tot això és un dels pilars més importants de l'SGSI.

1.6. Família d'estàndards ISO/IEC 27000

En una demostració clara de la importància que la seguretat de la informació té per a l'èxit de les organitzacions, l'ISO i l'IEC (International Electrotechnical Comission, organització d'àmbit mundial dedicada a l'estandardització en el mercat de l'electrònica i tecnologies relacionades) han elaborat conjuntament tot tipus de normes, estàndards, guies i informes tècnics relacionats amb les TIC i, més particularment, amb les tècniques de seguretat.

L'ISO/IEC ha reservat la família de normes ISO 27000 per a tractar diferents aspectes d'aquesta temàtica, de la mateixa manera que s'ha dut a terme amb la qualitat i la família ISO 9000, o la gestió mediambiental amb l'ISO 14000. El treball sobre la família ISO 27000 és coordinat per un subcomitè (el subcomitè 27 –SC27– dins del JTC1: Joint Technical Committee 1) que s'organitza d'acord amb grups de treball dedicats a diferents temàtiques: sistemes de gestió de la seguretat de la informació, criptografia i mecanismes de seguretat, criteris d'avaluació de la seguretat, serveis i controls de seguretat, gestió d'identitats i tecnologies relacionades amb la privadesa, etc.

El conjunt de normes ISO 27000 estan creades per experts, sota la coordinació de l'organització ISO i IEC. Cal entendre que les normes que crea l'ISO es fan sota les característiques i els principis següents:

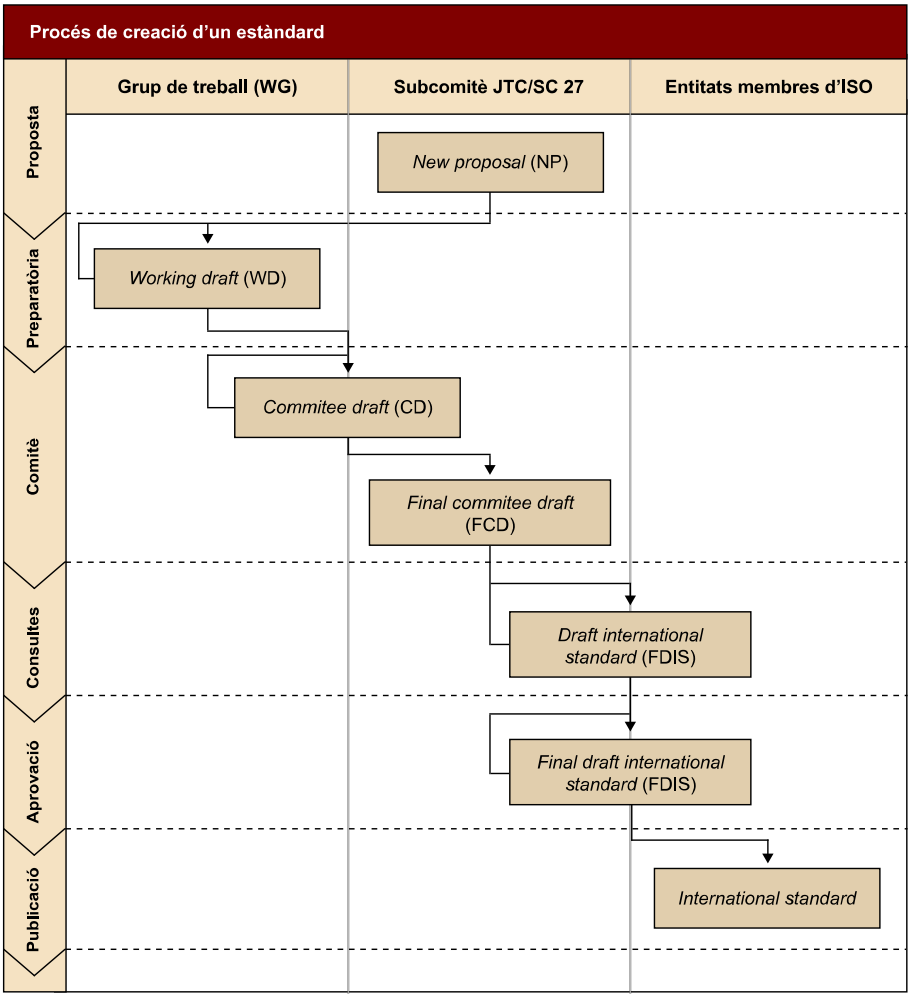
- Consens. Es té en compte el punt de vista de totes les parts involucrades: proveïdors, fabricadors, usuaris, grups de consumidors, laboratoris d'assajos i científics, governs, professionals reconeguts del sector i organitzacions investigadores.

- Àmplia aplicabilitat. Les solucions, les normes, els estàndards o els informes tècnics emesos han de ser d'aplicabilitat global, a tot el món.

- Voluntariat. La creació d'estàndards és un esforç autoregulat pel mercat, per la qual cosa tots els participants són parts rellevants d'aquest mercat i actuen de manera voluntària. Els voluntaris són acceptats d'acord amb

uns criteris que demostrin la pertinència de la seva acceptació i la vàlua professional.

Els estàndards que es creen segueixen un procés de sis fases, que s'inicia quan el subcomitè conjunt JTC/SC27 vota una nova proposta. Aquest procés està reflectit en el cicle de vida següent:



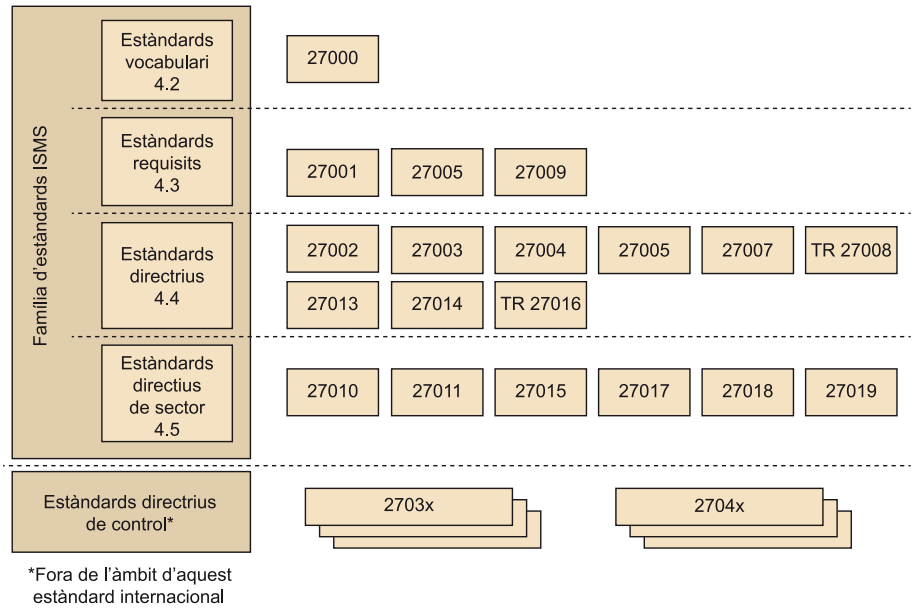
Cicle de vida d'un estàndard internacional ISO/IEC

És important notar que cada cinc anys els estàndards passen una fase de revisió i, en cas necessari, si es considera que els canvis seran molt profunds, el subcomitè inicia de nou el procés.

És interessant destacar que l'esforç d'organitzar les normes relacionades amb la gestió de la seguretat de la informació, sota un mateix grup de normes, té com a objecte tant fer més senzill el coneixement de les mateixes, com facilitar la seva promoció i posar fi al gran i variat nombre de normes, guies i informes tècnics que hi ha sobre la matèria. A més, respecte al material ja existent, s'està fent una tasca considerable d'actualització.

La família de normes ISO/IEC 27000 és un conjunt en evolució i creixement constants, però està organitzada amb una certa idea de jerarquia. La norma inicial que estableix els fonaments és l'ISO/IEC 27000, la qual és d'accés gratuït[2] i, a més de definir i unificar cert vocabulari, presenta de manera gràfica el conjunt i les relacions existents entre les diferents normes i es representa a continuació:

(2)Lloc web de l'ISO amb les normes gratuïtes: http://standards.iso.org/ittf/publiclyavailablestandards/



Conjunt de normes ISO/IEC 27000. Font: ISO/IEC 27000:2016

Les normes més interessants de comentar són les següents:

- La norma introductòria:
  - L'ISO/IEC 27000 proporciona una introducció i visió de conjunt de tot el marc ISO 27000 i facilita un glossari comú.

- Les normes que defineixen requeriments:
  - ISO/IEC 27001. És la norma que recull els requisits per a la implantació d'un sistema de gestió de la seguretat de la informació (ha estat traslladada al marc espanyol el 2007). La implantació d'un SGSI segons aquesta norma es pot certificar.

  - ISO/IEC 27006. És la norma que defineix els requeriments específics (aquesta norma en complementa una de més general, l'ISO/IEC 17021) per a entitats de certificació que vulguin acreditar-se en el marc de l'ISO/IEC 27000 i desitgin certificar SGSI contra la norma ISO/IEC 27001.

- Les normes que faciliten guies de bones pràctiques o de controls:
  - ISO/IEC 27002:2005. Es tracta del codi de bones pràctiques per a la gestió de la seguretat de la informació, i recull un complet i ampli catàleg de controls i bones pràctiques en la matèria. És el conjunt de

controls que la Norma ISO/IEC 270001 pren com a referència a l'hora de seleccionar controls de seguretat.

– ISO/IEC 27005:2008 facilita una guia per a la gestió dels riscos de seguretat de la informació, i proporciona un marc per a fer una anàlisi de riscos. Està inspirada en l'ISO/IEC Technical Report 13335-3.

– L'ISO/IEC 27003 facilita una guia per a implementar un SGSI segons la norma ISO/IEC 270001.

– L'ISO/IEC 27004 proveeix una guia i suggereix mecanismes per a mesurar l'eficiència d'un SGSI.

– L'ISO/IEC 27007 és una guia per a l'auditoria de SGSI (àmpliament basada en l'ISO 19011).

– L'ISO/IEC TR 27008 és un informe tècnic que dóna les guies per a l'auditoria dels controls de seguretat.

- Les normes de caràcter sectorial:
  – L'ISO/IEC 27010 ofereix guies per a la gestió de la seguretat en les comunicacions entre diferents sectors, posant especial relleu en infraestructures crítiques i sistemes industrials.

  – L'ISO/IEC 27011 defineix les directrius per a la gestió de la seguretat i la informació en el sector de les telecomunicacions. Estarà alineada amb una recomanació de l'ITU (X.1051).

  – L'ISO/IEC 27035 substitueix un informe tècnic ja existent amb modificacions menors i relacionat amb la gestió d'incidents de seguretat.

El treball del subcomitè JTC1/SC27 sobre tècniques de seguretat pot seguir-se en el lloc web de l'ISO[3].

(3)Lloc web de l'ISO amb totes les normes en les quals treballa el subcomitè JTC1/SC27: http://www.iso.org/iso/iso_technical_committee%3Fcommid%3D45306

Tot aquest marc normatiu està en continu desenvolupament i posa a disposició de les organitzacions les eines per tal que puguin implementar els seus SGSI conformement a les millors pràctiques reconegudes. Aquest marc normatiu contempla, a més, tots els aspectes dels SGSI: implementació, revisió, auditoria i certificació.

2. Certificació de SGSI contra l'estàndard ISO/IEC 27001

Fins ara, hem estat parlant dels sistemes de gestió de la seguretat de la informació (SGSI) com una eina per a millorar el bon govern de les TIC. Aquesta eina influeix per tant en el govern corporatiu, mitjançant la reducció dels riscos de la informació i, per tant, dels riscos en el negoci.

També hem vist que les organitzacions ISO i IEC han establert un marc de referència per a la gestió de la seguretat: la família de normes ISO 27000. D'aquest marc destaca la Norma ISO/IEC 27001, que dóna els requisits per a la implantació d'un SGSI. Per tant, les organitzacions interessades a millorar la gestió de la seguretat de la informació tenen a la seva disposició un marc de referència que, a més de recollir les millors pràctiques de la indústria en aquesta temàtica, pot ser certificat. És a dir, les organitzacions tenen l'oportunitat de certificar el seu SGSI (una vegada implantat) i exposar públicament que una tercera part confiable (l'entitat de certificació) ha auditat el seu SGSI i ha determinat que aquest s'ajusta a la norma. Això implica el reconeixement que la informació en l'organització està gestionada segons un marc que n'assegura la seguretat.

En aquest apartat, repassarem els avantatges que comporta una certificació i, posteriorment, descriurem les principals característiques de la Norma ISO/IEC 27001. Hi destacarem els aspectes de la norma que constitueixen un requisit i, per tant, són comprovats durant una auditoria de certificació.

2.1. Beneficis de la certificació

Els beneficis dels SGSI que s'han exposat anteriorment repercuteixen directament en el funcionament intern de les organitzacions. No obstant això, hi ha el problema de transmetre al mercat la millora que representa aquesta nova forma de gestió de la seguretat. La necessitat de certificar la gestió de la seguretat sorgeix de la dificultat de transmetre confiança en la manera com les organitzacions protegeixen la seva informació. Transmetre aquesta confiança a clients, proveïdors i societat en general és especialment crucial quan el servei o bé que s'intercanvien les organitzacions no és material, sinó que es tracta de simple i pura informació.

