Implantació d'un sistema de gestió de la seguretat de la informació (SGSI)

PID_00253137

Silvia Garre Gui
Antonio José Segovia Henares
Arsenio Tortajada Gallego

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.

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.

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.

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

Introducció

En mòduls anteriors s'ha parlat de la seguretat de la informació com un concepte molt més ampli que el de seguretat informàtica, ja que se centra en la protecció de la informació, un dels actius més importants de qualsevol organització, enfront de qualsevol problema, incidència, discontinuïtat, etc., independentment del suport en què estigui aquesta informació (suport paper, digital, electromagnètic, etc.) i en qualsevol moment del seu cicle de vida.

S'ha presentat també la importància de l'anàlisi de riscos com a punt de partida per a qualsevol acció que calgui fer en matèria de seguretat de la informació. La màxima eficiència s'aconsegueix quan sabem com estem, a quins riscos ens enfrontem i quin és el nivell de risc que està disposada a assumir l'organització. S'ha vist també que l'anàlisi de riscos no és una acció puntual, sinó que és indispensable mantenir-la actualitzada en el temps.

Tot plegat porta a la conclusió que la seguretat no és un producte, sinó que es tracta d'un procés, una activitat que ha de tenir continuïtat. En concret, es tracta del procés de mantenir l'organització en un entorn de risc gestionat, i més en concret encara, en el llindar de risc volgut, mitjançant un seguiment continu i una inversió proporcional i justificada.

En aquest mòdul ens centrarem a estudiar com s'ha d'implantar el procés de la gestió de la seguretat de la informació, quins són els passos que s'han de seguir, els aspectes que s'han de tenir en compte, els riscos possibles i els estàndards de referència que ens ajuden a avançar amb confiança.

Encara que dins d'aquest mòdul descriurem l'objectiu i contingut dels estàndards reconeguts internacionalment, la finalitat no és fer una descripció detallada del contingut d'aquests estàndards. No obstant això, la implantació d'un sistema de gestió de la seguretat de la informació passa incondicionalment per un bon coneixement de les normes internacionals, de manera que us recomanem molt que les llegiu i les conegueu.

Objectius

Els objectius que persegueix aquest mòdul són els següents:

1. Donar algunes nocions sobre els organismes que es dediquen a crear normes.

2. Donar una visió general del contingut de la família 27000 de l'ISO.

3. Conèixer les bases dels sistemes de gestió i, en concret, del cicle de Deming.

4. Conèixer les pautes per a implantar un sistema de gestió de la seguretat de la informació.

5. Tenir clar quin és el marc documental necessari per a implantar un SGSI.

1. Què és un sistema de gestió de la seguretat de la informació

La seguretat de la informació es pot enfocar des de diferents punts de vista, amb diferents objectius i segons diferents aproximacions.

Una organització que posi en pràctica alguns controls de seguretat bàsics, com ara un tallafoc o *firewall*, un antivirus, un control d'accés físic i una política de contrasenyes, tot plegat dirigit i gestionat des de l'àrea de sistemes d'informació, podria considerar que gestiona la seguretat de la informació. És ben sabut, però, que "una cadena és tan forta com la seva baula més feble" i, per tant, l'aplicació d'aquests controls de manera arbitrària, sense haver analitzat abans quines són les debilitats principals, no és una garantia de seguretat.

A hores d'ara entenem que un enfocament sistemàtic de la seguretat, plantejat des d'una anàlisi inicial de riscos i alineat amb l'estratègia i els objectius del negoci, i entès com un procés independent i no com una activitat puntual, no garanteix la seguretat de la informació, però proporciona molts més elements de control que permeten minimitzar l'aparició d'incidències i reaccionar de la manera més adequada i eficient quan se'n produeix una, de manera que en minimitza l'impacte.

Segons el *Diccionari de la llengua catalana*:

- **Sistema**: Conjunt d'elements materials relacionats entre si que constitueixen un tot orgànic, generalment subjecte a unes lleis o normes.
- **Gestionar**: Fer gestions per aconseguir (alguna cosa).

Si analitzem la definició que el diccionari fa de *sistema* i de *gestionar*, podem concloure que un sistema de gestió és el conjunt d'accions relacionades entre elles que ens permeten aconseguir un objectiu del negoci.

El desenvolupament d'un sistema de gestió de la seguretat de la informació (SGSI) es basa principalment en la normativa següent:

- ISO/IEC 27001: especificacions per als sistemes de gestió de la seguretat de la informació.

- ISO/IEC 27002: codi de bones pràctiques per a gestionar la seguretat de la informació.

- ISO Guide 72: guia per a justificar i desenvolupar sistemes de gestió.
  És una guia que recull els requisits per a qualsevol sistema de gestió (amb independència de l'àmbit d'aplicació que tingui).

2. Normatives reconegudes internacionalment

Una norma o estàndard és un acord documentat que conté especificacions tècniques o altres criteris precisos que es poden utilitzar de manera consistent, com ara normes, guies o definicions de característiques que asseguren que els materials, productes, processos i serveis s'ajusten al propòsit que tenen.

L'elaboració de normatives a escala internacional proporciona beneficis tecnològics, econòmics i socials, ja que:

- Proporciona eficiència, seguretat, salubritat i qualitat al desenvolupament, la producció i provisió de productes i serveis.
- Facilita el comerç i les relacions internacionals.
- Facilita la compatibilitat i interoperativitat de mercaderies i productes, amb una importància especial en l'àmbit de les noves tecnologies, i redunda, per tant, en una millora dels costos.
- Proporciona solucions a problemes comuns.
- Proporciona als governs una base tècnica per a legislar en matèria de salut, seguretat i medi ambient.
- Permet compartir avenços tecnològics i bones pràctiques de gestió.
- Protegeix els consumidors i usuaris en general en relació amb els productes i serveis adquirits.

Hi ha normes dirigides a sectors molt concrets i també normes més transversals, però, en qualsevol cas, són normes dirigides a qualsevol que les vol aplicar, independentment de la grandària de l'organització on es volen implantar, de manera que són sempre un bon punt de partida per a treballar, per l'ampli reconeixement i l'àmplia validació que tenen a escala mundial.

A continuació, es presenta alguna de les organitzacions que promouen o lideren l'aprovació de normes a escala internacional i nacional.

2.1. BSI

En el camp de la seguretat de la informació, la primera organització que va treballar per establir un estàndard comú va ser el British Standard Institute. Aquesta organització, fundada el 1901, va ser la primera entitat nacional de normalització a escala mundial.

Moltes de les normes reconegudes internacionalment avui dia parteixen d'una norma prèvia del BSI: ISO 9000 (qualitat), ISO 14000 (gestió mediambiental), ISO-IEC 27000 (seguretat de la informació), ISO 10002 (gestió de reclamacions), ISO 20000 (gestió de serveis de les TIC).

En matèria de seguretat, també cal destacar l'OHSAS 18001, per a seguretat i salut laboral, i també la BS 25999, de continuïtat de negoci.

Actualment, el grup BSI té oficines en prop de cent països, i ofereix bàsicament tres línies de servei: certificació de sistemes de gestió i productes, desenvolupament d'estàndards nacionals i internacionals i formació sobre estàndards.

2.2. ISO: International Organization for Standardization

L'ISO (Organització Internacional per a la Normalització o, en anglès, International Organization for Standardization) és el desenvolupador i publicador d'estàndards internacionals més important que hi ha.

Es tracta d'una organització no governamental fundada el 1947, que actualment representa cent seixanta-dos països i té la seu central a Ginebra (Suïssa).

Els seus membres pertanyen tant al sector públic com al privat, de manera que l'ISO facilita el consens perquè proposa solucions que representen tant els requisits del negoci i la indústria com els interessos més amplis de la societat.

La seva àmplia representativitat avala l'aplicabilitat de les solucions a escala internacional.

L'organització promou el desenvolupament d'estàndards internacionals per a millorar l'intercanvi internacional de béns i serveis i fomentar la cooperació en els camps intel·lectual, científic, tecnològic i econòmic.

Els estàndards ISO són revisats com a mínim cada cinc anys per un grup d'experts.

El ventall dels estàndards ISO va des dels sectors més tradicionals, com l'agricultura o la construcció, fins a l'enginyeria elèctrica i les TIC (tecnologies de la informació i la comunicació). En aquests últims camps, l'ISO col·labora amb la Comissió Electrotècnica Internacional (IEC) i la Unió Internacional de

Telecomunicacions (ITU), especialitzades en aquests sectors. Addicionalment, ISO desenvolupa alguns estàndards transversals, d'aplicació a qualsevol sector, com per exemple en qüestions de metodologia o sistemes de gestió.

Alguns dels estàndards ISO més coneguts són aquests:

- ISO 9001: gestió de la qualitat.
- ISO 14001: gestió mediambiental.
- ISO 216: unificació de mides de paper.
- ISO 27001: gestió de la seguretat de la informació.

Les normatives de seguretat es treballen en el Comitè Tècnic de Tecnologies de la Informació (JTC1), i concretament en el subcomité 27.

Procés de creació de normatives internacionals

Hi ha tres vies possibles per a crear les normatives:

- **Fast track**: hi ha consens entre tots els membres del grup de treball sobre el contingut del document resultant. En aquest cas, es pren una normativa que ja existeix en algun país i s'adopta amb caràcter internacional. El procés dura aproximadament un any. Per exemple, ISO 27002: es va adoptar la norma BS 7799.

- **Medium track**: els membres del comitè estan d'acord en l'essència del document resultant, però no hi ha acord en alguns aspectes concrets de caràcter menor. En aquest cas s'inicia un procés de discussió, que dura uns tres anys.

- **Slow track**: hi ha consens en la necessitat d'elaborar una normativa, però hi ha grans diferències en els plantejaments dels diferents membres del comitè. En aquest cas es parteix de zero i el procés dura uns cinc anys.
  Per exemple, en l'ISO 27001 es partia de dos corrents divergents: el primer donava suport a una visió semblant a la BS 7799:2 (part 2); el segon era més partidari de la visió de l'UNE 71502. La versió final és més a la vora d'aquesta segona opció.

2.3. Entitats certificadores

Les entitats certificadores són bàsicament organitzacions que s'encarreguen d'auditar les empreses que han implementat un estàndard ISO certificable (per exemple, ISO 27001, o ISO 9001, o ISO 14001, o ISO 22301, etc.) i, en cas que la empresa auditada compleixi amb els requisits específics de l'estàndard, l'entitat certificadora pot emetre un certificat, que tindrà una durada de tres anys. Durant aquest temps, l'entitat certificadora auditarà anualment l'empresa per realitzar-ne un seguiment pel que fa al compliment de l'estàndard.

A Espanya hi ha multitud d'entitats certificadores, entre les més conegudes es troben: AENOR, BUREAU VERITAS, Applus+, SGS, BSI, etc.

La majoria d'aquestes entitats operen a tot el món, és a dir, poden auditar empreses en qualsevol país, i poden emetre els seus certificats corresponents, encara que normalment perquè el certificat que emeten tingui certes garanties, les entitats certificadores han d'estar acreditades per un organisme d'acreditació nacional, que és una part independent i pròpia de cada país. En el cas d'Espanya, l'Entitat Nacional d'Acreditació (ENAC) és la que acredita les entitats certificadores que volen emetre certificats ISO a Espanya, de manera que a Espanya les entitats certificadores han d'estar acreditades per ENAC.

En el cas del Regne Unit, l'entitat acreditadora és United Kingdom Accreditation Service (UKAS), de manera que les entitats certificadores que vulguin emetre certificats al Regne Unit han d'estar acreditades per UKAS.

En realitat, qualsevol entitat certificadora (AENOR, BUREAU VERITAS, etc.) pot auditar els processos d'una empresa que es vol certificar en un estàndard (com per exemple ISO 27001), però les entitas certificadores també han de seguir uns estàndards per fer les auditories i emetre certificats, i és l'entitat nacional acreditadora (ENAC, en el cas d'Espanya) qui pot garantir que s'estan seguint aquestes directrius, atès que l'entitat nacional acreditadora auditarà també els processos de les entitats certificadores.

Una entitat certificadora que no estigui acreditada pot emetre certificats igualment, però com que no està acreditada (per ENAC, UKAS o alguna altra) no podrà proporcionar garanties suficients als seus potencials clients del fet que els certificats que emet tinguin una validesa, ja que el procés no està supervisat per una entitat acreditadora independent.

Cal destacar i diferenciar el concepte d'entitat certificadora i organització que desenvolupa normatives. En el cas concret d'Espanya, a més d'AENOR, que ja sabeu que és una entitat certificadora, tenim la figura de l'entitat UNE, que és una organització que s'encarrega del desenvolupament i de la difusió de normes tècniques a Espanya. Fins fa poc, AENOR feia les funcions d'entitat certificadora, i també la funció de l'actual entitat UNE (és a dir, fins fa poc publicava estàndards, i també els certificava). No obstant això, des de l'any 2017 s'han desdoblat les funcions de cada entitat i, actualment, UNE i AENOR són oficialment organitzacions independents.

3. La família ISO 27000

Les normes ISO 27001 i ISO 27002 són les que actualment tenen més difusió i acceptació a escala internacional, de manera que ens hi centrarem per treballar sobre la implantació dels sistemes de gestió de la seguretat de la informació (SGSI).

3.1. Història de la norma

- **1995**. Primera publicació oficial de la BS 77991:1 (codi de bones pràctiques en seguretat de la informació).

