Introducció a la seguretat de la informació

PID_00253136

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.

Índex

Introducció

El concepte de *seguretat* és molt antic. Des de temps immemorials, els humans han fet esforços per protegir allò que consideraven que era seu o que tenia un valor que s'havia de preservar i han pres mesures per a fer-ho.

En la societat actual, un dels principals béns que cal protegir, aquell que representa un valor més important per als negocis, és la informació, i per això hi ha aquesta necessitat de protegir-la, ja que el món està cada vegada més connectat, i els atacs a les infraestructures, les xarxes i els sistemes són cada vegada més sofisticats.

Al llarg d'aquest mòdul es fixaran els conceptes i pilars bàsics sobre els quals s'assenta la gestió de la seguretat de la informació, es revisaran breument diferents aproximacions de models de gestió, es presentarà el marc normatiu entorn de la seguretat de la informació i, finalment, es parlarà d'alguns estàndards reconeguts internacionalment en aquesta matèria.

Objectius

Els objectius que persegueix aquest mòdul són els següents:

1. Entendre què s'entén per *seguretat de la informació*, i la diferència que té respecte del concepte de *seguretat informàtica*.

2. Conèixer els pilars sobre els quals s'assenta la seguretat de la informació: confidencialitat, integritat, disponibilitat i d'altres, i els diferents tipus de mesures de seguretat.

3. Presentar breument diferents models de gestió adoptats avui dia per les organitzacions.

4. Donar a conèixer la principal legislació espanyola amb implicació en seguretat de la informació.

5. Descriure succintament els principals estàndards de reconeixement internacional, que parlen sobre seguretat de la informació.

1. Què és seguretat de la informació

Com es deia en la introducció d'aquest mòdul, avui dia la informació és un dels principals actius, si no el principal, de moltes companyies. La necessitat de protegir un dels actius de més valor per a la companyia ha fet que moltes organitzacions hagin dedicat una infinitat de recursos a aquest fi.

La mena de tasques dutes a terme en aquest sentit i de mesures de seguretat implantades han variat molt en el temps. La digitalització de la informació, Internet i l'evolució de les noves tecnologies han esdevingut les introductores de grans canvis, a causa de l'aparició de noves amenaces que no s'havien imaginat mai abans.

A això hi cal afegir els nous models de gestió que es van imposant i que aquestes noves tecnologies propicien, en passar de gestionar-ho absolutament tot de manera interna en l'organització en un extrem, a contractar serveis d'informàtica en núvol (*cloud computing*) a l'extrem oposat.

És important no confondre el terme *seguretat de la informació* amb el terme *seguretat informàtica*, ja que, si bé el primer engloba el segon, no són sinònims. La seguretat informàtica s'ocupa únicament de la seguretat dels sistemes d'informació i, per tant, queda circumscrita a l'àmbit de la informació automatitzada, de manera que és un terme molt més restrictiu que el de *seguretat de la informació*, que s'ocupa de la informació **en totes les seves formes** (oral, escrita, impresa, electrònica, òptica, electromagnètica, etc.) i **en qualsevol moment del seu cicle de vida** (creació o captura, manteniment, distribució i ús, i emmagatzematge, arxiu i destrucció), per protegir-la de qualsevol amenaça que comporti pèrdua o disminució del valor que té.

De tot això es dedueix que la seguretat de la informació és una qüestió que afecta tota la companyia, ja que tota l'organització treballa amb informació i, per tant, requereix una gestió coordinada i transversal, la qual cosa comporta planificació i gestió, i no pot ser improvisat, sinó que ha de ser considerat com un procés més de la companyia que interactua amb la resta dels processos del negoci.

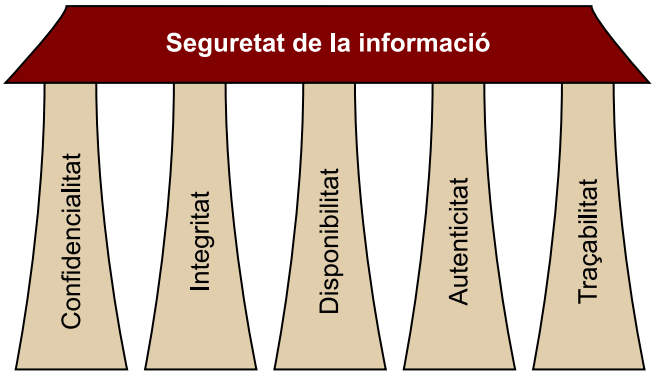
2. Dimensions de la seguretat de la informació

Tradicionalment, parlar de *seguretat de la informació* era referir-se als tres pilars bàsics:

- **Confidencialitat**: només les persones autoritzades tenen accés a la informació sensible o privada.
- **Integritat**: la informació i els mètodes de processament d'aquesta informació són exactes i complets, i no s'han de manipular sense autorització.
- **Disponibilitat**: els usuaris que hi estan autoritzats poden accedir a la informació quan ho necessitin.