L'única manera de transmetre confiança en la gestió de la seguretat és superant una revisió independent de les mesures de seguretat de l'organització. Mitjançant aquesta revisió independent, les organitzacions certifiquen que la seva gestió és bona, i que es fa d'acord amb unes normes d'eficàcia reconeguda.

La certificació d'un SGSI no és un procés gaire diferent del d'altres tipus de certificacions i, per tant, té uns avantatges que són àmpliament reconeguts, i que són els següents:

- Factor diferenciador davant la competència. L'obtenció d'un certificat es pot publicitar. De fet, les entitats de certificació donen tot un seguit d'indicacions de la manera com es pot utilitzar el certificat per a l'autopromoció. Gràcies a aquest certificat, l'organització pot augmentar la seva reputació, credibilitat i confiança entre els clients i les organitzacions col·laboradores. El certificat és, per tant, un element diferenciador davant la competència.

- Reduir el nombre d'auditories de segones parts. Amb l'augment de l'externalització d'activitats que no es consideren primordials, les organitzacions proveïdores i clients es troben davant la necessitat d'intercanviar cada vegada més informació propietària. Davant aquest escenari, tradicionalment, les organitzacions clientes s'havien reservat el dret de fer auditories de segona part, per a verificar la seguretat dels processos aplicats sobre la seva informació en el proveïdor. No obstant això, el certificat demostra a la resta d'organitzacions (especialment clients) la capacitat per a gestionar correctament la seguretat de la informació. Per tant, no calen (o almenys estan menys justificades) auditories de segones parts. En tot cas, es podrà assegurar que hi ha un procés d'auditoria interna i es podran facilitar informes al client. Per tant, el certificat serveix com a demostració fefaent del tracte que es dóna a la informació facilitada pel client o per les organitzacions col·laboradores.
  És interessant comentar que les auditories que segueixen l'estàndard SAS70 de l'AICPA tenen per objecte cobrir aquest punt. Recordem del mòdul 1 que 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. No obstant això, aquest estàndard està centrat a auditar processos, persones, tecnologies i sistemes que poden tenir impacte en l'estat dels comptes financers. El seu abast no és, per tant, tan ampli com el que dóna la certificació de l'SGSI.

- Complir requisits del mercat (de clients o reguladors). Com s'ha dit en el punt anterior, alguns mercats s'han reglamentat fins al punt que l'existència d'un SGSI certificat és un valor afegit de què ja disposa la pràctica totalitat dels competidors (similar a la situació a la qual s'ha arribat amb els sistemes de gestió de la qualitat). Davant aquest escenari, és cada vegada més freqüent que l'obtenció de certificats sigui un requisit previ perquè dues organitzacions estableixin relacions de negoci (sempre que impliquin intercanviar informació). Per tant, l'obtenció d'un certificat facilita l'establiment de relacions comercials amb companyies de mida gran o institucions governamentals i, en general, obre noves possibilitats de negoci en entorns en què la certificació es veu com un requisit.

D'altra banda, de vegades, el requisit no és exactament disposar d'un SGSI certificat, sinó complir un marc legal determinat.

En el cas de la protecció de la privadesa, el marc legal seria el de la LOPD a Espanya o la HIPAA (*Health Insurance Portability and Accountability Act*) als Estats Units.

Un altre exemple de requisit podria ser la gestió correcta de la comptabilitat i dels riscos operatius o financers en societats que cotitzen en borsa. En aquest cas, el marc legal seria la *Sarbanes-Oxley Act* als Estats Units, i els acords de Basilea II en un àmbit més internacional. De manera més o menys general, aquests marcs legals exigeixen que els riscos als quals la informació està sotmesa estiguin gestionats adequadament. En aquestes situacions, l'organització pot acreditar, mitjançant la certificació del seu SGSI, que els riscos són gestionats i que es compleix el marc legal.

- Facilita o abarateix les primes de risc d'assegurances. Les organitzacions recorren, o fins i tot de vegades es veuen obligades, a contractar assegurances per a operar en un mercat determinat o amb un client determinat. Entre les organitzacions amb més interès en què se'ls demostri fefaentment que els riscos són gestionats correctament, hi trobem les companyies asseguradores. Les primes d'aquestes assegurances es poden veure reduïdes en cas que hi hagi un SGSI. En aquests casos, la companyia asseguradora exigirà que l'SGSI estigui certificat. Per tant, la reducció d'aquesta prima impacta positivament en el ROI de l'SGSI, i això és degut directament a la certificació de l'SGSI, i no tan directament a la seva pròpia existència.

- Augmenta la confiança interna en qualitat de la gestió de la seguretat. Des del punt de vista intern, la revisió periòdica de l'SGSI per part d'un tercer independent, l'entitat de certificació, aporta a la direcció més confiança en l'execució correcta del procés.
  L'operació d'un SGSI és una tasca complexa que necessita adaptar-se al llarg del temps. La necessitat d'adaptació pot estar motivada per una mala implementació d'algun aspecte de l'SGSI, o bé per una variació de l'entorn o dels objectius del negoci. Aquestes desviacions fan necessària l'execució d'auditories internes de manera periòdica. La confiança plena que el procés d'auditoria interna és correcte i serà capaç de detectar aquestes desviacions la proporciona el procés de certificació.
  Com es dirà més endavant, el procés de certificació no es produeix únicament en el moment en què s'avalua l'SGSI, sinó que es revisa amb una certa periodicitat, habitualment de manera anual. L'auditoria de certificació contínua permetrà a la direcció de l'organització certificada obtenir una comprovació que l'SGSI és capaç d'autocorregir-se i d'autoajustar-se a canvis de l'entorn.

- Augmenta la conscienciació en seguretat en tots els nivells de l'organització, des del nivell d'usuari fins a la mateixa direcció. Finalment, un altre benefici poques vegades apreciat en la certificació és la capacitat de conscienciar l'organització. D'una banda, l'SGSI dóna una gran importància a la formació i capacitació del personal en matèria de seguretat de la informació. D'altra banda, exigeix a la direcció un grau de compromís elevat amb la seguretat. Per tant, l'esforç de mantenir la certificació impli-

ca una renovació constant del compromís de la direcció i una formació contínua del personal en matèria de seguretat.

2.2. Reconeixement de la certificació

Tots els beneficis de la certificació de l'SGSI que s'han exposat anteriorment estan íntimament lligats al grau de reconeixement de l'entitat de certificació. Quan una organització que ha implantat un SGSI decideix fer el pas de certificar-lo, s'haurà de plantejar el grau de reconeixement que vol que tingui el seu certificat, és a dir, s'haurà de plantejar a quin mercat vol arribar i qui vol que conegui la seva certificació. Sobre la base de la resposta a aquestes preguntes, es decidirà per una entitat de certificació o una altra.

Aquesta decisió ens porta a dues preguntes: quin tipus d'autoritat té una entitat per a poder determinar que l'SGSI d'una organització s'ajusta a una norma? Fins a quin punt el mercat pot confiar en el treball d'aquesta entitat?

De manera general, una entitat de certificació és una institució legal que, a partir d'una auditoria de tercera part, certifica que l'auditat duu a terme una activitat d'acord amb un marc de referència. La capacitat per a poder certificar això es basa en el professionalisme dels auditors, la independència entre l'auditor i l'auditat, i l'ús de procediments estandarditzats i auditats per una entitat superior. En el mòdul anterior, s'ha al·ludit a l'existència de les entitats d'acreditació, que són les encarregades de garantir la qualitat del treball de les entitats de certificació.

2.3. Reconeixement de l'entitat d'acreditació

Part del reconeixement del certificat emès per una entitat de certificació és determinat pel nivell de reconeixement de l'entitat d'acreditació a la qual aquesta estigui adscrita. La mateixa Unió Europea reconeix la important tasca que l'acreditació representa per a cohesionar els diferents mercats europeus ("Principis de l'acreditació a Europa", certif. 9/94):

"L'acreditació és fonamental per al funcionament correcte d'un mercat transparent i orientat a la qualitat a Europa (Unió Europea i Espai Econòmic Europeu). És fonamental per a la indústria, que per a ser plenament competitiva necessita un servei adequat en aquest àmbit. És fonamental per a les autoritats públiques, tant nacionals com europees, a fi d'obtenir un grau suficient de confiança en els certificats expedits en qualsevol lloc d'Europa, i així facilitar la lliure circulació de productes a tot l'EEE. És fonamental per als mateixos organismes d'avaluació de conformitat (que operin tant en el sector regulat com en el no regulat), perquè puguin demostrar de manera independent la seva competència tècnica i per a garantir una competència transparent i orientada a la qualitat entre aquests."

Les entitats d'acreditació[4] són les encarregades de controlar, periòdicament, que les entitats de certificació fan les seves tasques d'acord amb les normes que regeixin la seva activitat. A més, les entitats d'acreditació són l'autoritat sobre aquest tema dins d'una àrea d'aplicació. Per tant, també hi ha un cert nivell de reconeixement per a les entitats d'acreditació. Habitualment, són organitzacions nacionals públiques o semipúbliques sense afany de lucre, i estan gestionades conjuntament per diferents organitzacions del mercat. Per tant, tenen un reconeixement implícit dins de la seva àrea d'actuació (habitualment un país).

(4)No s'han de confondre amb les entitats d'acreditació de l'àmbit de les infraestructures de clau pública (PKI: *public key infrastructure*), amb les quals no mantenen cap relació excepte que s'anomenen de la mateixa manera.

L'acreditació a Espanya

A Espanya, aquesta tasca recau en l'ENAC (Entitat Nacional d'Acreditació), una institució autònoma tutelada per l'Estat i designada per a mantenir el sistema d'acreditació nacional d'acord amb les normes internacionals i les directrius de la Unió Europea. Per tant, el seu reconeixement intern en el mercat espanyol és avalat per l'Estat.

Perquè els certificats tinguin un reconeixement ple fora de l'àmbit estatal, les entitats d'acreditació signen acords de reconeixement mutu o s'agrupen en entitats supranacionals que tenen la mateixa finalitat.

El procés d'acreditació, molt similar a un de certificació, té les característiques següents:

- L'organització que sol·licita l'acreditació ha de ser una entitat legalment identificable, amb personalitat jurídica. Abans de plantejar-se sol·licitar l'acreditació, haurà de disposar del personal i de l'experiència necessaris per a la realització de les activitats per les quals es vol acreditar. A més, haurà de conèixer i complir els criteris d'acreditació.

- L'avaluació de la capacitat tècnica es duu a terme en dues fases:
  - Estudi dels documents que descriuen la manera com l'entitat fa les activitats (sistema de gestió, mètodes i procediments de treball, competència del personal, etc.).
  - Avaluació *in situ* de com treballa l'entitat.

- Els resultats de l'avaluació es recullen en un informe que s'envia al sol·licitant, el qual ha de respondre indicant les accions correctores que consideri pertinents.

- Amb l'informe d'avaluació i la resposta del sol·licitant, la comissió d'acreditació pren una decisió. Si és positiva, s'emet el certificat d'acreditació.

Les acreditacions concedides són vigilades mitjançant avaluacions periòdiques, per a comprovar que les entitats acreditades continuen complint els requisits d'acreditació. Si en algun moment es constata que l'entitat incompleix

algunes de les obligacions de l'acreditació, es pot arribar a suspendre temporalment o retirar l'acreditació. Això es farà fins que es demostri de nou el compliment dels requisits d'acreditació.

2.4. Requisits d'una entitat de certificació

Les entitats d'acreditació vigilen que les entitats de certificació facin la seva feina d'acord amb diferents estàndards i procediments. Això és el que es denomina *procés d'acreditació de l'entitat de certificació*.

En el marc de la seguretat de la informació, la norma a la qual s'ha de cenyir el treball de l'auditor és, en termes generals, la Norma ISO/IEC 17021 (*Conformity assessment – Requirements for bodies providing audit and certification of management systems*). Aquesta norma està a més complementada per la Norma ISO/IEC 27006 (*Requirements for bodies providing audit and certification of information security management systems*), que ofereix certs detalls que han de servir de guia per a les entitats de certificació que es vulguin especialitzar en la certificació de SGSI.

Els requisits de la Norma ISO/IEC 17021 s'exposen a continuació:

Primerament, la norma parteix d'uns principis que són els que defineixen les bases que donen validesa a les auditories de tercera part. Aquests principis han de dirigir l'activitat de l'entitat de certificació, i el seu incompliment és clarament una amenaça. L'entitat de certificació ha d'obtenir la confiança del mercat amb la pràctica diària, mitjançant el compliment d'aquests principis. Una prova d'incompliment malintencionat d'aquests principis pot comportar la pèrdua de l'acreditació.

S'entén que aquestes auditories estan basades en els **principis** següents:

- **Imparcialitat**. S'ha de mantenir i transmetre imparcialitat al mercat perquè el judici que emet l'entitat de certificació sigui respectat. No obstant això, l'entitat de certificació competeix amb altres entitats de certificació i, per tant, l'auditat és el seu client. Això és una amenaça que s'ha de tractar escrupolosament.