- **1998**. Publicació oficial de la BS 7799:2 (especificacions dels sistemes de gestió de la seguretat de la informació).

- **1999**. Publicació oficial de la BS 7799. Parts 1 i 2.

- **2000**. Publicació de la primera versió de la norma ISO-IEC 17799:2000 (codi de bones pràctiques en seguretat de la informació).

- **2002**. Publicació de la nova versió de la BS 7799:2 i publicació oficial d'Aenor de la norma UNE - ISO-IEC 17799 (codi de bones pràctiques en seguretat de la informació (que en realitat va ser una traducció al castellà de l'original ISO/IEC 17799)).

- **2004**. Publicació oficial de l'UNE 71502:2004 (especificacions per als sistemes de gestió de seguretat de la informació (SGSI)).

- **2005**. Publicació oficial de l'ISO-IEC 17799:2005 (codi de bones pràctiques en seguretat de la informació). 15/10/2005: publicació de l'ISO/IEC 27001:2005 (especificacions dels sistemes de gestió de la seguretat de la informació).

- **2007**. 13/2/2007: publicació de l'ISO-IEC 27006:2007. 1/7/2007: la norma ISO/IEC 17799:2005 passa a dir-se ISO 27002:2005. 28/11/2007: publicació de la norma ISO 27001 a Espanya com a UNE - ISO/IEC 27001:2007, que realment és una traducció al castellà de l'original ISO/IEC 27001:2005.

- **2008**. 4/6/2008: publicació de l'ISO-IEC 27005:2008.

- **2009**. 30/4/2009: publicació de l'ISO-IEC 27000:2009. 7/12/2009: publicació de l'ISO-IEC 27004:2009.

- **2010**. 1/2/2010: publicació de l'ISO/IEC 27003:2010.

- **2011**. Actualització de la ISO/IEC 27005:2011.

- **2013** (1/10/2013). Publicació de l'actualització de la ISO/IEC 27001 (nova estructura d'apartats, comú amb altres estàndards ISO com ISO 9001, ISO 14001, etc.) i de la ISO / IEC 27002:2013 (de 133 controls de la versió anterior, es redueix a 114 controls, es millora l'estructura i s'introdueixen alguns controls nous).

- **2014** (novembre). Publicació de la traducció de la ISO/IEC 27001:2013 (versió original en anglès) a la UNE ISO/IEC 27001:2014 (versió traduïda al castellà).

- **2015** (juliol). Publicació de la traducció de la ISO/IEC 27002:2013 (versió original en anglès) a la UNE ISO/IEC 27002:2015 (versió traduïda al castellà).

- **2016**. Actualització de la ISO/IEC 27000:2016, i de la ISO/IEC 27004:2016.

- **2017**. Actualització de la ISO/IEC 27003:2017, i actualització de la UNE-EN ISO/IEC 27001:2017 i UNE-EN ISO/IEC 27002-2017.

3.2. Descripció del contingut dels estàndards de la família ISO 27000

- **27000**. Defineix conceptes i vocabulari que surten en els diferents estàndards de la sèrie de normes ISO 27000.

- **27001**. Conté les especificacions per a implantar un sistema de gestió de la seguretat de la informació. Té l'origen en la BS 7799-2:2002, a la qual substitueix. És la norma certificable.

- **27002**. És el codi de bones pràctiques per a la gestió de la seguretat de la informació. Té l'origen en la BS 7799 (part 1) i l'ISO-IEC 17799.

- **27003**. És una guia d'implementació dels SGSI, de l'ús del model PDCA i dels requisits de les diferents fases d'aquest model. Té l'origen en l'annex B de la norma BS 7799:2 i en la sèrie de documents publicats per BSI al llarg dels anys amb recomanacions i guies d'implantació.

- **27004**. Especificació de les mètriques i tècniques de mesura aplicables per a determinar l'eficàcia d'un SGSI i dels controls que hi estan relacionats. Aquestes mètriques s'usen fonamentalment per a mesurar els components de la fase *do* del cicle PDCA.

- **27005**. Estableix les directrius per a gestionar el risc en matèria de seguretat de la informació. Dóna suport als conceptes generals especificats en la norma ISO-IEC 27001 i s'ha dissenyat per a ajudar a aplicar satisfactòriament la seguretat de la informació basada en un enfocament de gestió de riscos. La publicació d'aquesta norma revisa i retira les normes ISO-IEC TR 13335-3:1998 i ISO-IEC TR 13335-4:2000.

- **27006**. Especifica els requisits i proporciona una guia per a acreditar entitats d'auditoria i certificació de sistemes de gestió de seguretat de la informació.

- **27007**. Representa una guia d'auditoria d'un SGSI.

- **27017**. Representa un codi de bones pràctiques, similar a la ISO 27002 però amb mesures de seguretat de la informació específiques enfocades a la provisió i l'ús de serveis *cloud*.

- **27018**. Representa un codi de bones pràctiques, similar a la ISO 27002 i ISO 27017, però amb mesures de seguretat específiques enfocades a la protecció d'informació personal en entorns *cloud*.

- **27032**. Representa un codi de bones pràctiques, similar a la ISO 27002 però amb mesures de seguretat específiques enfocades a la ciberseguretat.

Hi ha altres normes de la sèrie de caràcter més específic per a un àmbit o sector. Paga la pena destacar l'ISO 27799, publicada el 12 de juny del 2008. La norma defineix les directrius per a donar suport a la interpretació i aplicació de l'ISO 27002 en el sector sanitari. A diferència de la resta de normes, aquesta no la va desenvolupar el subcomité JTC1/S27, sinó el comitè tècnic TC 215.

4. ISO-IEC 27002: codi de bones pràctiques per a gestionar la seguretat de la informació

Aquesta norma és una base comuna per a desenvolupar:

- Normes de seguretat organitzatives.
- Pràctiques efectives de gestió de la seguretat.
- La confiança en les relacions amb terceres organitzacions.

Un aspecte important és que sempre s'ha d'aplicar de conformitat amb la legislació i els reglaments aplicables.

La norma s'utilitza en diferents organitzacions per a cobrir qualsevol dels objectius següents:

- Formular els requisits i objectius de seguretat de la informació.
- Assegurar que els riscos de seguretat es gestionen de manera efectiva en termes de costos.
- Assegurar el compliment de lleis i regulacions.
- Implementar i gestionar els controls necessaris per a assegurar que s'aconsegueixen els objectius de seguretat que ha definit l'organització.
- Definir nous processos de gestió de la seguretat, o identificar i aclarir els processos que ja hi ha.
- Fer que la direcció conegui l'estat de les activitats de gestió de la seguretat.
- Conèixer el grau de compliment de polítiques, directives i estàndards adoptats per l'organització, per part d'auditors interns o externs.
- Establir polítiques, directives, estàndards o procediments de seguretat de la informació en les relacions amb tercers.
- Convertir la seguretat de la informació en un facilitador del negoci.
- Proporcionar informació rellevant sobre l'estat de la seguretat de la informació a clients.

4.1. Estructura de la norma

4.1.1. Introducció

Control

Pràctica, procediment o mecanisme que redueix el nivell de risc.

La norma consta d'una primera **part introductòria (apartat 0)**, en el qual es descriuen els antecedents i el context de l'estàndard, i també s'ofereix un concepte molt clarificador sobre el que és la seguretat de la informació. D'altra banda, també s'estableix com una organització pot identificar els seus requisits de seguretat, i com pot fer una selecció de controls. En aquest apartat introductori també es parla sobre la possibilitat que una organització desenvolupi unes directrius pròpies (incloent-hi nous controls que no estiguin en l'estàndard). Finalment, es comenta el cicle de vida de la informació i les consideracions que s'han de tenir en compte, i també es parla sobre la ISO/IEC 27000, que, en la versió més recent, inclou un glossari dels termes utilitzats en tots els estàndards de la sèrie ISO/IEC 27000.

4.1.2. Apartats

- **Apartat 1: objecte i camp d'aplicació**
  Segons recull l'ISO, aquest estàndard internacional estableix guies i principis generals per a iniciar, implementar, mantenir i millorar la gestió de la seguretat de la informació en una organització. Els objectius apuntats en aquest estàndard proporcionen una guia general sobre els objectius de seguretat de la informació acceptats comunament.
  Els objectius de control i controls d'aquest estàndard s'han d'aplicar per a satisfer els requeriments identificats en una anàlisi de riscos. L'estàndard es pot utilitzar com una guia pràctica per a desenvolupar estàndards de seguretat organitzativa i pràctiques efectives de gestió de la seguretat, i pot ajudar a crear confiança en les relacions amb terceres organitzacions.

- **Apartat 2: normes per a consulta**
  Es fa referència a la ISO/IEC 27000, que té un glossari dels termes que utilitzen els estàndards de la sèrie ISO/IEC 27000.

- **Apartat 3: termes i definicions**
  Novament es fa referència a la ISO/IEC 27000, atès que és aquest estàndard el que ara agrupa totes les definicions de termes.

- **Apartat 4: estructura de la norma**
  Finalment, es dedica un apartat a parlar sobre l'estructura de l'estàndard, compost principalment per 14 capítols, amb 35 categories, i 114 controls de seguretat de la informació.

- **Apartats del 5 al 18**
  – Cadascun dels apartats, o capítols, configura una secció o domini.

- Cada domini recull un objectiu o uns quants objectius de control de la seguretat.
- Cada objectiu inclou un control o uns quants controls que es poden aplicar per a aconseguir l'objectiu de control.

L'ISO/IEC 27002:2013 presenta **14 dominis, 35 objectius de seguretat i 114 controls** a més de, com ja s'ha comentat, els apartats previs introductoris.

Com a comentari, direm que l'ISO 17799:2000 presentava 10 dominis, 36 objectius de control i 127 controls, mentre que la ISO/IEC 27002:2007 (versió prèvia a l'actual) presentava 11 dominis, 39 objectius i 133 controls.

Dominis de seguretat de l'ISO 27002

5. Polítiques de seguretat de la informació (1 objectiu, 2 controls)	6. Organització de la seguretat de la información (2 objectius, 7 controls)	7. Seguretat relativa als recursos humans (3 objectius, 6 controls)	8. Gestió d'actius (3 objectius, 10 controls)
9. Control d'accés (4 objectius, 14 controls)	10. Criptografia (1 objectiu, 2 controls)	11. Seguretat física i de l'entorn (2 objectius, 15 controls)	12. Seguretat de les operacions (7 objectius, 14 controls)
13. Seguretat de les comunicacions (2 objectius, 7 controls)	14. Adquisició, desenvolupament i manteniment dels sistemes d'informació (3 objectius, 13 controls)	15. Relacions amb proveïdors (2 objectius, 5 controls)	16. Gestió d'incidents de seguretat de la informació (1 objectiu, 7 controls)
17. Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci (2 objectius, 4 controls)		18. Acompliment (2 objectius, 8 controls)	

Dominis de seguretat de l'ISO 27002, especificant per a cada domini el nombre de controls que el componen i el nombre d'objectius de control totals per domini.

4.2. Com cal interpretar la informació de cada domini

Cadascun dels dominis de l'ISO, tal com hem comentat, conté:

- Un mínim d'un objectiu de control que cal aconseguir.
- Un control o uns quants controls que es poden implantar per a aconseguir aquest objectiu.

La descripció de cadascun dels controls s'estructura en tres parts:

- Control: definició del control específic.
- Guia d'implantació: proporciona informació detallada per a implantar el control.
  Es tracta només d'una guia i, per tant, no es podrà aplicar sempre íntegrament; la responsabilitat d'analitzar quina és la millor manera d'implantar el control és de l'organització.

- Informació addicional: proporciona informació que pot ser necessari tenir en compte, com per exemple consideracions legals o referències a altres estàndards.

Exemple d'objectiu de control

11.1. Àrees segures

Objectiu

Prevenir l'accés físic no autoritzat, els danys i la interferència a la informació de l'organització i als recursos de tractament de la informació.

11.1.1. Perímetre de seguretat física

Control

S'haurien d'utilitzar perímetres de seguretat per a protegir les àrees que contenen informació sensible, a més dels recursos de tractament de la informació.

Guia d'implantació

S'haurien de considerar i implantar, quan sigui adequat, les directrius següents per als perímetres de seguretat física:

a) Els perímetres de seguretat haurien d'estar clarament definits, i la situació i fortalesa de cada perímetre hauria de dependre dels requisits de seguretat dels actius dins del perímetre i dels resultats de l'avaluació del risc.

b) Els perímetres d'un edifici o instal·lació que conté els recursos de tractament de la informació haurien de ser físicament sòlids (per exemple, no haurien d'existir buits en el perímetre o àrees en què es puguin produir ruptures fàcilment); les teulades i murs externs i el paviment del lloc haurien de ser de construcció sòlida i totes les portes externes haurien d'estar adequadament protegides contra els accessos no autoritzats mitjançant mecanismes de control, per exemple barres, alarmes, panys, etc.; les portes i finestres haurien d'estar bloquejades quan no estiguin ateses i s'hauria de considerar una protecció externa per a les finestres, especialment per a les que es troben a nivell del sol.

c) Hauria de situar-se una àrea de recepció atesa o altres controls d'accés físic a les instal·lacions o l'edifici; s'haurien restringir els accessos a les instal·lacions i edificis únicament al personal autoritzat.

d) Les barreres físiques haurien, quan sigui aplicable, de ser construïdes per a prevenir els accessos físics no autoritzats i la contaminació ambiental.

e) Totes les portes del perímetre de seguretat que actuïn com a tallafocs haurien d'estar dotades d'un sistema d'alarma, monitorades i provades conjuntament amb les parets, per establir el nivell requerit de resistència d'acord a les normes regionals, nacionals i internacionals; s'hauria operar d'acord amb els codis locals de protecció contra incendis en mode de fallada segur.

f) S'haurien d'instal·lar sistemes de detecció d'intrusió adequats d'acord amb les normes regionals, nacionals i internacionals i ser provats periòdicament per a donar cobertura a totes les portes externes i finestres accessibles; les àrees no ocupades haurien d'estar

dotades d'un sistema d'alarma en tot moment; s'haurien també de cobrir altres àrees, per exemple, la sala d'ordinadors o les sales de comunicacions.

g) Els recursos de tractament de la informació gestionats per l'organització haurien d'estar físicament separats d'aquells gestionats per terceres parts.