No obstant això, darrerament es consideren també altres dimensions de la seguretat, previstes per la mateixa legislació vigent:

- **Autenticitat i no-repudi**: hi ha garantia de la identitat dels usuaris o processos que tracten la informació i de l'autoria d'una determinada acció.
- **Traçabilitat**: és possible reproduir un històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció.



Els pilars de la seguretat de la informació

Finalment, també pot ser útil, en treballar en seguretat de la informació, prendre en consideració la **privadesa**, que garanteix que només les persones autoritzades tenen accés a informació de caràcter personal. És important notar que *confidencialitat* i *privadesa*, encara que estan molt relacionades, no són sinònims, ja que la privadesa es refereix únicament a dades de caràcter personal

que poden ser públiques o no, mentre que la confidencialitat es refereix a informació, personal o no, que la companyia, pel motiu que sigui, vol protegir de ser difosa obertament.

Totes les dimensions de seguretat són rellevants i s'han de prendre en consideració de la mateixa manera, encara que depenent del tipus d'informació que s'està tractant té més importància l'una o l'altra.

Exemple

Si l'objectiu és protegir la informació de nòmines d'una companyia, la confidencialitat i la integritat són les dimensions més rellevants.

Si, en canvi, l'objectiu és protegir un lloc web de comerç en línia, possiblement són més importants la integritat i la disponibilitat.

Si l'objectiu és protegir un lloc web mitjançant el qual els ciutadans fan tràmits electrònics amb l'Administració, la disponibilitat, la integritat i la traçabilitat passen per davant.

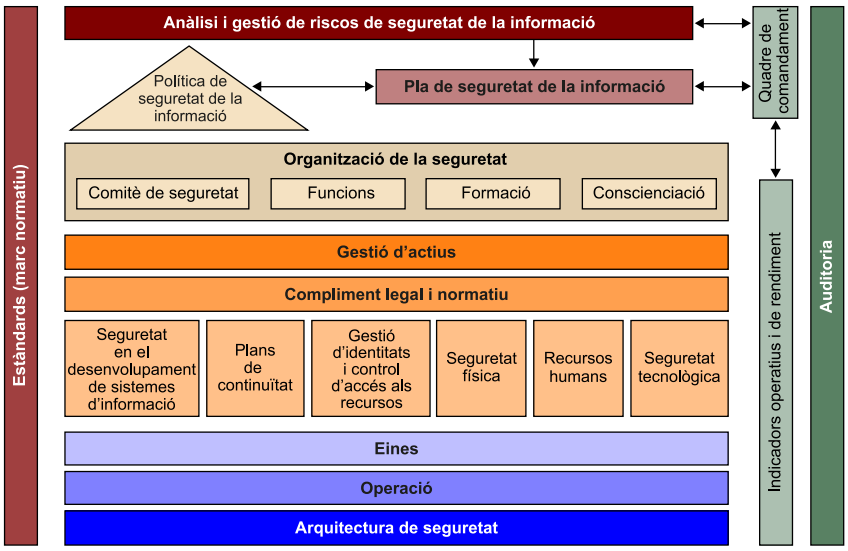
I si l'objectiu és protegir un sistema de comunicació als ciutadans per a emergències nacionals, la disponibilitat és primordial.

3. Gestió de la seguretat de la informació

La seguretat de la informació és, per tant, un procés de la companyia que s'ha de gestionar i que requereix dedicació de recursos personals i econòmics. És indispensable una bona definició de l'organització de la seguretat de la informació i una bona assignació de funcions, perquè aquesta seguretat sigui realment eficient i quedi incorporada al dia a dia de la companyia.

La gestió de la seguretat de la informació comporta un gran nombre d'activitats, que s'enuncien en aquest punt, i que es tractaran al llarg del curs. L'esquema següent presenta d'una manera senzilla les activitats que cal abordar en matèria de seguretat de la informació i que, com s'observa, són organitzatives o tècniques i, a vegades, també jurídiques.

Depenent de l'estat de maduresa de l'organització pel que fa al desplegament de la seguretat de la informació, cal prioritzar les activitats d'una manera o una altra, però, a la llarga, la gestió de la seguretat requereix que l'organització dediqui esforços a cadascuna de les activitats plasmades a continuació:



El procés de gestió de la seguretat de la informació

3.1. Models de gestió

Hi ha diferents models de gestió de la seguretat de la informació, i tots són vàlids. Cada organització ha d'analitzar quin d'aquests models s'adapta millor a la seva idiosincràsia i les seves característiques.

