Seguretat i auditoria de la informació

PID_00269279

Santiago Codolà Vilahur

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

Santiago Codolà Vilahur

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

Primera edició: setembre 2019
Autoria: Santiago Codolà Vilahur

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

Índex

1. Informació i seguretat

1.1. El valor de la informació

En l'entorn empresarial, moltes vegades s'utilitzen els termes *dades* i *informació* com a sinònims; si bé estan relacionats, és necessari distingir aquests conceptes perquè són molt diferents.

Així, les **dades** són «grups de símbols no aleatoris que s'erigeixen en representació d'alguna cosa (quantitats, objectes, accions, etc.)». Es constitueixen a partir de caràcters: poden ser la combinació de lletres, números o símbols que conformen una paraula, xifra o imatge que es refereix a alguna cosa. Descriuen fets empírics, successos i entitats. Però, aïlladament, poden no contenir informació humanament rellevant. Per exemple, el codi 840280985G per si sol no aporta informació. Necessitem saber a què es refereix aquest codi o paraula. Pot ser un número de document d'identitat o l'identificador d'un producte; en el primer cas necessitem saber a qui es refereix, i en el segon quin producte representa.

Les dades són la matèria primera imprescindible per a aconseguir informació; per a això és necessari que hi hagi un procés d'elaboració que sigui capaç de manejar-les i convertir-les en informació. Es converteixen en informació quan són útils per a algun propòsit, i una vegada que són processades obtenen un significat, un propòsit i una utilitat; és a dir, quan a les dades s'hi agrega quelcom més (intel·ligència) es converteixen en informació.

Figura 1.

Una dada es converteix en informació si és capaç de contestar una pregunta o solucionar un problema d'informació; és a dir, la informació es vincula a «les dades que fan falta per a prendre decisions».

La diferència entre dada i informació no rau en el contingut del conjunt de caràcters donat, sinó més aviat en la seva utilitat per a prendre una decisió.

En definitiva, les dades, per a convertir-se en informació, han de tenir una sèrie de característiques:

- **Ser útils**. Han de servir en el procés de presa de decisions influint en les accions que s'adoptin.

- **Ser rellevants**. Si no són rellevants no serviran per a respondre una pregunta o proporcionar coneixement sobre alguna cosa.
- **Ser interpretables**. Si no tenen un significat, si no se'n pot interpretar el sentit, no serviran per al procés de presa de decisions.
- **Ser perceptibles**. Si no es perceben, perquè no arriben al destinatari o perquè arriben molt difuminades entre una gran quantitat d'altres dades, l'usuari no podrà processar-les.

La **informació** és un conjunt organitzat de dades processades, que constitueixen un missatge que canvia l'estat de coneixement del subjecte o sistema que rep aquest missatge, i per tant té algun tipus d'influència sobre les nostres accions, ja que pot intervenir en el procés de presa de decisions o es pot utilitzar per a reduir el nivell d'incertesa o la realització de càlculs. No obstant això, cal considerar que el mateix conjunt de caràcters pot ser una dada o una informació per a individus diferents, de manera similar al fet que el que és matèria primera per a una empresa pot ser el producte final per a una altra. Per exemple, per a un despatx d'advocats, un informe pericial és una part de la seva matèria primera, que s'utilitzarà i combinarà dins d'un determinat procés judicial, que és el seu producte final. Per contra, per a qui ha elaborat l'informe pericial, aquest ja és el producte final. Quelcom semblant passa amb les dades i la informació, ja que allò que considerem informació en un nivell de l'empresa pot ser solament una dada en un altre.

La informació s'utilitza en la majoria de les branques científiques com a pedra angular sobre la qual fonamentar la presa de decisions. Apareix així un terme imprecís, ampli i emmotllable en funció de l'entorn en el qual s'utilitzi; aquesta situació es desenvolupa fins a tal punt que en molts casos s'obvia la definició del terme per considerar que una cosa tan comuna i propera a totes les facetes de la nostra vida no necessita demostració. En realitat, ens trobem davant un concepte que pot ser abordat des de nombrosos angles i perspectives (lingüística, comunicació, matemàtiques, ciències socials, informàtica, etc.).

En general, s'assimila informació a «tot allò que redueix la incertesa». Aquesta és una visió molt àmplia que enuncia un problema de causa-efecte que no es correspon exactament amb la realitat, ja que no solament redueix la incertesa sinó que la pot ampliar; més aviat caldria dir «tot allò que varia la incertesa». La informació és la diferència entre un estat d'incertesa i un altre immediatament posterior, que pot apropar-nos a la realitat o allunyar-nos-en, tenint en compte que la incertesa és la manca de coneixement o absència d'informació sobre una àrea d'interès.

La teoria econòmica ens diu que la terra, el treball i el capital han estat tradicionalment els recursos econòmics fonamentals; no obstant això, cada vegada amb un major reconeixement, la informació s'ha establert en quart lloc com a recurs estratègic decisiu donada la seva enorme importància econòmica.

De fet, ningú no dubta que la informació és poder, per la qual cosa cada vegada són més les organitzacions que empren una part important dels seus mitjans per a obtenir-la i controlar-la.

La informació té encara més importància en els moments de caos, incertesa, desequilibris i ajustos, i arriba a ser tant o més valuosa que els recursos materials, humans i financers de què disposa l'empresa. Això es deu al fet que l'empresa, per a poder ser competitiva en una economia cada vegada més globalitzada, ha de ser capaç d'obtenir, seleccionar, processar i aplicar correctament la informació rellevant per a afrontar cada problema.