- **Competència**. La qualitat del treball fet és directament proporcional al nivell de competència que tingui el personal en la matèria. Per tant, se n'haurà de cuidar la capacitació contínua.

- **Responsabilitat**. L'entitat de certificació és responsable d'executar les auditories de tercera part d'acord amb els principis i les normes establerts.

- **Transparència**. S'ha de facilitar obertament i veraçment informació sobre l'estatus d'un certificat o el procés de certificació, respectant sempre la confidencialitat de la informació concreta.

- **Confidencialitat**. Aquest principi limita l'anterior al mínim necessari per a informar adequadament el mercat sobre l'estat dels certificats emesos. En cap cas no es facilitaran detalls d'implementacions en els auditats.

- **Resolució de queixes**. Cal suposar que tot procés de certificació implicarà certes queixes, certs conflictes o diferències de parer entre l'auditat i l'entitat de certificació. Per tant, es pressuposa que l'entitat de certificació farà tot el possible per a investigar i resoldre aquests conflictes.

2.4.1. Requisits generals

A més dels principis que regeixen les auditories que fan les entitats de certificació, la Norma ISO/IEC 17021 té els **requisits generals** següents:

- **Responsabilitat legal**. L'entitat de certificació s'ha de constituir amb una forma legal que pugui assumir les conseqüències legals de les activitats que duu a terme.

- **Contracte / acords de certificació.** Tota auditoria de certificació ha d'estar enquadrada en un acord legal entre auditat i auditor.

- **Control sobre les decisions de certificació**. L'entitat de certificació ha de mantenir, en tot moment, el control sobre les decisions que afectin un certificat o procés de certificació, sense transferir mai aquest control a terceres organitzacions.

- **Gestió de la imparcialitat**. Tal com s'ha dit, la imparcialitat és un principi que guia totes les auditories de terceres parts i, per tant, de certificació. L'estàndard dóna els requisits sobre com s'han de gestionar les activitats que garanteixin aquesta imparcialitat.
  Els requisits que s'hauran de complir per a assegurar la imparcialitat són:
  – Cap unitat de l'entitat legal que constitueixi l'entitat de certificació no pot estar directament involucrada en tasques de consultoria.

  – L'entitat de certificació té el deure de vigilar situacions de risc per a la seva imparcialitat, per exemple controlant les relacions de les altres empreses del grup empresarial.

  – L'entitat de certificació s'haurà d'abstenir de participar en processos de certificació quan altres entitats vinculades a aquesta estiguin involucrades en la consultoria del sistema de gestió sota certificació. Es con-

sidera que han de passar almenys dos anys des del final de les tasques de consultoria.

– L'entitat de certificació haurà d'analitzar els riscos contra la imparcialitat i documentar quines mesures es prenen per a mitigar-los. A més, haurà d'estar en disposició de demostrar que s'han eliminat.

Les relacions típiques entre diferents entitats que poden posar en perill la imparcialitat de l'entitat de certificació són: mateixos propietaris o directiva, personal compartit, pagament de comissions per assenyalament d'oportunitat de negoci, recursos financers o materials compartits, etc.

- **Responsabilitats i finançament**. S'exigeix a les entitats de certificació que facin provisions de fons o contractin assegurances de responsabilitat per a cobrir, adequadament, els riscos de les seves operacions. Així mateix, se'ls exigeix estar en disposició de demostrar que les seves finances no comporten un punt de pressió que en pugui comprometre la imparcialitat.

- **Estructura organitzativa i comitè per a la imparcialitat**. L'estructura organitzativa de l'entitat de certificació també ha de complir certs requisits relacionats amb les funcions de la direcció. Té especial rellevància el fet que les entitats de certificació estan obligades a disposar d'un comitè que vetlli per la seva imparcialitat. Es tracta d'un comitè en el qual han d'estar representades les parts interessades en el procés de certificació. La Norma ISO/IEC 17021 suggereix que aquest comitè estigui constituït per:
  – Clients de l'organisme de certificació: organitzacions certificades per l'organisme de certificació, associacions empresarials o d'un altre tipus que tinguin interès que els seus associats siguin certificats.

  – Clients de les organitzacions els sistemes de gestió de les quals s'han certificat.

  – Administració: ministeris amb responsabilitats en l'activitat de què es tracti o organitzacions governamentals dedicades a la promoció de l'ús de sistemes de gestió.

  – Associacions de consumidors.

  – Entitats de certificació: personal que treballi per a l'entitat de certificació (s'inclouran en aquest grup totes les persones que hagin mantingut o mantinguin una relació amb l'entitat de certificació).

  El comitè té l'obligació de controlar la imparcialitat i les seves responsabilitats estan reflectides en l'estàndard. Si l'entitat de certificació desoeix les recomanacions del comitè, aquest ha de poder acudir lliurement a altres entitats per a reportar la situació, sempre que es respecti la confidencialitat de la informació manejada (informació de les empreses certificades o en procés de certificació).

- **Estructura i gestió dels recursos humans involucrats**. L'estàndard també especifica requisits respecte al personal involucrat en les auditories de certificació de sistemes de gestió. En general, s'exigeix que el personal involucrat es trobi en tot moment capacitat per a fer les assignacions que corresponguin. Per a això, s'exigeix que hi hagi uns processos documentats i clars sobre la selecció de recursos humans, la gestió de la seva formació, certificacions professionals que siguin necessàries i verificació de l'acompliment de les funcions d'auditoria. L'estàndard ISO/IEC 27006 aporta detalls més concrets dels requisits que han de complir els auditors. Aquests requisits estan alineats amb els corresponents de la Norma ISO 19011, la qual hem comentat en el mòdul anterior.
  D'altra banda, l'estàndard és flexible i permet l'ús d'auditors externs i també l'externalització de part de l'activitat. Això es pot fer sempre que hi hagi una signatura prèvia d'acords de confidencialitat i d'adhesió als mateixos procediments i principis que regeixen per a l'ens de certificació. Respecte a l'externalització, cal destacar que, en cap cas, no es pot externalitzar la decisió respecte a un certificat. Aquesta responsabilitat sempre ha de recaure en l'entitat de certificació, que es pot basar en treballs fets per entitats externes. A més, és interessant notar que l'estàndard dóna la possibilitat a l'auditat de rebutjar algun membre de l'equip auditor, i l'entitat de certificació estarà obligada a gestionar aquest conflicte.

- **Gestió de la informació relativa a la certificació**. Per tal de facilitar la transparència, la norma dóna certs requisits sobre quina informació s'ha d'oferir i de quina manera.
  - La informació que es faci pública ha de ser sempre veraç i no ambigua, incloent-hi la informació referent a publicitat dels seus propis serveis. Aquests requisits afecten, en gran manera, la informació que les entitats de certificació ofereixen públicament, sobretot a través de les seves pàgines web.

  - S'ha d'oferir informació sobre l'estat de cada certificat, tant al mateix auditat com a tota la comunitat. A aquesta última, s'ha d'oferir un directori de certificats amb l'estat de cadascun.

  - La norma estableix diferents requisits respecte a quina informació ha de ser confidencial (tot el relacionat amb el detall del procés de certificació). També estableix requisits sobre els acords de confidencialitat que hi ha d'haver entre els auditors propis, externs i experts.

2.4.2. Requisits específics sobre el procés de certificació

L'estàndard dóna els requisits que ha de complir el procés d'auditoria en totes les seves parts, des d'aspectes generals fins a la definició de les fases que s'han de passar i les tasques que s'inclouran en cadascuna d'aquestes fases.

Com a requisits generals, estableix:

- Hi ha d'haver un procediment per a seleccionar l'equip auditor i comunicar el perfil i l'historial professional d'aquest a l'auditat. D'aquesta manera, l'auditat pot fer comentaris i rebutjar algun membre si ho considera apropiat. Això inclou també l'obligació dels auditors d'informar sobre la seva imparcialitat.

- L'auditoria ha de ser planificada en temps i recursos. S'ha d'elaborar un pla d'auditoria i s'ha de documentar el temps previst i el finalment dedicat a l'execució. El dimensionament de l'auditoria tindrà en compte la grandària i la complexitat del sistema que s'ha d'auditar. La Norma ISO/IEC 27006 dóna unes taules per a ajudar a calcular l'esforç d'una auditoria sobre la base de diversos paràmetres. En aquest aspecte, l'ISO/IEC 17021 és menys precisa. A més, l'ISO/IEC 27006 proporciona més criteris per a complir els requisits de competència dels auditors en funció de la complexitat de l'SGSI que s'ha d'auditar.

Aquest conjunt estricte de requisits que s'aplica a les entitats de certificació és el que garanteix el reconeixement i el bon nom d'una determinada certificació.

2.5. Tipus d'auditoria en el procés de certificació

En el moment de definir els requisits sobre el procés d'auditoria de certificació, es tenen en compte diferents subtipus d'auditories que hi ha al voltant del procés de certificació: auditories inicials, auditories de seguiment i manteniment, auditories de recertificació, auditories especials, entre altres.

Les auditories inicials de certificació són les que constitueixen el cos central del contingut d'aquest mòdul. També són el tipus més desenvolupat i formalitzat per l'estàndard ISO/IEC 17021.

Vegeu també

En l'apartat "Procés de certificació de SGSI contra l'ISO 27001", es detallarà com s'ha de fer aquest procés d'acord amb la Norma ISO/IEC 27006.

Les auditories de seguiment i manteniment s'utilitzen per a comprovar que l'auditat continua complint el marc de referència. Cal notar que l'auditoria certificarà la situació de l'SGSI en un moment donat, per la qual cosa totes les entitats de certificacions atorguen el seu segell de certificació amb una validesa definida en el temps (habitualment, tres anys). Durant aquest període de validesa, l'organització certificada haurà de passar auditories de seguiment i manteniment per a demostrar que el seu SGSI continua complint la norma de referència. Passat el temps de validesa de la certificació, l'organització se sotmetrà a una auditoria de renovació. L'abast de les auditories de seguiment és molt més reduït que el de la de certificació o renovació, mentre que la de certificació i de renovació tenen un abast idèntic o almenys molt similar.

Finalment, les auditories de recertificació s'usen en els casos en què una organització ha vist revocat o suspès temporalment el seu certificat, i les auditories especials s'usen per a la resolució o investigació de queixes.

2.6. Estructura de l'estàndard ISO/IEC 27001

La Norma ISO/IEC 27001 va ser aprovada l'octubre del 2005 i revisada el 2013. En tractar-se d'una norma que té un ampli seguiment, segueix en contínua millora, per la qual cosa es pot esperar que es produeixin revisions futures. No obstant això, no és la primera en la seva especialitat. L'organització britànica d'estandarditzación BSI (British Standard Institute) va crear la Norma BS-7799 ja el 1995, que contenia una primera versió del catàleg de bones pràctiques per a la seguretat de la informació. Aquesta mateixa organització va crear posteriorment, el 1999, la Norma BS-7799-2, amb els requisits per a un sistema de gestió de la seguretat de la informació que escollís els seus controls de la BS-7799. Totes dues normes van ser la base per a la creació de les normes ISO/IEC 27002:2005 i ISO/IEC 27001:2005, respectivament. La Norma ISO/IEC 27002:2005 va ser inicialment l'ISO/IEC 17799:2000, que es va revisar el 2005 i va donar lloc a l'ISO/IEC 17799:2005. El 2007, aquesta norma va experimentar un canvi de denominació que va donar lloc al nom actual: ISO/IEC 27002:2005. No obstant això, com que únicament es tracta d'un canvi de denominació, no se n'ha modificat l'any d'aprovació (2005). L'última gran revisió realitzada va ser l'any 2013, quan es va modificar substancialment l'orientació del model de referència per a la millora continuada sobre el qual implementar els sistemes de gestió de la seguretat de la informació, proporcionant més claredat i també més flexibilitat.

