Seguretat i auditoria de la informació

Guia de l'assignatura

PID_00269890

Amadeu Albós Raya

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

Amadeu Albós Raya

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per la professora: Helena Rifà (2019)

Primera edició: setembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció

La irrupció de les tecnologies de la informació i la comunicació (TIC) en tots els àmbits de la vida quotidiana i el volum de dades, informació i coneixement que s'ha derivat d'aquest fet han provocat que la seguretat de la informació s'hagi convertit en un factor d'especial importància tant en l'àmbit personal com en el professional.

Si bé les problemàtiques de seguretat són diferents en cada entorn per la seva mateixa idiosincràsia, sí que presenten aspectes comuns que és imprescindible conèixer per tal de protegir-se adequadament dels riscos i prevenir possibles incidents.

La seguretat de la informació va més enllà de la simple definició de *confiança* en el conjunt ordenat de dades. L'abast n'és força més ampli i inclou mesures tant preventives com reactives en les organitzacions i els sistemes informàtics, que han de permetre salvaguardar i protegir la informació tot garantint els principis bàsics de seguretat i privacitat de la informació de conformitat amb la Llei general de protecció de dades (LGPD).

En aquesta assignatura ens centrarem en tots aquells aspectes que faciliten treballar i transferir la informació de forma segura i d'acord amb la LGPD. Farem un repàs de les tecnologies i metodologies que han de permetre gestionar i controlar que la informació es manté de manera segura dins dels paràmetres fixats per l'organització, i també com l'establiment de polítiques i la realització d'auditories ajuden al bon govern de la seguretat. Plasmarem així els dos eixos principals de l'assignatura: la planificació i la implantació, d'una banda, i l'auditoria i l'anàlisi, de l'altra.

Objectius

Els objectius principals que es volen assolir amb aquesta assignatura són els següents:

1. Conèixer els conceptes generals que s'apliquen a la seguretat de la informació.

2. Conèixer els sistemes d'informació i entendre els mecanismes de seguretat principals per protegir-los i detectar-ne incidents.

3. Conèixer els processos d'implantació i d'auditoria de la seguretat de la informació, així com també les normatives i els estàndards.

4. Conèixer els mecanismes de govern de la seguretat dins de l'organització.

1. Seguretat, privacitat i protecció de la informació

1.1. Presentació

D'un temps ençà, el món de les comunicacions viu una revolució en pràcticament tots els àmbits. La quantitat de dades que es generen, transfereixen i processen avui dia no para de créixer i genera una necessitat de donar el valor i la protecció que correspon a la informació que en resulta.

Més enllà de l'acompliment legal pel que fa a la recollida i al tractament, la informació també pot presentar característiques de privadesa, sensibilitat o restricció en determinats contextos que la poden posar en el punt de mira dels atacants, ja sigui per aconseguir-la, per modificar-la o per destruir-la.

La progressió dels riscos i de les amenaces que afecten els sistemes d'informació i, per extensió, dels continguts que processen, no fan sinó justificar la necessitat d'establir mecanismes de protecció per minimitzar l'impacte i les possibles conseqüències per a l'organització en cas que es produeixi un incident de seguretat.

1.2. Objectius

Els objectius que es pretenen assolir són els següents:

- Conèixer el valor de la informació i la necessitat de protegir-la en contextos determinats.
- Conèixer les implicacions de trencar la cadena de seguretat de la informació.
- Identificar contextos amb requisits de seguretat de la informació.
- Conèixer l'estat actual dels atacs informàtics a escala mundial.
- Identificar el paper de la tecnologia en l'evolució de la ciberdelinqüència.

1.3. Continguts

Els continguts que es desenvoluparan són els següents:

- Concepte d'informació, flux i cicle de vida de la informació.
- Propietats de seguretat de la informació: confidencialitat, integritat i disponibilitat.
- Legislació entorn de la privacitat de la informació.
- Mesures bàsiques de seguretat informàtica.

1.4. Guia d'estudi

El tractament de dades és una realitat que fa molt de temps que dura, però amb la informatització de gairebé totes les realitats de la vida quotidiana ha fet un important pas endavant.

El concepte d'**informació** com a resultat del processament de dades és essencial per comprendre el suport que aporten les tecnologies de la informació i la comunicació. En aquest sentit, tant el context d'interpretació de les dades com les característiques d'utilitat, rellevància, interpretació i percepció que han de presentar, són bàsiques per entendre que **la informació és tot allò que redueix la incertesa**.