La informació és un element bàsic en l'empresa, i per aquest motiu les empreses, enfront de circumstàncies com l'expansió i la diversificació d'activitats o la variació constant dels empleats en plantilla, senten la necessitat d'estructurar i formalitzar els seus sistemes d'informació amb el seu nivell directiu. I tot això perquè la informació és la matèria primera imprescindible en totes i cadascuna de les fases que comporta una presa de decisions, entesa com el procés dirigit a seleccionar i executar una acció que resol un problema i permet executar uns objectius establerts. Constitueix, doncs, un recurs estratègic, el mateix que els recursos humans, financers, tecnològics o comercials.

És un recurs que té una sèrie de característiques peculiars que la diferencien d'altres recursos existents en l'empresa. Aquestes característiques són:

- **Transportabilitat.** Es pot transportar instantàniament d'un lloc a un altre del món.
- **Il·limitada.** L'ésser humà no consumeix informació, sinó que la crea constantment; els recursos d'informació són inesgotables.
- **Subjectivitat.** És difícil assignar un valor objectiu a la informació. El valor de la informació depèn de qui l'usi; l'hi assigna el subjecte d'acord amb les seves necessitats concretes en un determinat moment. El subjecte sol percebre el valor d'una informació com el cost de disposar-ne. L'evolució del valor de la informació és difícilment previsible: pot tenir un valor extraordinari avui i no tenir-ne cap demà.

1.2. Fluxos d'informació

La irrupció de les noves tecnologies ha comportat passar d'unes dades i informació discretes, moltes vegades costoses d'obtenir i que afectaven parts específiques d'una organització, a un flux constant i creixent que afecta totes les parts, des de l'alta direcció fins al recepcionista. Ara la dificultat rau a gestionar el flux d'informació a causa de la velocitat amb la qual es genera, filtrar i identificar la que es necessita, en el moment adequat; això dona pertinència a la informació.

L'ideal seria que una organització fos capaç d'identificar, captar, classificar i analitzar una gran quantitat d'informació útil (mercantil, financera, econòmica, tecnològica, regulatòria, etc.) i fer-la arribar a les persones adequades per generar conclusions i implementar accions que responguin de manera òptima a les condicions del mercat.

En tota organització solen coexistir tres tipus bàsics de fluxos d'informació, i com més gran és l'habilitat de l'organització per a manejar aquests fluxos més importància adquireixen els actius intangibles que es basen en aquests fluxos.

En primer lloc, l'organització obté informació de l'entorn amb la finalitat de determinar quins productes necessita el mercat i quines tecnologies hi ha per a cobrir-los; és el que denominem **informació ambiental o externa**.

En segon lloc, la mateixa organització genera internament informació, que sorgeix del processament de la informació ambiental i la derivada de les relacions en l'organització; és la que cridem anomenem **informació interna**.

I, finalment, l'organització dona a conèixer els productes i serveis que l'empresa produeix, i això es denomina **informació corporativa**.

Vegem-ho més detingudament:

1) Informació ambiental o externa. És la informació que entra en una organització procedent de l'entorn. És essencial per a poder tenir èxit en els mercats actuals, i fonamentalment ha de buscar:

- Capacitat de respondre a les necessitats del mercat. L'organització obté informació procedent de l'entorn amb la finalitat de determinar estratègies, com per exemple quins productes necessita el mercat.
- Adquisició d'habilitats tecnològiques. L'organització obté informació procedent de l'entorn amb la finalitat de determinar les tecnologies existents, el correcte funcionament de les funcions de R+D, i la formació, i augmentar l'habilitat tecnològica de l'organització.

Les organitzacions necessiten informació sobre dos entorns molt diferents: immediat i remot. Per a informar-se de cadascun d'aquests dos entorns, hi ha **fonts informals** d'informació (no es registren enlloc i es basen en relacions personals) i **fonts formals** (es registren en paper, per mitjà electrònic o en qualsevol tipus de suport físic).

- **Entorn immediat.** És constituït per aquells elements amb els quals una organització ha de tractar diàriament: clients, proveïdors, distribuïdors, competidors, fonts de finançament i reguladors.
- **Entorn remot.** És aquell al qual l'organització no s'ha d'enfrontar diàriament, però del qual ha de monitorar la informació amb la finalitat d'identificar els canvis i tendències que exigeixin una adaptació de les es-

tratègies de l'organització a mitjà i llarg terminis. És un context més ampli: el clima polític, la situació econòmica, les tendències socials i les innovacions tecnològiques. Cada dia l'entorn remot es fa més immediat gràcies a les TIC.

2) Informació interna. L'organització assimila i processa tota aquesta informació externa alhora que la rep, i la uneix a la informació interna generada per la mateixa organització, la qual cosa l'ajuda a desenvolupar els productes i serveis que ofereix posteriorment als clients. En tota organització cal distingir dos grans tipus d'informació interna.

- Les organitzacions generen una gran quantitat d'informació **operacional**, informació que resulta del mateix funcionament rutinari de l'organització (llistes de clients, catàlegs de productes, llistats de l'inventari en magatzem, registres comptables, dades numèriques de control de la maquinària), i que sol ser **formal** i fàcilment emmagatzemable en algun tipus de registre físic.
- Les organitzacions generen coneixements com a resultat de l'assimilació o digestió d'informació interna i externa, i de l'explotació de les capacitats creatives dels seus membres (es dissenyen nous productes, es milloren els processos, s'optimitzen els mecanismes de gestió, etc.). Aprenen i el seu coneixement s'acumula en forma saber fer. Aquesta informació és bàsicament **informal** i s'emmagatzema en l'experiència de les persones.