Informació addicional

La protecció física pot aconseguir-se mitjançant la creació d'una o més barreres físiques al voltant de les instal·lacions de l'organització i dels recursos de tractament de la informació. L'ús de barreres múltiples proporciona protecció addicional, de manera que la fallada d'una barrera en particular no vol dir que es comprometi immediatament la seguretat.

Una àrea segura pot ser una oficina que es pugui tancar amb clau o diverses sales envoltades per una barrera interna i contínua de seguretat física. Poden ser necessàries barreres addicionals i perímetres de control d'accés físic entre àrees dins del perímetre de seguretat que tinguin diferents requisits de seguretat. S'haurien de proporcionar consideracions especials relatives a la seguretat dels accessos físics, per a edificis que alberguen diferents organitzacions.

L'aplicació de controls físics, especialment en les àrees segures, hauria d'adaptar-se a les circumstàncies tècniques i econòmiques de l'organització, segons s'estableixi en l'avaluació del risc.

Font: ISO/IEC 27002:2013

L'ISO en estudi, tal com indica el títol, és una guia de bones pràctiques. Amb això el que volem expressar és que és un bon full de ruta per a seguir, però no s'ha de considerar com una norma que s'ha de seguir al peu de la lletra, sobretot pel que fa a les pautes de la guia d'implantació, ja que no s'han pas de posar totes en pràctica ni tampoc no han pas de ser totes aplicables a la situació concreta de l'organització. D'altra banda, cal recalcar que aquest estàndard no és certificable, com sí ho és la ISO/IEC 27001.

4.3. Dominis de l'ISO

A continuació, s'enumeren els catorze dominis de seguretat, amb una menció breu dels objectius de control de cadascun d'aquests dominis i un resum general del contingut que tenen.

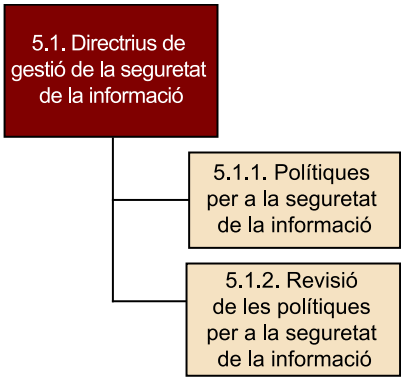
És important destacar que l'estàndard, per a la implementació d'alguns controls, requereix informació documentada, és a dir, en alguns casos no n'hi ha prou a implementar el control, cal tenir un document associat al control. En aquests casos, l'estàndard indica clarament quin control ha de tenir informació documentada.

En els apartats següents, s'indiquen quins són els controls per a cada domini que requereixen informació documentada.

4.3.1. Polítiques de seguretat de la informació

S'ha de tenir una normativa comuna de seguretat que reguli les línies mestres sobre la manera de treballar de tota l'organització en matèria de seguretat. Tot el personal implicat en l'abast del SGSI ha de complir les polítiques de seguretat de la informació definides per l'organització, i han de ser revisades periòdicament.

ISO 27002: domini sobre política de seguretat de la informació

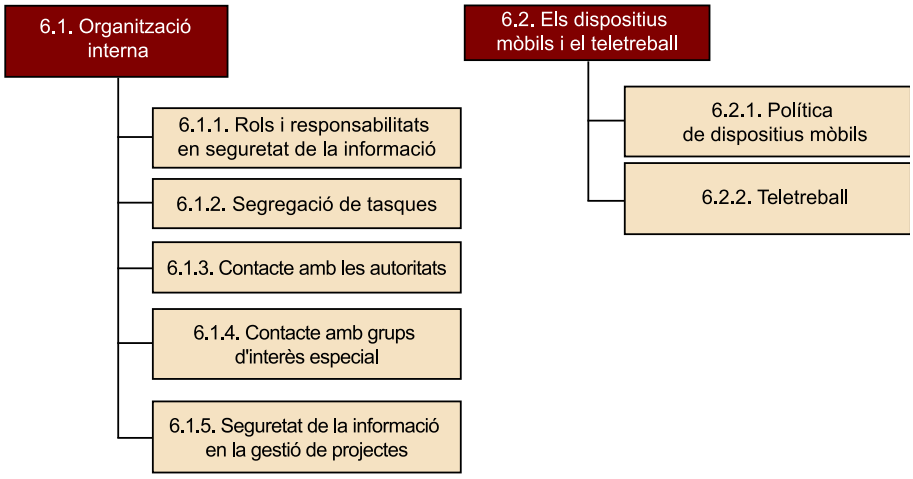


4.3.2. Organització de la seguretat de la informació

Cal establir una estructura organitzativa i el funcionament d'aquesta estructura tant de manera interna com de portes enfora. Habitualment les organitzacions solen establir un responsable de seguretat de la informació (o CISO, per les seves inicials en anglès: *Chief Information Security Officer*), encara que aquest paper no és obligatori, i ni tan sols és esmentat per l'estàndard.

També es consideren dins d'aquest domini els controls relatius a la política de dispositius mòbils (fet per al qual moltes empreses defineixen una política BYOD - *Bring Your Own Device*), i el teletreball (no aplicable per a moltes empreses).

ISO 27002: domini sobre organització de la seguretat de la informació



4.3.3. Seguretat relativa als recursos humans

Tot el personal de l'organització ha de ser coneixedor de les seves responsabilitats envers la protecció de la informació, per garantir la seva seguretat i un ús correcte, amb major importància com més confidencial o sensible sigui la informació a la qual tenen accés.

Per tant, s'haurà de prestar especial atenció a aquest tema en el moment de la contractació del personal, establint les clàusules contractuals i els procediments adequats per a garantir que el procés de canvi de funcions, la sortida de l'organització o terminació de contracte es realitza de manera ordenada i garantint la recuperació per part de l'organització d'informació i equips, a més de la denegació de tots els drets d'accessos (físics o lògics) a la persona que abandona la companyia.

Per tant, aquest domini cobreix el procés complet:

- Abans de la contractació: selecció de candidats, recerca de referències, antecedents, etc.

- Un empleat treballa per a l'organització: formació, sensibilització, etc. en matèria de seguretat de la informació, sancions en cas d'incomplir polítiques, etc.

- L'empleat finalitza la seva relació laboral amb l'organització.

4.3.4. Gestió d'actius

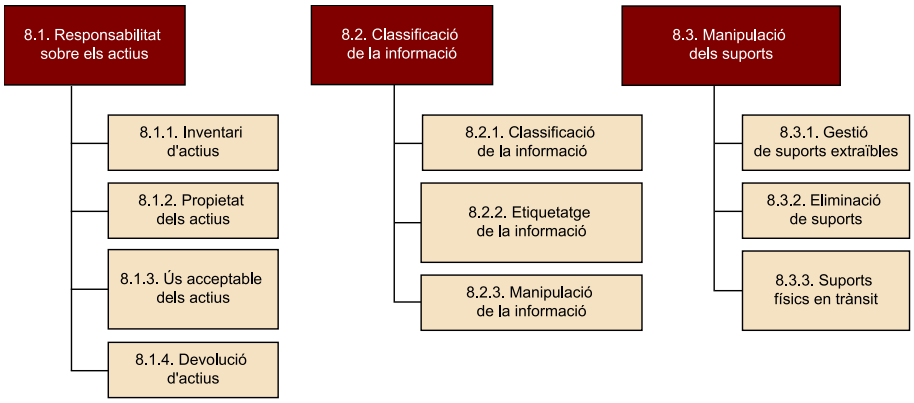
Per a protegir la informació en termes de confidencialitat, integritat, autenticitat, traçabilitat i disponibilitat, és imprescindible saber quins són els actius crítics que cal protegir (informació, programari, maquinari, serveis, persones, etc.). Per tant, cal fer una identificació dels actius crítics per a desenvolupar i mantenir l'activitat, i definir-ne els responsables, que són les persones que decidiran sobre l'ús que se'n pot fer i el tipus de control que s'hi ha d'exercir.

En concret, cal classificar la informació i definir qui n'és el propietari o responsable, per a determinar usos, prioritats, accessos i nivells de protecció necessaris en tot el cicle de vida d'aquesta informació.

També es fa necessària la definició d'una normativa interna per a l'ús adequat dels actius de l'organització, amb l'objectiu sempre de protegir la informació.

Es considera dins d'aquest domini de controls la gestió de suports d'emmagatzematge (discs durs, *pendrives*, CD, DVD, etc.).

ISO 27002: domini sobre la gestió d'actius



Nota: per als controls «8.1.1 Inventari d'actius» i «8.1.3 Ús acceptable dels actius» es requereix informació documentada.

4.3.5. Control d'accés

L'accés a la informació i als recursos en general (aplicacions, sistemes de processament, infraestructures de comunicació, etc.) s'ha de controlar tenint en consideració els requeriments del negoci i de seguretat de la informació.

Això comporta la definició de criteris d'accés a la informació segons el principi de necessitat i la premissa que «tot està en general prohibit, excepte allò específicament permès», i tenint en compte aspectes com l'accés físic i l'accés lògic, en local o remot.

Serà necessari definir normes que recullin aquests criteris per a cada tipus d'informació o recurs, a més de procediments de gestió (alta, baixa i manteniment) de l'accés dels usuaris o processos, polítiques de contrasenyes, etc.

S'hauran de realitzar revisions periòdiques sobre els permisos i privilegis d'accés a cada recurs.

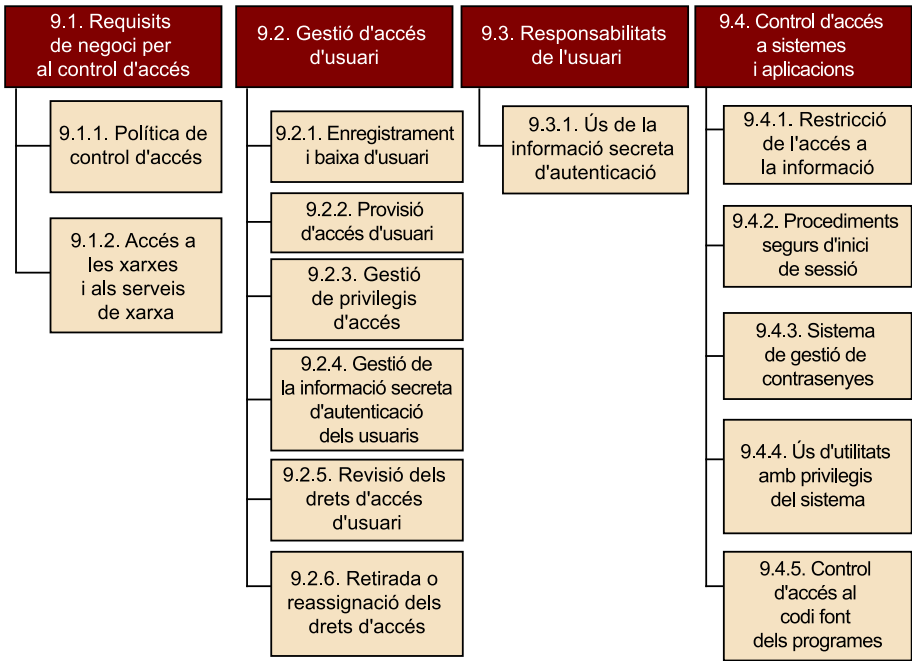
Tots els usuaris que accedeixin als sistemes d'informació han d'estar associats a un identificador personal i hauran de passar per un procés d'identificació, autenticació i autorització. S'evitarà l'ús d'usuaris genèrics, excepte en el cas d'impossibilitat tecnològica, que haurà de ser justificada i aprovada formalment, amb el compromís de regularització en el moment en què la impossibilitat desaparegui.

L'organització ha de poder saber en tot moment qui té accés a quina informació i a quins recursos, i també qui accedeix a una determinada informació o recurs.

L'accés remot als sistemes haurà de garantir un nivell de seguretat equivalent al de les connexions en mode local.

L'organització també ha de definir les normes i els procediments d'ús de la informació fora dels locals habituals.

ISO 27002: domini sobre el control d'accessos

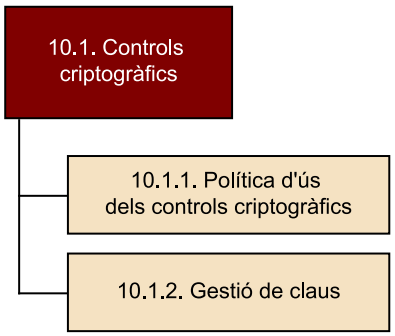


Nota: el control «9.1.1 Política de control d'accés» requereix informació documentada.