3.1.1. Gestió interna de la seguretat

La seguretat la gestiona íntegrament personal propi, cosa que requereix la contractació de personal especialitzat.

Aquest model ha de tenir un responsable de seguretat de la informació, a qui doni suport un equip de treball, la grandària del qual varia segons la tipologia de la companyia.

Com a punts forts cal destacar el coneixement del negoci i la implicació del personal. Com a punts febles, el cost de contractació i la falta de flexibilitat en el dimensionament dels equips.

3.1.2. Gestió externalitzada de la seguretat

La companyia subcontracta una empresa externa per gestionar-ne íntegrament o parcialment la seguretat. El personal extern pot estar situat internament o fer una gestió en remot segons les activitats subcontractades.

Com a punt fort cal destacar l'alta especialització, ja que es tracta de personal altament qualificat i amb experiència, que aporta el valor d'estar treballant amb altres clients. Com a punt feble, la falta de coneixement del negoci i la possible desconfiança del personal intern.

Aquest model requereix establir un bon contracte, en què quedin definides clarament les responsabilitats d'una part i de l'altra, i també els acords de nivell de servei (ANS).

Les empreses que ofereixen serveis de gestió de seguretat de la informació en remot solen rebre el nom de *centre d'operacions de seguretat* o *security operations center* (SOC). Un SOC es caracteritza pel fet de disposar dels serveis següents:

- Avançades eines de gestió i monitoratge de la seguretat dels sistemes d'informació.
- Avançades eines de detecció d'incidències de seguretat des d'un punt centralitzat.
- Personal altament especialitzat i coneixedor dels últims avenços de la tecnologia.

Habitualment, el SOC opera monitorant la seguretat dels clients 24 × 7 (24 hores, 7 dies a la setmana).

Les activitats més típiques d'un SOC són la protecció contra intrusions i atacs externs. Habitualment presta serveis d'anàlisi d'activitat de tallafoc, IDS, IPS, antivirus i en general codi maliciós, i també detecta vulnerabilitats, encara que pot oferir serveis de configuració segura del maquinari i del programari, monitoratge de la disponibilitat de sistemes, auditories de seguretat, proves

de penetració, assistència tècnica, etc. A més, acostuma a tenir capacitat de reacció per a contenir les incidències. Òbviament, un SOC disposa de procediments d'actuació clarament definits i estandarditzats, i en destaca el d'escalat d'incidències al client.

3.1.3. Model mixt

Hi ha una organització interna en seguretat de la informació, que es recolza en un equip de personal especialitzat extern.

Aquest model reuneix els punts forts dels models anteriors i elimina els punts febles.

És habitual que el personal intern desenvolupi les tasques més organitzatives i menys tècniques, de manera que la part més tècnica queda en mans de personal extern expert.

3.2. Punt de partida

Sigui quin sigui el model de gestió escollit per la companyia, el procés d'implantació de la seguretat de la informació no es pot engegar si abans no s'han treballat els quatre punts següents:

- **Coneixement del negoci**. La seguretat de la informació ha d'estar al servei del negoci, de manera que és imprescindible conèixer l'activitat del negoci i els objectius que té, amb la finalitat d'aplicar una seguretat que suporti aquests objectius de manera eficient i proporcional als riscos que cal mitigar. Per tant, és necessari entendre quins són els processos de negoci que es duen a terme, i identificar els més crítics, cosa que permetrà prioritzar accions.

- **Anàlisi de la situació de partida**. Abans de començar a aplicar mesures de seguretat, és important fer una anàlisi de la situació de partida, amb la finalitat de conèixer l'estat de la seguretat i el nivell d'eficiència que té, tant en l'àmbit tècnic com en l'organitzatiu. Això permetrà identificar la distància entre la situació de partida i la situació volguda i definir un pla per a acostar-les.

- **Anàlisi de riscos**. Més endavant s'estudiarà detalladament en què consisteix l'anàlisi de riscos, que és un dels fonaments per a una bona gestió de la seguretat, però, tal com indica el nom, l'anàlisi de riscos analitza quins són els riscos a què està exposat el negoci, a partir de la valoració de quin és l'impacte per al negoci en cas de materialització d'una amenaça.

Exemple

Imaginem-nos una empresa de producció de maquinària per comanda o *on-demand*, per a la qual és imprescindible mantenir operativa la línia de producció 24 x 7 per a complir els acords de nivell de servei establerts amb els seus clients. En aquest cas, la disponibilitat és la dimensió més crítica del procés i cal analitzar de manera prioritària quines possibles amenaces contra la disponibilitat es poden materialitzar i, per tant, poden produir interrupcions en la producció.