3) Informació corporativa. Així denominem la sortida de la informació des d'una organització cap a l'exterior. Tota organització que vulgui sobreviure ha d'esforçar-se a emetre cap a l'entorn un missatge diferenciat que li permeti ser clarament percibible pels consumidors. Hi ha dos tipus principals de missatges:

- Una organització pot dur a terme accions de comunicació **directes**: llançar una campanya publicitària, explotar la seva imatge mitjançant accions de patrocini, iniciar un procés de R+D amb la finalitat de generar un producte molt concret; en aquest cas, la informació que s'emet a l'entorn és continguda en el producte en forma de tecnologia aplicada.
- Una organització pot dur a terme accions de comunicació **indirectes**, a través de la ruta operacional: una organització que cuidi la qualitat dels seus productes està escampant, potser sense saber-ho, informació per l'entorn, ja que en satisfer els clients amb productes de qualitat aconsegueix una imatge de marca i un prestigi que els mateixos clients s'encarreguen de difondre entre els seus coneguts.

1.3. El valor de la informació

Tal com hem dit, una de les característiques de la informació és la subjectivitat, en el sentit que la informació no té un valor absolut: el valor l'hi assigna el subjecte que la utilitza d'acord amb les seves necessitats concretes en un moment determinat.

Per tant, aquest valor serà determinat per segons com afectin l'usuari les propietats que qualifiquen l'estructura interna de la informació:

- **Significat** (semàntica). Del significat extret d'una informació, cada individu n'avalua les conseqüències possibles i adequa les seves actituds i accions de manera concorde a les conseqüències previsibles que es dedueixen del significat de la informació. Això es refereix a les regles que ha de seguir l'individu o el sistema expert per a modificar les seves expectatives futures sobre cada possible alternativa.
- **Importància** (relativa al receptor). És a dir, si conté alguna qüestió important. La importància de la informació per a un receptor es referirà al grau en què canvia l'actitud o la conducta dels individus. En les societats modernes, els individus obtenen dels mitjans de comunicació de massa una gran quantitat d'informació, però una gran part és poc important per a ells, perquè altera de manera molt poc significativa la seva conducta. Això es refereix al grau quantitatiu en què s'han d'alterar les expectatives futures. De vegades se sap que un fet fa més o menys probables algunes coses; és important veure quant menys probables seran unes alternatives respecte a les altres.
- **Vigència** (en la dimensió espai-temps). Es refereix a si la informació està actualitzada o desfasada. En la pràctica la vigència d'una informació és difícil d'avaluar, ja que en general accedir a una informació no permet conèixer immediatament si aquesta informació té vigència o no.
- **Validesa** (relativa a l'emissor). S'avalua si l'emissor és fiable o pot proporcionar informació no vàlida (falsa). Té a veure amb el fet de si els indicis han de ser considerats en la reavaluació d'expectatives o han de ser ignorats per no ser indicis fiables.

L'anàlisi d'aquestes propietats de la informació i del seu contingut és el que determina que l'usuari de la informació prengui les seves decisions de manera més coherent. Conseqüentment, es pot establir que la informació té valor perquè ens ajuda a prendre decisions.

A partir d'aquesta valoració qualitativa i bastant intuïtiva de la informació, en l'àmbit empresarial es pot precisar una valoració més quantitativa. Un principi que es pot aplicar és definir que el valor de la informació per a prendre una decisió determinada és igual a la pèrdua produïda per prendre la decisió errònia (la decisió contrària a la que es prendria si es tingués la informació perfecta), per la probabilitat que aquesta pèrdua es produeixi. És a dir, el màxim que una organització està disposada a pagar per una informació és el que podria deixar de guanyar si tingués la informació perfecta multiplicat per la probabilitat d'aquesta pèrdua.

Però igual que una informació té un valor per a una organització que l'ha obtinguda, quan es refereix a persones també té un valor, més qualitatiu (confidencialitat, seguretat, reputació, etc.), molt més difícil de quantificar per a

la persona a la qual correspon; es pot considerar que aquest valor s'ha cedit temporalment a una organització assumint que no hi haurà deterioració ni pèrdua en aquest valor.

En qualsevol cas, la informació, quantificada o no, és un actiu més (intangible i volàtil) d'una organització, i com a tal cal protegir-la i protegir-se de la seva deterioració, desaparició o robatori; hi ha l'agreujant que l'organització actua com a dipositària d'un valor de tercers sobre el qual, en cas de mal ús o deterioració, es poden exigir responsabilitats.

2. Nocions bàsiques de seguretat de la informació

2.1. Definició

Quan es parla de seguretat en l'àmbit de les TIC sovint es confonen els conceptes de *seguretat de la informació* i *seguretat informàtica*. I encara que tots dos són realment importants i similars, hi ha diferències entre ells.

Quan apliquem el terme de *seguretat a la informació* estem indicant que aquesta informació té una rellevància especial en un context determinat i que, per tant, cal protegir-la. Així, doncs, podem definir la **seguretat de la informació** així:

> Conjunt de mesures tècniques, organitzatives i legals que permeten a l'organització assegurar la confidencialitat, integritat i disponibilitat de la seva informació.

Fins a l'aparició i difusió de l'ús dels sistemes informàtics, tota la informació d'interès d'una organització es guardava en paper i s'emmagatzemava en grans quantitats d'arxivadors voluminosos. Dades de clients, proveïdors de l'organització o empleats quedaven registrades en paper, amb tots els problemes que implicava després el seu magatzematge, transport, accés i processament.

Els sistemes informàtics permeten digitalitzar tot aquest volum d'informació i redueixen l'espai ocupat, però, sobretot, en faciliten l'anàlisi i el processament. Es guanya en «espai», accés, rapidesa en el processament de la informació i millores en la seva presentació.

Però apareixen altres problemes lligats a aquestes facilitats. Si és més fàcil transportar la informació, també hi ha més possibilitats que desaparegui «pel camí»; si és més fàcil accedir-hi, també és més fàcil modificar-ne el contingut; etc.