Figura 1. El procés de les dades (context, interpretació, etc.)

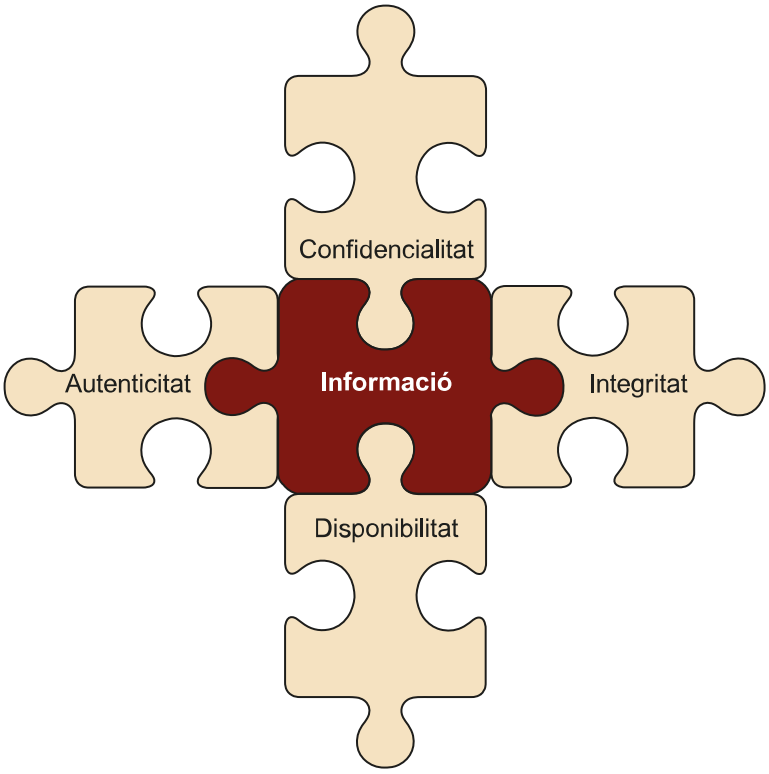
De fet, avui dia, la informació és un recurs estratègic per a qualsevol organització. Gràcies a la informació es pot conèixer l'estat de les entitats a les quals fa referència, es poden prendre decisions adequades i coherents amb aquest estat o, inclús, se'n pot obtenir coneixement amb el processament massiu d'informació diversa que resulta fonamental en l'estratègia de qualsevol organització.

Però hi ha informacions de molts tipus i no totes requereixen la mateixa consideració. Els **fluxos d'informació** que té l'organització seran un dels punts de partida per valorar quina és la informació que tracta una organització, quin valor té i com de necessari és protegir-la davant de situacions diverses (com la pèrdua, l'exposició o el segrest). Valorar aquests aspectes ens farà donar significat, importància, vigència i validesa a la informació per així poder determinar amb exactitud quines implicacions té per a l'organització.

El **sistema d'informació** és el suport per excel·lència a l'hora de processar les dades. La seva digitalització no només en facilita el tractament, sinó que el cost de la còpia, la modificació o la transmissió és ínfim en termes absoluts, la qual cosa per si mateixa ja suposa un risc si no es manté sota control.

De fet, les **propietats de seguretat de la informació**, això és, la **confidencialitat**, la **integritat** i la **disponibilitat** (addicionalment també l'**autenticitat**) s'han de poder garantir en tota circumstància, tant si la informació s'està transferint, com si està emmagatzemada o en tractament.

Figura 2. Propietats de seguretat de la informació: confidencialitat, integritat, disponibilitat (i autenticitat)



En aquest sentit, la normativa ISO/IEC 27000 té com a objectiu establir un marc de suport i de bones pràctiques per desenvolupar un **sistema de gestió de la seguretat de la informació** (SGSI) que permeti garantir la seguretat de la informació, reduir els riscos inherents al seu tractament, estalviar costos tot orientant i complementant correctament les mesures, garantir la gestió activa de la seguretat i complir amb la legislació vigent. Tot això permetrà sustentar tant la seguretat tècnica com la jurídica.