Hi ha amplis catàlegs d'amenaces; alguns exemples d'amenaces a la disponibilitat són inundació o incendi, tall del subministrament elèctric, baixa de personal clau i caiguda del sistema informàtic de control de la producció.

El risc és més gran com més probabilitat hi ha d'ocurrència de l'amenaça, d'una banda, i com més gran és l'impacte sobre el negoci, de l'altra.

El coneixement del risc a què està exposat la companyia, o dit d'una altra manera, la capacitat de treballar en un entorn de riscos gestionats, millora la presa de decisions en matèria de seguretat de la informació i facilita la priorització d'accions.

- **Compliment legal**. És indispensable conèixer quina és la legislació que és d'aplicació a la companyia (internacional, nacional, autonòmica, sectorial, etc.), ja que aquesta legislació pot exigir l'aplicació de certes mesures de seguretat que s'han d'incorporar obligatòriament al procés de gestió del risc.

3.3. Mesures de protecció

Control de seguretat

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

Una vegada l'organització sap quins són els riscos a què està exposada i determina quin és el nivell de risc màxim que està disposada a assumir, s'han de seleccionar les mesures de seguretat que cal implantar, anomenades també *controls de seguretat*. Òbviament, en aquest procés ha de regir el principi de proporcionalitat, ja que el cost d'aplicació d'una mesura no ha d'excedir mai el cost derivat de la materialització d'una amenaça.

3.4. Tipus de controls de seguretat

1) Segons la naturalesa del control: tècnics i organitzatius

Les mesures de seguretat tècniques són, per exemple, un antivirus, un tallafoc, la configuració d'un sistema, un sistema d'alimentació ininterrompuda o el xifratge de les comunicacions.

Les mesures de seguretat organitzatives són, per exemple, l'elaboració de polítiques, normes i procediments, la definició de funcions de seguretat, l'elaboració del pla de continuïtat de negoci o la formació i conscienciació.

2) Segons si els controls actuen sobre la reducció de la probabilitat o la reducció de l'impacte

Si, com s'ha vist, el risc és una combinació de probabilitat de materialització d'una amenaça i impacte sobre el negoci, diferenciem dos tipus de controls: els que redueixen la probabilitat d'ocurrència d'una amenaça i els que redueixen l'impacte sobre el negoci en cas de materialització d'aquesta amenaça.

Exemple

Un sistema d'alimentació ininterrompuda redueix l'impacte en cas que es produeixi un tall de subministrament elèctric, ja que si es produeix la incidència el que fa és mantenir els sistemes crítics en marxa durant el temps suficient per a aconseguir un tancament ordenat. No evita la indisponibilitat del sistema, però redueix les conseqüències que pot provocar un tall sobtat.

D'altra manera, un sistema de detecció d'incendis redueix la probabilitat que s'arribi a produir un incendi, actuant sobre la probabilitat de materialització de l'amenaça, gràcies a una detecció primerenca.

3) Segons la finalitat del control

Depenent del moment del cicle de vida d'una incidència en què actuï el control, diferenciem els controls següents:

- **Preventius**. Actuen perquè el risc no es materialitzi, i redueixen així la probabilitat d'ocurrència de l'amenaça.

Exemple

Els tallafocs, ja que són una mesura per a prevenir la possible intrusió d'un *hacker*.

- **De detecció**. Detecten la incidència que s'ha produït per reaccionar amb la màxima celeritat possible.

Exemple

L'IDS (sistema de detecció d'intrusions o *intrusion detection system*). Aquest control no redueix el risc d'accés sense autorització als sistemes de l'organització, sinó que fa saltar una alarma en cas que succeeixi.

- **Correctius**. Permeten reduir el dany o la recuperació de la situació normal una vegada s'ha produït la incidència.

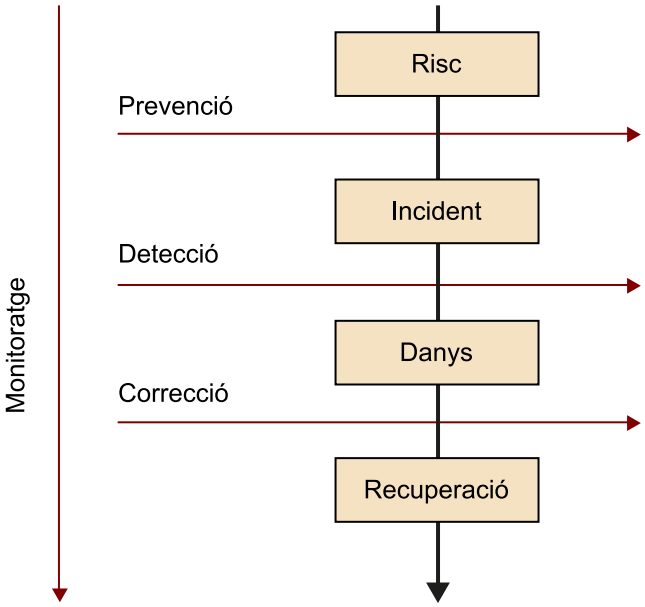
Exemples

- **Sistema d'extinció d'incendis i sistema d'alimentació ininterrompuda**. Redueix el dany que es provocarà.
- **Còpies de seguretat**. Permeten tornar a la situació anterior a la incidència, i recuperar així la informació en l'estat en què es trobava.

- **De monitoratge**. Permeten recollir evidències i fer un seguiment per a analitzar anomalies, tendències, conductes poc habituals o incidències detectades.

Exemple

El sistema de gestió de traces. En cas d'una incidència de seguretat, es pot analitzar la causa que la va provocar, i també els passos que es van dur a terme per a resoldre-la. Alhora, permet introduir els canvis necessaris per a evitar que torni a passar.



Tipus de controls de seguretat de la informació

Encara que la majoria dels controls tenen una finalitat bàsica, n'hi ha que en poden cobrir més d'una.

Exemple

La implantació d'una metodologia de desenvolupament de programari es pot considerar probablement com un control tant preventiu com de detecció. Una metodologia d'aquest tipus ha d'incloure la seguretat de la informació en totes les fases: des de la presa de requisits fins a la fase de proves, passant pel desenvolupament del codi font per a evitar determinades vulnerabilitats típiques. Un programari nou no verificat per a comprovar que s'han cobert tots els requisits de seguretat establerts al començament no ha de passar mai a producció. Aquí resideix el caràcter preventiu de la metodologia, ja que permet detectar deficiències o vulnerabilitats abans que puguin ser explotades. D'altra banda, un bon programari es desenvolupa amb determinats controls i avisos o missatges que poden donar pistes d'un mal funcionament o un mal ús. En aquest sentit es pot considerar una mesura de detecció.

4. Normativa legal a Espanya

En realitat, l'aplicació de mesures de seguretat és una qüestió opcional en una companyia, excepte en cas que hi hagi una norma legal que n'estableixi l'obligatorietat.

Per tant, és indispensable saber quina és la normativa legal d'aplicació a l'activitat que desenvolupa la companyia, sia a escala internacional, europea, nacional, autonòmica o local, sia a escala sectorial (per exemple, hi ha legislació específica del sector sanitari, mediambiental, etc.).

A continuació, es presenten algunes de les normes legals amb més afectació general sobre la seguretat de la informació a Espanya. Qualsevol professional dedicat a la seguretat de la informació ha de tenir nocions sobre el contingut d'aquestes normes i ha d'haver llegit com a mínim l'exposició de motius inicial. Es poden consultar totes en el *Butlletí Oficial de l'Estat*:

- Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, coneguda habitualment com a *LOPD*.

- Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD.

- Reglament de la UE 2016/679, de 27 d'abril del 2016. Reglament general de protecció de dades (RGPD), que substituirà l'actual normativa vigent i que es començarà a aplicar el 25 de maig de 2018. Aquest període de dos anys té com a objectiu permetre que els estats de la Unió Europea, les institucions i també les empreses i organitzacions que tracten dades vagin preparant-se i adaptant-se per al moment en què el Reglament sigui aplicable.

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

- Reial decret 3/2010, de 8 de gener, pel qual es regula l'esquema nacional de seguretat en l'àmbit de l'administració electrònica, conegut habitualment com a *ENS*. Aquest reial decret és únicament d'aplicació a l'Administració pública.

- Reial decret 4/2010, de 8 de gener [esquema nacional d'interoperabilitat (ENI)], pel qual es regula l'esquema nacional d'interoperabilitat en l'àmbit de l'Administració electrònica.

- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, coneguda habitualment com a *LSSI*.

- Llei 50/2003, de 19 de desembre, de signatura electrònica.

- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions i a les xarxes públiques de comunicacions.

5. Estàndards de seguretat de la informació

Hi ha estàndards de seguretat de la informació amb reconeixement a escala internacional, aplicables a qualsevol tipus d'organització, independentment de la seva activitat o grandària. Aquests estàndards o normes són guies de referència o fulls de ruta molt bons per a gestionar la seguretat de la informació.

A continuació se n'exposen alguns. Normalment no són normes gratuïtes i, un cop adquirides, l'autorització d'ús està restringida exclusivament a l'organització que l'ha adquirit.

1) Normes ISO relatives a la seguretat de la informació.

- ISO 27000: conté termes i definicions emprats en tota la sèrie 27000.
- ISO 27001: norma principal de la sèrie. Especifica els requisits per a la implantació d'un SGSI.
- ISO 27002: guia de bones pràctiques per a la gestió de la seguretat de la informació.
- ISO 27003: directrius per a la implantació d'un SGSI.
- ISO 27004: mètriques i tècniques per a la gestió de la seguretat de la informació.
- ISO 27005: directrius per a la gestió del risc en la seguretat de la informació.
- ISO 27006: requisits per a l'acreditació d'entitats que proporcionen certificació de SGSI.
- ISO 27007: guia per a auditar el SGSI.
- ISO 27008: guia d'auditoria dels controls seleccionats en el marc d'implantació d'un SGSI.
- ISO 27010: guia per a gestionar la seguretat de la informació en comunicacions entre sectors.
- ISO 27011: guia de gestió de seguretat de la informació per a telecomunicacions.
- ISO 27012: requisits i directrius de gestió de seguretat de la informació en organitzacions de serveis d'e-administració.
- ISO 27013: guia per a la implementació integrada d'ISO 27001 i ISO 20000-1.
- ISO 27014: guia de govern corporatiu de la seguretat de la informació.
- ISO 27015: guia de SGSI per a organitzacions del sector d'assegurances i finances.
- ISO 27016: guia de SGSI per a aspectes econòmics de les organitzacions.
- ISO 27031: guia de continuïtat de negoci referent a tecnologies de la informació i comunicacions.
- ISO 27032: guia sobre ciberseguretat.

2) Altres normatives ISO.

- ISO 22301. Gestió de la continuïtat de negoci
- ISO 31000. Gestió de riscos, principis i guies

3) Cobit (objectius de control per a la informació i tecnologies relacionades o *control objectives for information and related technology*). Cobit és un marc de treball o model de sistema de control intern per a governar les TIC que s'ha convertit a escala internacional en un estàndard *de facto*. Aporta un marc de referència que cada organització ha d'adequar a la realitat del seu negoci per a establir els punts següents:

- Com aconsegueix la informació que necessita, l'organització?
- Com garanteix la consecució dels objectius de l'empresa, la contribució de les TIC?
- Com es gestionen els riscos tècnics?
- Com es protegeixen els recursos crítics?
- Com controla l'organització i com mesura les TIC?

Cobit defineix cinc àrees de treball clau:

- Alineació estratègica.
- Lliurament de valor.
- Administració de riscos.
- Administració de recursos.
- Mesurament de l'acompliment.

Àrees de Cobit

4) ITIL. Aquest acrònim, derivat de l'anglès *information technology infrastructure library* (biblioteca d'infraestructura de tecnologies de la informació), és un marc de treball per a gestionar les tecnologies de la informació i proveir les empreses dels serveis d'aquestes tecnologies. És un conjunt de bones pràctiques per a planificar els serveis de les TIC de la companyia, proveir-la d'aquests serveis i donar-hi suport.

La versió actual d'ITIL és la v.3, que basant-se en el cicle de vida d'un servei treballa sobre cinc eixos bàsics:

- Estratègia del servei.
- Disseny del servei.
- Transició del servei.
- Operació del servei.
- Millora contínua del servei.

Que es complementaven amb bones pràctiques sobre:

- Gestió de la infraestructura de les TIC.
- Gestió de la seguretat.

- Perspectiva de negoci.
- Gestió d'aplicacions.
- Gestió d'actius de programari.

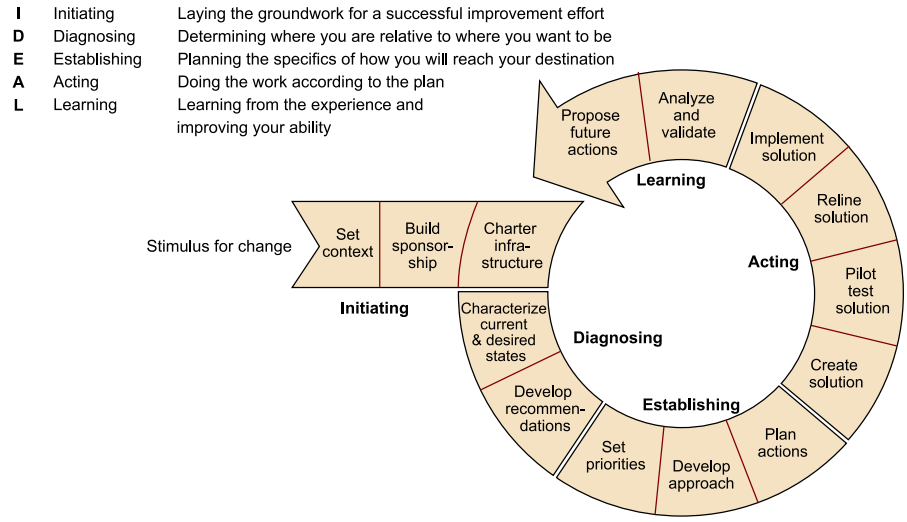
Òbviament, aquesta norma no és específica de seguretat de la informació, però va bé conèixer-la en cas que la nostra organització l'hagi adoptada, ja que complementa el procés de gestió de la seguretat de la informació en molts aspectes.

5) Model de maduresa de capacitats o *capability maturity model* (CMM) i SSE–CMM. El CMM és un marc de treball per a millorar processos, que proporciona a les organitzacions els elements essencials per a desenvolupar processos eficients i de qualitat. Es pot utilitzar per a fer la millora de processos en un projecte, en una divisió o en tota una organització. Ajuda a integrar funcions de l'organització tradicionalment aïllades i a establir els objectius de millora d'un procés, i proporciona un punt de referència per a comparar processos.

És aplicable en el desenvolupament de productes i serveis, en el muntatge, la gestió i provisió de serveis, i també en l'adquisició de productes i serveis.

6) Model de maduresa de capacitats en l'enginyeria de seguretat de sistemes o *system security engineering capability maturity model* (SSE-CMM). És un model derivat del CMM, que descriu les característiques essencials dels processos que hi ha d'haver en una organització per a assegurar una construcció segura de sistemes.

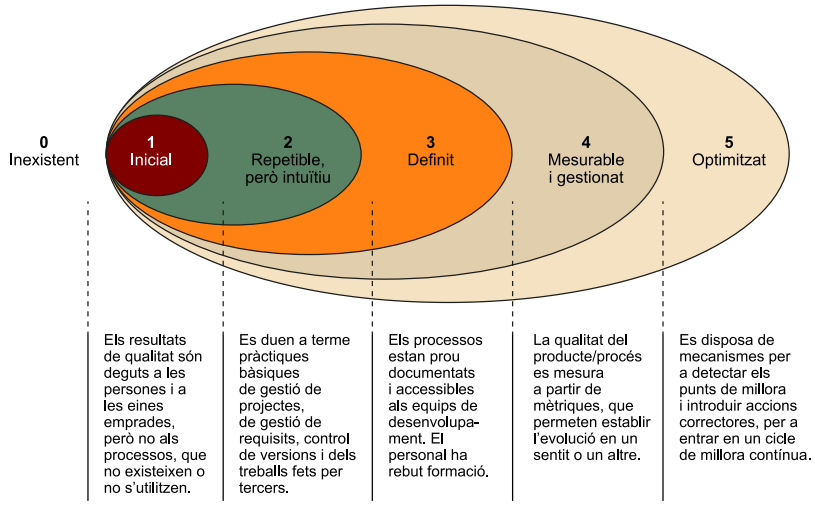
Es pot esquematitzar en cinc fases d'alt nivell:



Esquema del CMMI

Es fa referència a aquesta metodologia de millora dels processos de desenvolupament i manteniment de programari en les versions inicials (CMM) i de millora en general dels processos d'una organització o projecte en la seva última versió (CMMI), no com a guia per a implantar la seguretat de la informa-

ció, sinó perquè el concepte de *maduresa* s'utilitza habitualment en l'àmbit de la seguretat de la informació per a mesurar l'estat de la seguretat o, dit d'una altra manera, per a mesurar el grau d'implantació dels controls de seguretat. Així, doncs, és habitual que quan es fan auditories o avaluacions internes sobre l'estat de la seguretat, o l'estat d'implantació d'alguna norma o estàndard, es descrigui l'estat a partir de la definició CMM de maduresa dels controls.



Els nivells de maduresa del CMM

L'aplicació del model de maduresa permet establir criteris objectius per a avaluar l'eficàcia dels controls gràcies a la repetibilitat de la mesura, de manera que en permet analitzar l'evolució en el temps.

Exemple d'aplicació del model de maduresa a un control de seguretat de la informació

Control: "Les responsabilitats en seguretat de la informació estan definides".