Des de l'aparició dels grans sistemes aïllats fins als nostres dies, quan el treball en xarxa és l'habitual, els problemes derivats de la seguretat de la informació també han anat canviant i evolucionant, però són aquí i les solucions han hagut d'anar adaptant-se als nous requeriments tècnics. Augmenta la sofisticació de l'atac i això augmenta la complexitat de la solució, però l'essència és la mateixa.

Referent al terme de ***seguretat informàtica***, també hi ha diferents definicions. Nosaltres ens quedem amb la definició oferta per l'estàndard per a la seguretat de la informació ISO/IEC 27001, que va ser aprovat i publicat a l'octubre del 2005 per la International Organization for Standardization (ISO) i per la International Electrotechnical Commission (IEC):

> «La seguretat informàtica consisteix a implantar un conjunt de mesures tècniques destinades a preservar la confidencialitat, la integritat i la disponibilitat de la informació, i pot, a més, incloure altres propietats com l'autenticitat, la responsabilitat, la fiabilitat i el no-repudi.»

O, dit amb altres paraules, la seguretat informàtica es refereix a la protecció de les infraestructures de les tecnologies de la informació i comunicació que donen suport a una empresa.

Com veiem, el terme *seguretat de la informació* és més ampli, ja que engloba altres aspectes relacionats amb la seguretat més enllà dels purament tecnològics.

2.2. Bases de la seguretat de la informació

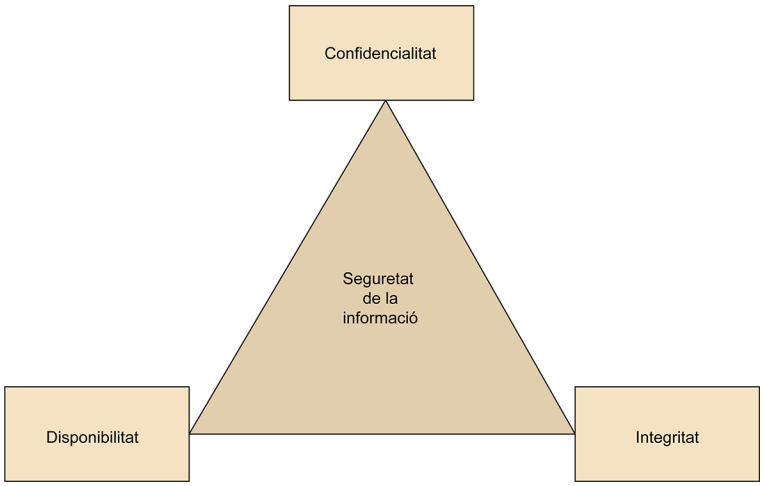
En general, la informació serà segura si podem garantir tres paràmetres, coneguts per la sigla CID (CIA en anglès):

Confidencialitat: implica l'accés a la informació únicament pels qui estan autoritzats; és a dir, l'accés a la informació es fa solament mitjançant autorització i de forma manera controlada.

Integritat: comporta mantenir l'exactitud i completesa de la informació i els seus mètodes de procés, la qual cosa implica modificar la informació solament mitjançant autorització.

Disponibilitat: comporta l'accés a la informació i els sistemes per a tractar-la per part dels usuaris autoritzats en el moment que ho requereixin, la qual cosa significa que la informació ha de ser accessible mitjançant autorització.

Figura 2.



2.2.1. Confidencialitat

En general, el terme *confidencial* fa referència a «que es fa o es diu en confiança o amb seguretat recíproca entre dues o més persones».

En termes de seguretat de la informació, la confidencialitat fa referència a la necessitat d'ocultar o mantenir el secret sobre una determinada informació o recursos.

L'objectiu de la confidencialitat és, llavors, prevenir la divulgació no autoritzada de la informació.

En general, qualsevol empresa pública o privada i de qualsevol àmbit d'actuació requereix que certa informació no sigui accedida per diferents motius. Un dels exemples més típics d'aquesta informació és la de l'exèrcit d'un país. A més, és sabut que els assoliments més importants en matèria de seguretat sempre van lligats a aspectes estratègics militars.

D'altra banda, sovint determinades empreses desenvolupen dissenys que han de protegir dels competidors. La sostenibilitat de l'empresa, i el seu posicionament en el mercat, poden dependre de manera directa de la implementació d'aquests dissenys, i, per aquest motiu, s'han de protegir mitjançant mecanismes de control d'accés que assegurin la confidencialitat d'aquestes informacions.

Un exemple típic de mecanisme que garanteixi la confidencialitat és la criptografia, l'objectiu de la qual és xifrar o encriptar les dades perquè resultin incomprensibles a aquells usuaris que no disposen dels permisos suficients.

Però, fins i tot en aquesta circumstància, hi ha una dada sensible que cal protegir, i és la clau d'encriptació. Aquesta clau és necessària perquè l'usuari adequat pugui desxifrar la informació rebuda; en funció del tipus de mecanisme

d'encriptació utilitzat, la clau pot o ha de viatjar per la xarxa i pot ser capturada mitjançant eines dissenyades per a això. Si es produeix aquesta situació, la confidencialitat de l'operació portada a terme (bancària, administrativa o de qualsevol tipus) queda compromesa.

2.2.2. Integritat

En general, el terme *integritat* fa referència a la qualitat d'*íntegre* i indica «que no manca de cap de les seves parts», i, en relació amb una persona, «recta, proba, irreprotxable».

En termes de seguretat de la informació, la integritat fa referència a la fidelitat de la informació o recursos, i normalment s'expressa referent a prevenir el canvi impropi o desautoritzat.

L'objectiu de la integritat és, llavors, prevenir modificacions de la informació no autoritzades. La integritat fa referència a les dades i l'origen:

- la integritat de les dades és el volum de la informació
- la integritat de l'origen és la font de les dades, anomenada *autenticació*

És important posar l'accent en la integritat de l'origen, ja que pot afectar l'exactitud, credibilitat i confiança que les persones posen en la informació.