Això implica que la seguretat de la informació no és un resultat, sinó un procés iteratiu ordenat en fases de **planificació**, **implantació**, **verificació** i **actuació** (PDCA, de la sigla en anglès de *plan, do, check, act*). Com s'assenyala a la Llei general de protecció de dades (LGPD) i al Reglament general de protecció de dades (RGPD), l'enfocament als riscos i la responsabilitat proactiva són els eixos principals per garantir la seguretat de la informació.

Aquest plantejament requereix l'**anàlisi prèvia** de l'organització abans d'establir **controls físics**, **tècnics** i **organitzatius**, entre els quals figuren:

- les còpies de seguretat,
- el control d'accés a la informació,
- les limitacions en la utilització d'aplicacions,
- el control dels dispositius externs,
- el xifratge de dades,
- els protocols d'eliminació d'informació, o

- el control de la contractació de serveis al núvol.

1.5. Materials

Els materials d'estudi d'aquesta activitat són els següents:

- Seguretat i auditoria de la informació.
- Protecció de la informació (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf).

2. Fonaments de seguretat informàtica

2.1. Presentació

La simplicitat, la immediatesa i la ubiqüitat amb les quals avui dia es poden explotar les tecnologies de la informació i la comunicació són, sense cap mena de dubte, una part dels factors que han portat a l'omnipresència actual.

Però aquesta accessibilitat dels serveis a tots els públics amaga la complexitat de moltes solucions tècniques i la transmissió constant de tot tipus d'informació en totes direccions, realitats que posen de manifest la necessitat de combinar diverses mesures per tal d'assegurar que el sistema d'informació garanteix les propietats de seguretat en tota circumstància, des dels aspectes físics i arquitecturals del sistema fins a la transmissió de dades i l'explotació dels serveis per part dels usuaris.

De fet, totes aquestes mesures de seguretat van encaminades a protegir el sistema de la multitud de riscos i amenaces a les quals està sotmès, i a minimitzar l'impacte que puguin tenir els atacs o incidents de seguretat, en cas que es produeixin.

2.2. Objectius

Els objectius que es pretenen assolir són els següents:

- Conèixer els mecanismes de seguretat informàtica més habituals.
- Conèixer els mecanismes criptogràfics més utilitzats en l'actualitat.
- Identificar la complementarietat dels diferents mecanismes de seguretat.
- Identificar contextos d'aplicació de la criptografia com a element de seguretat.
- Comprendre l'evolució de la seguretat informàtica i la necessitat d'actualització.

2.3. Continguts

Els continguts que es desenvoluparan són els següents:

- El sistema d'informació, els components i el funcionament.
- La seguretat física i perimetral dels sistemes d'informació.
- La seguretat dels serveis i les comunicacions dels sistemes d'informació.

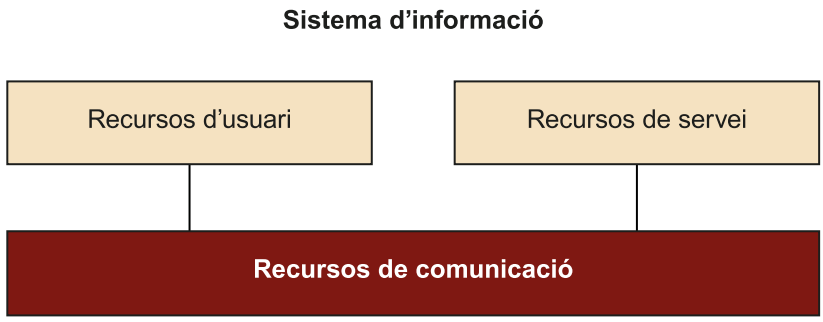
2.4. Guia d'estudi

Si bé no és estrictament necessari utilitzar la tecnologia per processar les dades, avui dia difícilment se'n pot prescindir per realitzar qualsevol tasca, per simple que sigui.

El **sistema d'informació** representa la base per al tractament d'informació i està format per la combinació coherent de recursos humans, materials i lògics. Aquests recursos s'estructuren funcionalment en **infraestructura**, **serveis** i **comunicacions**.

Els recursos d'usuari, de serveis i de comunicacions són els components essencials de la infraestructura i permeten realitzar les tasques, comunicar els nodes i explotar els serveis, ja siguin locals, remots o híbrids, que són els que combinen ambdues característiques.

