Desenvolupament d'alguns objectius de control de l'SGSI

PID_00253135

Silvia Garre Gui
Arsenio Tortajada Gallego
Antonio José Segovia Henares

Universitat Oberta de Catalunya

Silvia Garre Gui

Enginyera Superior en Telecomunicacions per la Universitat Politècnica de Catalunya. Directora àrea TIC Departament de la Vicepresidència, i d'Economia i Hisenda (CTTI - Generalitat de Catalunya). Certificada en CRISC (*Risk and Information Systems Control*) i CISM (*Information Security Manager*) per ISACA.

Arsenio Tortajada Gallego

Enginyer Superior en Informàtica per la Universitat Autònoma de Barcelona. Consultor/Auditor de Seguretat de la Informació en diferents organitzacions. Certificat CISA / CDPP / ISO 27001 i ISO 22301 Lead Auditor. Ha impartit cursos i seminaris sobre seguretat informàtica en diferents institucions.

Antonio José Segovia Henares

Enginyer en Informàtica, i Enginyer Tècnic en Informàtica de sistemes per la UOC. Expert en Seguretat de la Informació, *hacker* ètic i professional expert qualificat en el RGPD. Des del 2010, qualificat com a Auditor Líder en ISO 27001, i qualificat també en altres esquemes com ISO 27018, ISO 22301, i ISO 20000, per diverses entitats certificadores. *Blogger* i ponent de *webinars* sobre la Seguretat de la Informació a nivell mundial.

Índex

Introducció

En el mòdul anterior s'han presentat els passos per a implantar un SGSI, prenent com a referència les normes de la família ISO 27000, en concret la ISO/IEC 27003 – Guia per a la implementació d'un sistema de gestió de seguretat de la informació.

Aquest mòdul se centra a desenvolupar aspectes clau per a incidir en alguns dels objectius de control de la norma, com són el marc normatiu o l'organització de la seguretat de la informació. Tots dos aspectes són relativament senzills a simple vista, però, no obstant això, són passos previs que requereixen un esforç important de tota l'organització, ja que sovint impliquen canvis que s'han de gestionar convenientment per a "derrocar" certes barreres que, en cas contrari, compliquen considerablement implantar l'SGSI.

S'aborda també el plantejament d'un cas concret de política o norma, com és la classificació de la informació, que és la base per a bona part de la resta del marc normatiu, i que torna a ser una tasca àrdua perquè implica un canvi en la manera habitual de treballar del personal.

A continuació es presenten algunes reflexions sobre les característiques que ha de tenir una eina per a gestionar l'SGSI.

Finalment, es proporcionen algunes nocions sobre les auditories de certificació, de molta utilitat en cas que la companyia vulgui obtenir la certificació, sia com a garantia interna de bona gestió, sia pensant en tercers, com a segell d'una bona gestió de la seguretat de la informació.

Objectius

Els objectius que persegueix aquest mòdul són els següents:

1. Aprofundir en alguns aspectes imprescindibles per al bon desenvolupament d'un SGSI.

2. Saber en què consisteix el marc normatiu de la seguretat, com s'han de desenvolupar normes i guies de bones pràctiques i en què consisteix una política de seguretat de la informació.

3. Aprofundir en l'àmbit de l'organització de la seguretat de la informació. Entendre quines estructures hi són necessàries i quin és el model de relació imprescindible amb la resta de la companyia.

4. Assentar les bases per a una política de classificació de la informació.

5. Saber en què consisteix una auditoria de certificació d'SGSI per a preparar-se en cas de voler la certificació.

1. Desenvolupament d'un marc normatiu de seguretat de la informació

En el mòdul anterior vèiem que dins de la fase de planificació del SGSI, concretament en les subfases P. I, "Definir la política de seguretat", i P. IV, "Definir polítiques d'alt nivell", s'ha de disposar d'una normativa comuna de seguretat que reguli les línies mestres sobre la manera de treballar de tota l'organització en matèria de seguretat de la informació.

Per tant, cal establir un marc normatiu que empari qualsevol acció que es dugui a terme en matèria de seguretat de la informació, que, com veurem, l'ha d'aprovar la direcció.

No obstant això, abans de començar el desenvolupament d'aquest marc normatiu, cal fer fer una reflexió sobre què contindrà aquest marc normatiu, quina mena de documents inclourà, com es desenvoluparan, amb quins objectius i quina estructura, qui serà el responsable de fer-ho i quin serà el procés de cadascun dels documents abans d'aprovar-los.

L'adopció d'un mètode sistemàtic i clar aporta, com veurem, uns quants beneficis.

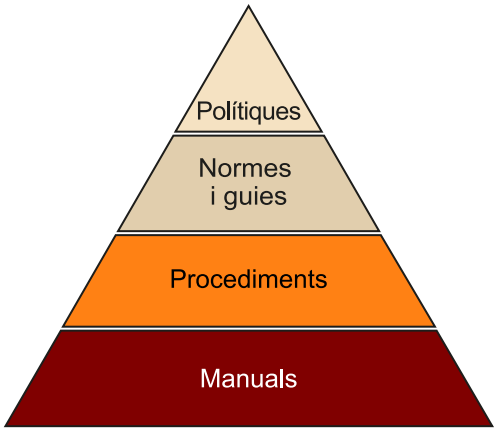
1.1. La piràmide jeràrquica de documentació

Un aspecte tan bàsic com la terminologia és una qüestió que cal resoldre en primera instància, ja que facilitarà que els diferents tipus de documents que es creïn es classifiquin correctament de bon començament i s'elaborin tenint en compte un conjunt de consideracions importants per a cadascun. Tot plegat permetrà que qui els llegeixi tingui molt clar si són normatius o no.

Si no es fa, el que passarà és que els departaments de la companyia aniran elaborant documentació, la nomenaran segons sembli més convenient al responsable de fer-ho i seguiran una estructura més o menys semblant, però no homogènia, que complicarà la lectura i interpretació d'aquests documents. Abans d'adonar-nos-en hi haurà a la companyia normes, normatives, polítiques, guies, processos, procediments, fluxos, llibres blancs, llibres normatius, manuals, instruccions, manuals d'operació, recomanacions, experiències, etc., de manera que gairebé serà impossible establir jerarquies i dependències entre uns i altres.

En el món de la seguretat de la informació, com en d'altres, se sol utilitzar la piràmide jeràrquica de documents:

La piràmide documental



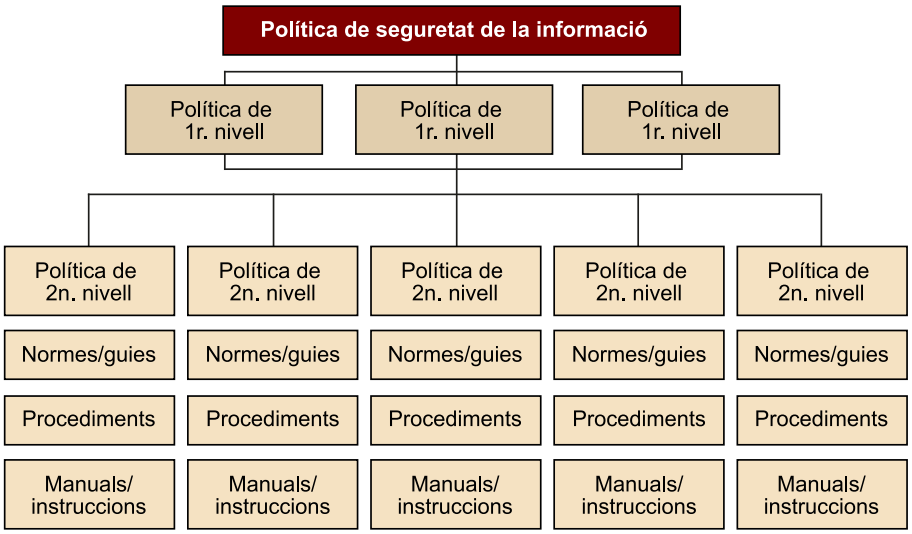
Com més amunt de la piràmide, més directrius generals o estratègiques i menys nivell de concreció. Alhora, més estabilitat, és a dir, poca variació en els documents, i necessitat que la direcció els aprovi.

En canvi, com més avall de la piràmide, més nivell de detall, orientació a personal més especialitzat, molta necessitat d'actualització de la documentació i aprovació a nivells inferiors.

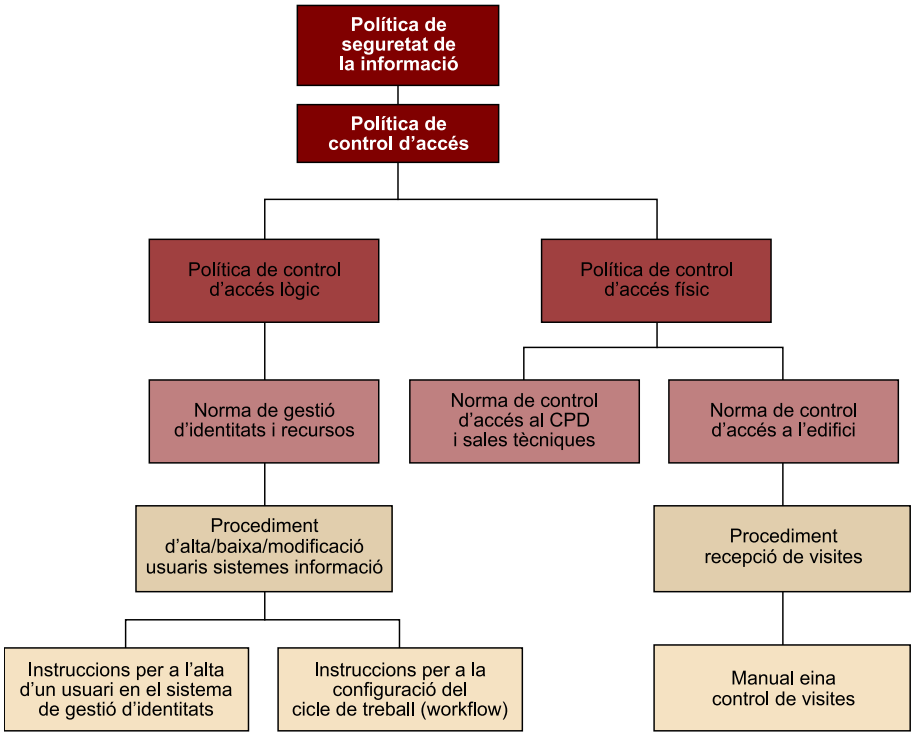
Per norma general, un document de nivell superior es desenvolupa en documents de nivell inferior.

Vegem un possible esquema de desenvolupament del marc normatiu:

Exemple d'estructura de polítiques i normes



Si ho traduïm a un possible cas pràctic:



En la literatura s'hi poden trobar altres plantejaments de piràmide, amb més o menys nombre de nivells. El que importa, no obstant això, no és escollir aquest model o l'altre, sinó adoptar-ne un, el que s'ajusti més a les pràctiques de l'organització, donar-lo a conèixer, implantar-lo i mantenir-lo.

Per a cada tipus de document és important definir els punts següents:

- Tipus d'informació que ha de contenir (nivell de detall).
- Nivell d'obligatorietat en el compliment. Així, doncs, una norma s'ha de complir obligatòriament, mentre que una guia és una recomanació de bones pràctiques.
- Qui ha d'aprovar el document.
- A qui s'ha de divulgar.

És habitual trobar marcs normatius en què per sota de la política de seguretat de la informació hi pengen les polítiques que es corresponen amb els diferents dominis de l'ISO.

D'ara endavant, per a referir-nos a un document del marc normatiu, independentment de la tipologia que tingui, ens referirem a un **estàndard**.

En el món de les tecnologies de la informació i la comunicació (TIC), un estàndard és un acord documentat que conté criteris precisos o especificacions, vàlids per a utilitzar-los consistentment com a regles, directrius o definicions de

característiques i tasques, que assegurin que certs productes, sistemes, processos o serveis són adequats al propòsit que tenen, i per tant, el terme *estàndard* engloba qualsevol dels tipus de documents definits en la piràmide jeràrquica.

Un estàndard pot cobrir qualsevol àrea TIC per a la qual es detecti una necessitat. En l'àmbit de l'SGSI parlem del marc normatiu de seguretat de la informació, però el marc normatiu pot definir estàndards sobre qüestions molt diverses, com ara comunicacions, plataformes d'accés a serveis, plataformes de prestació de serveis, utilització de serveis, gestió de serveis (definició i construcció de programari, bases de dades, interfícies d'usuari, control del funcionament, consecució d'objectius, quadres de comandament, gestió d'incidències, contractació de personal, etc.), compliment legal, etc.

En l'elaboració dels estàndards es poden tenir en compte aspectes molt diversos i l'enfocament que s'hi doni depèn de la necessitat concreta a què es pretengui donar resposta. Per tant, un estàndard pot abordar, per exemple, qüestions funcionals (relació de l'usuari amb les TIC), físiques (sobre l'entorn i els equips), de seguretat (física, lògica, operativa, legal, etc.), d'integració (interoperativitat entre sistemes), de qualitat, o de seguiment i control.

Definim a continuació els quatre tipus de document que recull la piràmide jeràrquica proposada:

1.1.1. Polítiques

- **Contingut**. Recullen directrius estratègiques, d'alt nivell, sota les quals s'empara qualsevol acció en matèria de seguretat de la informació. Tot document de nivell inferior ha de desenvolupar una política. Si es vol, es poden definir polítiques de primer nivell i de segon nivell.
  En seguretat de la informació, la política per excel·lència és la política de seguretat de la informació.

- **Caràcter normatiu dels controls especificats**. S'han de complir obligatòriament dins de l'àmbit descrit en la mateixa política, excepte que l'àmbit mateix reculli alguna excepció.

- **Aprovació**. La política de seguretat de la informació i, en general, les polítiques de primer nivell les ha d'aprovar formalment la direcció de la companyia.

- **Divulgació**. A tot el personal.

1.1.2. Normes i guies

- **Contingut**. Les normes i guies es generen quan es considera important a escala de tota la companyia que se segueixi una mateixa solució o un procés homogeni per a una necessitat determinada amb l'objectiu d'optimitzar recursos, l'eficiència o la seguretat de l'organització.
  Les guies i normes desenvolupen les polítiques en qüestions més concretes i específiques. Així, doncs, en l'exemple anterior, la política de control d'accés físic es desenvolupava mitjançant la norma de control d'accés al CPD i les sales tècniques, i mitjançant la norma de control d'accés a l'edifici.

- **Caràcter normatiu**. Les normes s'han de complir obligatòriament, mentre que les guies són recomanacions de bones pràctiques. En l'àmbit de la seguretat de la informació, tot el que es pot dictar com a norma és més efectiu. No obstant això, no sempre és possible redactar una norma i implantar-la immediatament, sia per la dificultat del procés d'aprovació (cas típic en una administració pública en què una aprovació pot requerir mesos), sia perquè es tracta d'aspectes no prou consensuats o perquè l'organització no està preparada i necessita un temps d'adaptació. En aquest cas, val més aprovar una guia i donar-la a conèixer perquè l'organització s'hi vagi familiaritzant i s'iniciï la gestió del canvi que es requereix, que no pas aprovar una norma que no complirà ningú i que l'única cosa que farà és generar rebuig no solament devers aquesta norma, sinó devers tot el marc normatiu. Una bona pràctica és publicar guies i donar a conèixer el termini d'adaptació previ al pas a norma.
  Les normes i guies es desenvolupen en procediments i manuals o instruccions.
  En el cas de les guies, l'aplicació parcial o total de les bones pràctiques la determina una anàlisi de la conveniència o proporcionalitat entre els beneficis que aporta la reducció del risc que comporta aplicar les recomanacions, i el cost o l'esforç que implica aplicar-les pel que fa a implantació i gestió del canvi.
  Qualsevol excepció a l'aplicació íntegra de les guies o normes l'ha d'haver aprovada prèviament el responsable que correspongui. Hi ha d'haver, per tant, un procediment de gestió d'excepcions.

- **Aprovació**: la direcció o un comitè que hagi designat aquesta direcció.

- **Divulgació**: a tot el personal especificat en la mateixa guia o norma.

1.1.3. Procediments

- **Contingut**. Presenten un conjunt d'accions que cal dur a terme per a aconseguir un determinat objectiu. Normalment hi intervenen actors de diferents àrees o departaments, de manera que sol ser necessari adaptar els

procediments quan es produeixen canvis organitzatius en la companyia. Els procediments donen suport a la implantació d'una norma o guia, per la qual cosa les normes o guies acostumen a referenciar procediments en el seu redactat. En són possibles exemples un procediment de recepció de visites, de sol·licitud de serveis, de gestió d'incidències o d'escalat de peticions.

- **Caràcter normatiu**. Els procediments s'han de complir obligatòriament.
- **Aprovació**. Els sol elaborar i aprovar la persona que n'és responsable.
- **Divulgació**. A totes les persones que hi estan implicades.

1.1.4. Manuals o instruccions

- **Contingut**. Són llistes de tasques o instruccions detallades per a fer determinades accions o utilitzar eines concretes. Acostumen a dependre de l'entorn tecnològic, de manera que s'han d'adaptar quan es produeixen canvis de producte o versió. Per exemple, manuals d'ús d'eines o instruccions de configuració de programari o d'actualització de pegats.

- Els manuals o instruccions els proporcionen generalment els fabricants i distribuïdors de productes. No obstant això, també es poden generar internament, sobretot a l'entorn de l'operació o explotació dels sistemes d'informació i telecomunicacions. En aquest cas els ha d'aprovar el responsable que correspongui.

- **Caràcter normatiu**. Solen ser de compliment obligat.
- **Aprovació**. Ho ha de fer el responsable corresponent.
- **Divulgació**. A les persones que han de dur a terme l'actuació.

1.1.5. Altres documents

El marc normatiu pot portar associats altres tipus de document, com per exemple els següents:

- **Formularis**. Són plantilles (en format electrònic o de paper) destinades a generar un document que persegueix una finalitat concreta. Corresponen a models de contractes, cartes, sol·licituds, registres, que una vegada emplenats adquireixen validesa, generalment, mitjançant la signatura d'acceptació del document. Generalment estan associats a normes o guies,

o a procediments. Per exemple, una sol·licitud d'alta d'usuari, una acceptació d'obligacions per part de personal extern o una sol·licitud d'excepció de seguretat.

- **Experiències**. Recullen projectes que s'han dut a terme en departaments o àrees de l'organització, o en altres companyies de la matriu, que poden resultar d'interès, ja que poden ajudar a formar-se una opinió, especialment en les àrees en què no hi ha estàndards, sia perquè la tecnologia no és prou madura o perquè resulta difícil aconseguir el consens.

1.2. El cicle de vida d'un estàndard

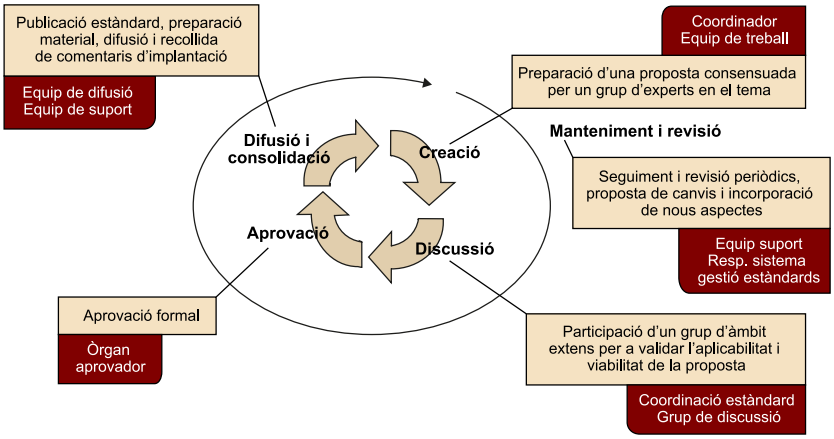
El cicle de vida d'un estàndard es divideix en sis fases:

- Determinació de la necessitat.
- Creació.
- Discussió.
- Aprovació.
- Difusió i ajust.
- Manteniment i revisió.

El plantejament general és que, a partir d'haver detectat una necessitat, un grup de treball elabora una proposta de solució, que és debatuda públicament en un grup de discussió, elevada a aprovació definitiva i, finalment, divulgada. Una vegada tancat aquest procés, comença una altra fase de seguiment i observació de l'estàndard, que en provoca l'actualització o modificació quan els canvis o les noves realitats ho requereixen.

El procés d'elaboració d'estàndards parteix d'una filosofia iterativa: en les fases de creació i discussió es refinen els resultats fins que es considera que el producte està a punt; després d'un període de manteniment i revisió de l'estàndard, es pot tornar a començar amb el procés de creació d'una altra versió que progressivament millori l'estàndard i l'adeqüi a les noves realitats. A partir d'aquesta nova versió es repeteixen consecutivament les fases de discussió, aprovació i difusió de l'estàndard.

El cicle de vida d'un estàndard



1.2.1. Determinació de la necessitat

El primer pas és determinar quins aspectes de la seguretat de la informació s'han de cobrir, i definir els beneficis esperats i la necessitat i àmbit que cal cobrir, especialment quan l'estàndard té caràcter normatiu. Aquesta fase la impulsa el responsable del sistema de gestió dels estàndards.

En aquesta fase cal designar una persona que coordini tot el procés de definició, i també l'equip de treball amb què treballarà el coordinador, i l'equip de discussió a què se sotmetrà el document abans d'aprovar-lo. El fet de designar el coordinador i l'equip de treball implica, per descomptat, la corresponent dotació amb prou recursos per a dur a terme la tasca assignada.

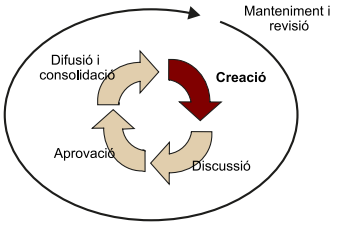
Responsable del sistema de gestió dels estàndards

- **Funció**. És la persona responsable de controlar el marc general d'estàndards, vetllar pel desenvolupament del marc de treball establert, controlar versions, garantir un procés de revisió periòdic i consensuar canvis en el marc de treball quan es rebin requisits en aquest sentit. Aquesta figura simplement vetlla perquè els estàndards es mantinguin actualitzats en el temps, i hi implica a cada moment els actors necessaris. Per tant, no és indispensable que tingui un perfil tècnic, perquè no ha de tenir un coneixement profund del contingut dels estàndards.

- **Composició**. La responsabilitat del sistema de gestió es pot dividir en diferents àmbits d'actuació. El responsable de cada àrea d'actuació és responsable del cicle de vida dels estàndards que van a parar a la seva òrbita. Així, doncs, hi pot haver un responsable d'estàndards TIC, d'estàndards de seguretat de la informació, d'estàndards de qualitat, etc.

1.2.2. Creació

Una vegada són clars l'abast i els beneficis que s'esperen obtenir, el grup de treball elabora una proposta de document. Per a fer-ho, s'analitzen possibles experiències dins de l'organització, i l'estat de l'art de la tecnologia si es considera necessari.



Fase de creació de l'estàndard

L'objectiu d'aquesta fase és tenir una primera versió de l'estàndard. Les tasques d'aquesta fase les fa el grup de treball que estableix internament el procés de creació i discussió interna del document (mitjançant reunions, fòrums, correu electrònic, etc.). Per a fer-ho, és útil disposar d'eines de col·laboració.

Durant aquesta fase és important analitzar l'impacte d'implantació de l'estàndard, sia econòmic o organitzatiu, ja que és un dels aspectes clau per a aprovar-lo.

Quan el coordinador considera que s'ha aconseguit un document correcte i amb prou consens, s'obre la fase de discussió.

Coordinador de l'estàndard

Funció. És responsable del procés global de definició de l'estàndard.

- Coordina l'equip de treball i l'equip de discussió.
- Decideix quan l'estàndard passa d'una fase a una altra.
- És responsable de garantir el traspàs de coneixement necessari a l'equip de manteniment i revisió.
- Forma part de l'equip de difusió i fa propostes en relació amb el material divulgatiu.

Composició. Sol assumir el rol una persona especialista en la matèria o amb prou coneixement general per a assumir la coordinació.

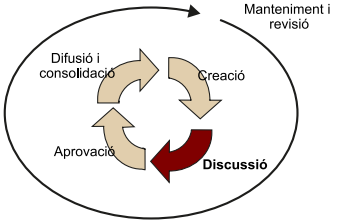
Grup de treball

Funció. Crear un estàndard consensuat per a presentar-lo al grup de discussió.

Composició. El coordinador de l'estàndard, alguna altra persona que pertanyi a l'àrea del coordinador, representants de les àrees que hi estan implicades més directament: recursos humans, sempre que l'estàndard afecti el personal; assessoria jurídica, si la temàtica ho requereix; i experts en la matèria, si se'n té l'oportunitat. El grup l'han de formar sis o set persones com a màxim.

1.2.3. Discussió

Durant aquesta fase s'exposa la proposta de document a un col·lectiu més ampli de l'organització (idealment amb representativitat general), amb l'objectiu d'enriquir-lo amb aportacions, incorporar algun punt de vista que potser no s'havia tingut en consideració en la fase anterior i, sobretot, validar l'aplicabilitat en l'organització de tot el que s'ha recollit en l'estàndard.



Fase de discussió de l'estàndard

El coordinador s'encarrega de recollir tots els comentaris que ha aportat el grup de discussió i de debatre'ls amb el grup de treball. En principi, tant si les aportacions són acceptades com si no, s'ha de respondre a tots els comentaris rebuts.

Quan el coordinador considera que el document és apte per a aprovar-lo, l'estàndard queda **pendent d'aprovació** i s'acaba aquesta fase.

Quan el coordinador envia el document a validar al grup de discussió és important indicar el termini disponible per a enviar comentaris i fer un recordatori uns dies abans que expiri aquest termini. Un termini recomanable és de quinze dies, i s'ha de mirar de no superar les tres setmanes.

D'altra banda, és important sol·licitar respostes als destinataris, tant si tenen comentaris per fer com si estan d'acord amb el document.

És recomanable que el coordinador guardi un registre de tots els comentaris i les respostes produïdes durant aquesta fase.

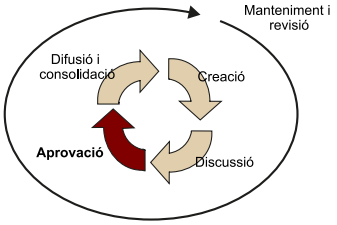
Grup de discussió

Funció. Validar l'estàndard, analitzar-ne l'aplicabilitat a la companyia i aportar-hi comentaris. S'ha d'aprovar de manera consensuada abans d'enviar-lo a aprovació.

Composició. Representació de tots els departaments o àrees de la companyia (inclosos recursos humans i assessoria jurídica), de convidats experts si se'n té l'oportunitat i de personal de proveïdors als quals pot afectar la implantació de l'estàndard si escau.

1.2.4. Aprovació

En aquesta fase, l'organisme corresponent duu a terme l'aprovació formal del document. El document s'envia prèviament a l'òrgan aprovador, que pot sol·licitar modificacions. Una vegada fetes, se sotmet a aprovació i se'n determina la data d'entrada en vigor.

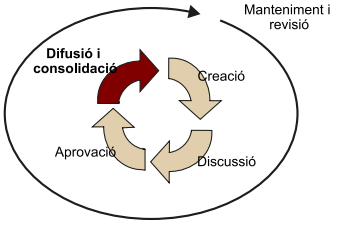


Fase d'aprovació de l'estàndard

Quan l'òrgan aprovador és d'alt nivell (comitè de direcció, per exemple), cal fer una presentació que resumeixi els objectius de l'estàndard, l'àmbit d'aplicació d'aquest estàndard, l'impacte d'implantació que té (sia econòmic o no) i les persones que participen en els grups de treball i de discussió.

1.2.5. Difusió i consolidació

Una vegada aprovat, s'ha de fer arribar el document a tots els afectats definits dins de l'àmbit d'aplicació de l'estàndard, per a donar-lo a conèixer i començar el seguiment de la implantació.



Fase de difusió i consolidació de l'estàndard

La difusió de l'estàndard s'ha de considerar com una acció en positiu en què es posa èmfasi no solament en els aspectes normatius o de recomanació, sinó també en tots els beneficis que aporta a l'organització el fet de tenir un estàndard.

Alguns dels canals que es poden usar per a la difusió són els següents:

- Publicació en la intranet, en un espai dedicat.
- Emissió de notes (correu electrònic, circular interna, etc.) relatives a la publicació del nou estàndard, amb un enllaç que hi porti.
- Inclusió de la notícia en xats o fòrums corporatius.
- Accions presencials en àmbits sensibles i clau.
- Sessions formatives.

Per a fer-ne difusió, sol ser útil tenir persones clau a cada àrea de l'organització, que són les que s'encarreguen de divulgar de manera efectiva i de recordar l'existència dels estàndards en el seu àmbit.

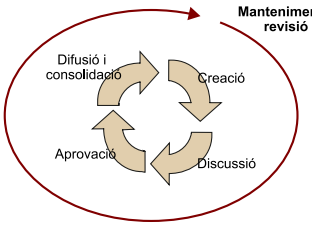
Des del moment de l'aprovació i en paral·lel amb la difusió, els usuaris afectats poden emetre queixes, consultes, suggeriments o fins i tot requisits que no cobreix l'estàndard, perquè es tinguin en compte en les noves versions que se'n facin.

És important que els usuaris coneguin aquest procés de validació de la implantació i l'utilitzin. Per a fer-ho, pot ser útil habilitar bústies de correu o persones de contacte a les quals dirigir aquestes aportacions. És habitual que es focalitzin en els canals de suport a usuari, que centralitzen la recollida de comentaris i els fan arribar al coordinador de l'estàndard, que decideix si cal començar un cicle de revisió o bé si es pot esperar a versions posteriors. En aquest últim cas, l'estàndard passa a la fase de manteniment i revisió, es dissol l'equip de treball i passa a fer-se'n càrrec l'equip de suport, sota la supervisió del responsable del sistema de gestió.

En l'àmbit formal, el fet de superar la fase de difusió i consolidació significa que l'estàndard ha estat contrastat per l'experiència i el contingut passa a ser consolidat i estable.

1.2.6. Manteniment i revisió

Els estàndards no s'han d'entendre com a documents tancats, sinó que són documents vius immersos en un procés de millora.



Fase de manteniment i revisió de l'estàndard

Des del moment en què es publica l'estàndard, hi ha d'haver un equip que vetlli pels aspectes següents:

- Donar resposta a preguntes i dubtes que es derivin de la implantació de l'estàndard.

- Mantenir la infraestructura que sosté la publicació i difusió dels estàndards i les publicacions afins.

- Vetllar per la implantació correcta de l'estàndard.

- Parar esment en possibles canvis organitzatius o tecnològics que obliguin a modificar l'estàndard i comunicar la necessitat de fer-ho al responsable del sistema de gestió dels estàndards.

- Proposar canvis en el contingut o la redacció de l'estàndard, depenent de les incidències, els problemes o els malentesos detectats.

- Portar un registre de totes les modificacions possibles que s'han de preveure en versions posteriors.

En cas de disposar d'un documentalista, és important que participi en el procés d'estructuració i gestió documental dels estàndards.

1.3. Contingut mínim d'un estàndard

És important definir el format d'un estàndard i quin n'ha de ser el contingut i l'estructura mínima abans de posar-se a redactar. Tenir una plantilla ofereix diferents beneficis:

- Un format comú permet a qui ho llegeix identificar a simple vista que es tracta d'un estàndard.

- Exposar la informació sempre en el mateix ordre facilita trobar allò que es busca.

- Una terminologia comuna facilita la comprensió a qui ho llegeix.

- Evita que es passin per alt aspectes importants en la redacció.

- Ofereix una imatge de coherència i ordre, que reforça el pes del document.

L'estructura d'un estàndard no és una llista tancada. A continuació presentem una proposta que es pot prendre com a referència i adaptar a la casuística i cultura pròpia de cada organització.

En principi, qualsevol estàndard ha de contenir els apartats que s'exposen a continuació. Depenent del tipus d'estàndard, no obstant això, es poden crear diferents plantilles. Així, doncs, per exemple, en un procediment és bastant habitual que hi hagi un fluxograma. Es pot considerar com un apartat addicional o com a part del desenvolupament del procediment, però d'una manera o altra s'ha d'establir que tot procediment ha de contenir un fluxograma.

Alhora, hi ha alguns estàndards més tècnics que poden estructurar el contingut d'una manera comuna i també s'hi pot establir una plantilla comuna. Per posar un exemple, tota guia de protecció d'un entorn tecnològic possiblement s'ha de referir a aspectes com la configuració inicial, el control d'accés, el monitoratge o l'auditoria, i aquests podrien ser seccions predefinides en la plantilla d'aquest tipus d'estàndard.

A part de definir uns apartats mínims, s'ha de crear un estàndard de notació per a indicar que hi ha una paraula en el glossari de termes, per a marcar de manera diferenciada un document referenciat o per a saber com s'ha d'actuar si un determinat apartat no aplica.

Vegem, doncs, una proposta de contingut de **plantilla mínima** d'estàndard.

1) Encapçalament/peu del document

Habitualment, hi apareix el següent:

- El logotip de la companyia.
- El tipus d'estàndard: política, norma, guia, etc.
- La codificació de l'estàndard.
  La codificació ha de reflectir com a mínim el tipus d'estàndard, una numeració i el número de versió.
- El número de pàgina i el nombre total de pàgines.
- El número de versió.
- L'estat del document: aprovat, en discussió, en revisió, etc.
- La protecció de l'estàndard, si es considera necessari, contra còpia no autoritzada. En aquest sentit, són molt útils les llicències Creative Commons per a la protecció d'obres amb alternatives molt diferents. Així, doncs, per exemple, en el cas de les administracions públiques, en què és relativament habitual publicar obertament el marc normatiu, és habitual el tipus de llicència Creative Commons que autoritza a copiar i millorar els estàndards, però no a obtenir-ne beneficis econòmics.

2) Objectiu i motivació

Amb quina finalitat s'emet l'estàndard. Quin és l'origen o la causa de l'emissió.

3) Àmbit i vigència

- **Àmbit**. Es refereix, d'una banda, a qui va dirigit el document, si pot ser, especificat en forma de perfils. Per exemple, caps de projecte, operadors, tècnics de sistema o usuaris en general.
  D'altra banda, es refereix a quin és l'**àmbit d'aplicació**: tota la corporació, només una companyia de la corporació, un edifici de la companyia, una fàbrica, etc.

I si és possible, també al **tipus de recurs afectat**. Per exemple, tots els servidors de xarxa o totes les comunicacions entre seus.
Si hi ha alguna limitació o restricció sobre l'aplicabilitat d'algun dels controls, és aconsellable incloure-ho en aquest apartat.

- **Vigència**. S'especifica quan entra en vigor l'estàndard i si s'hi concedeix un període d'adaptació.

4) Compliment legal i d'estàndards de seguretat

Fa referència a la normativa legal aplicable o a estàndards reconeguts. En aquest apartat, es podria portar el control de quins són els apartats de l'ISO 27002 als quals es dóna cobertura.

5) Descripció

Tal com ja s'ha comentat, aquest apartat es pot desglossar en diferents apartats, que varien segons el tipus d'estàndard.

És en aquest punt on es descriuen les mesures de seguretat que especifica l'estàndard, amb independència de si són normes o recomanacions. En el cas de polítiques o normes, es pot donar el cas de recollir tant normes com recomanacions; en aquest cas, ha de quedar clar de quin tipus de mesura o control es tracta.

Això es pot aconseguir, per exemple, amb la notació dels controls:

- Normes
  - N1
  - N2

- Recomanacions
  - R1
  - R2

6) Control

És la descripció de qui durà a terme el control de compliment de l'estàndard i com ho farà. En els estàndards amb caràcter normatiu, si no es realitza cap tipus de control, és difícil que es respecti l'estàndard.

Sempre que es produeixi una incidència relacionada amb la política o norma és aconsellable fer una revisió de compliment i completesa del document.

És habitual que el control es faci en dos nivells.

- Seguiment periòdic. És un seguiment mensual o trimestral, a partir d'indicadors, informes de compliment dels principals aspectes de la política o norma.

- Auditoria periòdica. L'auditoria dels estàndards no és una fase pròpiament dita del cicle de vida dels estàndards, però és una activitat paral·lela indispensable per diversos motius:
  - Permet saber el grau d'implantació de l'estàndard i, per tant, l'efectivitat que té i reportar-ho a la direcció.
  - Permet controlar la gestió correcta de les excepcions.
  - Permet saber els incompliments que es repeteixen de manera recursiva i que, possiblement, requereixin una revisió.
  - Proporciona reflexions i aportacions de millora per a versions posteriors.
  - Permet detectar vulnerabilitats de l'organització.
  - Proporciona als usuaris responsables de complir-los la certesa que els estàndards hi són per a complir-los i que no són "decoratius".

Com bé diu el proverbi:

> "Cosa manada, no és feta si no és vigilada."

Desgraciadament, el món de la seguretat de la informació funciona bastant "a cop de control", és a dir, que no hi ha la conscienciació generalitzada que la seguretat és necessària perquè sigui aplicada de manera global i proactiva, sinó que s'han d'establir normes de compliment obligat i controlar que es respectin.

Per tant, és important que l'àrea de la companyia sobre la qual recau la funció auditora o de control intern inclogui dins del pla d'auditories el compliment dels estàndards de manera sistemàtica i que més o menys cada dos anys faci un repàs general del marc normatiu complet.

Òbviament, s'han de facilitar els informes d'auditoria com a mínim al responsable de l'incompliment i al seu responsable directe, al responsable de seguretat de la informació i al responsable del sistema de gestió d'estàndards. El responsable de seguretat de la informació té la responsabilitat d'analitzar el perquè dels incompliments, de fer un seguiment del pla d'acció establert per a corregir-los i de reportar periòdicament la situació a la direcció.

7) Penalitzacions

Són accions de penalització o conseqüències en cas d'incompliment.

8) Divulgació

Identificació del responsable de la divulgació i dels mitjans amb què es fa.

9) Revisió

Fa referència a la data de la pròxima revisió prevista i a les causes o les hipòtesis per les quals s'ha de fer una revisió abans de la data prevista.

Com més avall de la piràmide de documentació, més freqüència de revisió.

10) Glossari de termes

És la definició de terminologia utilitzada en la redacció del document, per a aclarir conceptes o evitar ambigüitats (termes tècnics, conceptes molt propis de la companyia o sector, abreviatures, etc.).

11) Documentació referenciada

És la relació de documents a què s'ha fet referència al llarg del document: polítiques, normes, procediments, manuals, etc. Si és possible, la documentació s'ha de referenciar mitjançant el codi i nom que té, però no mitjançant la versió, per a evitar l'actualització de l'estàndard davant canvis de versió en els documents referenciats.

12) Paraules clau

És la relació de termes que poden servir per a localitzar el document en cas de recerca (molt útil en gestors documentals).

13) Històric del document

Cada vegada que es produeix un canvi de versió es fa una descripció breu dels canvis introduïts i el motiu d'aquests canvis, per a facilitar el seguiment de versions.

En cas que l'estàndard substitueixi un altre estàndard que ja és obsolet, s'ha de fer constar en aquest apartat.

1.4. Fitxa de l'estàndard

A part de la plantilla d'estàndard, és recomanable tenir una fitxa de l'estàndard, com un document a part, en què es reculli informació com la següent:

- Classificació de l'estàndard.
  Segurament, a l'hora de publicar els estàndards, els agruparem per tipologia. Per exemple, operació, administració, arquitectura o d'usuari.

- Dates del cicle de vida: dates previstes i reals de començament i final de cada fase.

- Components dels grups de treball i discussió.

- Comentaris rebuts i respostes donades. Dins d'aquesta informació se solen posar de manifest algunes vulnerabilitats dels sistemes, de manera que la fitxa s'ha de conservar com un document de caràcter restringit.

- Qualsevol altra informació rellevant sobre l'estàndard que no hagi de formar part del document publicat.

1.5. La redacció de l'estàndard

Hi ha una àmplia literatura sobre el marc normatiu i la redacció d'estàndards que es pot consultar. En aquest mòdul només farem una introducció als aspectes clau, mitjançant **deu regles d'or** o consells pràctics que cal tenir en compte a l'hora de redactar un estàndard.

1) Respectar l'ordre de redacció dels apartats i reflexionar sobre cadascun d'aquests apartats. Abans de desenvolupar el contingut de l'estàndard, és molt important tenir clar el motiu pel qual es desenvolupa i a qui va dirigit. Val la pena dedicar un temps a pensar sobre aquests aspectes, ja que són determinants per al contingut.

D'altra banda, hi ha apartats com el de control o penalitzacions que solen ser complicats, però cal dedicar un temps a pensar-hi. A vegades, val més no posar un control si després no hem de ser capaços de fer-ne el seguiment.

Pel que fa a les penalitzacions, varien segons el tipus de companyia, però, en qualsevol cas, s'han d'establir i consensuar amb la direcció per a rebre'n el suport si cal.

2) No copiar un estàndard d'uns altres estàndards. La literatura i Internet són replets d'estàndards de tota mena publicats per companyies i administracions públiques. És correcte basar-se en altres estàndards per a redactar els de la nostra companyia, ja que que ens serveixen de punt de partida i ens facili-

ten la feina. No obstant això, és un error copiar-los sense fer les reflexions que comentàvem en el punt anterior i sense adaptar-los a la casuística i cultura de la nostra companyia, error que pot portar l'estàndard al fracàs.

3) El contingut ha de ser suficient. Un document pobre en contingut no justifica l'esforç de portar-lo a aprovació. Segurament es pot incloure en un altre estàndard o agrupar-se amb altres conceptes, per a crear un estàndard amb més contingut.

4) Pensar abans de començar si l'estàndard s'ha de complir obligatòriament o no. El vocabulari i temps verbal que s'utilitza en la redacció varia segons si es tracta d'una norma o una recomanació.

5) Estructurar bé el contingut. L'apartat "Descripció", en què es desenvolupa l'estàndard, ha d'estar ben estructurat, de manera que s'agrupin els controls que tenen alguna cosa en comú i s'ordenin sempre de més a menys importància, i de menys a més nivell de detall (primer el general, per a baixar després al detall).

6) Cada control ha de ser un punt auditable per si mateix. En estàndards de caràcter normatiu, és molt important que cada control sigui auditable independentment, cosa que facilita molt la funció auditora i permet un seguiment més senzill del nivell de compliment. D'aquesta manera, quan arriba un auditor i audita el control N15, per posar un exemple, ha de ser capaç de dir si és conforme o no, sense ambigüitats. És a dir, en cap cas no ha de dir que es compleix la primera part del control, però no la segona.

Això pot implicar tenir un nombre més gran de controls, però redunda en claredat i efectivitat en el seguiment.

7) Utilitzar un llenguatge senzill i no fer faltes ortogràfiques ni errades de redacció. Utilitzar un llenguatge directe, frases curtes i estructures gramaticals senzilles i poc rebuscades, comprensibles per a tothom a qui va dirigit el document. Parar esment en els correctors ortogràfics.

8) No donar mai per descomptat que se saben les abreviatures. Per òbvia que resulti, és recomanable que sempre que surti per primera vegada una abreviatura se'n detalli el significat i que sempre es reculli en el "Glossari de termes".

9) Com a mínim, una lectura de principi a fi sense interrupcions, com si fos la primera vegada que ho llegim. No donar per acabada la redacció del document fins que no s'ha aconseguit llegir-lo com a mínim una vegada sense interrupcions de principi a fi, amb la perspectiva d'algú que es troba el document per primera vegada. Adoptar aquesta mentalitat pot posar en alerta

del fet que es donen per coneguts alguns temes que no són obvis o que es deixa d'explicar qüestions complementàries que són necessàries per a comprendre l'estàndard.

10) Sotmetre sempre el document a discussió, i fer-ho amb esperit obert i humil. Va molt bé rebre comentaris a un estàndard, per poc rellevants que semblin, i parar esment en tots i cadascun d'aquests comentaris, ja que això ens pot posar en la pista de temes mal explicats, no considerats, etc., de manera que cal rebre tots els comentaris amb esperit positiu i obert. Pel que fa a l'esperit humil, segurament, qui revisa un document no és del tot conscient de l'esforç que implica escriure un estàndard des de zero, que sens dubte és molt més complex que revisar-lo, per la qual cosa és possible que els seus comentaris no tinguin prou sensibilitat devers l'autor, però l'autor també ha de ser conscient d'això i no tenir-ho en compte, i ha de treure el màxim partit dels comentaris rebuts.

2. Política de seguretat de la informació

L'estàndard per excel·lència en un **sistema de gestió de la seguretat** és, sens dubte, la **política de seguretat de la informació**, ja que constitueix el primer nivell de la piràmide jeràrquica en seguretat de la informació.

Com ja s'ha comentat, l'objectiu d'aquesta política és establir les directrius en seguretat de la informació, alineades amb els objectius del negoci i la legislació aplicable, i tot plegat confirmat i amb el compromís de la direcció de la companyia.

L'ISO 27002, a l'apartat 5, fa una descripció detallada de quin ha de ser el contingut de la política de seguretat de la informació i dels principals aspectes de la revisió d'aquesta política.

A continuació es comenten alguns aspectes importants que cal tenir en consideració en el moment de redactar-la:

- A la política de seguretat de la informació s'hi aplica tot el que s'ha exposat abans sobre el cicle de vida, el contingut mínim (o plantilla d'estàndard) i les deu regles d'or per a redactar-la, de la qual cosa es dedueixen alguns dels punts exposats a continuació.

- No es pot copiar la política d'una altra companyia. Es tracta d'exposar els objectius de seguretat, al servei d'aconseguir els objectius del negoci, de manera que és difícil que la política d'una empresa automobilística tingui gaire a veure amb la d'una empresa alimentària, per posar un exemple.
  Per tant, s'ha de personalitzar a la casuística pròpia i incorporar totes les lleis o normes sectorials que siguin aplicables, i a les quals s'ha de donar compliment, i que justificaran moltes de les mesures de seguretat que s'hagin d'implantar en la companyia.
  Alhora, si la companyia ha decidit accedir a la certificació de l'SGSI o simplement prendre una norma internacional com a guia de bones pràctiques, és interessant destacar-ho en aquest document.

- S'ha d'aprovar al més alt nivell de la companyia. La direcció ha de conèixer, aprovar i signar el contingut, i donar a conèixer el seu compromís amb aquesta política a la resta de la companyia. Per això, quan s'aprovi la política, és interessant que la difusió provingui de la direcció mateixa, perquè tot el personal tingui clar qui n'és el promotor principal.

- S'ha de divulgar a tot el personal de la companyia i terceres parts amb accés a informació.

Per això ha de ser un document generalista, que no entri en gaire detall, que doni la mínima informació necessària i que no utilitzi una terminologia gaire tècnica ni faci referència a noms de persones o productes concrets.

- La política no ha de ser un document extens; n'hi ha d'haver prou d'un parell de pàgines com a màxim, ja que si no és difícil que la llegeixi tot el públic a qui va destinada.

- La política ha de descriure què entén la companyia per *seguretat de la informació*, que generalment ha de fer referència a la confidencialitat, integritat i disponibilitat de la informació de la companyia, encara que s'hi pot incloure l'autenticitat, la privadesa i fins i tot la traçabilitat, tal com fa l'Esquema Nacional de Seguretat (RD 3/2010).

- Necessàriament, la política ha de fer esment de l'organització de la seguretat de la informació i descriure breument quins són els organismes o càrrecs principals en matèria de seguretat de la informació, amb una descripció breu de les seves funcions i referenciant, en tot cas, un altre document en què es reculli una descripció detallada de funcions.

- La política ha de recollir la necessària implicació de tot el personal per a treballar d'una manera segura.

- Alhora, ha de referenciar el marc normatiu que la desplega i ha de fer, si és possible, una descripció breu del contingut de cadascuna d'aquestes normes o polítiques de segon nivell.

- S'ha de revisar anualment i la direcció l'ha d'aprovar i corroborar anualment també. D'aquesta acció se n'ha de guardar registre (mitjançant una acta de reunió signada, per exemple).
  Alhora, pot requerir una revisió abans del termini previst en certes situacions com la materialització d'una incidència important de seguretat o canvis organitzatius rellevants.

L'aprovació d'una política de seguretat de la informació i, en general, d'un marc normatiu és un procés habitualment llarg, especialment en l'àmbit de l'Administració pública o de grans corporacions, de manera que és un dels primers passos que cal seguir, juntament amb la definició de l'organització de seguretat. No tenir la política de seguretat aprovada no ha de ser un impediment per a continuar progressant en la implantació de l'SGSI, però és important no abandonar-la, ja que és el pilar de tot el procés de gestió de la seguretat de la informació.

3. Organització de la seguretat de la informació

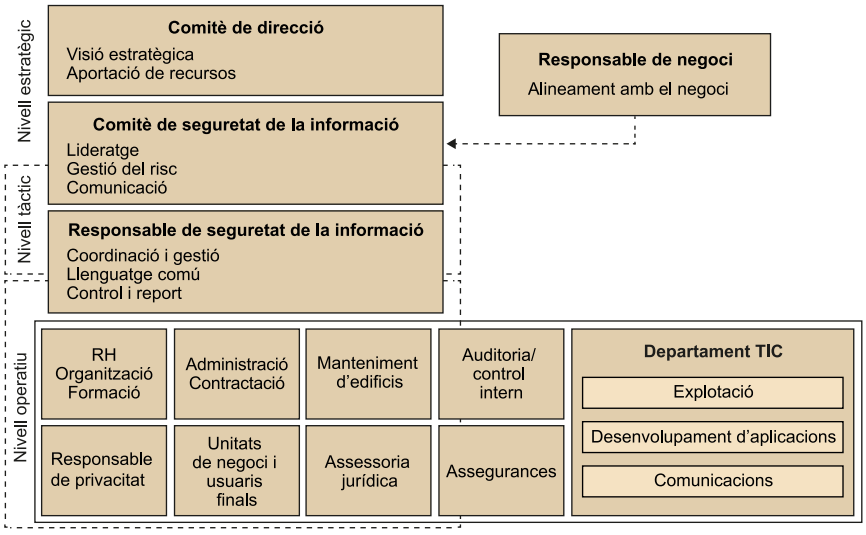
L'organització de la seguretat de la informació és una de les primeres tasques que cal abordar en la implantació de l'SGSI. Tots els esforços en matèria de seguretat de la informació seran inútils o molt poc eficaços si la companyia no té clar qui té autoritat, sobre quins aspectes i qui és responsable de quines tasques o de quins àmbits.

Per tant, cal crear una estructura interna amb responsabilitat directa sobre la seguretat de la informació. Aquesta estructura és molt variable segons la grandària i el tipus de companyia, però, sigui quina sigui, les funcions han de quedar clares i s'han d'atribuir a persones concretes, amb dedicació exclusiva o parcial.

Una altra vegada resulta indispensable que la direcció aprovi l'estructura organitzativa i l'assignació de funcions de seguretat i hi doni suport, per a dotar les persones amb responsabilitat en la matèria de l'autoritat i el temps necessaris per a exercir les seves funcions dins de la companyia.

A continuació s'exposa una possible estructura organitzativa de seguretat de la informació, habitual en moltes organitzacions.

Possible estructura organitzativa en seguretat de la informació



Aquesta estructura organitzativa revela que la seguretat de la informació implica tota la companyia i tot el personal, sia en l'àmbit estratègic o en un de més tàctic o operatiu.

A continuació es descriuen les funcions de cadascuna de les responsabilitats o dels òrgans definits, i també es fan alguns comentaris sobre qui és recomanable que assumeixi la funció.

3.1. El comitè de direcció de la companyia

Les funcions en matèria de seguretat de la informació del comitè de direcció de la companyia són les següents:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres d'un comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar riscos possibles introduïts per canvis en les funcions o en el funcionament de la companyia per a adoptar les mesures de seguretat més adequades.
- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en la matèria.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

Les decisions preses pel comitè de direcció en matèria de seguretat de la informació han de quedar recollides en acta.

3.2. El comitè de seguretat de la informació

Les decisions en matèria de seguretat de la informació les pren de manera consensuada un grup format per diferents responsables dins de la companyia.

Les funcions en matèria de seguretat de la informació del comitè de seguretat de la informació són les següents:

- Implantar les directrius del comitè de direcció.
- Assignar rols i funcions en matèria de seguretat.

- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.

- Validar el mapa de riscos i les accions de mitigació que ha proposat el responsable de seguretat de la informació.

- Validar el pla de seguretat de la informació o pla director de seguretat de la informació i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.

- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.

- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.

- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.

- Revisar les incidències més destacades.

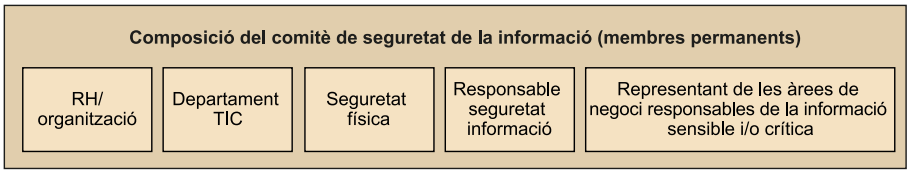
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució de l'SGSI.

Depenent de la grandària de la companyia, pot passar que el comitè de seguretat tingui els mateixos integrants que el comitè de direcció, però en grans companyies, o en l'Administració pública, sol ser un òrgan a part, dependent del comitè de direcció.

El comitè de seguretat de la informació sol tenir representació de diverses àrees de suport i també de les principals unitats de negoci (les que estan sotmeses a més riscos).

La composició és molt variable, però habitualment consta d'un grup de membres permanents i de convidats segons la temàtica.

Components habituals del comitè de seguretat de la informació



1) Membres permanents. Els membres permanents són el director de recursos humans, el director d'organització, el director de tecnologies de la informació i la comunicació, seguretat física (si existeix de forma diferenciada), el responsable de seguretat de la informació i els responsables de les àrees de negoci més crítiques o sensibles (unitats amb alts riscos, amb distribució territorial, etc.).

2) Membres per invitació. Són els representants d'altres unitats, com assessoria jurídica, auditoria o control.

Pel que fa a la freqüència de reunió, al començament de la implantació de l'SGSI és convenient que el comitè de seguretat es reuneixi sovint (cada dues setmanes o cada mes). Una vegada superades les dues primeres fases de l'SGSI (planificar i fer), n'hi pot haver prou d'una reunió cada dos o tres mesos, i sempre que sigui necessari en cas de crisi.

3.3. Responsable de seguretat de la informació

La designació d'un responsable de seguretat de la informació (RSI) és l'única via per a avançar de manera organitzada i gradual en seguretat de la informació, ja que garanteix que hi ha algú per a qui la seguretat de la informació és una prioritat.

Les funcions en matèria de seguretat de la informació dels RSI són coordinar les accions orientades a garantir la seguretat de la informació en qualsevol de les formes que té (digital, òptica, paper, etc.) i en tot el cicle de vida d'aquesta informació (creació, manteniment, distribució, emmagatzematge i destrucció), per a protegir-la en termes de confidencialitat, privadesa, integritat, disponibilitat, autenticitat i traçabilitat.

Tot plegtat es concreta en els punts següents:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.

- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius en matèria de seguretat de la informació.

- Desenvolupar i mantenir el document d'*Organització de la seguretat de la informació* en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les responsabilitats en seguretat i també una descripció detallada de funcions i dependències.

- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.

- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.

- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).

- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.

- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.

- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.

- Vetllar pel compliment legal (LOPD, RD 3/2010, Esquema nacional de seguretat, Basilea, SOX, etc.) i coordinar les actuacions necessàries amb les unitats responsables.

- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.

- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.

- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.

- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

Depenent de la companyia, és possible que hi hagi alguna de les funcions enumerades que no siguin atribuïdes a l'RSI, cosa que no ha pas de ser un problema sempre que la funció estigui assignada a algú i hi hagi comunicació i una gestió coordinada entre responsables.

L'RSI pot delegar algunes de les seves funcions en segones persones, però en continua essent el responsable final i s'ha d'assegurar que es porten a terme correctament.

L'RSI s'ha de comunicar amb tot el negoci, però hi ha d'haver una relació estreta amb unitats com recursos humans o organització (seguretat relativa al personal i procediments transversals), àrea de les TIC (seguretat en l'operació, seguretat en el desenvolupament de nous sistemes d'informació, seguretat en les comunicacions, etc.) o seguretat física.

Algunes observacions sobre el càrrec

És molt recomanable que la funció d'RSI l'assumeixi personal intern. El percentatge de dedicació a les funcions de seguretat de l'RSI depèn de la problemàtica, les dimensions i les necessitats de cada organització. En companyies amb una certa grandària, és habitual que l'RSI gestioni un equip de professionals de seguretat, interns o externs (situats en instal·lacions pròpies o de manera remota).

Perquè l'RSI pugui desenvolupar les seves funcions, cal dotar-lo dels recursos humans o tècnics necessaris.

La funció d'RSI ha de recaure sobre una persona amb bons coneixements de l'organització i el seu negoci, de manera que sigui capaç de trobar l'equilibri adequat entre seguretat de la informació i la màxima rendibilitat de la tecnologia al servei dels interessos i objectius de l'organització.

Per a mantenir una segregació correcta de funcions i evitar conflictes d'interès, la responsabilitat de l'RSI no l'ha d'assumir el director de les TIC ni cap persona amb funcions que li permetin prendre decisions tècniques o operatives relacionades amb els sistemes d'informació.

L'RSI ha de tenir un perfil dialogant i integrador, saber treballar en equip i ser capaç de convertir-se en interlocutor entre els equips tècnics i els equips de negoci.

3.4. Delegat de protecció de dades

El Reglament general de protecció de dades vigent (RGPD, reglament de la UE 2016/679) estableix la figura del delegat de protecció de dades (DPD o també conegut com a DPO, de l'anglès *Data Protecion Officer*), que constitueix un

dels elements clau de l'RGPD, i un garant del compliment de la normativa de la protecció de dades en les organitzacions, sense substituir les funcions que desenvolupen les autoritats de control.

El delegat de protecció de dades haurà de tenir coneixements especialitzats de dret i, òbviament, de protecció de dades. Actua de manera independent i se li atribueixen una sèrie de funcions regulades a l'article 39 de l'RGPD, entre les quals destaquen informar i assessorar, així com supervisar el compliment del citat RGPD per part del responsable o encarregat.

3.5. Altres responsabilitats distribuïdes per la companyia

3.5.1. Responsables funcionals de la informació

Tenen les funcions següents:

- Classificar la informació de la qual són responsables segons la criticitat que aquesta tingui per a la companyia en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no-repudi, traçabilitat i impacte mediàtic i determinar l'ús que s'ha de fer de la informació i qui hi pot accedir.

- Tenir coneixement de la normativa general o sectorial aplicable a la informació de la qual són responsables, inclosa la normativa vigent en matèria de protecció de dades de caràcter personal.

- Definir els requisits de seguretat per al tractament de la informació, sia de manera automatitzada o manual, en tot el cicle de vida de la informació (creació, modificació, conservació i destrucció si escau).

- Fer el seguiment de l'estat de la seguretat dels sistemes d'informació que tractin la informació de què són responsables i gestionar la mitigació de riscos dins del seu nivell de decisió.

- Impulsar l'elaboració de plans de continuïtat de negoci, implicar-s'hi i definir procediments alternatius en cas d'indisponibilitat del sistema o falta d'integritat de la informació.

- Col·laborar a fer revisions i auditories de seguretat de la informació.

3.5.2. Personal en general

Tot el personal intern o extern amb accés a la informació de la companyia (treballadors, proveïdors en prestació de serveis) té les obligacions següents:

- Mantenir la confidencialitat de la informació.

- Fer un bon ús dels equips i de la informació a què tenen accés i protegir-la d'accessos no autoritzats.

- Respectar les normes i els procediments vigents en matèria de seguretat de la informació i vetllar perquè la respectin terceres parts en prestació de serveis.

- Utilitzar adequadament les credencials d'accés als sistemes d'informació.

- Respectar la legislació vigent en matèria de protecció de dades de caràcter personal i qualsevol altra legislació que sigui aplicable.

- Notificar, per la via establerta, insuficiències, anomalies o incidències de seguretat i situacions sospitoses que poden posar en perill la seguretat de la informació.

3.5.3. Àrea de tecnologies de la informació i comunicacions (TIC)

Té les funcions següents:

- Complir les polítiques, les normes i els procediments en matèria de seguretat de la informació. Col·laborar amb l'RSI a definir-los.

- Implantar en els sistemes d'informació els controls de seguretat prescrits i les accions correctores establertes i gestionar les vulnerabilitats detectades.

- Requerir la participació de l'RSI en nous projectes de desenvolupament o adaptació o implantació de productes de mercat, especialment quan puguin ser crítics en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no-repudi i traçabilitat, o puguin tenir un impacte mediàtic important.

- Requerir la participació de l'RSI en la implantació o gestió dels canvis de maquinari i programari.

- Garantir la inclusió de la seguretat en tot el cicle de vida de les dades (creació, manteniment, conservació i destrucció) i en els processos de gestió de maquinari i programari

- Adoptar mesures per a protegir la informació segons la classificació que n'ha fet el responsable de la informació.

- Col·laborar amb l'RSI a identificar riscos i a proposar solucions, i col·laborar en les revisions o auditories de seguretat que es duguin a terme.

3.5.4. Àrea de seguretat física

Té les funcions següents:

- Proporcionar els mitjans tècnics necessaris per a la protecció física de la informació, tant pel que fa a desastres físics (incendi, inundació, fallades de subministrament elèctric, etc.) com a accessos no autoritzats. La definició de controls que cal implantar s'ha de fer coordinadament amb l'RSI.

- Disposar de mesures de recuperació de la situació normal d'operació d'acord amb els requisits de continuïtat establerts pel negoci.

- Conèixer i implantar els procediments de seguretat establerts en la política de seguretat de la informació.

- L'RSI i el responsable de seguretat física s'han de reportar mútuament i tan aviat com puguin les incidències de seguretat detectades quan puguin afectar l'àmbit de competència de l'altra part.

- Implicar l'RSI en els projectes d'obra i rehabilitació d'edificis, per a tenir en compte *a priori* qüestions d'emplaçament d'elements de xarxa i comunicacions, protecció d'equips, etc.

3.5.5. Àrea de recursos humans

Té les funcions següents:

- Informar les unitats gestores de recursos d'informació sobre canvis o moviments de personal per a fer una bona gestió de recursos: altes, baixes definitives i temporals, canvis de categoria o de funcions, canvis organitzatius, etc.

- Treballar juntament amb l'RSI per a desenvolupar la política de seguretat de la informació en les qüestions referents al personal.

- Aplicar procediments disciplinaris en cas de vulneració del marc normatiu.

3.5.6. Àrea d'assessoria jurídica

Té les funcions següents:

- Col·laborar amb l'RSI a emetre noves polítiques i normes de seguretat i a investigar i resoldre incidències de seguretat quan se'n poden derivar accions legals (reclamacions de terceres parts, accions contra un treballador, etc.).

- Col·laborar amb l'RSI a definir clàusules específiques de seguretat de la informació i a incloure-les en els contractes amb terceres parts i contractes de personal extern.

- Informar l'RSI de nova legislació o canvis en la legislació aplicable, que poden tenir impacte sobre la seguretat de la informació, i donar suport a l'hora d'interpretar-los.

3.5.7. Altres àrees

Cada àrea dins de la companyia ha de col·laborar amb l'RSI a desplegar la seguretat en el seu àmbit d'actuació i a aconseguir treballar i fer treballar l'organització de manera segura. Així, doncs, també s'han d'identificar funcions de seguretat en els àmbits d'auditoria, assegurances, formació, organització, etc.

4. Classificació de la informació

La classificació de la informació és una qüestió molt complexa d'una banda, però essencial de l'altra, ja que és el que permet aplicar controls de seguretat proporcionals a la criticitat de l'actiu que cal protegir, en aquest cas, la informació; és a dir, permet protegir la informació segons el valor que té per a la companyia i focalitza els esforços en la informació de més valor.

Per tant, cal redactar una política de classificació de la informació, que novament la Direcció haurà d'aprovar i que s'haurà de donar a conèixer a tot el personal de la companyia.

La política de classificació ha de tenir en compte aspectes com aquests:

- Definir quines dimensions de seguretat es tindran en compte a l'hora de fer la classificació. Com a mínim, confidencialitat, integritat i disponibilitat, encara que es poden considerar altres criteris: autenticitat, traçabilitat, impacte mediàtic o visibilitat política, etc.

És habitual trobar polítiques de classificació que només tenen en compte la dimensió de la confidencialitat. No obstant això, depenent del tipus de negoci, la resta de dimensions poden resultar tan importants o més que la confidencialitat; en aquest cas també s'han de tenir en consideració.

- Definir el nombre de nivells de classificació per a cada dimensió i l'alineament que tenen amb possibles classificacions establertes per la normativa vigent (LOPD, Esquema nacional de seguretat, etc.). És important que la definició d'aquests criteris es faci en llenguatge de negoci (i no en llenguatge tècnic de seguretat).

- Definir els controls de seguretat que cal aplicar a cada nivell durant el tractament de la informació al llarg de tot el seu cicle de vida. Òbviament, els controls són més restrictius a mesura que augmenta el nivell de criticitat de la informació. En cada cas cal definir qui és el responsable de l'aplicació del control.

- Establir qui classifica la informació o qui n'és el propietari. Tal com es va veure en l'apartat d'organització, els primers responsables de la classificació de la informació són els responsables funcionals del negoci, ja que són els que saben millor la criticitat que té. Per tant, és indispensable que participin en l'equip de treball per a definir aquesta política.

- Precisar el sistema d'etiquetatge o marcatge de la informació (per a qualsevol tipus de format o suport), amb la finalitat que qualsevol persona que accedeixi a aquesta informació sàpiga a quin nivell pertany d'una manera ràpida i senzilla.

Exemple. Definició de criteris de classificació per a la confidencialitat

Nivell	Descripció
Baix	• Informació pública o disponible públicament. • La divulgació d'aquesta informació no implica un perjudici per a la companyia. • És aquella informació a la qual s'atorga accés lliure, dins i fora de la companyia, i no requereix mesures de protecció de confidencialitat.
Mitjà	• Informació a disposició de tot el personal de la companyia mitjançant la intranet, els taulers d'anuncis, etc., sense accés restringit. • Informació no accessible a terceres parts o entitats alienes a la companyia.
Alt	• És informació restringida a un grup concret de persones amb una identitat concreta i determinada que han estat identificades i autoritzades prèviament (normalment, comandaments intermedis), la divulgació de la qual pot comportar un incompliment greu de legislació, beneficis il·lícits, pèrdues o desprestigi per a la companyia (per exemple, informació relativa a canvis organitzatius o de recursos humans o esborranys de plecs de concursos públics d'import molt alt abans de publicar-los). • Tota la informació associada al desenvolupament de les tasques d'una àrea o d'unes quantes àrees o de parts d'aquestes àrees; per tant, l'accés ha d'estar restringit al personal implicat en aquestes tasques. Exemples: – Informació relativa a la configuració de sistemes de seguretat tant físics (control d'accés) com lògics (tallafoc, IDS/IPS). – Informació de configuració tècnica dels equips i dispositius de la infraestructura.
Molt alt	• És informació molt restringida, d'importància estratègica, concebuda exclusivament per a ser coneguda per un grup molt reduït de persones (normalment alta direcció), la divulgació de la qual pot comportar elevades pèrdues econòmiques o desprestigi greu per a la companyia. Exemple: – Contractes estratègics de la companyia. Decisions de caire polític. – Mapes de xarxa o d'adreces IP. Claus d'accés a sistemes d'informació o dispositius criptogràfics, etc. – Secrets industrials. – Altres.

El nombre de nivells depèn de cada organització i de la seva activitat de negoci. No obstant això, no és recomanable excedir els cinc nivells de classificació, ja que la tasca de classificació pot ser costosa i confusa.

Algunes de les definicions habituals molt orientades a la classificació en termes de confidencialitat són les següents:

Tres nivells

- Informació pública, com per exemple informació comercial de la companyia.

- Informació interna, com per exemple la política de seguretat o procediments interns de la companyia.

- Informació confidencial, com per exemple informació restringida a un grup reduït de persones (elaboració de pressupostos, nòmina de treballadors, procediments tècnics de còpies de seguretat, etc.).

Cinc nivells

- Informació pública: accés intern i extern.

- Informació interna: accés únicament al personal de la companyia.

- Informació restringida: accés a un grup concret, com per exemple el personal d'un departament.

- Informació confidencial: accés a un grup reduït i controlat de persones (nòmines, pressupostos, etc.).