Sovint passa que en parlar d'integritat de la informació no es dona en aquests dos aspectes. Per exemple, quan un diari difon una informació la font de la qual no és correcta, podem dir que es manté la integritat de la informació, ja que es difon per mitjà imprès. Però, com que la font d'aquesta informació és errònia, no es manté la integritat de l'origen, ja que la font no és correcta.

2.2.3. Disponibilitat

En general, el terme *disponibilitat* fa referència a una qualitat de *disponible* i, dit d'una cosa, «que se'n pot disposar lliurement o que està llesta per a usar-se».

En termes de seguretat de la informació, la disponibilitat fa referència al fet que la informació del sistema ha de romandre accessible a elements autoritzats.

L'objectiu de la disponibilitat és, llavors, prevenir interrupcions no autoritzades o controlades de l'accés a la informació.

En termes de seguretat de la informació, «una informació està disponible quan el seu disseny i implementació permeten deliberadament negar l'accés a dades determinades». És a dir, una informació està disponible si permet no estar disponible.

I una informació no disponible és tan negativa com no tenir informació. No serveix.

Com a resum, es pot concloure que la seguretat de la informació consisteix a mantenir l'equilibri adequat entre aquests tres factors. No té sentit aconseguir la confidencialitat per a un arxiu si és a costa que ni tan sols l'usuari administrador pugui accedir-hi, ja que s'està negant la disponibilitat.

Depenent de l'entorn de treball i les seves necessitats, es pot donar prioritat a un aspecte de la seguretat o a un altre. En entorns militars sol ser sempre prioritària la confidencialitat de la informació davant la disponibilitat. Encara que algú pugui accedir a la informació o fins i tot pugui eliminar-la, no en podrà conèixer el contingut, i reposar aquesta informació serà tan senzill com recuperar una còpia de seguretat (si les coses es fan bé).

En entorns bancaris és prioritària sempre la integritat de la informació davant la confidencialitat o disponibilitat. Es considera menys nociu que un usuari pugui llegir el saldo d'un altre usuari que el fet que pugui modificar-lo.

2.3. Estàndards per a gestionar la seguretat de la informació

Tal com hem vist, la informació és un actiu valuós del qual depèn el bon funcionament d'una organització. Aquesta informació pot ser afectada per diferents riscos i amenaces; per tant, mantenir-ne la integritat, confidencialitat i disponibilitat és essencial per a aconseguir els objectius de negoci.

Per aquesta raó, des de temps immemorials les organitzacions han posat els mitjans necessaris per a evitar el robatori i manipulació de les seves dades confidencials. Aquests mitjans se centren a aplicar un procés sistemàtic d'anàlisi de riscos.

L'anàlisi de riscos, en el context de la seguretat de la informació, és un procés sistemàtic per a fer una estimació del nivell de risc al qual són exposades les diferents parts (actius) que estan involucrades en els sistemes d'informació o els fan funcionar.

> Difícilment es poden prendre decisions sobre seguretat de la informació sense saber què hem de protegir, de quins perills ens hem de protegir, i quines poden ser les conseqüències en cas que es produeixi un incident de seguretat.

Aquest procés intenta identificar els perills (amenaces), és a dir, concretar quins incidents (voluntaris o accidentals) poden afectar les dades o informació, o el seu valor. També s'avalua la probabilitat que les amenaces es materialitzin i fins a quin punt afectarien els sistemes i les dades (quin impacte tindrien).

Les mesures de seguretat implantades són salvaguardes que poden reduir la probabilitat que succeeixi l'incident o poden disminuir els efectes negatius en cas que es produeixi l'incident. Quan es parla de gestionar el risc, es vol reduir el nivell de risc existent, i això s'aconsegueix implantant noves salvaguardes o millorant les existents.

La plasmació pràctica d'aquest procés sistemàtic per a poder estar preparats davant qualsevol imprevist i actuar amb rapidesa i eficàcia comporta implantar un sistema de gestió de seguretat de la informació (SGSI), gràcies al qual es poden analitzar els possibles riscos, establir les mesures de seguretat necessàries i disposar de controls que permetin avaluar l'eficàcia d'aquestes mesures. D'aquesta manera, es poden anticipar els possibles problemes i preparar-se en cas de qualsevol contingència.

Per a dur a terme tot el procés d'una manera més senzilla, es disposa de la família de normes internacionals ISO/IEC 27000. Les més importants són:

- La norma ISO/IEC 27000, que recull els termes i definicions emprats en la resta de normes de la sèrie. Amb això s'eviten diferents interpretacions sobre els conceptes que apareixen al llarg normes. A més, inclou una visió general de la família de normes en aquesta àrea, una introducció als sistemes de gestió de seguretat de la informació i una descripció del cicle de millora contínua.
- La norma ISO/IEC 27001, que és la principal de la sèrie. Es pot aplicar a qualsevol tipus d'organització, independentment de la seva grandària i activitat. La norma conté els requisits per a establir, implementar, operar, supervisar, revisar, mantenir i millorar un sistema de gestió de la seguretat de la informació. Recull els components del sistema, els documents mínims que n'han de formar part i els registres que permetran evidenciar el bon funcionament del sistema. Així mateix, especifica els requisits per a implantar controls i mesures de seguretat adaptats a les necessitats de cada organització. Aquesta és la norma que s'aplica per a certificar els sistemes de gestió de seguretat de la informació de les empreses que ho volen.
- La norma ISO/IEC 27002, una guia de bones pràctiques que recull les recomanacions sobre les mesures a prendre per a assegurar els sistemes d'informació d'una organització. Per a això, descriu 11 dominis (és a dir, àrees d'actuació), 39 objectius de control o aspectes a assegurar dins de cada àrea, i 133 controls o mecanismes per a assegurar els diferents objectius de control.