Figura 3. La infraestructura del sistema d'informació està formada per recursos d'usuari, de servei i de comunicacions

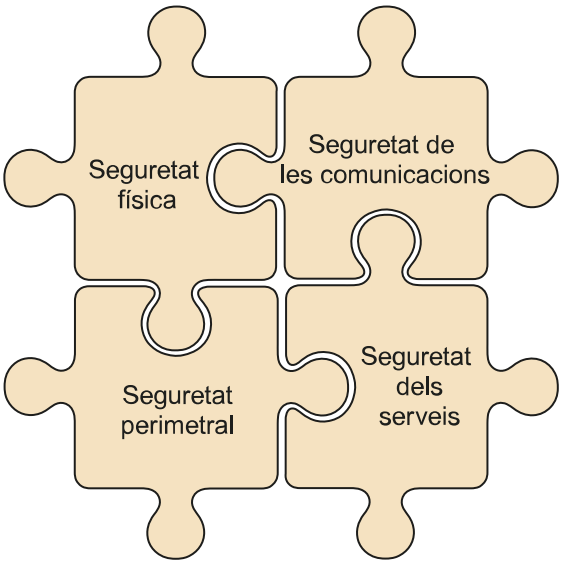


Tots aquests components han d'estar integrats perfectament en el sistema d'informació per tal d'acomplir els objectius, la qual cosa requereix d'un **disseny** i d'una **operativa** ben definida. Quant a la **infraestructura**, els segments de xarxa cablejada i sense fils i l'adreçament físic i lògic dels nodes es complementen amb protocols d'assignació d'adreces i de resolució de noms per completar el funcionament. Pel que fa als **serveis**, el disseny i l'operativa es fonamenten en paradigmes de comunicació i protocols de connexió que garanteixen l'intercanvi correcte de dades entre els extrems, fet que implica estandarditzar tant l'accés com la comunicació del servei.

La seguretat del sistema requereix assegurar els components anteriors, però també ha de fer front a l'evolució imparable de la tecnologia i dels requisits de les organitzacions, així com també a uns riscos i a unes amenaces que no deixen de créixer dia a dia.

La seguretat del sistema ha de començar per la **protecció física** dels recursos contra accessos indeguts, riscos naturals o la fallada de qualsevol dels suports, sense oblidar que cada recurs de la infraestructura necessitarà la protecció adequada d'acord amb les característiques i la funció que realitza.

Figura 4. La seguretat del sistema d'informació es basa en la seguretat física, perimetral, dels serveis i de les comunicacions



En aquest sentit, els **recursos d'usuari** han de garantir que no suposen un risc de seguretat per al sistema, tant des del punt de vista de la configuració com de la utilització per part de l'usuari. Els **recursos de serveis** necessiten garanties de funcionament tant del maquinari com del programari, sense perdre de vista que tenen accés directe a la informació que emmagatzemen (tot i que pot estar ubicada en altres recursos). Finalment, els **recursos de comunicació** poden presentar problemes de funcionament físic, però també requereixen que la configuració sigui segura. Un cas especial de dispositius és la internet de les coses, que per la seva pròpia casuística pot requerir actuacions específiques tant des del punt de vista funcional com operatiu.

Tots els recursos del sistema es comuniquen a través d'una **xarxa informàtica** que exposa tant els dispositius connectats com la informació que hi circula, fet pel qual requereix mesures determinades per garantir-ne la seguretat, com ara:

- la segmentació de la xarxa (sigui física o virtual) per aïllar zones amb requisits de seguretat específics,
- la parametrització de les xarxes sense fils,
- la implantació de tallafocs que garanteixin el filtratge de les comunicacions amb internet,
- les xarxes privades virtuals per connectar al sistema tots aquells usuaris i sistemes remots de forma segura,
- l'ús d'eines de detecció i protecció contra intrusos per monitorar el sistema i controlar els possibles atacs, o

- la creació de zones desmilitaritzades per publicar serveis a internet amb garanties de seguretat tant per als serveis com per al sistema local.

La implementació de mesures de seguretat d'infraestructura no ha d'oblidar la necessitat d'assegurar els **serveis** i les **comunicacions** que hi operen, processant una informació que ha de mantenir les propietats de seguretat amb mecanismes concrets:

- la **confidencialitat** es garanteix a través de la criptografia de clau privada o pública, aquesta última amb l'ajuda de la infraestructura de clau pública i les autoritats de certificació,

- la **integritat** es verifica amb funcions resum de les dades i es pot aplicar tant al contingut com a la font de les dades, i

- la **disponibilitat** es garanteix sobretot amb mesures d'infraestructura però també amb la implantació de polítiques i controls d'autorització.