- Informació secreta: accés a un grup molt específic i controlat de persones: resultats d'R+D+I, secrets industrials, etc.

El resultat d'una política de classificació de la informació és la definició dels controls de seguretat que cal aplicar per a cada nivell de classificació. Aquests controls cobreixen els requisits de seguretat per a cadascuna de les dimensions analitzades i, òbviament, també han de donar compliment als requisits de la legislació vigent.

La naturalesa de cada control de seguretat determina qui és el responsable d'aplicar-lo i en quin moment. Així, doncs, hi ha controls que s'han d'aplicar en el pla tècnic per part del personal de seguretat o l'àrea TIC (per exemple, instal·lar antivirus), controls que s'han d'aplicar des de les àrees de negoci (per exemple, definir accessos requerits per a un determinat usuari), controls que han d'aplicar els usuaris (per exemple, xifratge d'informació, confidencialitat en la transmissió d'aquesta informació per correu electrònic), etc.

Les fases inicials de qualsevol projecte són moments crítics per a garantir la seguretat de la informació, i molt especialment si es tracta de projectes de desenvolupament o implantació de sistemes d'informació. Si la companyia té una política de classificació definida, i al començament de qualsevol projecte

el negoci és capaç de classificar la informació que es tractarà, el procés d'anàlisi de requisits de seguretat se simplifica molt, ja que el nivell de classificació prescriu directament els requisits de seguretat que cal aplicar.

De tot això es dedueix que cal formar el personal en la política de classificació. No cal que tot el personal conegui al detall tota la política, sinó que tothom n'ha de conèixer la seva existència i, depenent de la tasca que exerceixi dins de la companyia, ha de ser format en les parts de la política que l'afecten: els responsables funcionals, en els criteris de classificació o reclassificació; els tècnics de sistemes, en els controls de seguretat que cal aplicar en l'operació de sistemes; els caps de projectes de desenvolupament, en tots els controls que cal tenir en compte des del començament, etc.

El personal en general també té un paper molt important a l'hora d'aplicar determinats controls durant el tractament de la informació. Per aquest motiu és habitual i molt recomanable publicar una norma sobre els usos permesos de la informació durant el seu tractament i les mesures de seguretat que cal aplicar en cada cas.

Exemple

Un resum d'aquest tipus de norma es pot recollir en una taula d'aquestes característiques:

	Pública		**Interna**		**Confidencial**	
	Paper	**Electrònic**	**Paper**	**Electrònic**	**Paper**	**Electrònic**
Etiquetatge	Sí	Sí	Sense requisits	Sense requisits	Sí, amb llista de distribució	Sí, amb llista de distribució
Impressió	n/a	Sí	n/a	Sí	n/a	Amb control d'accés a la impressora
Arxiu (mitjans fixos)	Sense restriccions	Sense restriccions	Sí Fora de l'abast de persones alienes al departament	Control d'accés	Protegit amb clau	Control d'accés

Alguns altres tipus de tractaments pels quals s'han d'establir els controls que cal aplicar són els següents:

- Arxiu (mitjans extraïbles / portàtils).
- Còpies.
- Transmissió (per fax, per correu postal, per correu ordinari, converses, etc.).
- Eliminació/esborrament/destrucció.
- Accés (concessió de privilegis d'accés).
- Divulgació a tercers.
- Traçabilitat.
- Reclassificació.

5. Eines per a un SGSI

Actualment hi ha al mercat diverses eines que donen suport a la implantació d'un SGSI.

Generalment són eines web, molt ergonòmiques i fàcils de navegar-hi, l'objectiu final i punt en comú de les quals és saber quin és l'estat de l'organització respecte del compliment dels controls de l'ISO, de manera que ofereixen totes la llista de controls, amb opcions d'entrada d'informació per a determinar el grau d'adaptació, generar informes, etc.

Depenent de l'eina, s'ofereixen altres funcionalitats molt orientades a donar suport a la implantació de l'SGSI:

- Inventari d'actius.
- Anàlisi de riscos.
- Elaboració del **pla de seguretat** o **pla de gestió del risc**.
- Seguiment de plans d'acció.
- Realització d'auditories.
- Seguiment de no-conformitats.
- Gestor documental.
- Fluxos d'assignació de tasques.
- Gestió d'incidències.

La selecció d'una eina és una tasca que no es pot fer amb presses, ja que cal seleccionar l'eina que encaixa més bé en la manera de fer de l'organització, tenint en compte aspectes com l'estructura de l'organització de la seguretat, el nivell de maduresa de la seguretat de la informació, els recursos disponibles per a actualitzar-la i mantenir-la, o la implicació que requereix d'altres figures de l'organització.

De fet, si tenim la possibilitat de començar a implantar l'SGSI per un abast tancat i reduït, i no hi ha requisits temporals estrets per a obtenir la certificació, el més recomanable és començar sense eines, o més ben dit, confeccionar eines senzilles a partir d'eines ofimàtiques. Això ens permet passar per una primera iteració de l'SGSI i tenir més clar què esperem d'una eina i què no n'esperem.

En qualsevol cas, abans de començar la selecció d'una eina, és recomanable fer una petita prospecció de mercat per a saber què hi ha al mercat i en quina forquilla de pressupost es mouen aquest tipus d'eines, amb l'objectiu de presentar el projecte a la direcció i obtenir el vistiplau al procés de selecció de l'eina.

A continuació es presenta un conjunt de recomanacions que cal tenir en compte a l'hora de seleccionar una eina, que de fet són vàlides per a qualsevol tipus d'eina.

5.1. Abans de veure les eines

- Definir els objectius que s'espera cobrir amb l'eina abans de començar a veure proveïdors i, si és possible, posar-los per escrit i segons una llista prioritzada.

- Tenir molt clar quines són les normes a què es vol donar cobertura amb l'eina. Per posar alguns exemples, SGSI, LOPD o pla de continuïtat de negoci (ISO 2230).

- Tenir en compte, si ja es té altres eines (d'anàlisi de riscos, d'auditoria, d'inventari d'actius, de gestió d'incidències, etc.), la capacitat d'integració amb aquestes eines, per a evitar haver d'entrar la informació per duplicat.

5.2. Durant la revisió d'eines disponibles

- Entendre totes les funcionalitats que ofereix l'eina i analitzar de quina d'aquestes funcionalitats se'n traurà rendiment i quines no es faran servir.

- Verificar amb el proveïdor el nivell de cobertura de cadascun dels objectius de la nostra llista.

- Verificar la cobertura de totes les normes que cal controlar, i verificar també, en cas de fallada d'alguna d'aquestes normes, la flexibilitat de les eines per a introduir altres marcs normatius o modificar els actuals. Aquest aspecte és especialment important si l'eina és estrangera, ja que la legislació varia d'un país a un altre.

- Sol·licitar una demostració a partir d'un cas pràctic, si pot ser, plantejat per l'organització mateixa, i implicar-hi, quan sigui possible, totes les persones que han de ser usuàries de l'eina.

- No descuidar-se de demanar els requisits de plataforma i programari (sovint aquestes eines es recolzen sobre bases de dades que requereixen llicència no inclosa en el preu de l'eina).

- Aclarir les possibilitats d'allotjament de l'eina (en recursos propis o bé en recursos del proveïdor mateix).

- Sondejar alternatives de llicenciament, segons la grandària de l'organització, depenent del que resulti més beneficiós per a l'organització (per usuari, per companyia, tarifa plana, escalat, etc.).

- Entendre el grau d'escalabilitat de l'eina (possibilitat de començar a implantar-la en una empresa del grup, per exemple, per a introduir-la més endavant en altres empreses).

- Entendre clarament què entra en el preu i què no hi entra (adaptacions, configuració i formació inicial, etc.), i també el preu del manteniment de les llicències en anys posteriors.

5.3. Altres recomanacions

Finalment, és recomanable fugir de nous desenvolupaments o eines que fa molt poc que han sortit al mercat; ja és prou complex implementar un SGSI per a haver de fer una verificació d'una versió beta de noves eines.

Com a conclusió de tot plegat, direm que una eina és un suport molt potent en la implantació de l'SGSI, sempre que es tingui molt clar què és el que se n'espera obtenir, ja que d'aquesta manera l'eina estarà al servei de la nostra organització i no la nostra organització al servei de l'eina.

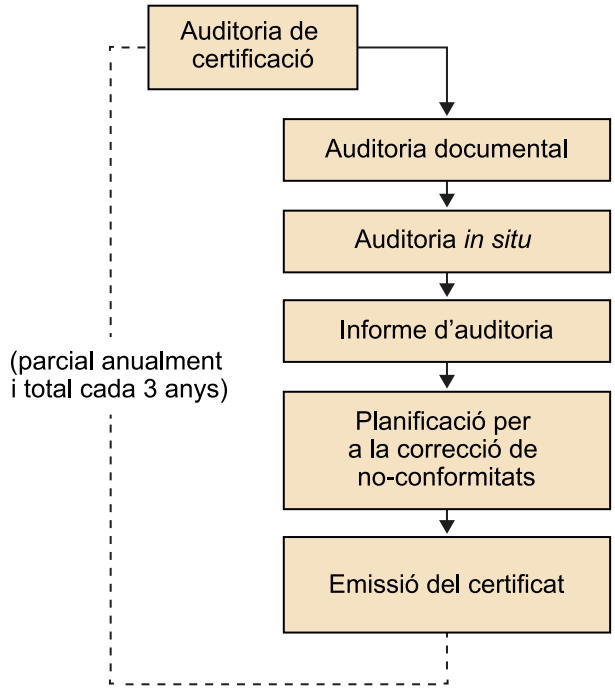
6. Certificació de l'SGSI

L'obtenció del certificat de l'SGSI és una decisió pròpia de cada companyia. Els motius per a obtenir-lo, entre altres, són comercials i d'imatge, per a millorar la confiança dels clients en la companyia, o bé són simplement perquè la companyia opta per imposar-se internament l'obligació de mantenir una bona gestió de la seguretat de la informació, mitjançant auditories externes periòdiques.

6.1. El procés de certificació

Tota auditoria de certificació consta de les etapes següents:

Passos de l'auditoria de certificació de l'SGSI



En una auditoria de certificació no s'auditen tots els controls recollits en la declaració d'aplicabilitat de la companyia, sinó que es fa una auditoria per mostreig, de manera que se selecciona entorn d'un 30% dels controls que són aplicables.

Una vegada obtingut el certificat, s'ha de fer anualment una auditoria de revisió de compliment de l'SGSI, de manera que cada tres anys s'ha d'haver fet una revisió completa dels controls, i es renova la certificació, sempre que no s'hagin produït canvis importants en l'SGSI (per exemple, la modificació de l'abast), cas en què pot ser que calgui tornar a començar el procés de certificació.

Per tant, en cicles de tres anys s'ha de fer una auditoria total per a:

- Verificar que tots els elements de l'SGSI interactuen entre si adequadament.

- Comprovar que l'SGSI continua essent efectiu després dels canvis en les operacions de l'organització.

- Corroborar el compromís de l'organització a mantenir l'efectivitat de l'SGSI.

En les auditories de revisió, l'entitat certificadora comprova que la companyia estigui fent un bon ús del certificat ja que si no és així podria comportar la retirada de la certificació a la companyia.

6.2. Característiques de l'auditoria

Una auditoria de certificació de la norma ISO 27001 compleix les característiques de tota auditoria. A continuació s'exposen algunes qüestions més específiques:

- Per a sol·licitar una auditoria, cal que el sol·licitant acrediti els requisits següents:
  - Hi ha el procés de revisió interna de l'SGSI i ha d'estar planificat.
  - L'SGSI és operatiu.
  - S'han implantat els procediments.
  - Hi ha registres que ho evidencien (habitualment es requereix sis mesos de registres com a mínim).