Quant al procés específic d'analitzar riscos, a Espanya s'utilitza bastant àmpliament la MAGERIT (metodologia d'anàlisi i gestió de riscos dels sistemes d'informació), creada pel Consell Superior d'Administració Electrònica.

2.4. Principis per a implantar un SGSI

La implantació d'un sistema de gestió de seguretat de la informació és una decisió estratègica que ha d'involucrar tota l'organització, que ha de rebre el suport i les normes de la direcció i que requereix dedicar-hi temps i recursos.

El seu disseny dependrà dels objectius i necessitats de l'organització, i també de la seva estructura. Aquests elements són els que definiran l'abast de la implantació del sistema, és a dir, les àrees que seran involucrades en el canvi. A vegades, no és necessari un sistema que impliqui tota l'organització; pot ser que sigui necessari solament en un departament, una seu en concret o una àrea de negoci.

L'objectiu d'un SGSI és protegir la informació; en implantar-lo, l'organització obté els beneficis següents:

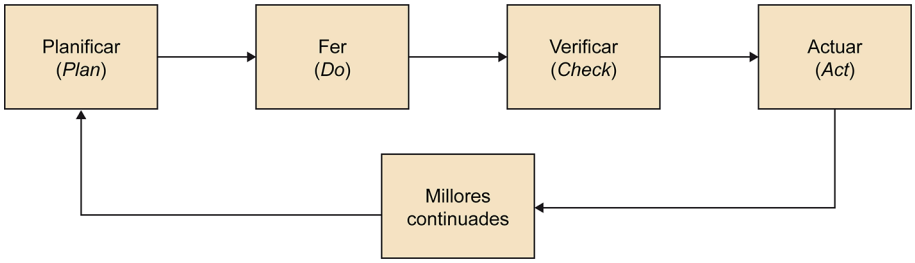
- S'obté una reducció de riscos perquè s'estableixen i segueixen controls sobre ells. Amb això s'aconsegueix reduir les amenaces fins a aconseguir un nivell assumible per l'organització. D'aquesta manera, si es produeix una incidència, els danys es minimitzen i la continuïtat del negoci està assegurada.
- Es produeix un estalvi de costos derivat d'una racionalització dels recursos. S'eliminen les inversions innecessàries i ineficients, com les produïdes per desestimar o sobreestimar riscos.
- La seguretat es considera un sistema i es converteix en una activitat de gestió. La seguretat deixa de ser un conjunt d'activitats més o menys organitzades i passa a transformar-se en un cicle de vida metòdic i controlat, en el qual participa tota l'organització.
- L'organització s'assegura que es compleix la legislació vigent i s'eviten riscos i costos innecessaris. L'entitat s'assegura que es compleix el marc legal que protegeix l'empresa d'aspectes que probablement no s'havien tingut en compte anteriorment.

En qualsevol cas, un SGSI no s'ha de considerar una situació estàtica; al contrari, donada l'evolució ràpida i dispar de l'element a gestionar, la informació i la seva seguretat, aquest element ha d'estar en contínua evolució. Per això, en la seva implantació, a partir de la fase inicial d'identificació dels actius d'informació que han de ser protegits i el grau de protecció, s'aplica el model PDCA, dividit en quatre fases en el qual, finalitzada l'última i analitzats els resultats, es torna a començar la primera.

La sigla PDCA corresponen als termes anglesos *plan*, *do*, *check*, *act* ('planificar', 'fer', 'verificar', 'actuar').

Amb això es plasma que la gestió de la seguretat és un procés que mai no s'acaba, ja que els riscos mai no s'eliminen però es poden gestionar. Dels riscos es desprèn que els problemes de seguretat no són únicament de naturalesa tecnològica, i per aquest motiu mai no s'eliminen íntegrament; i en conseqüència s'ha d'estar sempre alerta.

Figura 3.

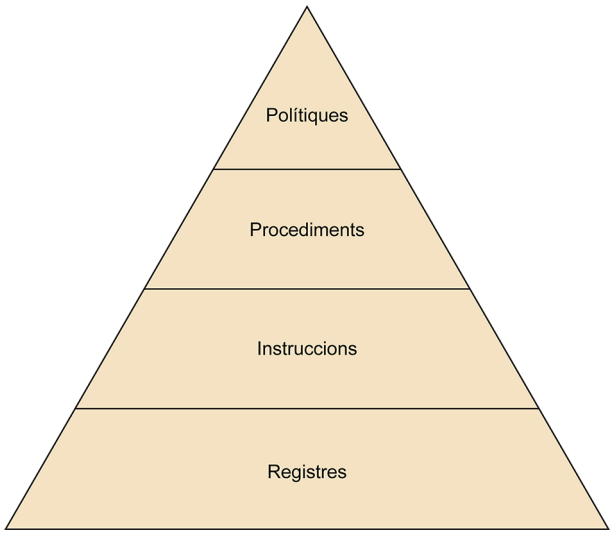


- La primera fase del model PDCA per a implantar el sistema és **planificar** (*plan*). Durant aquesta fase es fa un estudi de la situació de l'organització des del punt de vista de la seguretat per estimar les mesures que s'implantaran en funció de les necessitats detectades. No tota la informació de què es disposa té el mateix valor o està sotmesa als mateixos riscos. Per això, és important fer una anàlisi de riscos que valori els actius d'informació i vulnerabilitats als quals s'està exposat. Així mateix, és necessari gestionar aquests riscos per a reduir-los en la mesura del possible. Amb el resultat obtingut en l'anàlisi i la gestió de riscos s'estableixen uns controls adequats que permeten minimitzar els riscos.
- En la fase de **fer** (*do*) del model PDCA es duu a terme la implantació dels controls de seguretat seleccionats en la fase anterior. Aquests controls es refereixen als més tècnics i a la documentació necessària. Aquesta fase també requereix un temps de conscienciació i formació per a donar a conèixer al personal de l'empresa què s'està fent i per què.
- La tercera fase és **verificar** (*check*). En aquesta fase s'avalua l'eficàcia i l'èxit dels controls implantats. Per això, és molt important disposar de registres i indicadors que provinguin d'aquests controls.
- El model PDCA es completa amb la fase d'**actuar** (*act*), durant la qual es duran a terme les labors de manteniment del sistema. Si durant la fase de verificar anterior s'ha detectat algun punt feble, aquest és el moment de millorar-lo o corregir-lo i definir i aplicar mesures correctores, mesures preventives i mesures de millora segons convingui.