Bona part de les mesures de seguretat es basen en garantir que l'acció que realitza cada usuari és legítima, cosa que requereix un procés d'**autenticació de l'usuari** que pot estar basat en la combinació de múltiples factors que l'usuari coneix o posseeix (de fet, com més factors exigeixi el sistema, més garanties obtindrà de la identitat de l'usuari). Però no és suficient saber qui és l'usuari que interactua amb el sistema, cal a més un procés d'**autorització de l'usuari** per poder realitzar les accions que pretén dur a terme, perquè no tots els usuaris han de poder realitzar les mateixes tasques o accedir a la mateixa informació. Els **gestors d'identitat** permeten centralitzar aquestes funcions d'autenticació i d'autorització del sistema, a més d'altres de gestió i administració.

Per la seva banda, les solucions que presten les funcionalitats dels **serveis** han de ser robustes, verificades i de proveïdors contrastats, de manera que incorporin les mesures de seguretat actuals i no presentin vulnerabilitats.

No es pot completar l'escenari sense garantir que les **comunicacions** tanquen la cadena de seguretat entre els extrems (per defecte, les dades viatgen per la xarxa en clar, sense xifrar) perquè poden ser l'objecte d'atacs passius (escolta de comunicacions) i actius (denegació de servei, intercepció de dades, etc.). El **xifratge** permet garantir la confidencialitat i la integritat de les dades transmeses (no així la disponibilitat, que s'ha de garantir sobretot amb mitjans d'infraestructura) gràcies a protocols com el *transport layer security* (TLS), un dels més utilitzats per incorporar funcions de seguretat a tot tipus de protocols (per exemple, a la majoria de protocols d'aplicació del model TCP/IP).

Com en tot sistema d'informació, l'**usuari** és un factor clau per completar les mesures de seguretat implantades i la millor forma d'integrar-lo és mitjançant la formació i la promoció d'una cultura entorn la seguretat de la informació.

Aquest plantejament també ajuda a assegurar els continguts dels documents o missatges amb els quals treballa a diari, utilitzant els mecanismes de xifratge, signatura digital o inclús esteganografia.

2.5. Materials

Els materials d'estudi d'aquesta activitat són els següents:

- Fonaments de seguretat informàtica.

3. Gestió i auditoria de la seguretat de la informació

3.1. Presentació

Avui dia és relativament fàcil implementar mecanismes de seguretat atesa la diversitat de solucions que ofereix el mercat, però, com en d'altres aspectes de la informàtica, no té sentit la implantació de mesures si no es fa abans un procés metòdic que formalitzi des de la identificació de necessitats fins a la revisió periòdica.

La normativa ISO/IEC 27000 (i següents) estructura la comprensió, el plantejament i el desplegament dels mecanismes de seguretat de forma lògica i ordenada, així com també la revisió, la comprovació i l'auditoria de tots aquests elements per verificar que són coherents amb l'estratègia definida i actuen d'acord amb les previsions.

En aquest sentit, totes les actuacions en matèria de seguretat informàtica es materialitzen en el sistema de gestió de la seguretat de la informació (SGSI), que és el mitjà per garantir la seguretat de la informació de l'organització.

3.2. Objectius

Els objectius que es pretenen assolir són els següents:

- Conèixer la normativa ISO/IEC 27000 i la seva aplicabilitat.
- Conèixer el procés d'auditoria de la seguretat en les organitzacions.
- Cohesionar aspectes normatius i d'auditoria en contextos determinats.

3.3. Continguts

Els continguts que es desenvoluparan són els següents:

- La normativa ISO/IEC 27000, característiques, estructura i cicle de vida.
- L'auditoria de seguretat de la informació, principis, característiques i procés.

3.4. Guia d'estudi

En ocasions es pot tenir la percepció que la implantació (o inclús l'actualització o la millora) d'una solució de seguretat és suficient per protegir l'organització. Aquesta visió de la seguretat com un producte on la simple instal·lació resol una problemàtica (com ho faria una solució d'ofimàtica o una eina de cooperació) no s'ajusta a la realitat.