- **0-Inexistent**: no hi ha una definició de responsabilitats en matèria de seguretat de la informació.
- **1-Inicial (hi ha una aproximació)**: les responsabilitats principals s'assignen o assumeixen informalment. Cada persona sap la seva responsabilitat, però no la dels altres.
- **2-Repetible (existeix, amb moltes deficiències)**: se sap qui assumeix les funcions principals en matèria de seguretat de les TIC i de la resta del negoci, però les funcions de seguretat no estan definides ni documentades específicament, sinó que s'assumeixen individualment com a part d'altres funcions (per exemple, la direcció d'un projecte).
- **3-Definit (existeix, amb algunes deficiències)**: les responsabilitats en seguretat de la informació s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, s'han donat a conèixer i s'ha fet o planificat la capacitació de totes les persones que ho requereixin.
- **4-Mesurable i gestionat (existeix, i és correcte)**: les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, però no es fa una revisió anual per a verificar que totes les funcions s'han assignat bé i que els responsables desenvolupen la seva funció.
- **5-Optimitzat (existeix, i està integrada en un cicle de millora contínua)**: les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, es revisa periòdicament el desenvolupament

d'aquestes funcions i hi ha un procés per a detectar deficiències en l'assignació i coordinació de funcions i per a aplicar-hi correccions.

En una organització amb un grau de maduresa baix, es pot plantejar reduir el nombre de nivells de maduresa, i agrupar-ne alguns.

6. Estat de la seguretat

La vertiginosa evolució de la tecnologia fa difícil estar al dia de tota la tecnologia emergent i de l'evolució de la que ja hi ha.

No obstant això, per a un professional de la seguretat de la informació és imprescindible mantenir-se al dia de les tendències que hi ha, cap on evolucionen les solucions de seguretat, quin és l'estat real de la seguretat en el seu sector, entorn, país, etc., quines són les incidències de seguretat més rellevants que hi ha, etc.

Per tant, és important mantenir contacte amb el mercat i els proveïdors de solucions, assistir als esdeveniments del món de la seguretat que s'organitzen anualment en tots els nivells, llegir premsa especialitzada i consultar webs especialitzats en la matèria.

Entre molts altres webs de gran interès, cal destacar a l'Estat espanyol les adreces web següents:

- **Institut Nacional de Ciberseguretat d'Espanya (INCIBE)**. Institut nacional de Ciberseguretat d'Espanya: societat dependent del Ministeri d'Energia, Turisme i Agenda Digital (MINETAD) per mitjà de la Secretaria d'Estat i per a la Societat de la Informació i Agenda Digital (SESIAD), és l'entitat de referència per al desenvolupament de la ciberseguretat i de la confiança digital dels ciutadans, la xarxa acadèmica i de recerca espanyola (RedIRIS) i les empreses, especialment per a sectors estratègics. <https://www.incibe.es>

- **Centre Criptològic Nacional (CCN)**: organisme responsable de coordinar l'acció dels diferents organismes de l'Administració que utilitzin mitjans o procediments de xifra, garantir la seguretat de les tecnologies de la informació en aquest àmbit, informar sobre l'adquisició coordinada del material criptològic i formar el personal de l'Administració especialista en aquest camp. <https://www.ccn.cni.es>

- **Centre de Seguretat de la Informació de Catalunya (CESICAT)**: fundació del sector públic de la Generalitat de Catalunya, amb la participació majoritària directa i adscrita al Departament de la Presidència per mitjà de la Secretaria de Governança de les Tecnologies de la Informació i la Comunicació . <https://cesicat.gencat.cat>

CERT (Equip de Resposta davant Emergències Informàtiques o Computer Emergency Response Team)

És un centre orientat a analitzar i monitorar la Xarxa (Internet), per a detectar vulnerabilitats i comportaments anòmals, amb la finalitat d'alertar la comunitat sobre amenaces i incidències i actuar, si fa falta, en coordinació amb altres CERT locals, nacionals o internacionals.

Enllaços d'interès

- https://www.ccn-cert.cni.es
- https://www.certsi.es
- https://www.first.org

7. Professionals de la seguretat de la informació

La gestió de la seguretat de la informació requereix una combinació de professionals especialitzats que han de cobrir perfils de gestió, d'auditoria i tècnics.

A escala internacional hi ha moltes organitzacions l'activitat de les quals es focalitza en la seguretat de la informació i que ofereixen certificacions de seguretat per acreditar els coneixements, l'especialització i l'experiència dels professionals del sector.

Les certificacions professionals són un recurs molt estès en el món de la seguretat de la informació i hi ha molts professionals que se certifiquen. Per a fer-ho, pot ser que calgui acreditar un mínim d'experiència, i també mantenir aquesta certificació. Per a això, en molts casos es requereix pagar una quota anual a l'associació certificadora, i només és possible mantenint-se en actiu, participant en fòrums, seminaris, sessions formatives, etc., cosa que garanteix la qualificació dels titulars.

A continuació s'exposen els segells d'alguna de les certificacions més habituals en el sector, però no les úniques.

Un indicador de la importància de la certificació professional en seguretat de la informació és el fet que, cada vegada més, l'Administració pública requereix professionals certificats en la contractació de serveis sobre la matèria.

Certificacions en seguretat de la informació