En finalitzar les quatre fases, es prenen els resultats de l'última i es comença novament la primera.

L'avaluació contínua del sistema de gestió de seguretat de la informació ha d'estar documentada, i per a això s'utilitzaran els quatre tipus de documentació diferents que es representen en aquesta estructura piramidal:

Figura 4.



- En la cúspide hi ha les **polítiques** que senten les bases de la seguretat. Indiquen les línies generals per a aconseguir els objectius de l'organització sense entrar en els detalls tècnics. Tota l'organització ha de conèixer aquestes polítiques.
- En el segon nivell se situen els **procediments**, que desenvolupen els objectius marcats per les polítiques. En els procediments apareixen detalls més tècnics i es concreta com aconseguir els objectius exposats en les polítiques. Els procediments han de ser coneguts per aquelles persones que ho requereixin per a desenvolupar les seves funcions.
- En el tercer nivell apareixen les **instruccions**, que constitueixen el desenvolupament dels procediments. En les instruccions es descriuen les instruccions tècniques que s'han de seguir per a executar els procediments.
- En l'últim nivell hi ha els **registres**, que evidencien la implantació efectiva del sistema i el compliment dels requisits. Entre aquests registres s'inclouen indicadors i mètriques de seguretat que permetin avaluar la conseqüència dels objectius de seguretat establerts.

3. Seguretat tècnica i seguretat jurídica

Hi ha moltes definicions del terme *seguretat*. Simplificant, i en general, podem definir-la com la «característica que aplicada a un ens indica que aquest està lliure de tot perill, dany o risc».

Quan parlem d'informació ens referim a un ens que implica dos subjectes: la tecnologia que la sustenta i l'individu al qual fa referència. Per tant, en el cas d'un individu, el concepte de seguretat es tradueix com la certitud que la seva informació i drets són a resguard d'atacs violents i indeguts, i, si s'efectuen en el pitjor dels casos, es faran cessar amb urgència i els danys li seran rescabalats. En el cas de la tecnologia, la seguretat es tradueix en el fet que els components que la conformen estan lliures de tot perill, dany i risc; i, en el cas d'atac, s'actua ràpidament per evitar-los i restituir els danys.

Quant a la seguretat jurídica, el concepte al·ludeix a la certesa, l'ordre, la fermesa i la confiança en l'ordenament legal, tant en les relacions jurídiques entre particulars com en les relacions entre el ciutadà i l'Administració.

Sembla obvi que la seguretat jurídica en el món virtual (intrínsecament intangible) no es pot aconseguir de la mateixa manera i amb els mateixos instruments que la seguretat provinent del món preinformàtic (sustentat en allò tangible), i això adquireix noves tonalitats a la llum de la nova realitat. Per exemple, en el cas dels negocis, la forma exigida per als contractes, el registre públic, la certificació de les signatures i altres institucions no són mitjans de seguretat apropiats quan els contractes se celebren a distància, entre absents, sense escrits i fins de manera anònima; o, per a la informació, quan les mesures de salvaguarda física són inoperants si la informació està en suport intangible o en una cosa tan etèria com «el núvol».

A l'inici de l'ús dels ordinadors i les primeres xarxes de comunicacions, aquestes eren purament per a ús intern de les organitzacions i s'utilitzaven com a suport de comunicació de dades puntuals o enviament intern de correu electrònic. En aquestes condicions, la seguretat no rebia molta atenció. La «democratització» de la informàtica i la seva combinació amb les telecomunicacions han conduït a l'anomenada «societat de la informació». La informació ha esdevingut un dels motors de la nostra societat (un actiu per a les empreses i administracions públiques), i així s'ha convertit en un bé de gran valor i ha deixat de servir solament per a un fi concret i en un moment concret, ja que han desaparegut conceptes com temps i espai en relació amb el concepte d'oblit de la informació.

Actualment, les dades es recullen fins i tot abans del nostre naixement (dades mèdiques), i continuen acumulant-se al llarg de tota la vida. En cadascuna de les fases del nostre desenvolupament com a persones (escola, universitat, treball, salut, aficions, lectures, compres, crèdits…) es recullen dades que poden permetre, amb les eines oportunes, un coneixement de nosaltres fins i tot millor del que adquirim nosaltres mateixos. Davant d'això, la informació es converteix en una nova forma de poder per a qui la pugui recollir i tractar. Davant d'aquesta situació, garantir la seguretat de la informació i de les xarxes es converteix en un problema potencial de grans proporcions.

Els problemes de seguretat de la informació, tant en si mateixa com dels mitjans utilitzats per a accedir-hi o compartir-la, tal com s'ha apuntat en el subapartat «Bases de la seguretat de la informació», es poden dividir en quatre àrees interrelacionades: secret, validació d'identificació, no-repudi i control d'integritat. El secret té a veure amb mantenir la informació fora de les mans d'usuaris no autoritzats. Això és el que ve a la ment normalment quan la gent pensa en la seguretat de les xarxes. La validació d'identificació s'encarrega de determinar amb qui es parla abans de revelar informació delicada o fer un tracte de negocis. El no-repudi s'encarrega de les signatures. Finalment, el control d'integritat s'assegura que un missatge rebut és l'enviat realment i no alguna cosa que un adversari maliciós modifica en el camí o cuina pel seu compte, és a dir, que no s'altera en la seva integritat.