La seguretat de la informació no és un producte, sinó un procés, i el **SGSI** aporta un enfocament sistemàtic per tal d'afrontar el repte d'assegurar la informació en tot tipus d'organitzacions.

La família d'estàndards ISO/IEC 27000 són un grup de normatives que pretenen donar un marc conceptual, metòdic, estructurat i pràctic per implantar un SGSI en una organització. En especial, l'estàndard **ISO/IEC 27002** és una guia de bones pràctiques del sector per desenvolupar normes de seguretat, pràctiques de gestió i la confiança en la relació amb tercers.

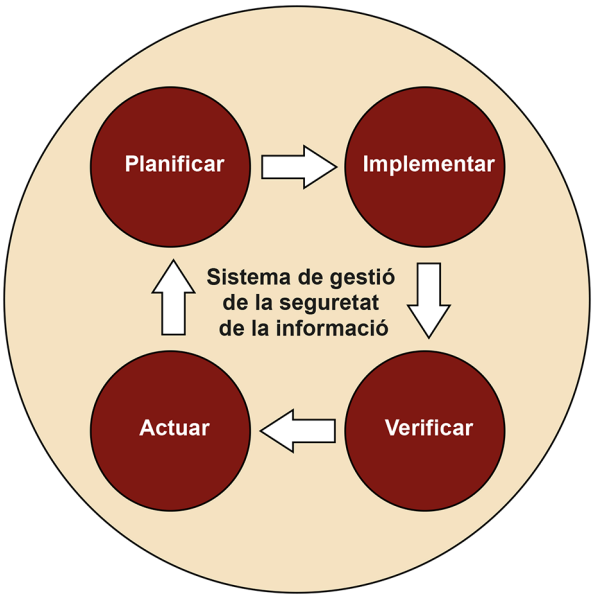
Un dels aspectes rellevants de la norma ISO/IEC 27002 són els **dominis de seguretat**, que recullen els objectius de control i els controls de seguretat que s'han d'aplicar per assolir l'objectiu definit. Per exemple, hi ha dominis per a la seguretat física i de l'entorn, per a la gestió d'incidents, per al control d'accés o per a la gestió de la continuïtat del negoci (entre molts d'altres). Cal tenir en compte que la implementació de la norma requereix l'aplicació de la legislació en vigor d'una banda i la contextualització amb l'organització en la qual s'implanta de l'altra.

Els **principis d'un SGSI** es basen en els aspectes següents:

- Definir una política general que emmarcarà totes les actuacions.
- Planificar la seguretat necessària per a l'organització (des de la identificació dels requisits fins a la preparació dels plans).
- Implantar i operar tots els elements de seguretat del sistema.
- Analitzar el rendiment amb el monitoratge i les auditories per detectar disfuncions.
- Establir millores (preventives, correctives o contínues).
- Revisar el sistema per assegurar l'adequació i el compliment dels objectius.

Totes aquestes fases del SGSI són una aplicació del cicle de Deming a l'àrea de seguretat, que consisteix en un cicle iteratiu de planificació (*plan*), implementació (*do*), verificació (*check*) i actuació (*act*).

Figura 5. Cicle de Deming aplicat a la seguretat de la informació (*plan*, *do*, *check*, *act*)



D'aquesta manera, el SGSI permet assolir un conjunt de beneficis concrets:

- Obtenir una visió única de la seguretat en l'organització.
- La implicació dels actors que intervenen en la seguretat.
- La gestió global i activa de manera que s'unifica la implementació de la seguretat.
- El control i seguiment amb la realització d'auditories.
- La millora continua de tots els elements de la cadena de seguretat a partir de les disfuncions detectades.
- L'optimització de recursos per garantir la complementarietat de les mesures implantades.

Com es pot veure, el **procés d'auditoria** és essencial per completar el cicle de millora de la seguretat, ja sigui per al compliment de la legalitat, per al control d'alguns aspectes específics o per a la revisió de la conformitat amb les bones pràctiques del sector. Per tal que sigui plenament efectiva, l'auditoria s'ha de cenyir a uns principis d'integritat i professionalitat, així com també de presentació justa i imparcial. Per aconseguir-ho, l'auditoria ha de ser independent de l'organització, ha d'estar enfocada plenament en la cerca de proves o evidències que demostrin la realitat i ha de guardar la confidencialitat dels resultats obtinguts.