4.3.6. Criptografia

És molt habitual, en qualsevol organització, intercanviar dades amb entitats externes, o desplaçar-se d'una oficina a una altra amb informació de l'organització, o transferir informació sensible per mitjà del correu electrònic, etc. En aquests casos, si la informació no es xifra amb un mecanisme adequat, podria accedir-hi personal no autoritzat. Per tant, es fa necessari establir una política de controls criptogràfics, per poder xifrar la informació amb mitjans d'emmagatzematge externs, discs durs de portàtils, connexions remotes, etc.

ISO 27002: domini sobre la criptografia



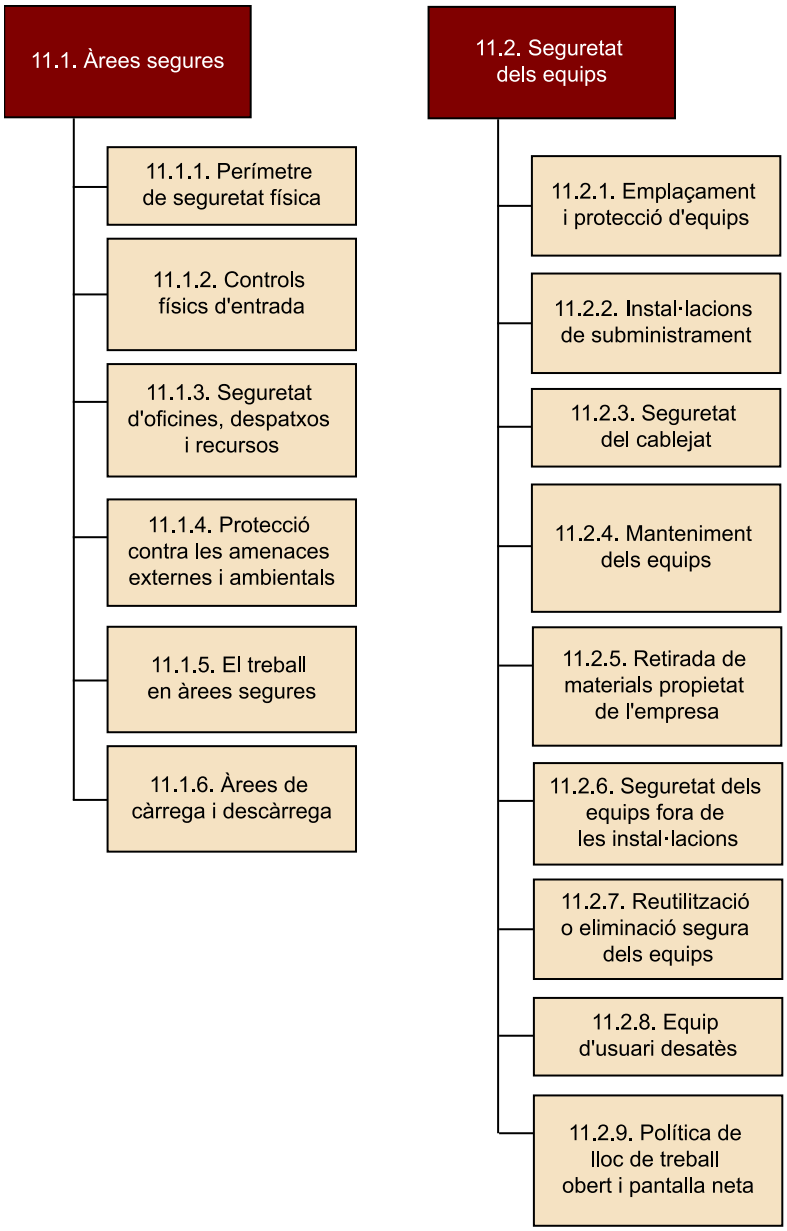
4.3.7. Seguretat física i de l'entorn

La informació i els equips que l'allotgen o transmeten han d'estar convenientment protegits per a evitar accessos físics indeguts i danys de qualsevol tipus. Òbviament, el nivell de protecció haurà de ser proporcional a la criticitat de la informació i els equips que es volen protegir, i dependrà òbviament dels riscos potencials.

Tenint en compte aquesta premissa, s'han d'adoptar mesures per a controlar l'accés físic a edificis i sales, i garantir la seguretat de la informació i els equips, i establir, si cal, àrees segures amb controls específics de seguretat perimetral, accés físic, protecció davant amenaces ambientals (foc, inundació, humitat...), continuïtat del subministrament elèctric, manteniment d'equips, etc.

L'organització també ha de definir les normes i els procediments d'ús de la informació fora dels locals habituals.

ISO 27002: domini sobre la seguretat física i de l'entorn



4.3.8. Seguretat de les operacions

Per garantir la confidencialitat, integritat, autenticitat, traçabilitat i disponibilitat de la informació, és indispensable disposar d'una correcta gestió i operació dels sistemes d'informació. En aquest sentit, els procediments per a assegurar una correcta configuració, administració i operació dels sistemes d'informació

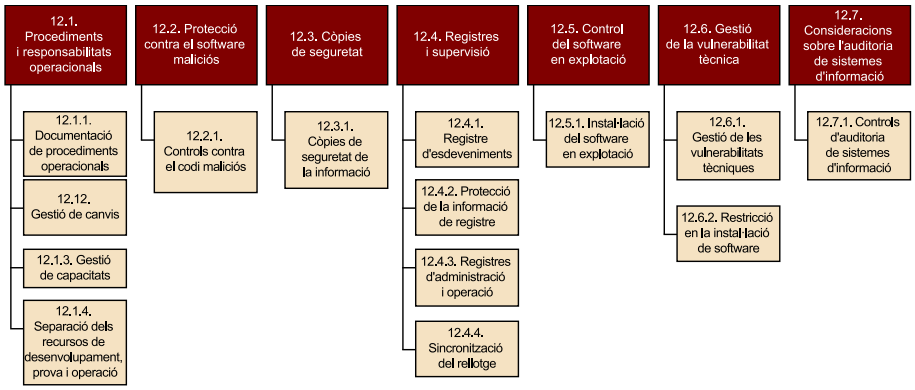
han d'estar clarament definits, i s'haurà de garantir, sempre que sigui viable, la segregació de funcions, la separació d'entorns de desenvolupament, prova i producció, la gestió del canvi i de la capacitat dels sistemes per a evitar incidents.

Així mateix, serà imprescindible definir els controls necessaris per a garantir la correcció i seguretat en l'operació: protecció davant programari maliciós, realització de còpies de seguretat que cobreixin les necessitats del negoci i proves de restauració periòdiques.

D'altra banda, també caldrà monitorar els sistemes per detectar qualsevol accés o ús d'informació o processos no autoritzats, així com registrar i gestionar les traces d'activitat dels sistemes, que permetin detectar problemes i incidents, verificar l'efectivitat dels controls establerts i donar compliment a la legislació aplicable pel que fa al monitoratge i la gestió de traces.

Finalment, també caldrà una gestió adequada de vulnerabilitats tècniques, per mitjà de l'actualització periòdica dels sistemes d'informació, o bé per mitjà de proves de *hacking* ètic i proves de penetració (*pentest*).

ISO 27002: domini sobre operacions



Nota: el control «12.1.1 Documentació de procediments operacionals» requereix informació documentada.

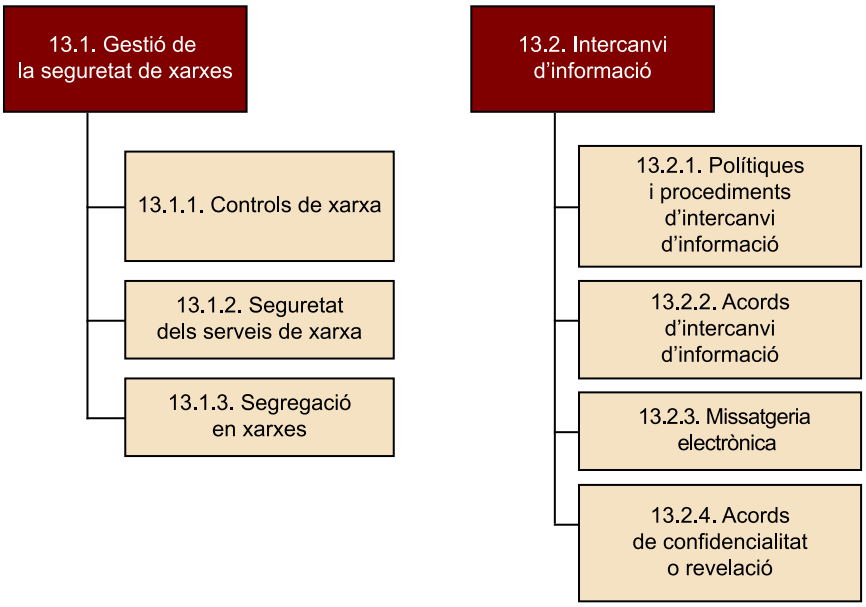
4.3.9. Seguretat de les comunicacions

Avui dia seria impensable tenir una empresa sense connexió amb l'exterior, és a dir, sense connexió, per exemple, a internet.

Perquè aquestes connexions amb l'exterior es duguin a terme d'una manera adequada, es fa necessària la gestió de la seguretat de les comunicacions, implantant controls de xarxa (tallafocs o *firewalls*), definint seguretat en serveis de xarxa, i segregant la xarxa (subxarxa o *subnetting*).

D'altra banda, les organitzacions solen intercanviar informació amb altres entitats externes, i per aquest intercanvi cal definir mecanismes adequats (polítiques, acords d'intercanvi, acords de confidencialitat, etc.).

ISO 27002: domini sobre les comunicacions



4.3.10. Adquisició, desenvolupament i manteniment dels sistemes d'informació

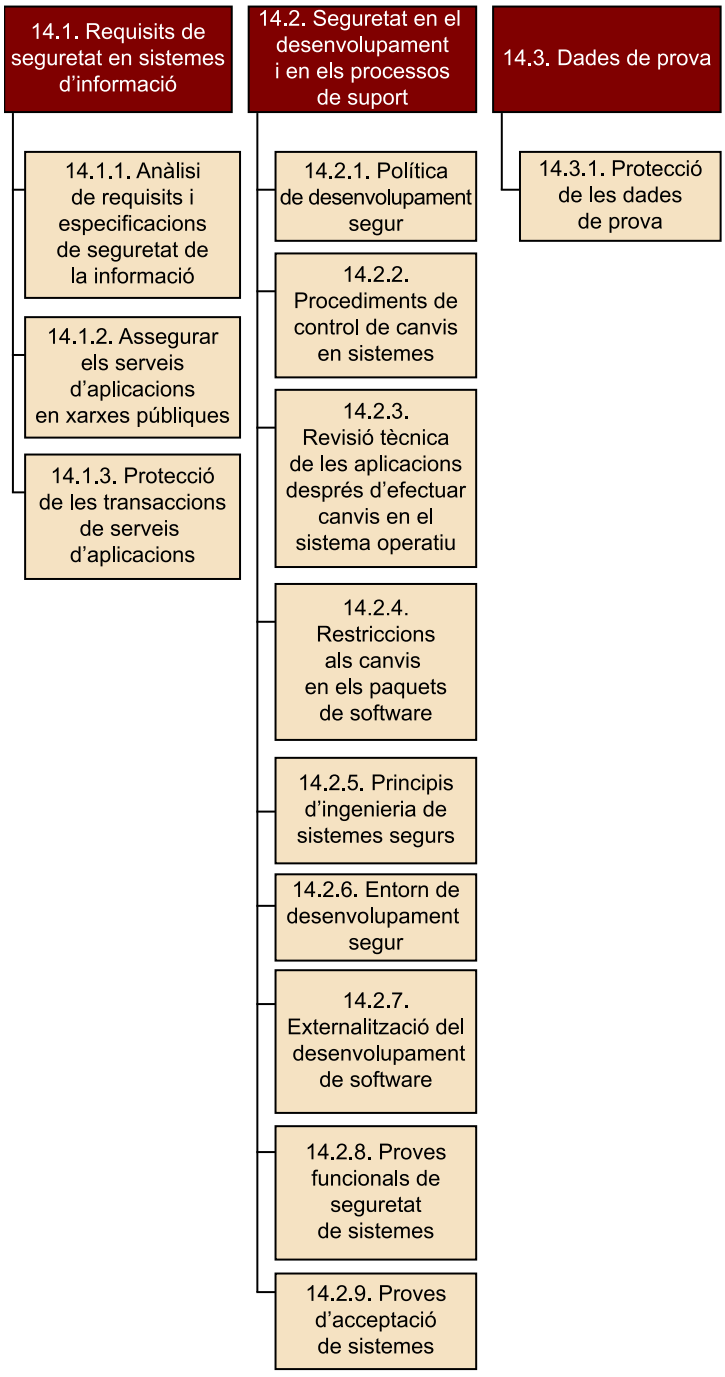
La seguretat ha de ser considerada en tot el cicle de vida de desenvolupament dels sistemes, és a dir, en l'anàlisi de requeriments i viabilitat, disseny, proves i acceptació final. Els requeriments de seguretat han de ser identificats i acordats en la fase inicial d'un projecte, abans d'iniciar el desenvolupament o implantació del sistema d'informació.