En aquesta situació, allò que la seguretat jurídica reclama és certesa, estabilitat i raonabilitat, a l'abast de la qual han de convergir tant les solucions normatives com les tecnològiques implicades en la seguretat tècnica de la informació.

En aquest sentit, mereix esment especial la consideració de la seguretat en la seva relació amb el dret a la intimitat (i el seu nou rostre actual: el dret a la protecció de les dades personals), el qual neix com una eina per a protegir el ciutadà davant aquesta nova realitat. No obstant això, cal no oblidar que no hi ha drets absoluts i, per tant, hi haurà altres drets i béns que també hauran de ser protegits.

El reconeixement explícit d'aquest dret és relativament recent i mostra una evolució que es pot examinar amb cicles successius, sentits diferents i enfocaments diversos, en el marc dels quals procedeix situar la protecció jurídica actual de les dades personals en general i del sector de les TIC en particular.

Inicialment, el dret a la intimitat va apuntar bàsicament a una protecció contra la publicitat d'actes o dades personals posats en coneixement del públic sense notícia o permís de la persona afectada. Posteriorment, aquest concepte es va estendre per abastar el dret dels individus, grups o institucions a determinar per si mateixos quan, com i amb quina extensió pot ser comunicada a tercers la informació sobre ells. Les TIC han replantejat la qüestió del dret a

la intimitat en atenció al risc que implica per a la persona l'estructuració de grans bancs de dades de caràcter personal, i particularment la potencialitat de l'entrecreuament d'informació que contenen.

Enfront del «poder informàtic» dels qui poden acumular informacions sobre cada persona en quantitat il·limitada, i memoritzar-la, usar-la i transferir-la com una mercaderia, el dret a la intimitat es configura com una nova forma de llibertat personal, ja no caracteritzada negativament com la possibilitat de refutar o evitar l'ús de dades referides a cadascú, sinó positivament com la potestat d'exercir un poder de control sobre les informacions referides a la pròpia persona. Consisteix en el que s'ha anomenat *llibertat informàtica*, que consisteix en el dret d'autotutela de la pròpia identitat informàtica, és a dir, el dret de vigilar les dades personals incloses en arxius automatitzats, de preservar la pròpia identitat informàtica o, el que és el mateix, de consentir, controlar i rectificar les dades informatives que concerneixen la pròpia personalitat. Al dret d'informar i de ser informat s'ha afegit el dret de protegir la llibertat de la informació com un bé personal, que constitueix un nou dret fonamental, propi de la tercera generació, que té per finalitat el control que ens correspon a cadascun de nosaltres sobre la informació que ens concerneix personalment.

Moltes vegades, les dades personals són facilitades voluntàriament pel mateix titular per accedir gratuïtament a algun servei o per obtenir onerosament un bé per internet sense tenir consciència que poden ser utilitzades per a finalitats diferents d'aquells per a les quals van ser recaptades. Però, altres vegades, les dades de l'internauta són proporcionades per ell de manera completament involuntària, ja que, una vegada que les dades surten del seu ordinador, desconeix la ruta que segueixen cap a la seva destinació, en quins punts intermedis s'emmagatzemen temporalment i qui pot accedir-hi, copiar-les, modificar-les i utilitzar-les per a qualsevol finalitat diferent d'aquella per la qual van ser lliurades.

Queda clar que els serveis TIC constitueixen un àmbit específic i peculiar per a protegir les dades personals per dues raons principals: d'una banda, perquè la interoperativitat i extensió creixents d'aquests serveis constitueixen per si mateixes un factor de risc per a la seguretat de la gestió de la informació en general i de les dades relacionades amb la intimitat en particular, i, d'altra banda, perquè el procés de comunicació requereix determinar i identificar els punts de terminació de la xarxa entre els quals es produeix la comunicació, uns punts que, per l'eventual identificació amb persones, poden arribar a ser considerats dades personals.

En qualsevol cas, allò que persegueix la seguretat jurídica és facilitar al ciutadà els mitjans que garanteixin el compliment de les normatives i la preservació del seu dret a la intimitat basant-se en la seguretat (tant física com lògica), la confidencialitat i el consentiment del ciutadà per a tractar les seves dades.

Bibliografia

Delpiazzo, C. E. (2007). «El principio de seguridad jurídica en el mundo virtual».*Revista de Derecho*(any VI, núm. 11).

Instituto Nacional de Tecnologías de Comunicación (INTECO) (2011). *Guía de apoyo Implantación de un SGSI en la empresa*[en línia]. <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>

Marí, J.; San José, C.; Miralles, R. M.; Ferreres, J. (2010). *El dret a la protecció de dades de caràcter personal. Autoritat catalana de protecció de dades*[en línia]. Escola d'Administració Pública de Catalunya. <http://virtual.eapc.cat/pluginfile.php/110864/mod_resource/content/1/dret_prot_dad/inici.html>

Martínez, F.«Tema 1: El subsistema de la Información de la Empresa. Universidad de Huelva».*Gestión de los Recursos de Información*[en línia]. <http://www.uhu.es/francisco.martinez/gri/_private/TEMA%201GRI.doc>

Martínez Musiño, C. (2010). «El valor de la información, su administración y alcance en las organizaciones».*Revista mexicana de ciencias de la información*(vol. 1, núm. 2, pàg. 10-20).

Mifsud, E. (2012). *Introducción a la seguridad informática*[en línia]. Ministerio de Educación, Cultura y Deporte. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>