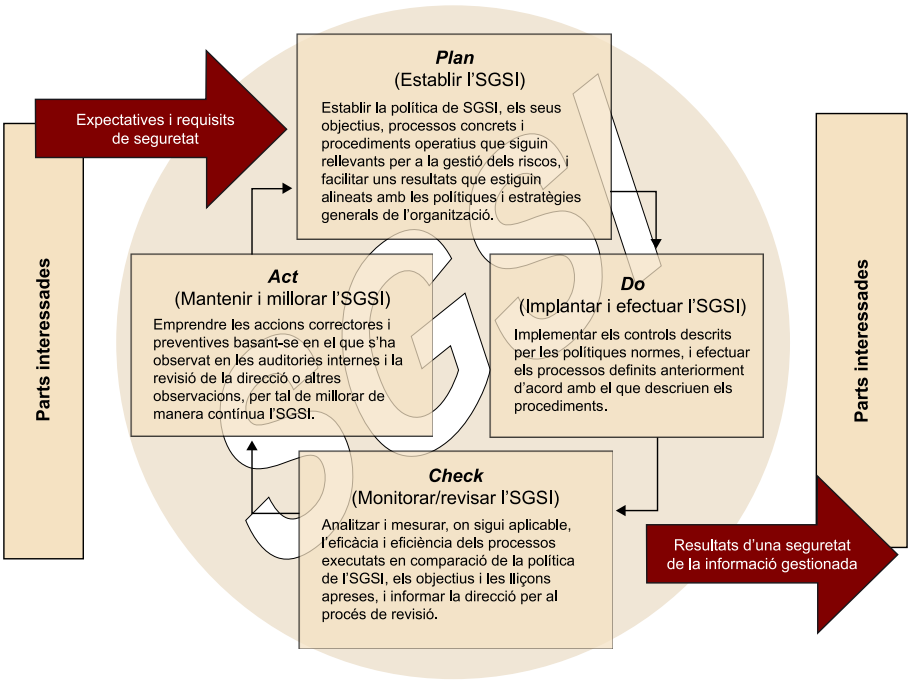
Actualment, l'ISO/IEC 27001 és l'únic estàndard acceptat internacionalment per a la gestió de la seguretat de la informació, i es pot aplicar en tot tipus d'organitzacions, sigui quina sigui la seva grandària o activitat. No obstant això, cal tenir en compte que malgrat que és un estàndard sobre seguretat de la informació i està molt lligat als sistemes d'informació, no és un estàndard sobre aspectes tecnològics sinó organitzatius, molts dels quals relacionats amb la gestió de les TIC, encara que no únicament. També s'hi tracten aspectes relatius a l'estructura organitzativa, la continuïtat de negoci i la conformitat legal. Per tant, és un estàndard que aborda la seguretat des d'un punt de vista holístic, combinant tots els aspectes que tenen una influència clara sobre aquesta.

S'ha d'entendre que l'SGSI plantejat per la norma està basat en uns principis:

- Suport de la direcció.
- Adaptabilitat de l'SGSI a la situació de l'organització.
- Aproximació a la gestió basada en processos de millora continuada i l'anàlisi de riscos i oportunitats.

La versió de 2005 plantejava molt fermament que el model de gestió continuada de la seguretat de la informació havia de basar-se en el conegut model PDCA. No obstant això, tal com s'ha comentat en apartats anteriors, en la revisió de 2013 aquesta visió tan rigorosa d'implementar el model PDCA va ser eliminada amb la finalitat de facilitar l'alineament de totes les normes d'estandardització de sistemes de gestió fetes per l'ISO i descrites en l'annex SL de la part 1 de les directives ISO/IEC. Aquesta flexibilització fa que, actualment, un SGSI pugui inspirar-se en altres models de millora contínua també molt populars, com per exemple SIX-SIGMA, basat en el model DMAIC (*define*, *measure*, *analyze*, *improve*, *control*), que d'altra banda està directament inspirat en el clàssic model de Deming PDCA. Amb la qual cosa, no hi ha molta diferència entre el plantejament de la norma de 2005, basat en el model PDCA, i l'actual de 2013, que no declara exactament quin model seguir, però sí que organitza els requeriments en un conjunt de set punts de compliment obligat.

L'aplicació del model PDCA, tal i com es planteja a la versió de 2005, a l'entorn de la seguretat de la informació es mostra en el diagrama següent. En aquest diagrama s'indiquen, de manera genèrica, les tasques associades a cadascuna de les fases del cicle PDCA.



Model PDCA per a l'SGSI segons Norma ISO/IEC 27001:2005

En comparació, la norma de 2013 va eliminar tota referència explícita a qualsevol model de gestió, però defineix set capítols principals que tot SGSI ha de complir (numerats segons la norma):

4. Context de l'organització,

5. Lideratge,

6. Planificació,

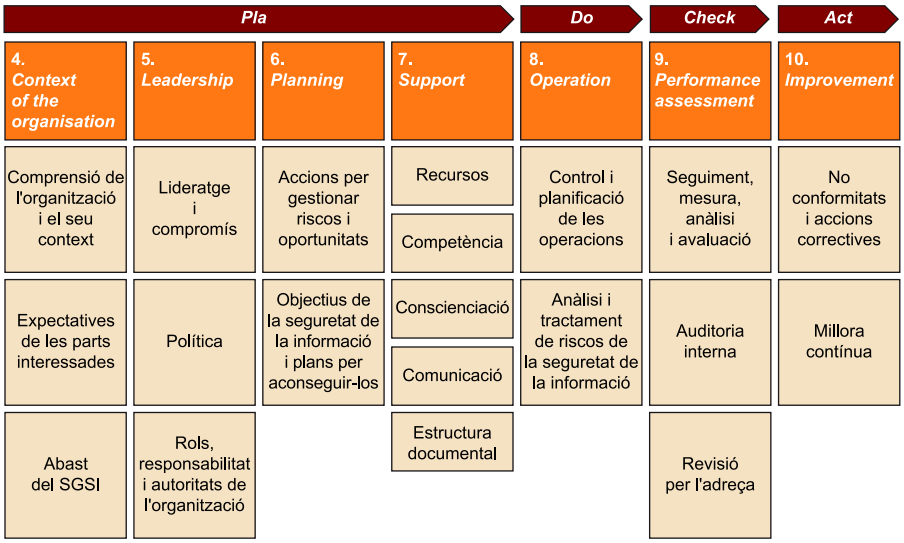
7. Suport,

8. Operació,

9. Avaluació de l'acompliment,

10. Millora.

Aquests punts poden assumir-se com a necessaris en qualsevol model de millora continuada. El següent diagrama indica en la fila superior les clàssiques fases del model PDCA i es pot observar com s'ajusta als diferents requeriments que han de complir els sistemes de gestió normalitzats per l'ISO. A més, en la pràctica ha comportat una clarificació de conceptes i simplificació a l'hora d'implantar aquests sistemes de gestió.



Alineament entre el model PDCA i els requeriments unificats per l'ISO per a tots els sistemes de gestió

Tant en la versió de 2005 com en la de 2013, es veu que el punt principal de partida del model és la comprensió dels requeriments de seguretat que ha de complir l'SGSI. En la versió de 2005 es parla d'expectatives i requeriments de les parts interessades (en anglès, *stakeholders*), mentre que en la de 2013 es parla de definir el "context de l'organització". En qualsevol cas, el que es vol expressar és que l'SGSI ha de complir amb les necessitats de l'organització i l'entorn en el qual es mou, i ha de produir uns resultats que compleixin aquests requisits. Els resultats, obtinguts mitjançant l'execució del cicle PDCA o qualsevol altre model de gestió, i requereix la implantació, l'operació i el mesurament d'uns controls de seguretat, els quals han de gestionar els riscos identificats per una anàlisi de riscos. L'anàlisi de riscos constitueix una de les pedres angulars del sistema i, per tant, és una part obligatòria. Totes les decisions s'han de basar en aquesta anàlisi. En aquest aspecte, no hi ha hagut canvi de parer entre les versions de 2005 i 2013, encara que sí que s'han flexibilitzat els requeriments

aplicables al procés que determinen les accions necessàries per a identificar, avaluar i tractar els riscos i les oportunitats. Igualment, amb la finalitat de facilitar la tasca d'alinear els diferents tipus de sistemes de gestió estandarditzats per l'ISO/IEC, per a aquest procés s'han donat unes directrius en una norma separada i comuna a tots aquests sistemes de gestió, l'ISO/IEC 31000, i així s'esmenta expressament en el text de la norma ISO/IEC 27001:2013.

Per tant, podem concloure que la gestió de la seguretat, ja sigui segons el clàssic model PDCA o qualsevol altre, constitueix un dels requisits generals de l'estàndard. La implementació d'un procés que no dugui a terme alguna de les fases o que, d'alguna manera, no es pugui relacionar amb el model, constituiria una no-conformitat greu que impediria la certificació del sistema de gestió.

Els requisits de l'estàndard ISO/IEC 27001:2013 estan organitzats en set parts. En les seccions següents, repassarem cadascuna d'aquestes parts de l'estàndard i destacarem els requisits que es revisaran especialment en una auditoria de certificació.

2.6.1. Definir el context de l'organització

Aquest tema es tracta en el punt 4 de l'estàndard Context de l'Organització, queinclou:

- **4.1 Comprensió de l'organització i del seu context**. L'organització ha de conèixer i també ser capaç de transmetre durant l'auditoria (probablement mitjançant algun tipus d'informació documentada) aquelles circumstàncies del seu entorn que porten a la necessitat de controlar la seguretat de la informació i que, al cap i a la fi, imposen a l'SGSI la implantació de determinats requeriments globals.

- **4.2 Comprensió de les necessitats i expectatives de les parts interessades**. Dins del context, mereix una part específica el fet de reconèixer que l'organització pot tenir altres parts interessades (clients, reguladors de mercat, altres empreses del seu grup empresarial, etc.) que també establiran requeriments a l'SGSI. Igualment, en l'auditoria, l'organització ha de poder mostrar que s'ha identificat a totes aquestes parts i els requeriments que imposen.

- **4.3 Determinació de l'abast de l'SGSI**. Aquest apartat és el que específicament exigeix a l'organització documentar quin és l'abast de l'SGSI, sobre quina part de l'organització (àrees de negoci, processos, persones, infraestructures físiques, infraestructures de TIC) aplica l'SGSI i també que el relacioni amb els requeriments dels punts 4.1 i 4.2. Aquest és el punt que l'auditor verificarà en allò que la norma defineix com a "informació documentada".

Informació documentada

La norma no especifica quina forma ha de prendre una "informació documentada", ja que actualment pot adoptar diverses formes i, per tant, ja no parla de documents concrets, sinó que demana que la informació estigui documentada conformement als requeriments que imposa en el punt 7.5.

2.6.2. Suport i lideratge per part de l'alta direcció

En el marc de l'SGSI, s'exigeix un alt compromís per part de la direcció, especialment de l'alta gerència. Aquest compromís ha de quedar plasmat i evidenciat pels seus actes. Es troba tractat de manera general en el punt 5 de l'estàndard Lideratge, però determina el següent:

- **5.1 Lideratge i compromís**. És crucial que l'SGSI compti amb el suport i lideratge de la màxima autoritat de l'organització atès que, d'una altra manera, no es pot garantir que l'SGSI pugui aconseguir els seus objectius, ja que l'alta direcció és qui garanteix els recursos i, alhora, qui ha de facilitar l'alineament de l'SGSI amb els objectius de negoci de l'organització. L'auditor comprova habitualment aquest punt mitjançant una reunió amb l'alta direcció, en la qual s'expliquen els objectius de negoci i els de l'SGSI i la manera en què l'alta direcció intervé en la governança de l'SGSI.

- **5.2 Política**. Aquest punt recull el compromís de la direcció en forma d'una política de seguretat recolzada per ella mateixa en forma d'informació documentada que l'auditor verificarà.

- **5.3 Rols, responsabilitats i autoritats en l'organització**. Dins de la faceta de lideratge hi ha la qüestió de com s'organitzen les diferents responsabilitats dintre de la governança de la seguretat. No es requereix una informació documentada, però l'auditor necessitarà conèixer com es reparteixen les funcions, i això sol resultar més fàcil quan es troben documentades.

2.6.3. Planificació

En aquest punt l'SGSI defineix els seus objectius d'acord amb allò establert anteriorment i a l'anàlisi de risc. Es desenvolupa en el punt 6 de l'estàndard, el qual inclou 2 aspectes fonamentals:

- **6.1 Accions per tractar els riscos i les oportunitats**. És en aquest apartat on s'imposen els requeriments relatius a la manera en què l'organització analitza el risc i el gestiona. L'estàndard no imposa aspectes molt concrets sobre com realitzar el tractament de riscospel que fa a la pràctica, però sí que demana el següent:
  a) prendre en consideració el context,
  b) identificar els riscos i les oportunitats per a la consecució dels objectius de l'SGSI,
  c) escriure i reflectir la metodologia de tot el procés, des de l'apreciació, l'avaluació i el tractament, mitjançant alguna informació documentada.
  No es donen requeriments concrets. Per tant, hi ha flexibilitat en les metodologies, però sí que s'entén que el procés ha de ser formal, ja que s'exigeix que es generin resultats consistents, vàlids i comparables.

d) Definir bé en el procés quins són els criteris per a l'apreciació del risc (identificar els riscos), per a l'avaluació (determinar el nivell de risc segons probabilitats d'ocurrència i impacte), així com els criteris segons els quals es tractarà el risc (no s'indica en l'estàndard, però habitualment són eliminar, reduir, o transferir).

e) Identificar un propietari per a cada risc, el qual a priori no té perquè ser directament l'alta direcció.

f) A l'hora de tractar el risc, l'estàndard exigeix que existeixi:

– Declaració d'aplicabilitat que ha d'indicar quins controls són seleccionats per tractar el risc. Aquests controls han d'escollir-se d'entre els inclosos en l'annex A de la norma ISO/IEC 27001, que és una translació literal de tots els controls de la norma ISO/IEC 27002, però es dóna llibertat a l'organització per incloure altres dissenyats per ella mateixa (en conseqüència, es poden prendre altres catàlegs de bones pràctiques, com per exemple, CoBIT o d'altres). De cada control s'ha d'indicar:

  1) Si aplica o no juntament amb la seva justificació, tant pel que fa a la inclusió com a l'exclusió.

  2) Si està implementat.

– Pla de tractament del risc. Pot ser el conjunt de projectes o activitats que es derivin de les decisions preses per tractar els riscos.

g) Tot el resultat del procés, inclosos els nivells finals de risc residual, ha de tenir l'aprovació per part del propietari del risc.

- **6.2 Objectius de seguretat de la informació i planificació per a la seva consecució**. Juntament amb l'anàlisi de riscos, aquest és l'altre gran eix per poder gestionar la seguretat en ser la manera d'avaluar si el SGSI està o no aconseguint els seus objectius.

  L'estàndard demana que:

  – Han de ser uns paràmetres de seguretat objectius. No és necessari que hi hagi una relació directa amb els controls aplicats (en anteriors versions de la norma s'entenia que havia de ser així) i s'han d'adaptar a la política de seguretat i al context de l'SGSI.

  – Han de ser preferiblement mesurables, encara que la norma ja indica que només si és possible. En la pràctica, és necessari que aquests siguin mesurables per complir la resta de requeriments de l'apartat, ja que han de ser comunicats.

  – S'ha de definir una planificació i assignació de recursos per realitzar el seguiment i la consecució dels objectius.

2.6.4. Suport

En aquest punt es defineixn els requeriments sobre els recursos que han de donar suport a l'SGSI en tots els seus aspectes. Es tracta en l'apartat 7 de l'estàndard i es recolza en 5 punts:

- **7.1 Recursos**. És necessari que hi hagi prou recursos (en sentit ampli: dedicació de persones, sistemes d'informació, instal·lacions, etc.) per a aconseguir els objectius de l'SGSI.

- **7.2 Competència**. És necessari que les persones que operen els diferents aspectes relacionats amb la seguretat estiguin degudament formades i de manera continuada. Hi ha d'haver suport documentat d'aquest pla de formació.

- **7.3 Conscienciació**. Tot el personal sota l'abast de l'SGSI ha de ser conscient de la política de seguretat de la informació i, en general, estar conscienciat de la seguretat en la mesura que afecti la seva activitat.

- **7.4 Comunicació**. Hi ha d'haver un procés per a comunicar tots els aspectes relacionats amb la seguretat, tant per a realitzar-los internament com externa.

- **7.5 Informació documentada**. Han de quedar documentats diversos aspectes de l'SGSI, d'una banda tots aquells necessaris segons la norma (explícitament la norma indica que determinats aspectes han de quedar en una informació documentada) i, en general, tots aquells que calguin per a l'operació de l'SGSI. La norma defineix els requeriments que apliquen, encara que no indica de cap manera en quin suport o en quina forma ha de ser. Fonamentalment, és necessari que la informació estigui correctament identificada, versionada, segueixi un procés de revisió i aprovació, i que estigui disponible i protegida d'acord amb el seu nivell de necessitat de confidencialitat.
  A continuació es detalla la informació documentada que la norma exigeix com a mínim:
  - abast,
  - política de seguretat de la informació,
  - procés d'avaluació i tractament del risc,
  - declaració d'aplicabilitat,
  - pla de tractament del risc,
  - objectius de seguretat de la informació,

- evidències de la capacitació o competència,
- qualsevol informació documentada d'origen extern a l'organització que sigui rellevant per a l'SGSI,
- qualsevol informació documentada referent a l'SGSI, com per exemple, procediments operatius,
- evidències del monitoratge i la mesura dels processos de l'SGSI,
- programa d'auditoria de l'SGSI i informació sobre les no conformitats,
- evidències de la revisió de l'SGSI per part de la direcció.
  No és estrictament necessari, però sí recomanable, que estiguin documentats els següents aspectes:
- procés de comunicació, així com les diferents comunicacions realitzades,
- mètodes per al monitoratge i la mesura dels processos de l'SGSI,
- rols, responsabilitats i autoritats.

2.6.5. Operació

En el punt 8 de la norma es recull la necessitat que l'organització operi els diferents processos que es deriven de l'aplicació del pla de tractament de riscos i l'operació dels controls seleccionats. Així mateix, en aquest punt es determina la necessitat de realitzar revisions de l'avaluació dels riscos a intervals planificats o bé quan es produeixin canvis importants. Això es realitza d'acord amb com s'hagi establert en el procés d'apreciació del risc, definit en aplicar el punt 6.1 de la norma.

2.6.6. Avaluació de l'acompliment

Aquest apartat 9 de la norma recull la fase de revisió d'un model de millora contínua. Es recolza en 3 punts:

- **9.1 Seguiment, mesura de l'anàlisi i avaluació**. L'eficàcia de l'SGSI i de la seguretat de la informació ha de ser avaluada. Hi ha d'haver informació documentada del resultat d'aquest monitoratge, per la qual cosa l'organització ha de determinar sobre què és necessari fer seguiment, què és necessari mesurar (processos, controls), com es realitzen el seguiment i el mesurament, cada quant es realitzen i qui és responsable de realitzar-los.

Aquests resultats són necessaris per a la revisió global de l'SGSI per part de la direcció.

- **9.2 Auditoria interna**. En aquesta es detallen els requeriments que han de complir les auditories internes, que a més han de ser coherents amb les directrius donades en la norma ISO/IEC 19011. Hi haurà d'haver un programa d'auditoria interna perquè hi hagi auditories de primera part que tinguin en compte:
  – possibles marcs regulatoris,
  – requeriments de seguretat de l'SGSI,
  – resultats d'auditories prèvies.

  Les responsabilitats assignades, els requeriments donats al programa d'auditoria i els resultats de les auditories internes han d'estar definits al programa i és necessari que hi hagi evidència de la seva execució per mitjà d'informació documentada.
- **9.3 Revisió per la direcció**. Es detallen els requeriments de la direcció de cara a revisar l'SGSI. S'ha de documentar la periodicitat de revisió, la qual se suggereix que no sigui superior a un any. Així mateix, és necessari que els resultats de la revisió realitzada per la direcció es desin com a part dels registres de l'SGSI.
  La revisió de la direcció ha de tenir en compte:
  – Noves vulnerabilitats i/o amenaces que no s'haguessin tingut en compte en l'última anàlisi de riscos o en els resultats de les apreciacions del risc realitzades durant l'operació de l'SGSI.
  – Els resultats d'auditories de l'SGSI.
  – Qualsevol tipus de retorn que es rebi de les parts interessades.
  – Tècniques, productes o procediments que podrien ser utilitzats per l'organització per a millorar l'eficiència i eficàcia de l'SGSI.
  – L'estatus de les accions correctives i preventives preses en el procés de revisió i manteniment de l'SGSI.
  – Resultats sobre els mesuraments de l'efectivitat dels controls.
  – El seguiment de les anteriors decisions del procés de revisió per part de la direcció.

  Els resultats de la revisió realitzada per la direcció han de quedar en forma d'informació documentada i incloure les decisions i accions empreses per tal de:

– millorar l'efectivitat de l'SGSI,

– modificar els procediments o controls necessaris per a respondre a canvis en les circumstàncies que envolten el negoci (nous requeriments o contractes, redisseny de processos de negocis, etc.),

– millorar la gestió dels recursos assignats a la gestió de l'SGSI.

2.6.7. Millora

Es determina en el punt 10, on es detallen els requeriments que han de complir les accions correctives i el tractament de les no conformitats destinades a millorar l'SGSI de manera contínua.

Les accions correctives tenen per objecte corregir i evitar la reaparició de no conformitats en l'SGSI. Hi ha d'haver un procediment documentat per a la detecció i realització de les accions correctives, el qual ha d'incloure els passos a seguir per tal de:

- Identificar no conformitats i determinar-ne causa.

- Preveure no conformitats potencials mitjançant la identificació de canvis o nous riscos en una actualització de l'anàlisi de riscos.

- Determinar i implementar les accions preventives (tot i que aquest concepte ha desaparegut en la versió de 2015 en comparació amb la versió de 2005, és rellevant i indirectament hi està recollit) que garanteixin que no reapareguin les no conformitats ja detectades i que no es materialitzin les potencials.

- Registrar els resultats de les accions realitzades.

- Revisar les accions dutes a terme.

3. Procés de certificació de SGSI contra l'ISO 27001

En els apartats anteriors, s'han tractat temes com els sistemes de gestió de la seguretat de la informació, i la certificació dels SGSI contra la Norma ISO/IEC 27001. No obstant això, no s'ha entrat detalladament en la descripció del procés ni en les tasques que durà a terme un auditor.

En aquest apartat, aprofundirem en el procés que se segueix per a fer una auditoria de certificació d'un SGSI segons la Norma ISO/IEC 27001. Aquest procés està regit per la Norma ISO/IEC 27006, la qual ja s'ha explicat en part. Aquí es tractaran els aspectes més pràctics del procés d'auditoria.

És important que quedi clar que el certificador no pretendrà dir si una organització és més o menys segura. El que pretén és verificar que l'organització gestiona la seguretat de la informació i té les eines adequades per a fer aquesta gestió de manera correcta. En definitiva, el certificador verifica l'SGSI.

3.1. Objectius del procés d'auditoria de certificació

Com s'ha dit, l'objectiu d'aquests processos de certificació és verificar la implantació correcta de la Norma ISO/IEC 27001, la qual fa referència a la gestió de la seguretat de la informació.

Els SGSI implantats per cada organització no han de ser necessàriament iguals. Les característiques de cada SGSI dependran de les particularitats de cada organització. L'ISO/IEC 27001 no obliga a tenir una determinada configuració dels aspectes de seguretat. La norma només indica els requisits del sistema de gestió i, a partir d'aquests requisits, cada organització determinarà com ha d'implantar el seu sistema de gestió.

3.1.1. Revisió de la implantació del model de millora contínua

Durant el procés de certificació, l'auditor tractarà de verificar que l'organització ha implantat l'SGSI seguint un model de millora contínua, d'acord amb els requisits de l'estàndard. És important destacar que el procés d'auditoria no examina el nivell de seguretat d'una organització, sinó que tracta només de verificar que la seva gestió de la seguretat s'ajusta a l'estàndard.

Per tant, l'auditor no pretén trobar incompliments en mesures concretes de seguretat, sinó garantir i verificar que l'organització:

- Té un sistema que permet gestionar la seguretat de la informació.
- Té les eines adequades per a implementar aquest sistema de manera correcta.

- Està capacitada per a millorar aquest sistema amb el pas del temps.

Si això és així, s'entén que l'organització coneix els seus riscos i té els mitjans necessaris per a controlar-los i anar millorant els controls que hi aplica.

L'auditor podria dictaminar si un determinat aspecte de la seguretat d'una organització és correcte o incorrecte. No obstant això, el que realment verificarà és que s'han disposat les mesures necessàries per a complir el model de gestió de millora contínua definit per l'estàndard.

Conceptualment i per simplicitat, prendrem com a referència el model de gestió clàssic PDCA, encara que no sigui explícitament necessari que l'SGSI implementat per una organització estigui plantejat segons els seus termes concrets.

El punt de partida de la revisió de l'auditor serà la fase "PLAN". En aquesta fase de la implantació de l'SGSI, es defineix l'abast del sistema de gestió, s'obté el compromís i el lideratge de la direcció i es fa l'anàlisi de riscos. Tota auditoria haurà de comprovar, mitjançant una reunió amb l'alta direcció, el seu nivell de compromís i alineament de l'SGSI amb els objectius de l'organització així com el seu compromís i la seva revisió de l'SGSI. D'altra banda, tota revisió que farà l'auditor estarà basada en l'anàlisi de riscos de l'organització. Recordem que l'anàlisi de riscos permet identificar quins controls de seguretat s'han d'implantar en una organització.

En la revisió de l'anàlisi de riscos, l'auditor no comprovarà que aquest està fet correctament, sinó que s'ha dut a terme amb la metodologia correcta. A més, l'auditor comprovarà que la direcció coneix aquesta anàlisi, que ha aprovat el seu enfocament i que assumeix els riscos que s'hi han detectat. Partint d'aquests riscos, l'auditor tractarà de verificar que s'han implantat les mesures de seguretat necessàries per a mitigar-los.

L'auditor pot dictaminar que l'anàlisi de riscos és incorrecta, en cas que s'hagi utilitzat una metodologia incorrecta, l'anàlisi no es correspongui amb l'abast de l'SGSI o no es fonamenti en actius, amenaces i vulnerabilitats. En circumstàncies normals, no obstant això, l'auditor assumirà que els riscos que l'organització ha considerat són els que realment l'afecten.

L'organització haurà de mostrar i defensar, davant l'auditor, la implantació d'unes determinades mesures de seguretat d'acord els riscos detectats.

Tornant al model PDCA, un altre dels aspectes més importants que l'auditor verificarà és com l'organització millora o actua (fase "ACT") segons els indicadors que hagi establert el seu sistema de gestió de la seguretat de la informació.

Hi ha tres maneres de millorar l'SGSI, partint de:

1) Apreciació periòdica del risc,

2) Evidències de funcionament de l'SGSI,

3) Resultats de l'auditoria interna.

Durant el procés d'auditoria, es tractarà de verificar que hi ha un procés de revisió per part de la direcció basat en aquests punts d'informació, que són coneguts per l'organització i que s'utilitzen per a aplicar els canvis en la seguretat.

3.1.2. Revisió dels controls ISO/IEC 27002

Quan l'auditor revisa la fase *do* del model PDCA, tractarà de determinar si els controls s'han implantat realment, i si s'ha fet tal com s'ha documentat.

Convé recordar que la selecció de controls és un dels elements més importants del que exigeix l'estàndard. Aquests controls, que són un element més dins del sistema de gestió, estan recollits en la Norma ISO/IEC 27002, encara que es poden utilitzar altres catàlegs de controls, com el COBIT. Si l'organització considera útil utlitzar altres catàlegs, l'SGSI implantat seguiria sent certificable.

Els catàlegs de controls, com per exemple ISO/IEC 27002 o COBIT, són altres normatives existents en l'àmbit de la seguretat de la informació, però no són auditables en si mateixos. Com que es tracta de catàlegs de bones pràctiques, contenen tot un seguit de controls que es poden o no implantar en una organització concreta. Únicament després d'un procés d'anàlisi del risc, l'organització estarà en disposició de fer una selecció coherent i fonamentada dels controls aplicables. Per tant, no és possible auditar la implantació de catàlegs de controls com la Norma ISO/IEC 27002. Són un element més, encara que fonamental, dels sistemes de gestió de la seguretat.

D'altra banda, hi ha la possibilitat de fer una anàlisi del grau d'implantació del catàleg de controls d'una norma. Se sol denominar *gap analysis*, i consisteix a determinar, per a cadascun dels controls, si està implantat i en quina mesura. No obstant això, aquesta anàlisi no permet treure conclusions sobre la qualitat de la gestió de la seguretat, ja que falta l'avaluació dels riscos que aquests controls pretenen controlar.

3.2. Procés d'auditoria

Dins dels diferents tipus d'auditories que distingeix l'estàndard ISO/IEC 27006, el tipus descrit amb més detall és el de l'auditoria inicial. De manera general, l'estàndard obliga les entitats de certificació a seguir un procés de, com a mínim, dues fases en l'auditoria inicial. Les fases se solen denominar *stage 1* i *stage 2*, encara que les entitats de certificació les poden denominar d'altres maneres.

Denominació comuna de les fases

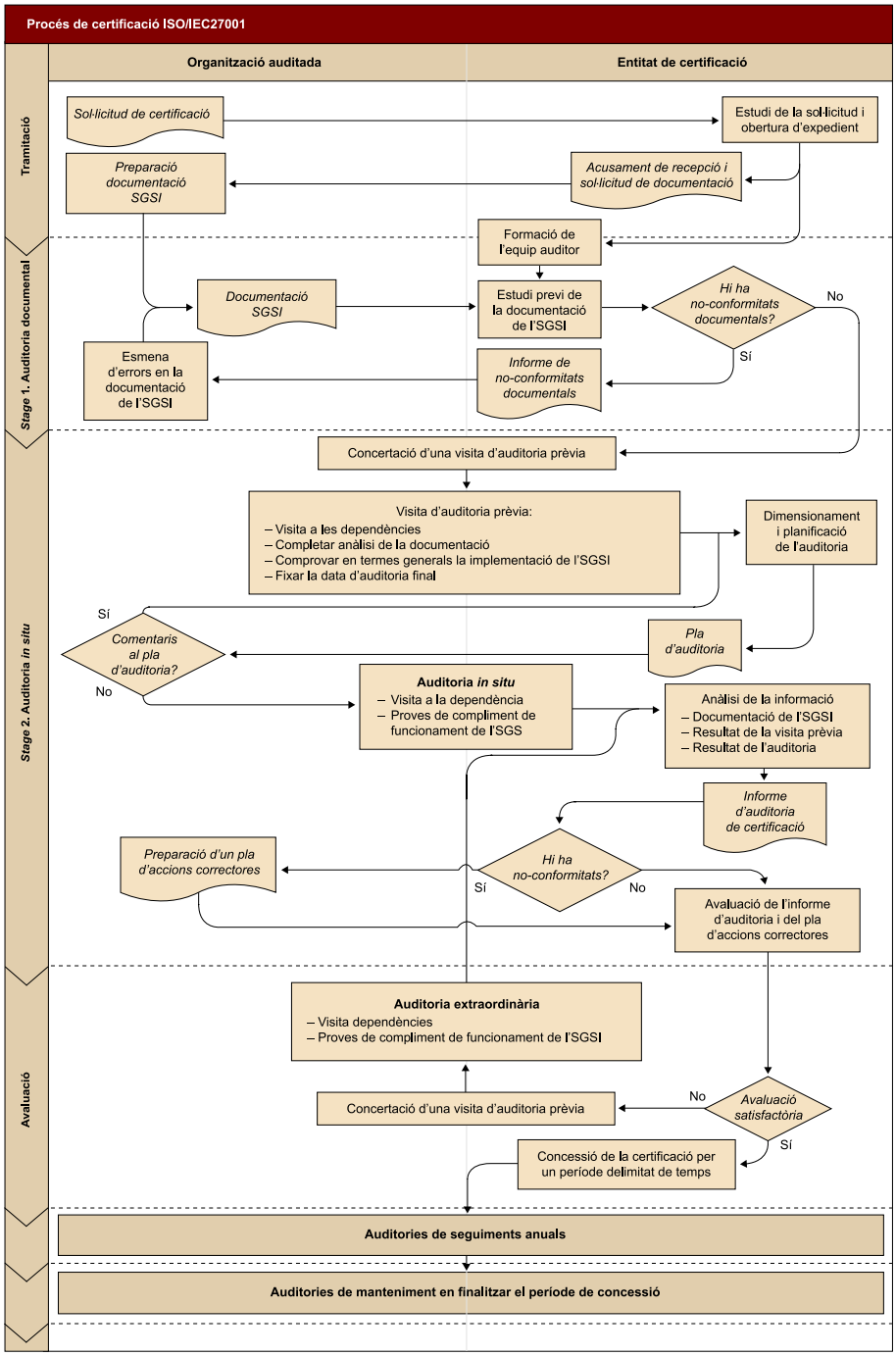
Una denominació comuna usada per les entitats de certificació seria *fase documental* i *fase in situ*, ja que aquests termes descriuen l'objectiu de cadascuna.

Aquesta separació en dues fases podria no complir-se si es justifica i es documenta la raó per la qual s'opta per un altre enfocament. Una raó per no complir aquesta separació en dues fases podria ser, per exemple, que l'organització auditada fos molt petita i es pogués executar tot el procés en una única fase.

3.2.1. Diagrama del procés d'auditoria

La Norma ISO 19011 defineix un procés general per a l'auditoria de sistemes de gestió, el qual ha estat adoptat per la Norma ISO/IEC 17021 i l'ISO/IEC 27006 per a definir el procés d'auditoria de certificació d'un SGSI. En seccions anteriors, hem vist de manera general el procés d'auditoria. A continuació, es detallarà aquest procés per al cas que ens interessa.

A Espanya, el procés d'auditoria que aplica cada entitat de certificació pot variar en certes fases o en la durada o importància que es doni a cadascuna. No obstant això, el procés complet per a fer una auditoria de certificació inclou les fases que es mostren en el diagrama següent:



Procés d'auditoria de certificació a Espanya

És interessant veure que, encara que en aquest diagrama l'auditoria documental i la primera visita documental estan separades, les entitats de certificació fan aquestes dues activitats de manera simultània la majoria de les vegades. És a dir, en una mateixa visita preliminar, es pot fer la presa de contacte i també l'auditoria documental, o es recull la documentació per a fer-la a les instal·lacions pròpies de l'entitat de certificació.

3.2.2. Fase de sol·licitud de la certificació

Un representant autoritzat de l'entitat que s'ha d'auditar ha de formalitzar una sol·licitud. En aquesta, es facilitarà alguna informació bàsica perquè l'entitat de certificació pugui determinar:

- Abast de la certificació.
- Característiques bàsiques del sol·licitant (nom, adreces).
- Informacions rellevants respecte a l'activitat, recursos humans i tècnics, funcions i relacions amb altres parts d'una organització més gran (si hi és aplicable).

La sol·licitud és estudiada per l'entitat de certificació. S'estudia especialment tot el que pugui implicar un compromís a la seva imparcialitat. Si l'entitat de certificació té alguna relació amb alguna entitat de consultoria, es determinarà si aquesta última ha tingut alguna relació amb l'entitat que s'ha d'auditar. És important entendre que les entitats de certificació haurien de prestar molta atenció a aquest aspecte per tal de defensar el seu bon nom i el prestigi de la certificació.

Si l'assignació d'auditoria es pot dur a terme, és necessari que s'estableixi un acord ferm entre el sol·licitant i l'entitat de certificació, el qual ha de fer el següent:

- Definir l'abast de l'auditoria.
- Comprometre el sol·licitant a facilitar tota la informació que se li requereixi en relació amb l'assignació.
- Comprometre el sol·licitant a complir tots els requisits del procés d'auditoria.

Una vegada formalitzat l'acord, es fan els arranjaments per a iniciar la primera fase de l'auditoria.

3.2.3. Planificació i dimensionament de l'auditoria

En el procés de planificació i dimensionament de l'auditoria, es determinen el nombre de dies que s'hi dedicaran, i el nombre i el tipus de recursos que compondran l'equip d'auditoria. Això és determinant tant per a l'èxit de l'assignació d'auditoria com per a l'èxit econòmic de l'entitat de certificació. No s'ha d'oblidar que, en la gran majoria dels països industrialitzats del nostre entorn (Europa, l'Amèrica Llatina), hi ha competència entre les diferents entitats de certificació, encara que siguin entitats sense ànim de lucre en alguns ca-

sos. Totes s'han de finançar, en part, amb els recursos que l'activitat d'auditoria genera. Per tant, ajustar tant com sigui possible els costos de l'auditoria té una relació directa amb el seu dimensionament.

La Norma ISO/IEC 27006, que regeix el procés d'auditoria de certificació dels SGSI, no dóna requisits estrictes quant a això. Això és a causa que s'entén que el dimensionament correcte de l'auditoria està relacionat amb la imparcialitat i el bon nom de l'entitat de certificació. No obstant això, aquesta norma dóna certes guies en un dels seus annexos. En concret, la seva proposta es basa a determinar inicialment la complexitat de l'organització que s'ha d'auditar d'acord amb uns quants criteris:

Complexitat	Alta	Mitjana	Baixa
Nombre d'empleats i personal extern fent tasques internes	>= 1.000	>= 200	<200
Nombre d'usuaris clients	>= 1.000.000	>= 200.000	< 200.000
Nombre de localitzacions	>= 5	>= 2	1
Nombre de sistemes d'informació (servidors)	>= 100	>= 10	<10
Grandària del parc de microinformàtica (equips de sobretaula o portàtils)	>= 300	>= 50	< 50
Nombre de persones dedicades al desenvolupament o a la integració d'aplicacions	>= 100	>= 20	< 20
Ús de la criptografia	Connexions externes de dades xifrades, amb ús de PKI, o amb requisits criptogràfics	Connexions externes de dades no xifrades, sense ús de PKI, i sense requisits criptogràfics	No té connexions de dades externes
Especificitat del marc legal que hi apliqui	Incompliments que poden comportar càrrecs judicials	Incompliments que poden provocar sancions o la pèrdua d'imatge	Incompliments que comporten pèrdues insignificants

Així mateix, la Norma ISO/IEC 27006 defineix una sèrie de sectors que es consideren d'especial risc. Per als casos en què l'organització candidata actua en algun d'aquests sectors, la norma proporciona uns criteris de complexitat diferents per a fer el dimensionament de l'auditoria.

Segons la complexitat resultant que s'assigni a l'organització, es determinen tant els coneixements i l'experiència dels membres de l'equip auditor com el càlcul del nombre de dies que s'han de dedicar a l'auditoria.

Respecte a la capacitació de l'equip auditor, si la complexitat és alta, s'aconsella que l'equip auditor disposi d'un coneixement avançat del sector en què es mou l'auditat. En canvi, si la complexitat és mitjana o baixa, n'hi hauria prou amb un nivell de coneixement adequat.

Respecte a la planificació, la norma dóna un mètode de càlcul que està extret de l'experiència pròpia de diverses entitats de certificació. Aquest mètode està basat en taules que relacionen el nombre de dies necessaris per auditar l'SGSI amb el nombre d'empleats de l'organització. A més, es reserven certs dies per a tasques de revisió i elaboració d'informes de la manera següent:

- 2 dies per a revisar els controls ISO/IEC 27002.
- D'1 a 3 dies per a revisar la documentació.
- D'1 a 3 dies per a elaborar els informes.
- Un temps addicional per cada localització extra que s'hagi de visitar.

De totes maneres, aquesta només és una recomanació o guia, que pot ser tinguda en compte o no per l'entitat de certificació segons les seves necessitats.

Selecció de l'equip auditor

La selecció de l'equip auditor es pot fer abans de la fase d'auditoria documental. No obstant això, conceptualment, i segons l'estàndard ISO 19011, s'hauria de fer després.

Respecte a la mida de l'equip auditor, aquest dependrà en gran manera de l'abast de l'auditoria. Habitualment, en el cas d'empreses de mida petita o mitjana, no sol ser habitual que l'equip auditor sigui de més d'una persona (l'auditor en cap) o dues. En el cas de grans empreses, sí que és possible que es creïn equips d'auditoria més nombrosos.

Quan es crea un equip d'auditoria, el líder de l'equip auditor hauria d'assignar a cada membre de l'equip la responsabilitat d'auditar parts específiques del sistema de gestió (processos, funcions, àrees o activitats concretes). Aquestes assignacions haurien de tenir en compte la necessitat d'independència, competència i ús efectiu de recursos per part dels auditors i experts tècnics. Es poden fer canvis en les assignacions de treball a mesura que progressa l'auditoria, per a assegurar-ne l'assoliment dels objectius.

Els requisits de coneixements més específics són els relacionats amb els capítols de la Norma ISO/IEC 27002. Es demana un cert nivell de coneixement sobre les àrees tractades en cadascun dels capítols de la norma. A continuació indiquem, per a cadascun dels capítols, el grau de coneixement o experiència que se sol exigir als auditors:

- Polítiques de seguretat. Coneixement i experiència en polítiques, i en la influència dels requisits de negoci en la seguretat de la informació.

- Organització de la seguretat. Coneixement general i experiència en processos de negoci i en estructures organitzatives.

- Gestió d'actius. Coneixements en valoració d'actius, inventariat, classificació i polítiques d'ús acceptable dels actius.

- Gestió de recursos humans. Coneixements generals sobre els processos d'un departament de gestió de recursos humans.

- Protecció física i de l'entorn. Coneixement dels riscos i controls habituals.

- Capítols d'ordre tècnic. Coneixement actualitzat i experiència en estàndards, tècniques i processos per a la gestió dels aspectes tècnics, i també un cert nivell de coneixement i experiència tècnica.

- Gestió d'incidents. Coneixement actualitzat i experiència en els processos per a la gestió d'incidents de seguretat.

  Per exemple, els aplicats pels equips de resposta davant incidents com els que descriu el CERT-CC del SEI (Software Engineering Institute) de la Universitat Carnegie Mellon.

- Continuïtat de negoci. Coneixement actualitzat i experiència en els estàndards (com el BS 25999), processos, plans i proves d'aquests.

- Compliment legal. Coneixement actualitzat i experiència dels tipus de relacions contractuals, i marcs legals més habituals (propietat intel·lectual, protecció i retenció de dades financeres, i protecció de dades de caràcter personal) i, si hi són aplicables, més específics: lleis antiterroristes, regulació de l'ús de controls criptogràfics, comerç electrònic, investigació i vigilància electrònica, intercepció de telecomunicacions i monitoratge del trànsit, etc.

A més d'aquests coneixements, que es poden cobrir mitjançant experts externs, els auditors sí que hauran de tenir un coneixement actualitzat i experiència en:

- La Norma ISO/IEC 27001 (molt especialment).
- Planificació d'auditories.
- Tipus d'auditories i metodologies.
- Anàlisi de riscos i metodologies.
- Cicle de Deming per a implementar un procés de millora contínua.

Una vegada designats els components de l'equip auditor, els seus membres haurien de revisar la informació pertinent relacionada amb les seves assignacions d'auditoria, i preparar els documents necessaris per a aquestes assignacions.

La planificació de l'auditoria

El líder de l'equip auditor hauria de preparar un pla d'auditoria per a subministrar la informació necessària a l'equip auditor i a l'auditat. El pla hauria de facilitar la programació i la coordinació de les activitats d'auditoria. La quantitat de detalls subministrats en el pla d'auditoria en reflecteixen l'abast i la complexitat. El pla d'auditoria hauria de ser prou flexible per a permetre canvis (per exemple, en l'abast de l'auditoria), els quals poden arribar a ser necessaris a mesura que progressen les activitats. No obstant això, els canvis en el pla d'auditoria solen ser poc freqüents. Únicament es donen en cas que es detectin no-conformitats més importants que portin l'auditor i l'auditat a replantejar l'abast de l'auditoria i la seva planificació.

El pla d'auditoria hauria d'incloure o descriure:

- L'abast i l'objectiu de l'auditoria. L'abast ha de plantejar també les unitats organitzatives, funcionals i/o els processos auditats.
- Les dates i els llocs on faran les activitats d'auditoria *in situ*.
- El temps i la durada esperats d'aquestes activitats, incloent-hi reunions amb la gerència de l'auditat i reunions internes de l'equip auditor.
- Els criteris de l'auditoria i qualsevol document de referència. En el nostre cas, es tracta òbviament de la Norma ISO/IEC 27001.
- Equip per part de l'entitat i del sol·licitant.
- Personal del sol·licitant amb responsabilitat dins de l'àrea afectada.
- Mostres de controls que s'han d'auditar.
- Contingut i estructura dels informes.
- Aspectes relacionats amb la confidencialitat que siguin rellevants.

El pla d'auditoria s'ha de presentar al sol·licitant abans del desenvolupament de l'auditoria *in situ*. L'auditat hauria de revisar i acceptar el pla d'auditoria almenys abans de començar les activitats d'auditoria *in situ*.

Qualsevol objecció presentada per l'auditor s'hauria de resoldre entre el líder de l'equip auditor, l'auditat i el client de l'auditoria. El pla d'auditoria ha de ser acceptat per totes les parts abans de continuar amb l'auditoria.

Consideracions sobre el mostreig

El procés d'auditoria dels controls presos de l'ISO/IEC 27002 pot no ser exhaustiu. L'equip auditor, abans d'iniciar l'auditoria presencial, pot fer una selecció dels controls que s'auditaran. En aquest sentit, la mostra de controls que cal verificar haurà de complir el següent:

- Incloure tots els controls crítics.
- Seleccionar controls que afectin les activitats més importants de l'organització.
- Seleccionar controls de totes les seccions.

- Seleccionar els controls de manera que s'auditin tots els departaments involucrats en l'SGSI.
- Donar prioritat a les àrees de més risc.
- Si no es troben problemes seriosos, s'auditarà un 20% dels controls aplicables.

El mostreig també és necessari quan hi ha un gran nombre de localitzacions sota l'abast de l'SGSI. En aquest cas, l'entitat de certificació s'ha d'assegurar que l'abast de l'auditoria s'ajusta el màxim possible a l'abast de l'SGSI. Per a això:

- Totes les localitzacions s'han de regir pel mateix SGSI, el qual ha d'estar gestionat de manera centralitzada. Aquest punt central ha d'estar dins de l'abast de l'auditoria.

- Les raons per haver d'optar per un mostreig han d'estar justificades i documentades.

- El mostreig s'ha de fer tenint en compte:
  - Els resultats de les auditories internes de l'SGSI.
  - Les revisions de la direcció.
  - La variabilitat de grandàries, complexitat dels sistemes d'informació i funcions de negoci de les diferents localitzacions.
  - Aspectes legals que puguin ser rellevants.

- Si una localització té uns riscos específics que siguin rellevants, ha d'estar inclosa en el mostreig.

- L'entitat de certificació ha d'estendre el seu abast a les futures auditories de seguiment, per tal d'anar englobant la resta de localitzacions.

3.2.4. Stage 1. Auditoria documental

La primera fase de l'auditoria –stage 1– té per objectiu la revisió de tota la documentació que forma part de l'SGSI. Aquesta revisió documental serveix per a verificar que s'ha creat un SGSI, que s'efectua d'acord amb la norma, i que s'hi han implantat els controls segons els riscos que l'organització ha detectat. A més, s'ha de revisar que aquests controls estiguin d'acord amb el que s'indica en la norma ISO/IEC 27001.

D'altra banda, l'auditoria documental té un objectiu secundari: entendre millor la idiosincràsia de l'auditat, el seu negoci, l'abast de l'SGSI i les seves característiques. Aquest coneixement ha de ser emprat en la fase següent, per tal d'agilitar i de fer més eficaces les proves d'auditoria i determinar la composició exacta de l'equip auditor.

A l'inici d'aquesta fase, se sol·licita a l'auditat que faciliti la documentació. Auditat i auditor acorden si la revisió de la documentació es farà en una visita presencial o a les instal·lacions de l'entitat de certificació. El que és habitual és que es faci la visita presencial, per tal de fer així una presa de contacte entre tots dos equips. Per descomptat, s'han de tenir en compte les consideracions de confidencialitat que l'auditat tingui sobre aquesta documentació. Per tant, es podria donar el cas que no sigui possible que la documentació surti de les instal·lacions de l'auditat.

Els resultats d'aquesta revisió sempre es documenten i es comuniquen a l'auditat abans de procedir a la fase següent.

Documentació que s'ha de revisar

La mínima documentació que s'ha de revisar en aquesta fase és la que estableix el punt sobre l'apartat Suport d'aquest material en comentar el punt 7.5 "informació documentada", i bàsicament es tracta dels següents:

- **Política de seguretat de l'organització**. La política pot estar en un document independent o no; això no és determinant. La política ha de ser una guia estratègica que proporcioni indicacions d'ordre general a tota l'organització de manera senzilla. Es pot arribar a expressar en un únic full, i aquest s'ha d'exposar de manera pública a les instal·lacions, atès que la política de seguretat ha d'estar distribuïda a tots els treballadors.
  L'auditor verificarà que la política fa esment a l'existència d'una altra documentació relativa a l'SGSI, i que aquesta es distribueix d'acord amb la necessitat de coneixement dels treballadors.
  En poques paraules, es revisaran els aspectes següents:
  – Definició de la seguretat.
  – Suport de la direcció a la implantació de l'SGSI.
  – Explicacions breus sobre polítiques, principis, pràctiques i compliments de seguretat.
  – Definició de responsabilitats.
  – Referències a altres documents.

- **Abast de la certificació**. Aquest abast condiciona la certificació i el desenvolupament de les auditories. L'auditor únicament revisarà el que fa referència a aquest abast, i tot el que pugui estar fora no es revisarà.
  Tal com s'ha apuntat, és possible que un SGSI no inclogui la totalitat de l'organització, sinó que es podria definir un abast d'un determinat procés o una àrea concreta de l'organització. En cas que es faci un canvi en l'abast de l'SGSI, s'haurà de refer totalment el procés de certificació.

- **Anàlisi de riscos de l'organització**. L'auditor prestarà especial atenció a l'anàlisi de riscos. Per començar, haurà d'estar formalment acceptat per la direcció de l'organització, i és obligatori que estigui documentat. La documentació haurà d'incloure tant la metodologia utilitzada, que ha de ser

coherent amb la complexitat de l'organització, com els resultats d'aquesta anàlisi de riscos i el seu pla de tractament.

L'auditor ha de determinar si l'anàlisi de riscos cobreix tot l'abast definit per l'organització, i si és acceptable en funció dels actius i la naturalesa d'aquesta. També ha de revisar que l'anàlisi de riscos i la seva gestió estiguin actualitzades.

En aquest sentit, és interessant destacar que el comitè conjunt JTC1 de l'ISO i l'IEC ha elaborat informes tècnics en què es detallen els principis per a l'anàlisi i posterior gestió del risc. Aquests informes tècnics han quedat recollits en les *Guidelines for the management of IT Security* (GMITS ISO/IEC TR 13335:1998). Aquestes guies han estat la base fonamental per a la realització de la Norma ISO/IEC 27005:2008. Així mateix, també té l'auditor a la seva disposició totes les normes de la família ISO/IEC 31000 com a guia sobre anàlisi de riscos. L'auditor emprarà aquestes normes com a referència per a determinar la qualitat de l'anàlisi de riscos.

- **La selecció de controls d'acord amb la declaració d'aplicabilitat**. L'auditor, d'acord amb els riscos analitzats, determinarà si s'han seleccionat els controls adequats per a mitigar-los. Així mateix, haurà de verificar que tots aquests controls de seguretat queden reflectits en la declaració de l'aplicabilitat, i que la direcció aprova el risc residual resultant d'implantar aquests controls.

  És important observar que, en la documentació, s'han de justificar tots els controls, tant si són seleccionats com si són descartats, així com el seu nivell d'implantació. En aquest sentit, s'haurà de defensar, davant l'auditor molt especialment, la no-implementació d'un control, i els motius poden ser:
  - No hi ha cap risc que el justifiqui.
  - Pressupost.
  - No hi ha viabilitat tecnològica.
  - No es pot implantar per falta de temps.
  - No hi és aplicable.

Les raons per a excloure controls han de ser sòlides i coherents.

Exemple d'extracte d'una declaració d'aplicabilitat

Control	Implantació	Sí/no	Justificació
6.3.1. Comunicació de les incidències de seguretat	Sí	Sí	És imprescindible per a detectar les incidències en un estat primerenc, i és una de les bases per al procés de millora contínua.
7.1.5. Àrees aïllades de càrrega i descàrrega	No aplica	No	No hi és aplicable, ja que l'organització no disposa d'àrees de càrrega i descàrrega.
8.7.2. Seguretat de suports en trànsit	No aplica	No	No hi és aplicable, ja que l'organització no envia suports físics amb informació sensible o confidencial.

El document de declaració d'aplicabilitat relaciona l'anàlisi de riscos amb la situació de la seguretat, tant per als auditors externs com interns.

Juntament amb l'abast i la política, constitueix la base de l'auditoria documental. L'auditor comprovarà la consistència dels plantejaments referents a la seguretat entre els tres documents. Especialment, l'auditor buscarà proves que demostrin que hi ha una relació entre la selecció dels controls i els riscos detectats en l'anàlisi. Finalment, revisarà la manera com els controls ajuden a gestionar el risc.

1) Documentació de gestió de l'SGSI. La documentació de l'SGSI haurà d'incloure una descripció sobre la manera com s'efectua el sistema. Aquesta documentació és la que descriurà com s'executa el procés de millora contínua PDCA. Habitualment, estarà organitzada de la manera següent:

- Estructura organitzativa per a suportar la funció de seguretat.
- Procediments per a mesurar l'eficàcia de l'SGSI i dels controls de seguretat.
- Normativa per a la gestió documental de tota la documentació.
  Respecte a la documentació que dóna forma i suport a l'SGSI, l'auditor ha de comprovar que la documentació:
  – Està datada i disponible.
  – Disposa de control de versions.
  – Es retira si és obsoleta.

En aquest aspecte, és important que la documentació sigui coherent i que estigui formalment aprovada pels qui hagin estat designats. A més, hi ha d'haver registres de funcionament de tots els aspectes de l'SGSI. Cal entendre que, en gran manera, l'SGSI està basat en decisions i, per tant, part d'aquests registres seran actes de reunions, ordres donades per escrit, etc. En certa manera, l'auditat estarà en disposició de presentar un registre o una prova del funcionament de l'SGSI, encara que aquest és un dels objectius de la fase següent de l'auditoria.

2) Documentació dels controls seleccionats. Els controls hauran d'estar descrits i això, a més, ha de ser la base per a la seva implantació posterior.

Informe de l'auditoria documental

Sobre la base de la revisió de la documentació, l'auditor ha d'establir un informe d'auditoria. La redacció d'aquest informe és una obligació de la part auditora.

De l'anàlisi de les proves d'auditoria de la fase 1, es pot arribar a tres situacions:

- **L'auditor detecta no-conformitats majors**. En aquest cas, l'auditor rebutja la certificació i proposa a l'empresa auditada que refaci la documentació

de l'SGSI i que, passat un temps, torni a requerir el procés d'auditoria. La realitat no és tan dràstica, i es posposa la realització de nou de la fase 1 a una data en què l'auditat hagi esmenat les no-conformitats.
Cal destacar, i això és vàlid també per a la fase 2, que l'auditor farà la seva tasca d'auditoria mentre no trobi no-conformitats majors. En cas que en trobi alguna, i segons la seva naturalesa, podrà continuar la seva tasca, però acabarà aturant el pla d'auditoria si sorgeixen més no-conformitats majors. És a dir, en una auditoria de certificació, l'auditat no pot esperar que es detectin totes les no-conformitats (majors i menors), amb l'objecte de disposar d'una llista de les accions que s'han de dur a terme.

- **L'auditor detecta no conformitats menors**. En aquests casos, l'auditor proposa a l'organització auditada que exposi una sèrie d'accions correctores. L'auditat haurà de proposar no solament la solució, sinó també un temps en què es resoldrà aquesta no-conformitat. L'auditor serà qui s'encarregui de decidir si aquestes solucions previstes solucionarien aquestes no-conformitats.
  En cas que l'auditor declini aquestes solucions, s'indicarà que haurà de tornar a sol·licitar l'auditoria. En cas que les solucions que planteja l'organització siguin acceptades per l'auditor, procedirà a requerir el pas a la segona fase de l'auditoria.

- **L'auditor no detecta no-conformitats**. En aquests casos, l'auditor proposa a l'organització que passi a la segona fase de l'auditoria.
  L'informe d'auditoria d'aquesta primera fase s'enviarà a l'organització perquè actuï en conseqüència. Una vegada arribats a la situació en què es pot progressar a la fase 2, auditor i auditat acorden la realització de la fase següent.

3.2.5. Stage 2. Auditoria presencial o *in situ*

La segona fase de l'auditoria és presencial i es fa a les instal·lacions de l'organització auditada. En aquesta fase, l'auditor fa entrevistes per verificar que el que s'indica en la documentació revisada realment reflecteix la situació real de l'organització.

Entre la revisió documental i aquesta segona fase *in situ* han de passar entre tres i sis setmanes obligatòriament. A més hi ha d'haver un pla d'auditoria comunicat a l'auditat, el qual servirà per a acordar aspectes logístics com, per exemple, dates exactes, llocs que s'han de visitar, pauses, reunions, etc.

L'objectiu de l'auditoria presencial és:

- Confirmar que l'organització compleix les seves polítiques i els seus procediments.

- Comprovar que l'SGSI desenvolupat s'ajusta a les especificacions de la Norma ISO/IEC 27001.
- Verificar que l'SGSI està aconseguint els objectius que l'organització s'ha marcat.

Per aconseguir aquests objectius, l'equip auditor ha de centrar la seva atenció en com l'organització auditada:

- Dóna suport a la política de seguretat des de la direcció.
- Analitza els riscos als quals està sotmesa la seva informació.
- Selecciona els controls basant-se en l'anàlisi de riscos.
- Relaciona l'anàlisi de riscos, la declaració d'aplicabilitat, el pla de tractament dels riscos i la política de seguretat.
- Implementa els controls tenint en compte els mecanismes de mesura de l'efectivitat d'aquests, i la consecució dels objectius de control.
- Revisa l'efectivitat del seu SGSI i dels controls.
- Duu a terme les auditories internes i la revisió interna per part de la direcció.

Relacions de l'auditoria

Una vegada el sol·licitant aprova el pla d'auditoria, es concreten les dates exactes per a la visita de l'equip auditor a les instal·lacions de l'organització. En aquestes revisions, l'equip auditor s'haurà de centrar en els aspectes següents:

- L'anàlisi de riscos.
- La declaració d'aplicabilitat.
- Els objectius que persegueix l'organització.
- Com es monitora, es mesura, s'informa i es millora.
- Les revisions de l'SGSI i de la seguretat.
- El grau d'implicació de la direcció.
- La coherència entre polítiques, anàlisis de riscos, objectius, responsabilitats, normes, procediments, dades de rendiment i revisions de seguretat.

Durant aquesta segona fase de l'auditoria, s'haurà de fer una visita a les instal·lacions de l'organització (almenys, a les instal·lacions dins de l'abast que s'ha de certificar). S'haurà de comprovar també que els controls que s'han seleccionat en la mostra compleixen el que exigeix l'estàndard. Això significa que es buscaran proves objectives sobre la implantació i el funcionament dels controls que conformen l'SGSI. Aquestes proves poden ser, per exemple, registres d'activitat (*logs*). En tot cas, les proves s'han de basar en mesures, en proves o en l'observació, i han de poder ser verificades. És important tenir en compte que l'auditor pot sol·licitar al personal de l'organització que li mostri com s'han generat les proves.

Durant aquesta segona fase de l'auditoria, algunes proves tenen un caràcter més tècnic, la qual cosa requerirà consultar els sistemes d'informació. No obstant això, els membres de l'equip auditor no poden tocar cap màquina. Només poden sol·licitar als empleats de l'organització que facin les activitats que volen avaluar, per a buscar proves que permetin decidir si un control està correctament implantat o no.

Per a l'execució de les proves d'auditoria, l'equip auditor convocarà reunions amb membres seleccionats de l'organització. En aquestes reunions, l'equip auditor obtindrà la informació necessària per a verificar la implantació correcta o incorrecta dels controls de seguretat. Així mateix, l'equip auditor també elaborarà informes sobre el que s'hagi observat durant les entrevistes, i redactarà documents de recomanacions (si escau). En finalitzar, l'equip auditor convocarà una reunió final amb la direcció de l'organització, per a explicar el que ha observat durant aquesta segona fase, i comunicar els resultats de l'auditoria.

Entrevistes

Una de les tècniques d'auditoria que més empraran els auditors seran les entrevistes. Aquestes poden estar o no complementades amb alguna prova tècnica però, tal com hem dit, serà executada per l'entrevistat.

La qualitat de l'entrevista d'auditoria depèn de l'habilitat de l'auditor per a fer preguntes. A l'hora de fer preguntes, l'auditor ha d'aconseguir que l'auditat se senti còmode, que no se senti interrogat. El tipus de preguntes que farà l'auditor han de ser obertes, de manera que l'auditat no pugui contestar sí o no, sinó que hagi de proporcionar explicacions àmplies.

Models de preguntes

• Qui ho fa?	• Cada quant es fa?
• Quan es fa?	• M'ho podries mostrar?
• On es fa?	• Com es fa?

Altres tipus de preguntes que es poden fer són:

- Preguntes d'opinió.
- Preguntes d'investigació.

- Preguntes no verbals (llenguatge corporal).
- Preguntes repetides.
- Preguntes sobre situacions hipotètiques.

L'objectiu d'aquestes entrevistes és extreure totes les proves necessàries per a verificar que l'organització actua tal com reflecteix la documentació lliurada a l'auditor.

Tancament de l'auditoria

Al final de l'auditoria, l'equip auditor s'ha de reunir amb el sol·licitant del resultat d'aquesta, i ha de fer el següent:

- Agrair la col·laboració.
- Recordar novament l'objectiu i l'abast de l'auditoria.
- Proporcionar un resum del resultat de l'auditoria.
- Informar de les recomanacions de l'equip d'auditoria.
- Preguntar si el sol·licitant té alguna qüestió que vulgui aclarir.
- Recollir la conformitat del sol·licitant.
- Tancar la reunió.

Les conclusions i l'informe d'auditoria s'han de basar en:

- Les dues etapes de l'auditoria conjuntament.
- Les no-conformitats oposades.
- La documentació, la implantació i l'efectivitat de l'SGSI.
- Fortaleses i debilitats de l'SGSI.
- El compromís de la direcció amb la millora contínua.

En aquest punt, igual que al final de la primera fase de l'auditoria, es poden produir tres decisions:

- **L'auditor detecta no-conformitats majors**. En aquest cas, l'auditor rebutja la certificació i informa de les no-conformitats greus. A més, proposa a l'empresa auditada que millori la implantació de l'SGSI i que, passat un temps, torni a requerir el procés d'auditoria.

- **L'auditor detecta no-conformitats menors**. Igual que en les conclusions de la fase 1, l'organització auditada ha de proporcionar una sèrie de propostes d'accions correctores (amb la designació de responsables i el compromís temporal de resolució), i arribar a un acord amb l'auditor per a poder progressar en el procés de certificació.
  En aquests casos, l'auditor proposa a l'organització auditada que exposi una sèrie de solucions per a aquestes no-conformitats. Després, serà l'auditor qui s'encarregui de decidir si aquestes solucions previstes solucionarien aquestes no-conformitats.
  L'auditat haurà de proposar no solament la solució, sinó també un temps en què es resoldrà aquesta no-conformitat.

En cas que l'auditor declini aquestes solucions, s'indicarà que haurà de tornar a sol·licitar l'auditoria. En cas que les solucions que planteja l'organització siguin acceptades per l'auditor, procedirà a requerir el pas a la segona fase de l'auditoria.

- **L'auditor no detecta no-conformitats**. En aquests casos, l'auditor proposa la concessió de la certificació a l'organització.

En funció d'això, l'equip auditor ha d'emetre la recomanació:

- Es recomana el registre, si es considera que l'SGSI s'ajusta a la norma.
- Es recomana la revisió en cas que s'hagin trobat no-conformitats, en l'espera de rebre un pla acceptable d'accions correctores.
- Es recomana tornar a auditar parcialment l'SGSI, si s'han trobat no-conformitats majors en una àrea concreta.
- Es recomana tornar a auditar, si s'han trobat no-conformitats majors en més d'una àrea.

Concessió de la certificació

La decisió final de concedir o no la certificació no la pren l'auditor en cap, sinó el comitè de certificació. Aquest està format per membres de l'organització auditora que no formin part de l'equip auditor. La decisió final es basarà en la informació recollida durant el procés d'auditoria (les dues etapes).

En cas que la recomanació de l'equip d'auditoria sigui un no, el comitè de certificació no haurà de canviar el criteri. En cas contrari, si la recomanació és un sí, el comitè de certificació pot canviar aquesta decisió i no lliurar el certificat.

En cas que s'emeti el certificat, l'entitat remetrà al sol·licitant una carta o un diploma en què s'indiqui com a mínim:

- El nom i l'adreça de l'organització.
- L'abast de la certificació.
- La data d'emissió del certificat i el període de validesa.
- La versió de la declaració d'aplicabilitat.

Una vegada s'ha obtingut la certificació, es procedirà a lliurar el certificat i s'entrarà en un cicle de revisió de la certificació. Aquest cicle consisteix a fer una auditoria parcial de manera anual. La certificació serà vigent durant, habitualment, tres anys.

En cas que, durant una de les revisions, l'auditor detecti que hi ha grans problemes de seguretat o no-conformitats, es podria arribar a retirar el certificat.