S'han d'implantar els controls necessaris per a:

- Garantir l'absència d'errors de procés, pèrdua d'informació, modificació no autoritzada o mal ús de la informació mitjançant les aplicacions.
- Garantir la confidencialitat i integritat de la informació, a més de l'autenticitat i no refutació d'accions realitzades sobre la informació.
- Protegir el programari i codi desenvolupat.
- Garantir l'ús de les millors pràctiques en el desenvolupament de codi segur.
- Generar registres o traces d'activitat.
- Establir les mesures necessàries per a garantir la seguretat de la informació en els entorns no productius.
- Establir els procediments que garanteixin quins canvis en el maquinari o programari no puguin comprometre la seguretat de la informació.

- Supervisar i monitorar els desenvolupaments contractats a terceres parts.

ISO 27002: domini sobre l'adquisició, el desenvolupament i el manteniment dels sistemes d'informació



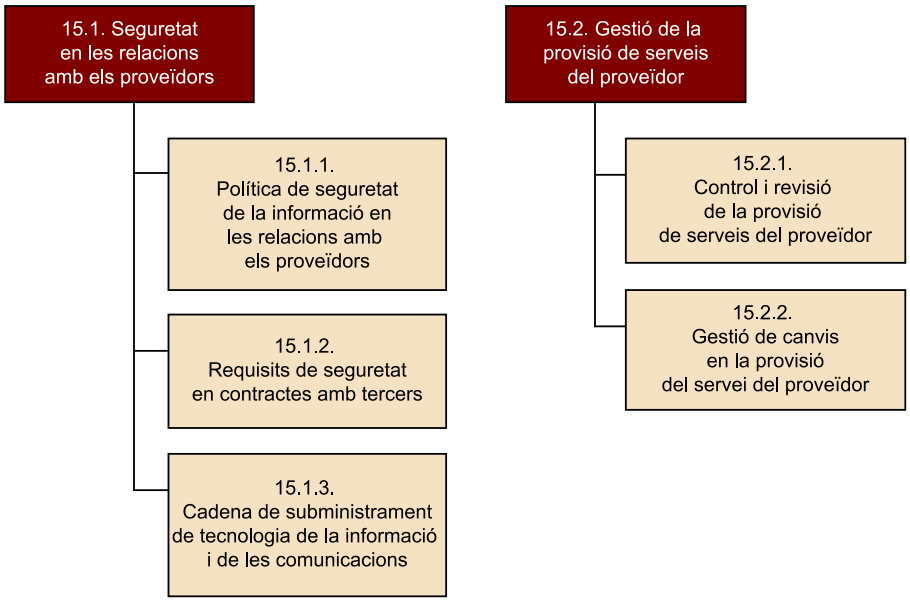
Nota: el control «14.2.5 Principis d'enginyeria de sistemes segurs» requereix informació documentada.

4.3.11. Relacions amb proveïdors

Cal definir unes mesures bàsiques per a la gestió de les relacions amb parts externes (proveïdors, consultors externs, auditors externs, etc.), per poder protegir d'aquesta manera la informació a la qual puguin tenir accés. Amb aquesta finalitat, el més habitual és establir acords amb aquestes parts externes, en

què es defineixin aquestes mesures, i després també se sol revisar el servei prestat per l'empresa externa i el compliment de la normativa de seguretat de l'organització.

ISO 27002: domini sobre les relacions amb proveïdors



Nota: el control «15.1.1 Política de seguretat de la informació en les relacions amb els proveïdors» requereix informació documentada.

4.3.12. Gestió d'incidents de seguretat de la informació

Cal assegurar que qualsevol incident o debilitat relacionada amb la seguretat de la informació es comunica de forma eficient perquè es puguin prendre, a temps i de forma ordenada, les accions correctives necessàries. Per a això, és indispensable establir i comunicar a totes les parts implicades els procediments de notificació i l'escalat d'incidents, establir-ne un monitoratge i un seguiment continuat i relacions amb agents externs quan escaigui (per ferne una millor gestió), a més de recollir evidències en la forma que el tipus d'incident requereixi.

4.3.13. Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci

La definició de plans de continuïtat de negoci té per objectiu protegir els processos i les activitats crítiques del negoci de contingències o desastres, i garantir el restabliment del funcionament normal en uns terminis acceptables des del punt de vista del negoci després d'una situació de desastre.

L'establiment d'un pla de continuïtat passa per l'anàlisi de quins són els processos crítics del negoci i quin és el risc al qual estan sotmesos, per mitjà de la determinació de quin seria l'impacte en cas que es materialitzés un desastre, un incident de seguretat, una pèrdua de servei o, en general, la pèrdua de disponibilitat.

La determinació i la quantificació del risc permet prendre decisions als nivells directius que correspongui sobre el grau de risc assumible, prioritzar les accions en seguretat de la informació i adoptar mesures, establint les salvaguardes necessàries (controls tècnics, procediments operatius, normatives d'usuari, clàusules contractuals...) de tipus correctiu o de detecció, segons correspongui.

L'anàlisi de l'impacte permet definir quins són els actius d'informació que s'han de protegir en funció de la seva criticitat per al negoci, i quins són els temps acceptables de recuperació. El pla de continuïtat haurà de tenir en compte aquests aspectes, a més de la definició de l'actuació esperada per part de totes les parts implicades i la seva formació. D'altra banda, cal provar el pla de manera periòdica.

S'ha de garantir l'actualització continuada del pla de continuïtat del negoci, a més de la seva disponibilitat en situació de crisi o emergència.

4.3.14. Compliment

Cal prendre les mesures necessàries per a garantir el compliment de qualsevol obligació legal, estatutària, reguladora o contractual, a més del compliment de la normativa vigent interna en matèria de seguretat de la informació.

És indispensable saber quina és la legislació aplicable en cada cas i fer-ne difusió dins de l'organització. Així mateix, s'ha d'establir un sistema de control periòdic i independent del compliment d'obligacions i, pel que fa al compliment de la normativa interna, establir un sistema d'autorització d'excepcions quan la causa estigui justificada.

5. Sistemes de gestió

Un sistema de gestió permet aconseguir els objectius d'una organització mitjançant:

- Una estructura organitzativa en què les funcions i responsabilitats s'han definit i assignat clarament.

- Els processos i recursos necessaris per a aconseguir els objectius.

- Una metodologia de mesura i d'avaluació per a valorar els resultats enfront dels objectius, incloent-hi la retroacció de resultats per a planificar les millores del sistema.

- Un procés de revisió per a assegurar que es corregeixen els problemes i es detecten oportunitats de millora que s'implementen quan estan justificades.

Els principis generals de qualsevol sistema de gestió són els següents:

- Ha de cobrir una necessitat de mercat.
- Ha de ser compatible amb altres sistemes de gestió.
- Ha de ser fàcil d'implantar.
- S'ha de poder implantar en qualsevol tipus d'organització.
- S'ha de basar en metodologies, pràctiques o tecnologies provades suficientment.
- Ha de ser fàcil d'entendre, sense ambigüitats ni condicionants culturals.
- Ha de permetre desenvolupar auditories.
- No ha d'especificar productes concrets, metodologies ni establir nivells de conformitat.

A continuació, s'exposen els elements comuns a qualsevol sistema de gestió:

- Política
  Per a demostrar el compromís de l'organització amb els requisits del sistema de gestió i establir uns principis i una orientació globals.

- Planificació
  - Identificar necessitats i requisits, i analitzar elements crítics.
  - Seleccionar elements que cal gestionar.
  - Establir objectius (generalment anuals i fixats per la direcció).
  - Identificar recursos humans i materials.
  - Identificar l'estructura organitzativa, les funcions i les responsabilitats.

  - Planificar els processos operatius.
  - Preparar plans de contingència per a esdeveniments previsibles.

- Implantació i operació
  - Controlar les activitats per a aconseguir els objectius.
  - Gestionar recursos humans.
  - Gestionar altres recursos.
  - Documentació i control.
  - Comunicació.
  - Relacions amb proveïdors i subcontractats.

- Anàlisi del rendiment
  - Monitoratge i mesures.
  - Estudi i gestió de no-conformitats.
  - Auditories del sistema de gestió.

- Millora
  - Accions correctives.
  - Millora contínua.

- Revisions de la direcció
  - Determinar el rendiment.
  - Assegurar-ne l'adequació permanent.
  - Assegurar-ne la suficiència i l'efectivitat.
  - Desenvolupar millores.
  - Plantejar nous objectius quan calgui.

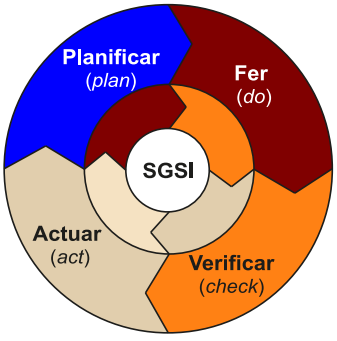
Darrere de totes aquestes fases hi ha el cicle de Deming, conegut també com a *cicle PDCA* (***p**lan **d**o **c**heck **a**ct*), que és un procés iteratiu de qualitat en quatre fases:

- *Plan*: establir els objectius i processos necessaris per a aconseguir els resultats esperats.

- *Do*: implantar els processos nous.

- *Check*: mesurar els processos nous i comparar els resultats obtinguts amb els esperats.

- *Act*: analitzar les diferències entre els resultats obtinguts i els esperats per a saber-ne les causes i plantejar-hi millores.



Cicle de Deming o cicle PDCA

6. Introducció a l'SGSI

Sistema de gestió de la seguretat de la informació

Un sistema de gestió de seguretat de la informació (SGSI) consisteix en polítiques, procediments, guies i recursos, i activitats associades, col·lectivament gestionats per l'organització, amb la intenció de protegir els seus actius d'informació. Un SGSI representa un enfocament sistemàtic per a l'establiment, la implementació, l'operació, el monitoratge, la revisió, el manteniment i la millora de la seguretat de la informació de l'organització, per aconseguir els seus objectius de negoci.

Font: ISO 27000:2014

La implantació d'un SGSI comporta els beneficis següents:

- **Visió comuna**: permet definir i divulgar unes directrius bàsiques en matèria de seguretat aprovades per la direcció, que assenten les bases de qualsevol acció relacionada amb el tractament de la informació.

- **Implicació de l'organització**: defineix l'estructura organitzativa per a gestionar la seguretat de la informació, i identifica funcions i responsabilitats des de l'alta direcció fins a l'usuari final, estableix els nivells de decisió necessaris i els procediments de divulgació o conscienciació per a implicar-hi tota l'organització.

- **Gestió global i activa**: permet gestionar la seguretat de la informació segons criteris comuns, procediments homogenis i un vocabulari compartit, i estableix els mecanismes per a garantir la vigència del sistema de gestió, de manera que es manté viu i evoluciona, i no queda obsolet una vegada implantat.

- **Control i seguiment**: permet disposar d'una metodologia de mesura i avaluació d'indicadors, amb la finalitat de valorar els resultats enfront dels objectius establerts i mantenir informada la direcció perquè pugui prendre decisions. Alhora, estableix els mecanismes per a autoavaluar-se i facilita que es facin auditories de seguretat de la informació quan correspongui.

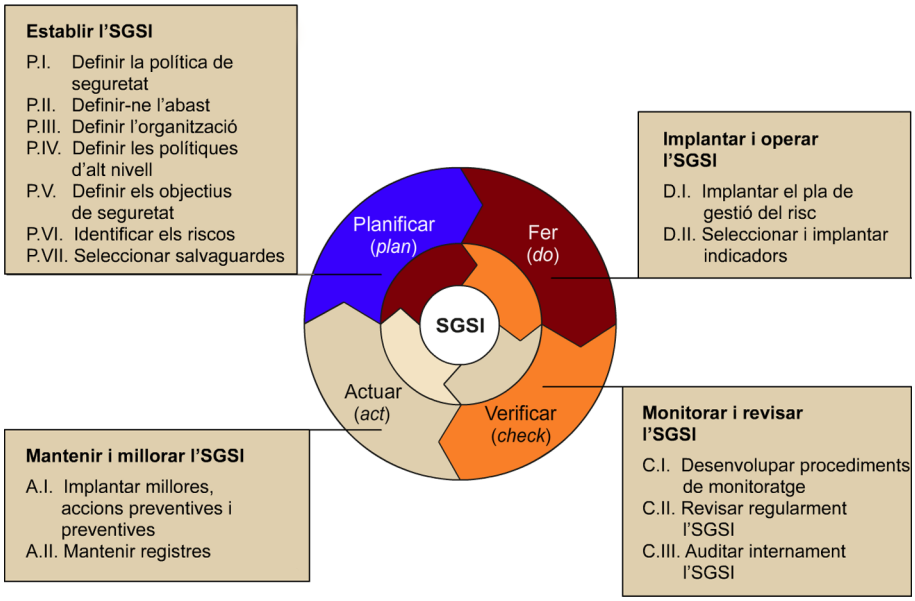
- **Millora contínua**: permet establir un procés per a anar aconseguint els objectius en diferents iteracions, de manera que el sistema de gestió s'amplia gradualment, i permet tenir en marxa un procés de revisió per a assegurar que es detecten i es corregeixen els problemes, que s'incorporen les lliçons apreses a cada nova iteració i que s'implanten millores justificades, cosa que permet evolucionar pas a pas.

- **Optimització dels recursos**:
  - Ús racional i més controlat de la informació.
  - Pressupost justificat, ajustat al risc real.

- Personal conscienciat i format en les seves responsabilitats.
- Estalvi de temps, ja que els procediments i criteris essencials s'han definit i comunicat clarament.
- Infraestructura ajustada a les necessitats reals del negoci.

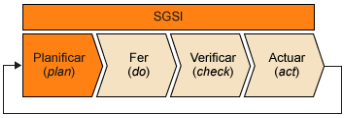
El desenvolupament d'un sistema de gestió de la seguretat de la informació es basa en l'ISO 27001 i l'ISO 27002, i també en el cicle de Deming, per a garantir l'actualització del sistema i la millora contínua, tal com es descriu en el gràfic següent:

Cicle de Deming aplicat als sistemes de gestió de seguretat de la informació



7. Planificar: establir l'SGSI

Abans d'emprendre accions cal planificar-les, és a dir, veure on som, on volem anar, quins mitjans tenim i sobre quin entorn volem treballar.



Planificar: primera fase de l'SGSI

En la imatge següent veiem quines són les etapes que constitueixen aquesta primera fase de planificació. A continuació, revisarem les característiques principals d'aquestes etapes.

7.1. P. I. Definir la política de seguretat de la informació

La política de seguretat de la informació estableix els principis i les línies d'actuació globals en qüestions de seguretat de la informació, alineats amb els objectius del negoci.

La política ha de demostrar el compromís de la direcció amb la seguretat de la informació i s'ha de donar a conèixer a tots els usuaris.

La política de seguretat de la informació es desenvolupa i es concreta en polítiques, normes, guies i estàndards de segon nivell.

Vegeu també

En l'apartat "Fer: implantar i operar l'SGSI" es donen algunes pautes per a implantar la política de seguretat de la informació.

7.2. P. II. Definir l'abast

Idealment, la seguretat de la informació ha d'estar gestionada en tots els àmbits de l'organització. La implantació d'un sistema de gestió de la seguretat de la informació és un procés continu de maduració i millora, però que habitualment comença abastant els processos més crítics de l'organització, per a anar englobant àrees menys crítiques en fases posteriors.

Així, doncs, una organització pot tenir implantat un SGSI per a un procés molt concret, com per exemple la producció d'un determinat producte, i la resta de l'organització no tenir mesures de seguretat. Si l'abast de l'SGSI s'ha limitat clarament a aquest procés, pot ser que la certificació del sistema de gestió tingui èxit, malgrat el mal estat de la seguretat de la resta de l'organització.

Per tant, el primer pas passa per establir l'abast del sistema de gestió en termes de processos, àrees organitzatives, emplaçaments i actius.

Declaració d'aplicabilitat

Document que recull la relació de controls de l'ISO 27002, especificant, per a cadascun d'aquests controls, si és d'aplicació o no a l'organització, juntament amb la justificació de la seva aplicabilitat, o una descripció de la manera com s'implementa en cas de ser-ho. Aquest document també es coneix com *State of Aplicability* (SOA).

Pautes d'implantació

Generalment, i això inclou la direcció, es pensa que definir l'abast de l'SGSI és un exercici senzill, però no ho és en absolut.

- És recomanable dedicar un temps a reflexionar sobre quins són els processos que es volen incloure en el sistema de gestió, perquè realment siguin els **processos més crítics**.
  S'ha de pensar que implantar un sistema de gestió de la seguretat comporta una dedicació de recursos i un esforç importants, i que no solament és un projecte de posada en marxa, sinó que mantenir actualitzat l'SGSI implica mantenir una dedicació permanent. Per aquest motiu va bé prendre's el temps necessari per a analitzar fins on s'ha d'implantar l'SGSI, i és indispensable consensuar aquest abast amb la direcció.

- Quan es comença a implantar un SGSI, sol ser recomanable començar per un procés tancat i transversal. Tancat en el sentit que impliqui un abast reduït, per a començar per una cosa més controlable i sobre la qual es pugui aprendre, de manera que quan s'abastin processos més "macro" es tingui un conjunt de lliçons apreses que facin més eficient la implantació. I transversal en el sentit que abasti diverses àrees o departaments de l'organització, ja que això permetrà una implantació de tota mena de controls (de recursos humans, d'operació, organitzatius, etc.) i permetrà assentar les bases per anar ampliant l'abast de l'SGSI en iteracions posteriors.

- Un aspecte important que cal considerar en la definició de l'abast és la inclusió o no de les activitats que duen a terme tercers per a l'organització. En general se solen presentar dues opcions:
  – Incloure l'activitat de tercers en l'abast mateix.
  – Excloure l'activitat de tercers de l'abast, i demostrar que s'han pres les mesures necessàries perquè aquest tercer doni compliment a la norma. Aquesta obligació s'ha de recollir clarament en el contracte amb el tercer, i l'organització s'ha de reservar el dret a l'auditoria, per a analitzar, quan ho consideri necessari, el nivell de compliment real.

- Quan es redacta l'abast és important ser precís i escriure en positiu, és a dir, explicar què hi ha inclòs en l'abast, més que no pas fer una definició general que inclogui un *excloent*.

- L'abast sol fer referència a la declaració d'aplicabilitat i la seva versió, que no és més que una relació dels controls de l'ISO, per a cadascun dels quals s'especifica si és d'aplicació o no, per a la qual cosa és determinant l'abast escollit. En cada cas, és a dir, s'apliqui o no un control, és necessari justificar-ne la causa.
  Cal destacar que, pel caràcter general de la norma, és bastant complicat que un control no apliqui. Normalment és aplicable un mínim del 80% dels controls.

A continuació, es presenten algunes definicions reals d'abast d'un SGSI:

- La gestió de la seguretat de la informació de les operacions de negoci, incloent-hi la consultoria de seguretat i subministrament d'eines de programari de seguretat. Tot plegat d'acord amb la declaració d'aplicabilitat referència 1.00.

- La implantació d'un SGSI que dóna suport al disseny i la fabricació d'equips per als mercats militar i civil. Això inclou el maquinari, el programari, la integració de sistemes i els serveis de consultoria d'acord amb la declaració d'aplicabilitat de l'SGSI referència 1.1.

- La gestió de la seguretat de la informació en el disseny, la implantació i el funcionament de la infraestructura tecnològica de l'organització. D'acord amb la declaració d'aplicabilitat, versió datada el xx/xx/xxxx.

- La gestió de la seguretat de la informació que cobreix totes les activitats associades amb el CPD d'Alcorcón que dóna suport als serveis d'allotjament segur. D'acord amb la declaració d'aplicabilitat, versió 1.0.

- Tota la informació i els sistemes que la processen per al desenvolupament de programari, la integració i els serveis de manteniment de les quatre instal·lacions en l'Índia. D'acord amb la declaració d'aplicabilitat, versió 1.0.

- El funcionament d'un SGSI per a les activitats relacionades amb el procés de cobraments i els serveis de validació associats. D'acord amb la declaració d'aplicabilitat de l'organització, versió 2.0.

- L'SGSI de banca per Internet de Banco 123 d'acord amb la declaració d'aplicabilitat versió 3.

- La gestió de la seguretat de la informació que cobreix totes les activitats desenvolupades per l'organització, com ara integracions de sistemes, incloent-hi la consultoria per al desenvolupament de programari d'aplicació IT, i els serveis de gestió de xarxes i sistemes de la companyia, d'acord amb la declaració d'aplicabilitat vigent, versió 3.0.

- La gestió de la seguretat de la informació en totes les activitats relacionades amb les vendes i la comercialització del disseny i la producció de memòries i sistemes, localitzats en les plantes de producció de Göteborg i Friburg. Això d'acord amb la declaració d'aplicabilitat versió 1.0.

- Information security management of the Information Service Center providing integrated systems management services, disaster recovery services, integrated security services, network Infra services and satellite communication services. This in accordance with the Statement of Applicability Issue 1.3.

- The information security management of the operation in the provision of commercial insurance broker services, in accordance to the Statement of Applicability Issue 3.0.

- Information security management system relating to the investigation of serious fraud. This is in accordance with the Statement of Applicability issue 1.0.

7.3. P. III. Definir l'organització de la seguretat de la informació

Qualsevol esforç per gestionar la seguretat de la informació és inútil si no s'assignen responsabilitats i funcions de manera clara i concreta, i no hi ha el suport de la direcció de l'organització.

Cada organització ha de crear el seu propi esquema organitzatiu intern, i ha d'assegurar en qualsevol cas que totes les responsabilitats i funcions en matèria de seguretat de la informació s'han assignat correctament i garanteixen, sempre que sigui possible, el principi de segregació de funcions.

Vegeu també

En el capítol següent es donen algunes pautes per a implantar l'estructura organitzativa en seguretat de la informació.

7.4. P. IV. Definir les polítiques d'alt nivell

Les polítiques d'alt nivell desenvolupen la política de seguretat de la informació en línies d'actuació més concretes. Les polítiques d'alt nivell preveuen en conjunt totes les àrees de seguretat de la informació.

Vegeu també

En el capítol següent es donen algunes pautes per a implantar un marc normatiu.

7.5. P. V. Definir objectius de seguretat de la informació

Cal establir objectius concrets de seguretat de la informació, que garanteixin que totes les iniciatives en seguretat de la informació s'han coordinat i orientat en una mateixa direcció, i s'han alineat amb els objectius del negoci. Els objectius de seguretat se solen definir anualment.

Òbviament, els objectius de seguretat sempre inclouen la reducció del risc a nivells que l'organització pugui assumir.

Pautes d'implantació

- Els objectius de seguretat s'han de definir a partir dels objectius del negoci, analitzant quina és la manera més bona de fer que la seguretat de la informació contribueixi a aquests objectius.
- De partida, els objectius de seguretat no s'han de definir pensant en el pressupost disponible, és a dir, per a contestar a la pregunta "què puc fer?", sinó que tenint en compte la situació de partida han de respondre a la pregunta "què vull fer?" o "com puc contribuir al negoci?".
  Hi ha moltes maneres de cobrir un objectiu de seguretat, i és després, en el pla de seguretat o pla de gestió del risc, en la segona fase de l'SGSI (*fer* o *do*), quan es determina com s'ha de donar cobertura a aquest objectiu o fins a quin punt és possible donar-hi cobertura.
- Els objectius de seguretat s'han de contrastar amb la direcció per a aconseguir-ne l'aprovació.

Possibles objectius de seguretat en una entitat bancària

- Reduir el frau.
- Millorar la confiança dels clients en la banca electrònica.
- Reduir temps en la recuperació dels sistemes d'informació en cas de desastre.

7.6. P. VI. Identificar els riscos

És molt important identificar els actius d'informació i establir el risc a què estan sotmesos, a partir de determinar quin serà l'impacte per a l'organització si es produeix una situació de falta de confidencialitat o privadesa, integritat o disponibilitat d'aquests actius.

La determinació del risc real a què estan sotmesos els actius d'informació permet a la direcció prendre decisions sobre el llindar de risc que pot assumir l'organització, i prioritzar les accions en matèria de seguretat de la informació, adoptant sempre mesures proporcionades.

Pautes d'implantació

- L'anàlisi de riscos ha de ser formal i estar documentada.
- La complexitat de l'anàlisi de riscos depèn de la criticitat dels actius que cal protegir.
- La metodologia utilitzada ha de ser coherent amb la complexitat i els nivells de protecció requerits.
- El grau de profunditat amb què s'ha de dur a terme l'anàlisi de riscos varia segons la maduresa de l'organització. Per a fer els primers passos es recomana fer una anàlisi d'alt nivell dels processos inclosos en l'abast, amb l'objectiu de detectar els punts de màxim risc. Més endavant, si escau, es pot fer una anàlisi més profunda dels processos inclosos en l'abast que es considerin més crítics.
- Ha de cobrir tot l'abast de l'SGSI.

Risc residual

És el risc romanent una vegada s'han aplicat els controls de seguretat.

- Els riscos canvien constantment, de manera que hi ha d'haver una metodologia i un procediment per a revisar-los i fer-ne el manteniment.
- La direcció ha d'aprovar formalment el risc residual, cosa que ha de quedar recollida en un document, que constitueix un "registre" de l'SGSI.

7.7. P. VII. Seleccionar controls de seguretat

Una vegada identificats els riscos que cal mitigar (riscos no assumibles) i els objectius de seguretat que es volen aconseguir, s'han de seleccionar els controls de seguretat necessaris. Aquests controls poden ser controls tècnics, procediments operatius, normatives d'usuari, clàusules contractuals, etc. La selecció de controls es pot fer a partir de l'ISO 27002, però també s'hi poden incloure altres controls que es considerin útils per a l'organització, no inclosos en la norma.

Pautes d'implantació

La selecció de controls s'ha de fer tenint en compte sempre el principi de proporcionalitat, i ha de quedar documentat en el document de la declaració d'aplicabilitat (en anglès, *statement of applicability* o SoA). Aquest document recull per a cada control de l'ISO si és d'aplicació o no a l'organització, i en ambdós casos és necessària la justificació. D'altra banda, és aconsellable incloure-hi, per als controls que sí que són aplicables, una explicació de la manera d'implementar el control (i fer referència a procediments, si escau) i quins són els riscos que evita. D'aquesta manera, el document estableix la relació entre l'anàlisi de riscos i l'estat real de la seguretat, i es constitueix així una eina molt útil d'auditoria, sia interna o externa.

Les raons per a no incloure-hi un control han de ser sòlides i coherents. Generalment els únics motius aplicables són:

- **La naturalesa de l'organització i la seva activitat**.
  No entra en l'abast, o afecta una activitat que l'organització no fa.

Exemple

- **Control 6.2.2. Teletreball**. L'organització que no realitzi teletreball no haurà d'aplicar aquest control.
- **Control 11.1.6. Àrees de càrrega i descàrrega**. No és aplicable si l'organització no disposa d'aquestes àrees.

- **El resultat de l'anàlisi de riscos**.
  El nivell de risc detectat no justifica la inversió per a la mitigació.

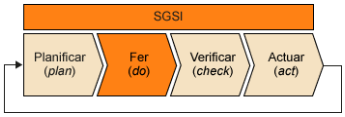
Exemple

- **Control 6.2.1**. Política de dispositius mòbils. No és aplicable, si l'anàlisi de riscos no ha detectat cap risc significatiu relacionat amb dispositius mòbils. Això es pot donar, per exemple, si es tracta d'una empresa en què els empleats utilitzen dispositius mòbils, però aquests no guarden cap tipus d'informació crítica de l'organització.

8. Fer: implantar i operar l'SGSI

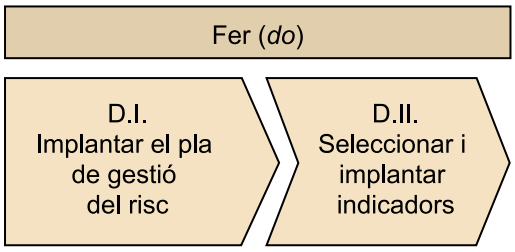
La segona fase de l'SGSI es compon bàsicament de dues activitats:

- Implantar el pla de gestió del risc.
- Seleccionar i implantar indicadors.



Fer: segona fase de l'SGSI

Etapes de la segona fase de l'SGSI: fer



Una vegada acabada la fase de planificació de l'SGSI, s'entra en la fase d'implantació, que consta bàsicament de dues etapes: una per a definir com es posarà en pràctica el que s'ha planificat en la fase anterior, que es concreta en un **pla de gestió de riscos** o **pla de seguretat**, que una vegada definit s'ha de dur a terme, i una altra per a seleccionar indicadors, que són els que permetran avaluar l'eficàcia i l'eficiència de les mesures implantades i, en definitiva, controlar l'evolució de l'estat de la seguretat de la informació.

Per tant, és la fase d'especificació de la manera de posar en pràctica els controls de seguretat seleccionats, quan s'implementaran, qui en serà responsable i amb quin pressupost, d'implementació real d'aquests controls i de la manera de mesurar l'èxit o fracàs de les accions fetes i, conseqüentment, de la rendibilitat de les inversions practicades.

8.1. D. I. Implantar el pla de gestió del risc

El **pla de gestió del risc** determina com i quan s'han d'implantar els controls seleccionats i es concreta en el **pla de seguretat de la informació**, a vegades anomenat també **pla director de seguretat de la informació**, que agrupa les accions en projectes, les prioritza definint accions a curt i mitjà termini (uns tres anys) i fa una estimació de costos. El pla de seguretat s'ha de presentar a la direcció per a aconseguir la seva aprovació i la dotació pressupostària necessària, pas previ a posar en marxa qualsevol projecte.

La implantació o revisió del pla de continuïtat de negoci acostuma a ser part d'aquest pla de seguretat.

El **pla de seguretat de la informació** és el que descriu com s'ha de dur a terme el compliment dels objectius de seguretat.

Pautes d'implantació

- La definició del pla de seguretat de la informació implica elaborar un pla d'acció per a complir els objectius i, per tant, és indispensable fer una estimació del cost de cadascun dels projectes abans de presentar-los a la direcció.
- El principi de proporcionalitat ha de regir com a element conductor del pla, ja que no ens ha de passar mai per alt que l'objectiu final no és la seguretat total, sinó portar la seguretat als nivells que pot assumir l'organització.
- Una bona proposta de pla de seguretat proporcional, coherent i ben justificat és, alhora, la base per a aconseguir el pressupost necessari i el suport de la direcció.
- Ha de quedar clar a quin objectiu o a quins objectius de seguretat definits en la fase de planificació de l'SGSI contribueix cadascun dels projectes proposats, ja que això facilitarà les decisions que ha de prendre la direcció.
- En aquest punt és important tenir en compte els controls que s'han aplicat abans (en cicles anteriors de l'SGSI, projectes de seguretat anteriors, mesures aplicades des d'alguna unitat de l'organització de manera aïllada, etc.), per a estudiar si aquests controls continuen essent efectius i, per tant, no cal adoptar mesures complementàries, o si aquests controls han perdut l'efectivitat i, per tant, s'han de substituir.
- En aquest sentit, també és important estar al dia sobre l'estat de la tecnologia i saber què ofereix el mercat, ja que la selecció d'una determinada tecnologia per a desenvolupar un control pot ser un factor clau d'èxit o fracàs.
- També és important "ser creatiu". Sovint es pensa que sense pressupost, o més ben dit, amb poc pressupost, no hi ha res a fer en seguretat, cosa que és completament falsa, ja que hi ha un bon nombre de controls purament organitzatius o bé que amb eines senzilles es poden implementar i donar bons resultats.

Aquesta fase del fer no s'acaba amb la definició del pla de seguretat, sinó que una vegada aprovat cal posar-lo en pràctica, segons la planificació establerta. Per tant, és una de les fases més llargues de l'SGSI, ja que inclou el seguiment dels diferents subprojectes que portaran a implementar les mesures de seguretat que l'anàlisi de riscos ha determinat com a necessàries en la fase anterior.

8.2. D. II. Seleccionar i implantar indicadors

Perquè el sistema es mantingui viu i actualitzat, cal avaluar-ne l'eficàcia de manera continuada. Per a fer-ho, s'han d'establir indicadors que permetin controlar el funcionament de les mesures de seguretat de la informació implantades, i també l'eficàcia i eficiència que tenen, i definir els mecanismes i la periodicitat de mesura d'aquests indicadors.

L'efectivitat de l'SGSI està proporcionalment relacionada amb l'efectivitat dels controls implantats. Per a disposar d'informació sobre l'eficàcia dels controls, és imprescindible implantar indicadors que ens proporcionin aquesta informació.

Un indicador és una mesura respecte d'una referència. Tot indicador consta de vuit components bàsics:

1) Nom de l'indicador. S'ha de seleccionar un nom significatiu, no massa llarg, que doni idea de quin és el mesurament que es fa.

2) Descripció de l'indicador. Explicació de l'objectiu de mesura d'aquest indicador.

3) Control de seguretat a què dóna suport. A quin control o controls dóna cobertura.

4) Fórmula de mesurament. Descripció de la fórmula aplicada per a obtenir la mesura. És important que els paràmetres que hi intervenen siguin concrets i no es prestin a ambigüitat.

5) Unitats de mesura. Les unitats de mesura han d'estar especificades clarament.

6) Freqüència de mesura. Cada quant s'ha de recollir la mesura. És possible establir una freqüència inicial durant un període, i una freqüència posterior més gran (per exemple, quinzenal els tres primers mesos, i mensual a partir del quart mes). En qualsevol cas, la freqüència depèn de la variabilitat en el temps de la mesura.

7) Quan sigui possible, valor objectiu i valor llindar, és a dir, respectivament, quin és el valor correcte per a la companyia i quin és el valor per sota del qual s'ha d'aixecar una alarma.

8) Responsable de la mesura. Sobre qui o, preferiblement, sobre quin càrrec recau la responsabilitat de proporcionar el resultat de la mesura.

Exemple

Imaginem-nos el cas que s'ha instal·lat un sistema d'autogestió de contrasenyes i un altre de control de privilegis d'accés en baixes laborals.

Nom indicador	*Backups*
Descripció	Mesura de l'eficàcia del control de controls de seguretat (*backups*)
Control de seguretat	A.12.3.1. Còpies de seguretat
Fórmula de mesurament	N.° de còpies fallides sobre n.º de còpies totals
Unitats de mesurament	Còpies fallides / Còpies
Freqüència de mesurament	Mensual
Valor objectiu **Valor de tall**	100% < 85% (saltarà l'alarma, si el mesurament és inferior al 85%)

Responsable de la mesura	Responsable de seguretat a partir de la informació proporcionada per l'eina de gestió de còpies de seguretat

Nom indicador	Control de privilegis d'accés en baixes laborals
Descripció	Control del funcionament del procediment de sortida d'empleats en la companyia
Control de seguretat	A.9.2.6. Eliminació o ajust de drets d'accés
Fórmula de mesurament	N.° de sol·licituds de baixa d'accés davant del personal (empleats, tercers, etc.) que deixa la companyia
Unitats de mesurament	Sol·licituds/persones
Freqüència de mesurament	Trimestral
Valor objectiu **Valor de tall**	100% < 75% (saltarà l'alarma, si el mesurament és inferior al 75%)
Responsable de la mesura	Responsable de seguretat a partir de formularis i informació de RR. HH.

S'ha d'elaborar un document que reculli tots els indicadors implantats, i la descripció de cadascun d'aquests indicadors amb les característiques que acabem de presentar.

A l'hora de seleccionar un indicador, **és important que el mesurament sigui fiable i repetible**, és a dir, que s'ha de basar en **evidències objectives**.

Hi ha diferents tipus d'indicadors.

Exemples d'indicadors

- **Indicadors de gestió**
  - Nombre d'hores de formació impartides.
  - Pressupost dedicat a personal de manteniment de sistemes.
  - Nombre de treballadors amb responsabilitats en seguretat de la informació.
  - Nombre de suggeriments de millora de l'SGSI rebuts dels treballadors.

- **Indicadors d'operació**
  - Temps total de caiguda d'un determinat servei en l'últim mes.
  - Nombre d'avaries d'equips informàtics en l'últim mes.
  - Trànsit mitjà del tallafoc.
  - Nombre d'intents de penetració detectats per l'IDS respecte del nombre d'intents rebutjats.
  - Nombre de virus detectats respecte del nombre d'incidències per virus.

- **Indicadors d'entorn**
  - Alertes per un virus nou.
  - Temps mitjà d'exposició d'un sistema des que es detecta una vulnerabilitat fins que s'aplica el pegat.
  - Alertes meteorològiques per onades de calor, tempestes elèctriques, inundacions...
  - Canvis en la legislació.

Nota

La definició d'indicadors dins de l'àmbit de l'SGSI és la diferència principal entre l'ISO 27001 i l'UNE 71502, i la BS 7799-2. A diferència de les dues primeres, aquesta última considera que n'hi ha prou de disposar de registres per a validar la implantació correcta de la seguretat de la informació en una organització, de manera que no hi cal definir indicadors.

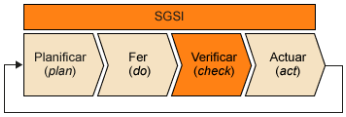
Pautes d'implantació

- Un mateix indicador es pot aplicar a diversos controls o fins i tot objectius o seccions completes de la norma.
- Al començament, els indicadors es defineixen per a vigilar que s'implanten els controls. Més endavant, passen a ser indicadors de millora contínua.
- La implantació d'un indicador requereix una dedicació de recursos, de manera que no s'han d'implantar indicadors que no siguin rellevants per a l'organització.
- És molt important ser rigorós en la recollida de la informació perquè aquesta informació sigui fiable, representativa i comparable en el temps.
- Un indicador que no aporta informació rellevant val més eliminar-lo.
- Un indicador adquireix la característica d'"indicador" en el moment en què és comparable, és a dir, que se'n pot saber l'evolució en el temps. Per això és important reflexionar sobre els indicadors que cal implantar abans de posar-los en pràctica, i intentar mantenir la mesura en el temps, per a tenir valors comparables i analitzar si realment s'està produint una millora en la seguretat de la informació. No obstant això, i com ja hem dit, si un indicador no proporciona informació rellevant, val més eliminar-lo.
- Sempre que sigui possible, s'ha d'automatitzar la mesura, per una qüestió d'eficiència (estalvi de temps d'un recurs que es pot utilitzar en altres funcions) i eficàcia (disminució o eliminació d'errors en el mesurament, és a dir, "repetibilitat").
- Una vegada més, és indispensable aplicar sempre el principi de proporcionalitat. L'esforç per a obtenir el mesurament ha de ser proporcional al valor de la informació que proporciona.

9. Verificar: monitorar i revisar l'SGSI

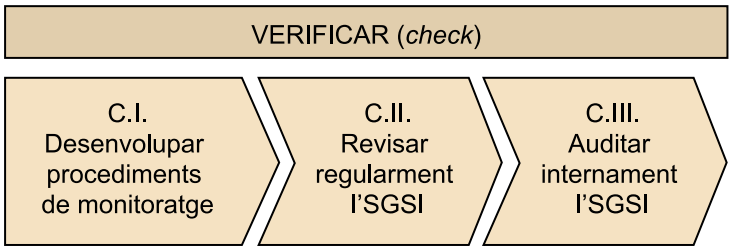
La tercera fase de l'SGSI es compon de tres etapes:

- C. I. Desenvolupar procediments de monitoratge.
- C. II. Revisar regularment l'SGSI.
- C. III. Auditar internament l'SGSI.



Verificar: tercera fase de l'SGSI

Etapes de la tercera fase de l'SGSI: verificar



Perquè el sistema es mantingui viu i actualitzat, també cal fer els passos següents:

- Fer un seguiment continuat de l'evolució dels indicadors de seguretat.

- Fer avaluacions de seguretat de la informació (del sistema de gestió, d'àrees o sistemes concrets, etc.) per part de personal intern o extern, per a detectar debilitats i establir accions correctives i de millora.

- Hi ha d'haver algú que vetlli per mantenir tota la documentació generada i per revisar-la periòdicament, incloent-hi la política de seguretat de la informació, els objectius, la resta del marc normatiu, l'anàlisi de riscos, els indicadors, el pla de continuïtat del negoci, etc.

Com a mínim cal una **revisió anual** del sistema de gestió global, i s'ha de fer que el màxim nivell directiu s'impliqui en la revisió dels components més estratègics del sistema. Hi ha d'haver un procediment que descrigui com s'ha de mantenir actualitzat l'SGSI.

9.1. C. I. Desenvolupar procediments de monitoratge

Cal fer un seguiment periòdic dels indicadors de seguretat de la informació, per saber-ne l'estat i evolució i, en definitiva, l'eficàcia; és a dir, per saber si el control contribueix a aconseguir l'objectiu de seguretat pel qual es va dissenyar. Com s'explicava en l'apartat anterior, sempre que sigui possible i econòmicament acceptable, és recomanable automatitzar els procediments de mo-

nitoratge, per a facilitar i fiabilitzar la generació dels informes de l'estat de la seguretat de la informació i la generació d'alarmes per a denunciar incidències o situacions de seguretat deficient que requereixin una actuació urgent.

9.2. C. II. Revisar l'SGSI

La direcció ha de revisar l'SGSI a intervals planificats, per a ratificar-ne la conveniència, adequació i eficàcia. Aquesta revisió ha de ser com a mínim anual, encara que al començament es recomana una periodicitat més curta.

Les revisions de la direcció de l'organització han de fer el següent:

- Tenir un procediment per a dur-les a terme.
- Identificar canvis en els nivells de risc, noves amenaces i vulnerabilitats.
- Identificar canvis en l'organització.
- Identificar canvis en la legislació.
- Revisar l'estat del sistema i la seva implantació.
- Analitzar que es compleixen els objectius de seguretat.
- Analitzar l'efectivitat dels controls implantats (evolució de l'estat de la seguretat).
- Establir accions correctives i de millora.
- Disposar de registres que evidenciïn aquestes revisions.

Per a saber l'estat dels controls i l'evolució que tenen en el temps, és habitual utilitzar models de maduresa predefinits, que introdueixen objectivitat en l'avaluació, ja que estableixen criteris estàndard fàcils d'entendre per personal aliè al món de la seguretat de la informació.

9.3. C. III. Auditories

La comprovació de la idoneïtat del disseny i la implantació de l'SGSI es fa amb auditories, que es poden dur a terme internament o contractant auditors externs. En qualsevol cas, els auditors han de complir els requisits següents:

- Han de ser independents, és a dir, no poden haver intervingut en el procés o treball auditat.
- Han d'estar qualificats en la matèria: coneixement del procés d'auditoria i de les normes auditades i, si pot ser, han de tenir experiència en el camp de la seguretat de la informació.

Aquestes auditories s'han de planificar correctament, perquè hi estiguin implicades totes les persones necessàries.

L'informe d'auditoria ha d'incloure com a mínim:

- Data de l'auditoria.
- Nom dels auditors.

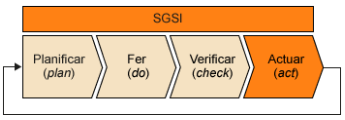
- Abast de l'auditoria: àrea, departament i/o processos auditats.
- Controls auditats.
- Conformitat de l'SGSI amb la norma, o grau d'adequació.
- No-conformitats detectades.
- Si l'auditoria no és de certificació, pot contenir, a més, recomanacions de millora.

Generalment, l'informe no recull com s'ha auditat un control, ni tampoc les evidències recollides per a l'auditoria, que formen part de la documentació de l'auditor.

10. Actuar: mantenir i millorar l'SGSI

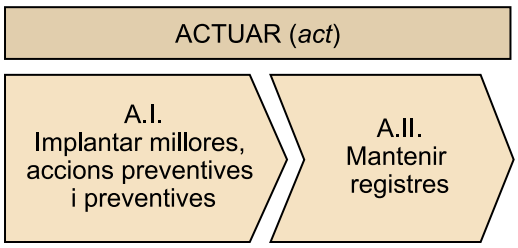
Finalment, la quarta i última fase del cicle de l'SGSI es compon de les dues activitats següents:

- Implantar millores i accions correctives.
- Mantenir registres.



Actuar: quarta i última fase de l'SGSI

Etapes de la quarta i última fase de l'SGSI: actuar



Del monitoratge i la revisió de l'SGSI i dels resultats de les auditories s'obtenen **propostes de millora i accions correctives**, que s'han de planificar dins del pla de seguretat de la informació.

Mantenir l'SGSI passa també per conservar un conjunt d'evidències que provin que polítiques, procediments, controls i indicadors no són definicions teòriques, sinó que es porten a la pràctica tal com especifica el sistema. Generalment, d'aquestes evidències se'n diu *registres*.

Els registres han de ser:

- Llegibles: s'han de conservar en un format accessible o recuperable.
- Identificables: s'hi ha d'assignar una codificació o nomenclatura significativa, que permeti localitzar-los amb relativa facilitat.
- Traçables: ha de ser possible saber l'evolució de les versions i s'han de preservar d'alteracions, és a dir, que s'han de protegir contra danys, deterioració, pèrdua o manipulació.

Si no hi ha requisits legals específics, els registres se solen guardar uns tres anys.

Per obtenir la certificació del SGSI és aconsellable disposar d'un mínim de temps de registres. Algunes entitats certificadores exigeixen un mínim de tres o sis mesos.

És indispensable desenvolupar un procediment que especifiqui com s'ha de fer la gestió dels registres, i establir-hi com se n'ha de fer la identificació, l'emmagatzematge, la protecció, la recuperació i l'eliminació (depenent del temps de vida establert).

Un registre pot adoptar moltes formes diferents: des de l'acta d'una reunió amb la direcció fins a una extracció de traces d'un sistema, passant per una llista d'assistents a un curs de formació.

11. Esquema documental de l'SGSI

Tal com hem vist fins ara, un sistema de gestió de la seguretat de la informació és un conjunt d'accions coordinades i dirigides a millorar la seguretat de la informació d'una organització, que abasta des de la fase de planificació i implantació fins a la fase de control o verificació i actuació per a la millora, en iteracions consecutives que persegueixen introduir l'organització en un cicle permanent de millora contínua per a, en definitiva, anar madurant el procés de la seguretat de la informació i fer-lo progressivament més eficient.

Al llarg de la descripció de les diferents fases, s'ha fet referència a polítiques, procediments, revisions, documents, plans...

En aquest apartat, presentem l'esquema documental de tot SGSI, de manera ordenada. La majoria de les entrades ja s'han referenciat en apartats anteriors, però en aquest punt es presenten de manera ordenada, amb dos objectius:

- Plasmar la coherència de tota la documentació referenciada.

- Tenir un índex al qual s'ha de donar compliment per a implantar un SGSI i, molt especialment, en cas que l'organització vulgui superar un procés de certificació.

Marc documental

- Principis de l'SGSI. (A vegades d'aquest apartat se'n diu *manual de seguretat*.)
  - Política de seguretat de la informació.
  - Abast de l'SGSI.
  - Breu descripció de l'activitat de l'organització i organigrama.
  - Objectius de seguretat de la informació.
  - Polítiques concretes d'alt nivell (es poden descriure detalladament o simplement fer-hi referència).
  - Organització de la seguretat de la informació (rols i responsabilitats de l'SGSI).

  - Com s'implanta la norma: referència a procediments, manuals, instruccions, etc.

- Metodologia d'anàlisi i tractament de riscos i procediments de revisió.

- Declaració d'aplicabilitat.

- Polítiques de seguretat de la informació d'alt nivell (si no s'han inclòs en els principis de l'SGSI).

- Inventari d'actius.

- Ús acceptable d'actius.

- Política de control d'accessos.

- Procediments d'operació per a la gestió de TI.

- Principis d'enginyeria de sistemes segurs.

- Política de seguretat de proveïdors.

- Procediment de gestió d'incidents de seguretat de la informació.

- Pla de continuïtat del negoci.

- Identificació de la legislació aplicable, i dels requeriments contractuals.

- Procediments:
  - Control documental de l'SGSI: descripció de la llista de documents que conformen l'SGSI, on se situen, com es revisen i versionen, com es codifiquen, etc.

  - Control de registres de l'SGSI: descripció de la manera de gestionar, emmagatzemar, destruir, etc., els registres que genera el sistema de gestió.

  - Revisió de l'SGSI per la direcció (descripció de la manera de dur a terme el procés de revisió).

  - Gestió d'indicadors (a escala conceptual, sense entrar en el detall de cadascun d'aquests indicadors: què és un indicador, qui els defineix, qui assigna la responsabilitat de la mesura, a qui es reporten, informe a direcció, accions en cas de compliment

reiterat d'un indicador, accions en cas d'incompliment reiterat, etc.).

– Formació en seguretat de la informació.

– Gestió d'accions correctives i de millora. Formulari de registre de no-conformitats.

– Actualització i revisió del pla de continuïtat de negoci (motius del canvi, freqüència de revisió, responsables, formació dels implicats, etc.). Aquest punt també pot formar part del mateix pla de continuïtat de negoci.

- Registres.
  – Resultats de l'anàlisi de riscos.

  – Document d'acceptació de la direcció del risc residual.

  – Seguiment dels objectius de seguretat de la informació establerts per la direcció.

  – Programes i resultats d'auditories.

  – Llista d'indicadors (fórmula de mesurament, responsable de la mesura, freqüència, valor objectiu de l'indicador, control de l'ISO amb què està relacionat).

  – Actes de reunions de revisió que fa direcció de l'SGSI, convocatòria de reunions, informes de revisió que ha elaborat el gestor de seguretat de la informació.

  – Correus electrònics que ha enviat la direcció, cursos de formació, etc.

  – *Logs* o diaris d'activitats d'usuari i esdeveniments de seguretat.

  – Formació impartida i qualificació de les persones que hi ha dins de l'abast de l'SGSI.

  – Informe de no-conformitats (pla de seguiment d'accions correctives i de millora, revisió d'efectivitat).

  – Revisions del pla de continuïtat del negoci.

– Formularis i documentació que prova que es compleixen els procediments.

Resum

Aquest mòdul s'ha centrat a presentar l'ISO 27001, de seguretat de la informació, el coneixement de la qual és indispensable per a qualsevol professional dedicat a gestionar la seguretat de la informació.

Així, doncs, s'han presentat, en primer lloc, l'ISO 27002 o guia de bones pràctiques en seguretat de la informació. Aquesta norma estableix la importància de l'anàlisi de riscos com a punt d'inici del procés de gestió de la seguretat de la informació. En segon lloc, s'han presentat catorze dominis de controls indispensables per a fer una gestió integral, que van des de qüestions organitzatives, com la política de seguretat o el marc normatiu, fins a aspectes de recursos humans, com la contractació, la formació o la signatura de clàusules de confidencialitat, passant per qüestions molt més tècniques, com la gestió de l'adquisició de productes, el desenvolupament d'aquesta adquisició o l'operació dels sistemes i les infraestructures TIC. Finalment, s'ha parlat de la importància del compliment legal i la protecció dels registres de la companyia, o la necessitat d'un pla de continuïtat de negoci.

L'ISO 27001, per la seva banda, descriu la implantació d'un sistema de gestió de la seguretat de la informació, basat en el *cicle de Deming* o *cicle PDCA*, que planteja la gestió de la seguretat com un procés de millora contínua, basat en la repetició cíclica de quatre fases: **planificar**, **fer**, **verificar** i **actuar**.

És materialment impossible resumir aquestes dues normes en unes quantes línies, però intentarem concretar quins són els factors crítics d'èxit de la implantació d'un SGSI en deu punts:

1) La política i els objectius de seguretat de la informació han d'estar alineats amb els objectius del negoci.

2) L'enfocament per a implantar la seguretat de la informació ha de ser consistent amb la cultura de l'organització.

3) Suport visible i compromís de la direcció.

4) Definició precisa i clara de l'abast de l'SGSI.

5) Bona comprensió de l'anàlisi i de la gestió del risc, i també dels requisits de seguretat de la informació.

6) Definició clara de les funcions en seguretat de la informació.

7) Conscienciació de la direcció i els treballadors en matèria de seguretat de la informació, i formació i capacitació quan sigui necessari.

8) Distribució a tots els treballadors i terceres parts que hi estan implicades de la política de seguretat de la informació, i també d'altres normes i estàndards vigents.

9) Sistema integrat i equilibrat de mesura que permeti avaluar el rendiment de la gestió de la seguretat de la informació i la introducció contínua de millores en la seguretat i el sistema de gestió d'aquesta seguretat.

10) Disposar de recursos humans i tècnics, que permetin gestionar la seguretat i mantenir el sistema de gestió.