Hi ha diversos tipus d'auditories, per bé que la diferenciació més estesa és si és interna o externa. L'**auditoria interna** pot ser realitzada per la mateixa organització o per un proveïdor de serveis de consultoria, i l'**auditoria externa** sempre serà realitzada per un organisme extern (i diferent, si escau, del proveïdor de serveis de consultoria que es pugui tenir contractat).

La realització d'auditories persegueix la conformitat del sistema, l'acompliment de la legislació, l'eficàcia de les mesures implantades i la detecció d'àrees de millora. Per tal d'assolir aquests objectius, cal establir un **programa** o un **cicle d'auditoria**, de manera que la continuïtat porti a una millora constant i sostenible al llarg del temps.

Realitzar el procés d'auditoria suposa una planificació prèvia dels aspectes que s'han de revisar:

- el treball de camp centrat en la realització de proves i l'obtenció d'evidències,
- la realització de l'informe que contrasta el plantejament amb les evidències, i
- el seguiment de la correcció o de la millora de les eventuals no conformitats.

Segurament, el treball de camp i l'obtenció d'evidències són els aspectes més destacables del procés d'auditoria. El primer perquè se centra en la realització de proves d'acompliment dels controls, i el segon perquè determina amb resultats confiables si la realitat de la seguretat de la informació coincideix amb la prevista, fet que portarà als resultat de l'auditoria en forma de conformitats, no conformitats, observacions o possibilitats de millora.

3.5. Materials

Els materials d'estudi d'aquesta activitat són els següents:

- Implantació d'un sistema de gestió de la seguretat de la informació (fins al sisè apartat, inclòs).
- Introducció a l'auditoria TIC i de seguretat TIC (apartats de l'1 al 4, ambdós inclosos).

4. El bon govern de la seguretat

4.1. Presentació

La seguretat de la informació, com qualsevol altre procés, requereix l'estructuració de les funcions i l'assignació dels recursos necessaris per complir amb els objectius. Aquesta necessitat no té una única resposta a causa de la diversitat de característiques que poden presentar les organitzacions i caldrà valorar la idiosincràsia de cadascuna d'elles per trobar el plantejament que més s'hi adapti.

Com en d'altres àrees, també existeixen models de gestió, normatives i estàndards que faciliten l'anàlisi, el disseny, la implantació, l'auditoria i la millora contínua de la seguretat de la informació en una organització. A més de reprendre les bones pràctiques del sector materialitzades en models i normatives, el bon govern de la seguretat també pot rebre el suport de consultors i professionals especialitzats en la matèria i dels organismes de control d'emergències de seguretat.

4.2. Objectius

Els objectius que es pretenen assolir són els següents:

- Comprendre els models, les normes i els organismes de suport que emmarquen la seguretat de la informació.
- Justificar el plantejament i la implantació de polítiques de seguretat de la informació.
- Desenvolupar el bon govern de la seguretat de la informació a través de polítiques coherents i cohesionades.

4.3. Continguts

Els continguts que es desenvoluparan són els següents:

- Models i estàndards de gestió de la seguretat, organismes externs de suport.
- Implementació del SGSI.
- El govern de la seguretat a través del desenvolupament de polítiques de seguretat.

4.4. Guia d'estudi

La gestió de la seguretat en una organització comporta un gran nombre de tasques que combinen aspectes tècnics, organitzatius i jurídics. Si bé inicialment es poden prioritzar algunes d'aquestes tasques, amb el pas del temps caldrà dedicar esforços per acomplir-les totes.

Es pot afrontar la gestió de la seguretat sota diverses perspectives o models de gestió. La **gestió** pot ser **interna** quan el personal de l'organització realitza les tasques, **externa** quan s'externalitza el procés com a servei, o **mixta** quan la realització de les tasques es reparteix entre el personal intern i un servei subcontractat.

En qualsevol cas, la gestió de la seguretat haurà d'iniciar-se considerant els aspectes següents:

- L'objecte de negoci de l'organització per facilitar la contextualització.
- La situació inicial de l'organització per valorar l'estat i l'eficiència de les mesures implementades.
- L'anàlisi de riscos per identificar els riscos als quals pot estar exposada l'organització i la informació que gestiona.
- El compliment de la legalitat vigent que afecta directament a l'organització (ja sigui general, sectorial, etc.).