- És possible auditar l'SGSI de manera conjunta amb altres sistemes de gestió, com per exemple un sistema de gestió de la qualitat o un sistema de gestió de la continuïtat del negoci (SGCN).

- Per a fer l'auditoria, l'equip auditor se centra en els punts següents:
  - L'anàlisi de riscos: com analitza els seus riscos la companyia i el criteri utilitzat per a determinar si un risc és significatiu o no.
  - La declaració d'aplicabilitat.
  - Els objectius que persegueix l'organització.
  - Com es monitora i mesura.

- Com s'informa i millora.
- Les revisions fetes sobre l'SGSI.
- El grau d'implicació de la direcció de la companyia.
- La coherència entre la política, l'anàlisi de riscos, els objectius, les responsabilitats, les normes, els procediments, les dades d'indicadors, les revisions fetes i la criticitat de la informació afectada.

- L'equip auditor no decideix si la companyia ha de rebre o no la certificació una vegada acabada l'auditoria, sinó que ho fa un comitè de certificació constituït per membres de l'entitat certificadora, entre els quals no consta cap membre de l'equip d'auditoria.

El comitè de certificació pren una decisió a partir dels punts següents:

- Una explicació de l'auditoria, incloent-hi un resum de la revisió documental.
- El resultat de l'avaluació de l'anàlisi de riscos.
- La gravetat de les no-conformitats detectades.
- La recomanació de l'equip d'auditoria.
- La resolució de no-conformitats detectades en auditories anteriors.

No-conformitat

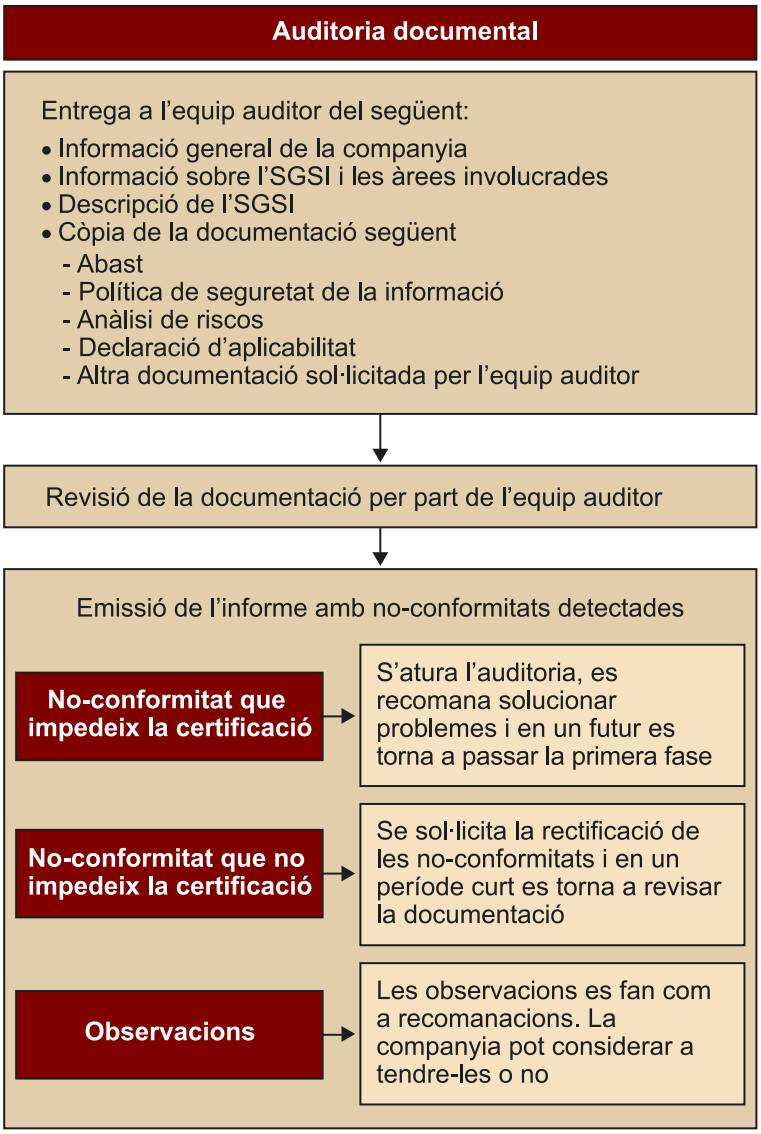
L'absència o fallada en la implantació o el manteniment d'un element o més elements requerits pel sistema de gestió, o bé una situació que, basant-se en evidències objectives, pot comportar un dubte raonable sobre la capacitat de l'SGSI de cobrir els objectius de seguretat de la companyia o complir la política.

Una no-conformitat pot ser relativa a la política de seguretat, a l'estàndard de gestió de seguretat de la informació, a procediments o a requisits legals. S'identifiquen tres tipus de no-conformitats, segons la criticitat de l'incompliment: no-conformitat major, no-conformitat menor i observacions. Generalment es considera no-conformitat major l'absència de qualsevol dels controls essencials que determina l'ISO 27002. Alguns exemples de no-conformitat major són absència de l'anàlisi de riscos, absència d'un sistema de gestió d'incidències, absència d'un pla de continuïtat de negoci, absència de procediments per a gestionar registres, canvis en l'SGSI sense aprovació formal, incompliment reiterat d'un procediment, i un nombre elevat de no-conformitats sobre una mateixa secció de la norma o un mateix departament.

6.3. L'auditoria documental

L'auditoria documental que es fa generalment a les oficines de l'entitat certificadora consisteix en les activitats següents:

Els passos de l'auditoria documental



6.4. El pla d'auditoria

Una vegada acabada l'auditoria documental, i comprovat que l'auditoria pot prosseguir, l'equip auditor elabora i presenta un pla d'auditoria.

El pla d'auditoria:

- Inclou l'abast i objectiu de l'auditoria.
- Identifica requisits especials.

- Determina la durada i els recursos necessaris tant de l'equip auditor com de les persones de la companyia que han d'atendre l'auditoria.

- Selecciona l'equip d'auditoria.

- Inclou una relació de la documentació enviada en l'auditoria documental a l'entitat certificadora.

- Estableix la mostra de controls que s'audita, per a la qual cosa es dóna prioritat a les àrees de més risc, incloent-hi:
  - Tots els controls essencials.
  - Controls que afecten les activitats més importants de la companyia.
  - Controls de totes les seccions de la norma.
  - Controls de manera que s'auditin tots els departaments de la companyia involucrats en l'SGSI.
  - No-conformitats detectades en auditories anteriors.

- Presenta l'agenda de les reunions.

- Informa sobre el contingut i estructura dels informes que es lliuraran quan s'acabi l'auditoria.

6.5. L'auditoria *in situ*

Entre l'auditoria documental i l'auditoria *in situ* passen de tres a sis setmanes. L'auditoria *in situ* es fa a les instal·lacions de l'entitat que sol·licita la certificació.

Els objectius d'aquesta fase de l'auditoria són els següents:

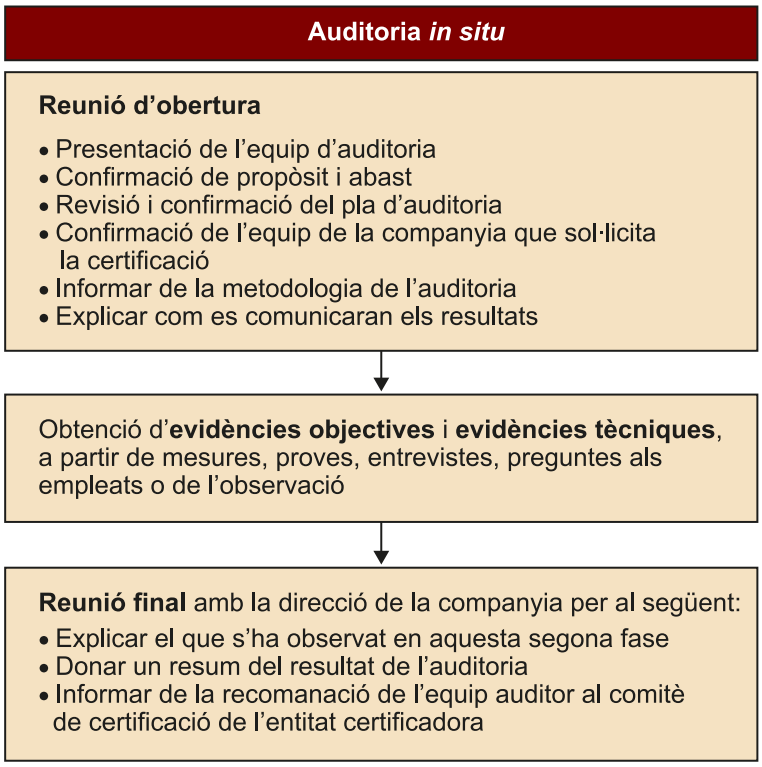
- Confirmar que la companyia sol·licitant compleix les seves polítiques i procediments.

- Comprovar que l'SGSI desenvolupat és conforme a les especificacions de la norma que s'ha de certificar.

- Verificar que l'SGSI està aconseguint els objectius que es va marcar la companyia.

L'auditoria *in situ* comprèn les activitats següents:

Els passos de l'auditoria *in situ*



6.6. L'informe d'auditoria

L'informe d'auditoria, que elabora l'equip auditor una vegada acabada l'auditoria *in situ*, inclou com a mínim:

- La data de l'auditoria.
- L'equip auditor.
- La identificació de la companyia sol·licitant de la certificació.
- L'abast i la norma de referència.
- La conformitat de l'SGSI amb la norma.
- Les no-conformitats detectades.

6.7. Obtenció de la certificació

Si la companyia corregeix o presenta un pla de correcció de les no-conformitats reportades en l'informe d'auditoria, l'entitat certificadora emet el certificat (carta o diploma), que com a mínim inclou:

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

Resum

En aquest mòdul s'han recollit algunes pautes per a desenvolupar alguns dels objectius de control de tot SGSI.

En primer lloc, s'ha abordat la creació del marc normatiu de seguretat de la informació, descrivint quina naturalesa ha de tenir i, sobretot, quin és el procés de creació i manteniment d'estàndards, vàlid per a qualsevol àmbit i no solament el de seguretat de la informació. S'ha dedicat una atenció especial a la forma i el contingut de la política de seguretat de la informació, ja que constitueix la base de tot SGSI.

Un altre dels pilars bàsics de l'SGSI se centra en l'organització de la seguretat de la informació. En segon lloc, doncs, en aquest mòdul s'ha presentat una proposta d'estructura organitzativa, en la qual és essencial la implicació de la direcció, l'existència d'un comitè de seguretat de la informació, amb participació de diverses àrees de la companyia, i la figura d'un responsable de seguretat de la informació. Per a tots plegats s'ha especificat quines són les seves funcions en matèria de seguretat de la informació, cosa que s'ha estès a les diferents àrees de la companyia, i al personal en general, ja que no es pot concebre un sistema de gestió de la seguretat de la informació si aquesta seguretat no forma part del dia a dia de tota l'organització.

En tercer lloc, s'ha dedicat un apartat a parlar del procés de classificació de la informació, que constitueix el primer pas per a determinar la importància que té una informació per a la companyia, cosa que permet definir les mesures de seguretat que cal aplicar en cada cas, i dedicar així més esforç a protegir la informació de més valor per al negoci.

Finalment, s'ha descrit succintament el procés de certificació en l'ISO 27001 i els passos d'una auditoria de certificació, dues qüestions que ha de conèixer una persona orientada a gestionar la seguretat de la informació.