Amb aquests resultats es podran identificar les mesures que permetran mitigar, controlar o eliminar els riscos de seguretat als quals ha de fer front l'organització. Aquests **controls de seguretat** es poden organitzar d'acord amb la **naturalesa** (tècnics i organitzatius), **actuació** (reducció de la probabilitat o de l'impacte) o **finalitat** (preventiu, de detecció, correctiu o de monitoratge).

Les **normatives** poden servir de guia i de suport per emmarcar totes aquestes tasques entorn de la seguretat de la informació; per exemple, la ISO/IEC 27001 (requisits de sistemes de gestió de la seguretat de la informació) i la ISO/IEC 27002 (codi de bones pràctiques). Però n'hi ha moltes d'altres, entre les quals destaquen ITIL (Information Technology Infrastructure Library), CMM (Capability Maturity Model) o SSE-CMM (System Security Engineering Capability Maturity Model). Es tracta d'eines que no només es poden utilitzar per a la gestió de la seguretat, sinó també per a la gestió general de les tecnologies de la informació i la comunicació en les organitzacions.

A més del marc que ofereixen les normatives, la gestió de la seguretat també pot tenir el suport d'organismes externs que centralitzen l'estat real de la seguretat a escala global i poden oferir solucions per gestionar les incidències eventuals, com, per exemple, l'INTECO (Institut Nacional de Tecnologies de la Comunicació, S.A.) a través del CERT (Computer Emergency Response Te-

am). D'altres entitats poden ajudar a obtenir certificacions de seguretat que garanteixin la conformitat de la seguretat de l'organització respecte d'alguna normativa concreta.

D'una manera o d'una altra, el desenvolupament d'un SGSI en l'organització requereix un desenvolupament per etapes:

- La **planificació**, on es defineixen les polítiques generals de seguretat, l'abast, l'anàlisi de riscos i la selecció de controls (entre d'altres).

- La **implementació**, on s'executa la implantació de totes les actuacions previstes (especialment dels controls) i se seleccionen els indicadors d'activitat.

- La **verificació**, on es monitora l'estat del sistema i es realitzen els controls de seguiment i les auditories.

- L'**actuació**, on s'implanten les millores i s'executen totes les accions preventives i correctives que s'han detectat.

Tot aquest desenvolupament acostuma a prendre forma documental considerant els principis del SGSI, la metodologia seguida, la declaració d'aplicabilitat del sistema, les polítiques de seguretat d'alt nivell, el pla de continuïtat del negoci, els procediments realitzats i els registres que s'obtindran (incloses les auditories).

De fet, el govern de la seguretat de la informació (i de les tecnologies de la informació i la comunicació en general) es materialitza amb la planificació i la implantació de les mesures, així com també amb el control i l'auditoria. Això és així perquè l'organització ha de fer front als requisits legals de seguretat, al creixement del capital intel·lectual i a la necessitat d'alinear el sistema d'informació amb els objectius estratègics de l'organització, però també a causa de la proliferació d'unes amenaces contra la seguretat que cada vegada són més nombroses i sofisticades.

Per tant, l'eficàcia del govern serà una realitat quan les tecnologies de la informació i la comunicació hagin estat ben planificades i gestionades i adequadament monitorades, fet que implica necessàriament l'auditoria periòdica, tant de la seguretat del sistema d'informació com del procés de gestió de la seguretat de la informació.

Figura 6. El govern de la seguretat de la informació es fonamenta en la planificació i la implantació de mesures de seguretat, i en l'auditoria i l'anàlisi de l'acompliment real

4.5. Materials

Els materials d'estudi d'aquesta activitat són els següents:

- Introducció a la seguretat de la informació (apartats 3, 5, 6 i 7).
- Introducció a l'auditoria TIC i de seguretat TIC (apartats 6 i 7).
- Implantació d'un sistema de gestió de la seguretat de la informació (apartats del 7 a l'11, ambdós inclosos).

Bibliografia

Albós, A. (2019). *Fonaments de seguretat informàtica*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Codolà, S. *Seguridad y auditoría de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Estevan, R. *Introducción a la auditoría TIC y de seguridad TIC*. Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Introducción a la seguridad de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Implantación de un sistema de gestión de la seguridad de la información (SGSI)*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

INCIBE (2018). *Protección de la información*. Instituto Nacional de Ciberseguridad. («Protege tu empresa»). <http://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf>