El sistema informàtic dins l'organització

El responsable d'informàtica

PID_00275595

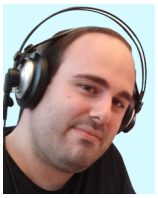
Manel Mendoza Flores
Javier Panadero Martínez
Miquel Colobran Huguet

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

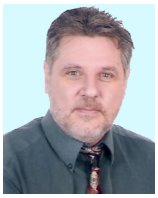
Manel Mendoza Flores

Enginyer de telecomunicacions, especialista en seguretat informàtica amb experiència en l'àmbit de l'administració pública i del sector privat. Diplomat en Ciències Empresarials per la Universitat Oberta de Catalunya (UOC) i en Gestió de Projectes (PMP). Durant la seva trajectòria formativa s'ha complementat amb diverses certificacions del món IT (Cisco, Microsoft, CISSP, etc.). Des de l'any 2011, col·labora amb la UOC en diversos àmbits de la docència, laboratoris en línia i direcció del TFG. Apassionat per les noves tecnologies, que combina amb les obligacions de la seva família i l'estima del Delta de l'Ebre, d'on és natural. Actualment, desenvolupa la seva ocupació com a expert de seguretat al sector privat en un entorn internacional.



Javier Panadero Martínez

Enginyer informàtic i doctor en Computació d'Altes Prestacions per la Universitat Autònoma de Barcelona (UAB). Des de 2019, és professor dels Estudis d'Informàtica, Multimèdia i Telecomunicació de la Universitat Oberta de Catalunya (UOC). Director del màster universitari en Enginyeria Computacional i Matemàtica. Ha elaborat diversos materials sobre administració de sistemes i programació. Els seus interessos de recerca inclouen la computació paral·lela i distribuïda, l'optimització i simulació de sistemes complexos i els algorismes intel·ligents.



Miquel Colobran Huguet

Doctor en Informàtica per la Universitat Autònoma de Barcelona (UAB). Consultor a la Universitat Oberta de Catalunya (UOC) d'assignatures sobre administració de sistemes i seguretat, i també d'informàtica i legislació en el grau i màster d'Informàtica i Multimèdia. Ha elaborat diversos materials i llibres sobre administració de sistemes, seguretat, informàtica forense i legislació aplicada a les tecnologies de la informació. La seva recerca s'emmarca dins de la seguretat, la influència de les TIC a la societat i l'enginyeria del coneixement.

Primera edició: setembre 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Manel Mendoza Flores, Javier Panadero Martínez, Miquel Colobran Huguet
Producció: FUOC

Índex

Introducció

En aquest mòdul, parlem del responsable d'informàtica i de la seva relació amb l'organització i el departament d'informàtica. En concret, del tipus de decisions que ha de prendre i de com es coordina amb la figura de l'administrador del sistema informàtic.

El sistema informàtic és l'eina, i els administradors, les figures que la mantenen en funcionament. Però el responsable d'informàtica és la figura que pren les decisions de la funció del sistema informàtic dins l'organització. Decideix què pot fer amb els recursos de què disposa el departament i té una visió de futur sobre què caldrà fer, és a dir, quina ha de ser la funcionalitat del departament d'informàtica dins el conjunt de l'organització en el moment present i futur.

El responsable d'informàtica també ha de gestionar aspectes com el pla estratègic i el pla de seguretat informàtic, que avui dia es poden implementar amb metodologies estàndards.

Al llarg d'aquest mòdul també s'indiquen alguns criteris que poden ajudar a prendre decisions, per exemple, en el moment de decidir sobre la implantació del programari o com s'ha d'actuar davant de problemes de seguretat. Finalment, es presenten metodologies àgils per a la millora i la implementació del programari.

Objectius

En els materials didàctics d'aquest mòdul, presentem els continguts i les eines per assolir els objectius següents:

1. Conèixer les responsabilitats del responsable d'informàtica.

2. Conèixer les decisions que ha de prendre el responsable del departament en el disseny d'una aplicació.

3. Saber com cal actuar davant d'un problema de seguretat.

4. Entendre el concepte de pla en una organització i conèixer-ne alguns dels que hi pot haver.

5. Conèixer les principals metodologies àgils dedicades a la gestió i la millora del programari.

6. Conèixer els principals plans de seguretat i mètodes estàndards de gestió dels riscos.

7. Aprendre a preveure les possibles amenaces i riscos que poden posar en perill el sistema informàtic i preparar-se per minimitzar-ne les conseqüències.

1. El responsable d'informàtica

Per poder ser eficient, el responsable d'informàtica ha d'exercir un paper molt important com a transmissor de la informació entre el departament d'informàtica i l'organització. Tal com mostra la figura 1, és el pont de comunicació en totes dues direccions (tècnicament parlant).

Figura 1. Típica estructura organitzativa, en què el responsable d'informàtica coordina l'equip de personal tècnic

Això vol dir que el responsable d'informàtica té informació relativa a la situació de l'organització que el personal tècnic no ha de conèixer necessàriament. A més a més, el responsable té cura de vetllar per un seguit de plans que porten a terme els administradors (o, fins i tot, altres departaments o els qui estan contractats externament) relatius a la informàtica de l'organització.

Tal com es veu a la figura anterior, la figura del responsable d'informàtica és qui gestiona els recursos del departament (tant humans com materials). Per tant, ha de tenir un coneixement complet de l'organització i del departament per aconseguir que tots dos elements es moguin amb la màxima sincronització possible. Ha d'aconseguir que el departament d'informàtica ajusti al màxim els objectius de l'organització amb els recursos que aquesta última li dona. A la pràctica, sempre és un canal de comunicació en els dos sentits per detectar necessitats, aconseguir recursos, ajustar objectius, etc.

El **responsable d'informàtica** gestiona els recursos del departament d'informàtica i fa d'enllaç entre el departament i l'organització.

1.1. El responsable d'informàtica i l'administrador de sistemes

Com hem dit, el responsable d'informàtica té una visió més global de tot. Per tant, necessita la figura de l'administrador, que és qui té cura dels servidors. Aquesta persona li ofereix la situació i la visió tècnica del departament

d'informàtica en cada moment. Per tant, el pot assessorar per prendre moltes decisions sobre el programari i el maquinari. A la pràctica, la majoria de decisions tècniques es prenen amb l'ajuda de l'administrador de sistemes.

2. Els plans

Totes les organitzacions, a fi d'estar coordinades i preparades per a qualsevol situació, segueixen un seguit de plans que els caps de cada departament han de preparar, revisar i tenir a punt.

2.1. Pla estratègic de l'organització

El pla estratègic és una planificació, normalment quinquennal o triennal, en què s'estableix l'orientació de l'organització per assolir els objectius que es proposa. Aquest pla estratègic de l'organització s'ha de concretar posteriorment en un pla estratègic per a cada departament vinculat al pla estratègic global.

Una **planificació estratègica** és un conjunt de propostes realistes per fixar els objectius de l'organització en un futur.

Com que el responsable d'informàtica ha d'establir el pla estratègic del departament d'informàtica, mirem com és, a grans trets, el pla estratègic d'una organització.

2.1.1. La planificació estratègica

Davant d'una societat canviant, l'organització s'hi ha d'adaptar per complir els seus objectius. La planificació estratègica és una eina útil i necessària per ajustar el funcionament de l'organització en el si de la societat.

La planificació estratègica ha de ser una eina per integrar tots els departaments en uns mateixos objectius i en un marc de treball comú.

La planificació estratègica, a fi de minimitzar els riscos i maximitzar els resultats, ha de plantejar estratègies i objectius simples, clars, assolibles i mesurables.

2.1.2. Metodologia

S'ha de recopilar informació interna i externa. L'externa prové de l'anàlisi de l'entorn per identificar les **oportunitats** i les **amenaces**. La informació interna permet identificar les **fortaleses** i les **debilitats** de la mateixa organització.

Vegeu també

Vegeu com es fa una anàlisi DAFO al subapartat «Anàlisi DAFO».

Entre els aspectes fonamentals que hi ha d'haver en l'anàlisi podem incloure, per exemple, l'avaluació dels serveis que es fan o els sistemes d'administració.

2.1.3. Components del pla estratègic

A continuació, es defineixen els principals components del pla estratègic:

- **Declaració de la missió**. La declaració de la missió intenta simplement determinar l'objectiu final al qual es pretén arribar.

- **Visió**. És el camí que cal seguir per aconseguir la missió. La visió serà la guia per a les accions que es duran a terme.

- **Problema estratègic general**. Consisteix a determinar els factors interns o externs que poden afectar la consecució de la missió.

- **Solució estratègica general**. Es basa a donar estratègies que permetin assolir la missió i, per tant, superin els problemes estratègics.

- **Objectius i estratègies**. Determinar els objectius i implementar les estratègies és clau per a la planificació. Els objectius, almenys pel que fa als departaments, han de ser de tipus qualitatiu. És a dir, han de ser quantificables per poder-ne mesurar el compliment i poder-los formular en accions estratègiques.

- **Pressupost i control**. Els objectius i les accions s'han de preveure en els pressupostos. Aquest element es basa a calcular el cost que tindran les accions del pla estratègic a l'organització.

2.1.4. Anàlisi DAFO

DAFO

DAFO és la sigla de: debilitats, amenaces, fortaleses i oportunitats

En anglès, SWOT: *strengths, weaknesses, opportunities and threats*.

En els darrers anys, l'anàlisi DAFO s'ha convertit en una eina de diagnòstic dins la direcció estratègica de l'organització. Juntament amb el diagnòstic financer i el funcional, formen les tres parts bàsiques per a l'anàlisi interna d'una organització.

L'objectiu és concretar en una taula (matriu) l'avaluació dels punts forts i febles de l'organització amb les amenaces i les oportunitats externes, tot això partint de la base que l'estratègia pretén aconseguir un ajustament adient entre la capacitat interna de l'organització i la seva posició competitiva externa.

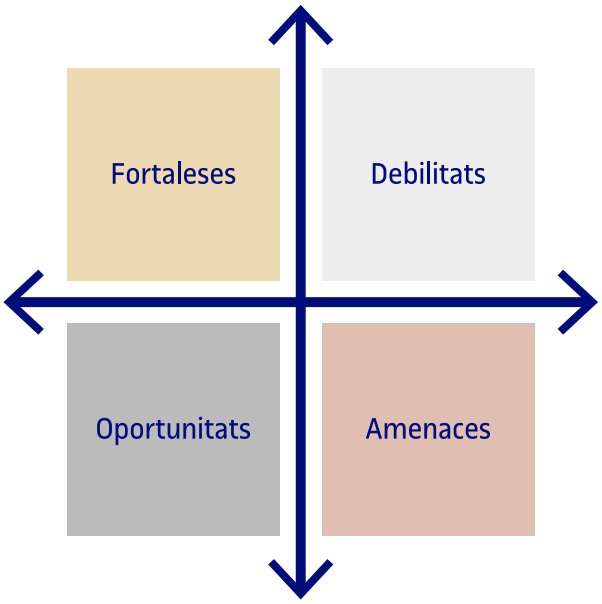
El més important és trobar el que ens permet identificar i mesurar els **punts forts**, els **punts febles**, les **oportunitats** i les **amenaces** de la nostra organització, que reunirem en aquesta taula. Les fortaleses i debilitats internes són molt importants, ja que ens ajuden a entendre la posició de la nostra organització

en un entorn concret. Cada organització ha de veure quines són les variables adients que en determinen la posició dins el mercat, segment o societat en que està immersa.

Una vegada definides aquestes variables, hem de fer un procés de *benchmarking* o anàlisi comparativa amb les millors organitzacions competidores (és possible que al llarg d'aquest procés identifiquem alguna oportunitat nova).

Finalment, la figura 2 recull les possibles estratègies. En aquesta matriu DAFO, a les columnes establirem l'**anàlisi de l'entorn** (1a. columna: amenaces, 2a. columna: oportunitats) i a les files, el **diagnòstic de l'organització** (1a. fila: punts forts, 2a. fila: punts febles). Cadascun dels quatre quadrants reflecteix les possibles estratègies que ha d'adoptar l'organització.

Figura 2. Exemple esquemàtic de la taula DAFO



L'estudi de la matriu es fa analitzant aïlladament cada quadrant. Per exemple, si ens mirem el primer quadrant (fortaleses) haurem d'identificar cadascun dels punts forts que hi ha a l'organització, juntament amb cadascuna de les amenaces de l'exterior que té. Així doncs, hem d'analitzar cada intersecció per veure les conseqüències i les accions que se'n poden derivar.

2.2. Pla de seguretat i anàlisi de riscos

Aquest pla ha de vetllar per la seguretat de tot l'equipament informàtic de l'organització. La responsabilitat del responsable d'informàtica és fer-lo i assegurar que es durà a terme correctament.

La ISO defineix el risc tecnològic com la probabilitat que esdevingui una amenaça usant vulnerabilitats existents d'un actiu o actius i generant pèrdues o danys. D'acord amb aquesta definició, hi ha diversos elements en joc (amenaces, vulnerabilitats, actius, etc.) i, per tant, hi ha moltes maneres d'enfocar el

risc. Nosaltres ho farem basant-nos en el pla de prevenció de riscos laborals. Com mostra la figura 3, el pla de prevenció es fonamenta en la idea que la seguretat forma part d'un mecanisme global de tres components: prevenció, seguretat i contingències. A continuació, es defineix cadascun d'aquests components:

- **Prevenció**: l'objecte d'interès en aquest component està en el **que es desitja protegir** Cal esbrinar què ens interessa protegir i quines solucions hi ha per protegir el nostre sistema.

- **Seguretat**: en aquesta fase hem d'«implementar» la seguretat. Aquest és el pla de seguretat, és a dir, **com protegirem** el nostre sistema.

- **Contingència**: hem de tenir present que els sistemes poden fallar, sigui per atacs a causa d'intrusos o per causes externes que no controlem, com ara els desastres naturals. Per tant, cal preveure els protocols d'actuació davant d'una situació d'aquestes característiques, és a dir, **què hem de fer quan falla la seguretat**.

Figura 3. Esquema genèric d'un pla de prevenció

2.2.1. Prevenció

El pla de prevenció, aplicat només a l'entorn informàtic, és un pla que implica analitzar els possibles riscos als quals pot estar exposat l'equipament informàtic i la informació que hi ha (a qualsevol mitjà d'emmagatzematge). Es tracta d'analitzar què pot passar i què volem protegir.

És molt important fer partícips els diferents actors de l'organització en el procés d'anàlisi, atès que cada actor podrà determinar amb més exactitud les relacions entre les aplicacions informàtiques i el negoci.

Anàlisi de riscos

Cal assegurar-se que es tenen en compte totes les possibles causes de riscos que poden provocar problemes al sistema. Per això, es fa una anàlisi de riscos, la qual es basa a calcular la possibilitat que tinguin lloc fets problemàtics, obtenir una valoració econòmica de l'impacte d'aquests successos negatius i contrastar el cost de la protecció amb el fet de tornar-la a crear o a comprar. Aquesta operació es repetirà amb la resta d'«actius» (equips informàtics, per exemple). A grans trets, els passos serien els següents:

1) Imaginar-se què pot passar (què pot anar malament).

2) Estimar el cost que comportaria per a l'organització.

3) Estimar la probabilitat que es doni cadascun dels possibles problemes. Això permet prioritzar els problemes i el seu cost potencial i desenvolupar el pla d'acció adient.

L'anàlisi de riscos passa primerament per respondre preguntes, com ara les següents:

- **Què pot anar malament?** Sovint es modelen els diferents escenaris de crisi amb diferents impactes, per ajudar l'organització a ser conscient de l'afectació.

- **Amb quina freqüència pot passar?** Aquesta és una de les variables més complexes de determinar i, per tant, una anàlisi de les dades històriques pot ajudar en aquesta quantificació.

- **Quines serien les conseqüències?** Se solen identificar totes les conseqüències i, posteriorment, es passa a una quantificació econòmica.

Fonamentalment, avaluar els riscos representa tenir clares qüestions com les següents:

- **Què s'intenta protegir?** Solen ser actius de l'organització, incloent les persones i els documents.

- **Quin valor li dona l'organització?** És molt important alinear els esforços amb el valor que tenen aquests per a l'organització.

- **De què es vol protegir?** Els riscos detectats anteriorment.

- **Quina és la probabilitat d'un atac?** Amb una monitorització dels mapes d'atacs podem prioritzar els atacs que tenen més probabilitats d'ocurrència dins de l'organització.

El **procediment** per fer un pla de riscos és el següent:

1) Avaluar els riscos en una reunió del responsable d'informàtica amb la resta de caps de departament per tractar els punts següents:

A quins riscos en seguretat informàtica ha de fer front l'organització?

- Al foc, que pot destruir l'equipament i la informació.
- Al robatori d'equipament i arxius.
- A actes vandàlics que malmetin l'equipament i els arxius.

- A fallades en l'equipament que fan malbé els arxius.
- A errades que malmeten els arxius.
- A virus, que malmeten l'equipament i els arxius.
- A accessos no autoritzats, que comprometen la informació.

Una vegada s'ha fet la relació, s'ha de preveure com es pot actuar per prevenir les causes i com cal actuar per minimitzar-ne els efectes.

2) S'ha d'**avaluar la probabilitat** que tingui lloc cadascuna d'aquestes causes. Per exemple:

Quina probabilitat hi ha que passi algun dels fets esmentats?

- El foc, que pot destruir l'equipament i la informació.
  - L'organització té alguna protecció contra incendis?
  - Calen sistemes d'aspersió automàtica?
  - Calen extintors? N'hi ha?
  - Són necessaris detectors de fums? N'hi ha?
  - El personal té alguna formació per actuar davant d'un incendi?

- Fallades de l'equipament, que poden malmetre la informació.
  - El personal informàtic duu a terme el manteniment dels equips dins els terminis previstos?
  - Quines són les condicions actuals del maquinari?

I així per a totes les causes que hagin aparegut en la reunió.

3) S'ha de determinar la **probabilitat** per a cada risc de forma **qualitativa**. La taula 1 mostra els diferents factors de riscos qualitatius. Per dur a terme aquesta quantificació qualitativa, es pot fer servir diverses tècniques:

- Posar-ho en comú amb diferents experts en la matèria i treure'n una valoració conjunta.
- Utilitzar dades estadístiques d'altres anys.
- Contrastar les estimacions amb fonts externes.

Taula 1. Ponderació de la probabilitat del risc de forma qualitativa

Factor de risc
Molt alt
Alt
Mitjà
Baix
Molt baix

4) Es fa el resum dels **riscos ordenats** pel seu factor de risc, en què es prioritzaran els que tinguin una probabilitat de risc més alta. A continuació, la taula 2 mostra un exemple de tipus de riscos associats al seu factor de risc.

Taula 2. Tipus de riscos ordenats pel factor de risc

Tipus de riscos	Factor de risc
Robatori	Alt
Fallades en l'equipament	Mitjà
Acció de virus	Mitjà
Robatori de dades	Baix
Foc	Baix
Frau	Molt baix

Anàlisi dels punts febles de la seguretat de la xarxa informàtica

Una de les tasques del departament d'informàtica és estudiar el maquinari, el programari, la seva localització, instal·lació, etc., tot amb l'objectiu de buscar escletxes en la seguretat. Qualsevol ordinador connectat a la xarxa de l'organització pot ser una font potencial per accedir al sistema. Això es pot aplicar tant a portàtils com a ordinadors amb placa de xarxa (wifi o cablejada).

5) Es farà una **relació de les tasques** actuals que es duen a terme respecte a la seguretat del sistema general.

- Es fa una còpia diària dels fitxers crítics de l'organització?
- Evitar el robatori. Tancament físic de les portes?
- Evitar el vandalisme. Porta principal sempre tancada?
- Problema dels virus. Està controlat tot el programari que entra i s'analitza amb un programari antivirus? Els programes de domini públic i d'ús compartit (*shareware*), només es fan servir si provenen de llocs fiables?

La prevenció o pla de prevenció es porta a terme per mitjà d'una **anàlisi de riscos**.

2.2.2. Seguretat

Aquest pla ha de vetllar per la seguretat de tot el sistema informàtic i, naturalment, de manera molt especial, per la informació de l'organització. La responsabilitat del responsable d'informàtica consisteix a elaborar aquest pla i assegurar que es durà a terme correctament.

Per mitjà del pla de prevenció hem analitzat què volem protegir i hem proposat solucions per fer-ho. En el pla de seguretat proposem la manera de dur a terme les solucions, és a dir, protocols, mecanismes, eines, tecnologia, assignació de responsabilitats, etc., perquè la seguretat sigui una realitat.

Una vegada més, és molt important que tots els procediments i protocols d'actuació no estiguin incomplint la legislació vigent en cap vessant, ja que si és així poden convertir-se en un forat de seguretat.

2.2.3. Contingències

El pla de contingències és, de fet, una conseqüència de l'anàlisi de riscos. Si sabem què volem protegir (i, naturalment, com es fa per mitjà del pla de seguretat), ara hem de decidir què fem davant d'una fallada del sistema o una escletxa de seguretat.

Un pla de contingències no tindria sentit si penséssim que el nostre pla de seguretat és perfecte. Desgraciadament, els sistemes de seguretat no ho són mai. Amb el pas del temps apareixen forats no descoberts abans, o errors de maquinari en els equips que poden convertir el sistema informàtic en vulnerable. O pitjor encara, una actualització del sistema (servidors, encaminadors, estacions de treball), que suposem que millora la seguretat, en realitat pot obrir noves esquerdes al nostre sistema sense que ens n'adonem. També podríem parlar de contrasenyes insegures o febles, rotació de personal dins de l'organització, etc., aspectes que hem de comprovar periòdicament per assegurar que el nostre sistema es manté segur.

Així doncs, hem de suposar que podem patir un incident de seguretat en qualsevol moment i hem de preparar-nos pel «pitjor» cas. Per tant, cal preveure les accions i les actuacions a dur a terme en aquestes situacions.

Amb el benentès que malgrat totes les mesures que es puguin prendre pot tenir lloc un desastre, el pla de contingències inclou un **pla de recuperació de desastres**, que té com a objectiu restaurar el servei informàtic al més aviat possible i minimitzar el cost i les pèrdues en la mesura que es pugui. Perquè el disseny del pla de contingències tingui sentit, s'ha de pressuposar el pitjor cas de tot, el **desastre total**. D'aquesta manera, el pla serà el màxim de complet i podrà incloure tota la casuística.

El **pla de contingències** haurà de tenir present:

- Si hi ha una pèrdua, l'assumim (en cost i temps) i tornem a començar des de zero.

- No podem assumir la pèrdua (per algun motiu, sigui cost, temps, etc.) i, per tant, necessitem una còpia de seguretat. Aquesta informació estarà dins del sistema de còpies i, possiblement, dins del pla de recuperació de desastres.

- També tindrem en compte els incidents, com per exemple, les fallades de maquinari o de programari que poden deixar inutilitzat totalment o parcialment el sistema informàtic, i confeccionarem els protocols a seguir davant d'aquest tipus de situacions.

2.3. Sistemes de gestió de seguretat de la informació (SGSI)

A causa de la complexitat de dur a terme un pla de seguretat, cal una metodologia. Per aquest motiu varen aparèixer els sistemes de gestió de la seguretat de la informació (SGSI).

En general, qualsevol sistema de gestió de la seguretat haurà de comprendre la política, l'estructura organitzativa, els procediments, els processos i els recursos necessaris per implantar la gestió de la seguretat de la informació dins d'una organització. Bàsicament, un sistema de gestió es caracteritza per:

- Cobrir els aspectes organitzatius, lògics, físics i legals.

- Ser independent de plataformes tecnològiques i mecanismes concrets.

- Ser aplicable a tot tipus d'organitzacions, independentment de la seva grandària i activitat.

- Tenir, com tot sistema de gestió, un fort contingut documental.

En els SGSI es defineix:

- **Actiu**: recurs del sistema d'informació o relacionat amb aquest necessari perquè l'organització funcioni correctament i assoleixi els objectius proposats per la direcció.

- **Amenaça**: esdeveniment que pot desencadenar un incident a l'organització, produint danys o pèrdues materials o immaterials en els seus actius.

- **Risc**: possibilitat que una amenaça es materialitzi.

- **Impacte**: conseqüència sobre un actiu de la materialització d'una amenaça.

- **Control**: pràctica, procediment o mecanisme que redueix el nivell de risc.

En aquestes metodologies, la seguretat consisteix en la realització de les tasques necessàries per garantir els nivells de seguretat exigibles en una organització. En conseqüència, la seguretat s'ha d'entendre com un procés.

Els riscos no s'eliminen, es gestionen.

Hi ha diferents metodologies per implementar un SGSI. Vegem-ne algunes.

2.3.1. MAGERIT

És un mètode formal per investigar els riscos que suporten els sistemes d'informació i per recomanar les mesures adients que s'haurien de prendre per controlar aquests riscos. És una metodologia pública desenvolupada pel Ministeri d'Administracions Públiques.

Consta de **quatre fases**:

1) Planificació de l'anàlisi i gestió de riscos: estimacions inicials dels riscos que poden afectar el sistema d'informació, el temps i els recursos necessaris per al seu tractament.

2) Anàlisi de riscos: es fa una estimació de l'impacte que tindran els riscos a l'organització. Aquesta àrea és molt important perquè un ús desproporcionat pot afectar negativament el rendiment. Cal establir un llindar de risc desitjable (tolerable) que s'ha de superar per ser objecte de tractament.

3) Gestió del risc: cal seleccionar possibles solucions per a cada risc. Són fonamentals els exercicis de simulació.

4) Selecció de salvaguardes: cal triar els mecanismes que implementaran les solucions elegides en la fase anterior.

2.3.2. ISO/IEC 27001:2013

El 15 d'octubre de 2005 neix l'estàndard ISO 27001:2005, que posteriorment evoluciona a la versió 2013 actual 7799. S'usa per a la implantació d'un SGSI.

La norma ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) és certificable i especifica els requisits necessaris per establir, implantar, mantenir i millorar un sistema de gestió de la seguretat de la informació segons el model PDCA. És consistent amb les millors pràctiques descrites en ISO/IEC 17799 i té el seu origen en la norma britànica British Standard BS 7799-2 publicada per primera vegada el

1998. Aquesta norma es va elaborar per poder certificar els sistemes de gestió de la seguretat de la informació implantats a les organitzacions per mitjà d'un procés formal d'auditoria.

La ISO/IEC considera l'organització com a totalitat i té en compte tots els possibles aspectes que es poden veure afectats davant dels possibles incidents que es puguin produir. Aquesta norma està estructurada en **catorze dominis de control** que cobreixen completament la gestió de la seguretat de la informació, en què cadascun d'ells es refereix a un aspecte de la seguretat de l'organització:

1) Política de seguretat
2) Aspectes organitzatius per a la seguretat
3) Seguretat lligada als recursos humans
4) Classificació i control dels actius
5) Control dels accessos
6) Xifratge
7) Seguretat física i ambiental
8) Seguretat en l'operativa
9) Seguretat en les telecomunicacions
10) Desenvolupament i manteniment dels sistemes
11) Relacions amb els subministradors
12) Gestió dels incidents de seguretat de la informació
13) Gestió de la continuïtat del negoci
14) Conformitat legal

Els dominis, a la vegada, defineixen diversos controls que componen l'auditoria ISO 27001:2013.

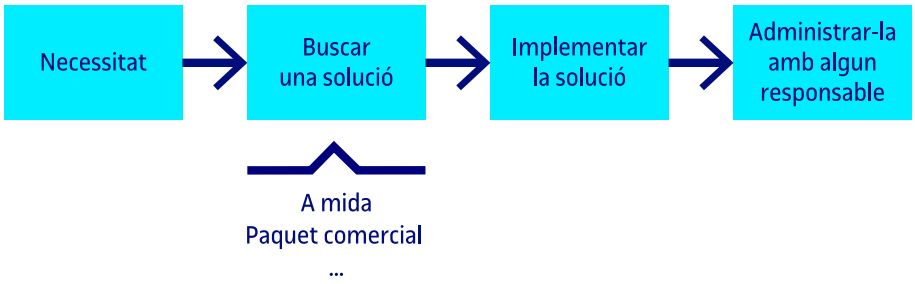
3. Implantació i disseny d'aplicacions

Com ja hem explicat a l'apartat anterior, en una organització pot aparèixer una necessitat com a conseqüència de canvis interns (noves orientacions) o canvis externs, o simplement per a la millora del seu funcionament. Aquesta necessitat pot afectar fins al punt que calguin modificacions importants de programari o, fins i tot, que se n'hagi de comprar un de nou. Si aquest és el cas, ens trobem amb la decisió de:

- Modificar el programari que tenim (si podem)?
- Comprar un programari estàndard?
- Crear-nos un programari a mida?

En aquest apartat donem unes pautes o indicacions que poden ajudar a resoldre aquest problema.

Figura 4. Partint de les necessitats de l'empresa, es comença buscant solucions per a una posterior implementació

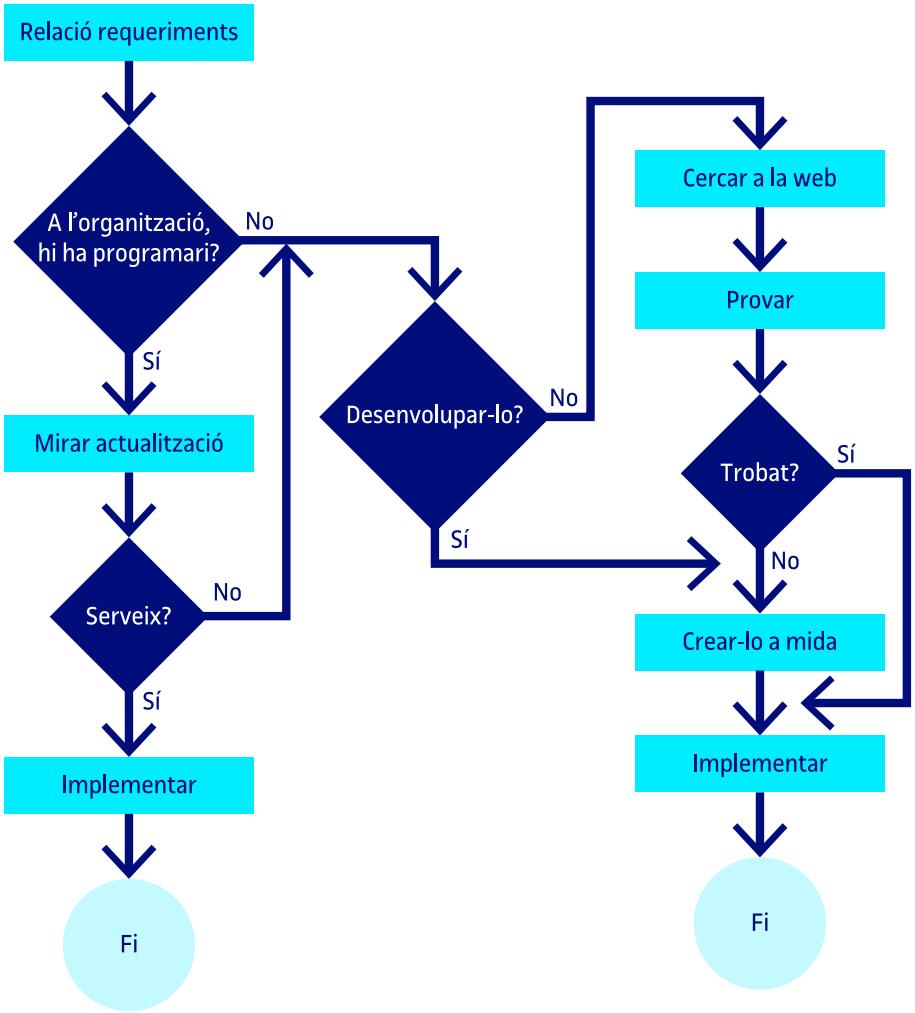


Com mostra la figura 4, a partir del moment en el qual es detecta una necessitat, hi ha tres etapes clarament diferenciades: buscar una solució, implementar la solució i, finalment, administrar-la amb algun responsable. Tots els passos els duen a terme figures tècniques però amb la supervisió de la figura del responsable d'informàtica, que és qui participa en les decisions, en estreta coordinació amb les figures dels administradors (tècnics).

Quan es detecta una necessitat, és el responsable d'informàtica qui pren les decisions finals sobre si es pot satisfer o no. Solucionar-la té un cost i, per tant, s'ha de veure si es pot dur a terme. El responsable d'informàtica coneix el pla estratègic de l'organització, els recursos econòmics, humans, etc., de què disposa. Amb aquesta informació i l'informe tècnic preliminar que s'ha fet en l'etapa d'anàlisi de la detecció de necessitats, podrem decidir si es pot resoldre o no.

Aquesta necessitat pot arribar a ser complexa, ja que si s'implanta un programari nou, afecta profundament tota l'estructura informàtica i també l'organització, atès que modifica la manera de treballar del personal. Així doncs, aquest és un mètode per intentar ser com més conservadors millor amb el programari que tenim per ajustar-lo a la necessitat que hi ha creada.

Figura 5. A partir dels requeriments, es comença la cerca de solucions per a l'organització



Davant d'una nova necessitat, els reposable d'informàtica ha de traslladar aquesta demanda a una relació de requeriments. Amb aquesta llista de requeriments comença el cicle de buscar una resposta adient a les demandes.

De vegades, es pot buscar actualitzacions o complements a solucions actuals, mentre que altres vegades s'ha d'iniciar desenvolupaments nous.

Molts cops, si a l'organització ja es té un programari que cobreix una part de les funcions, s'analitza l'opció d'ampliar el programari amb les noves demandes. En cas que no hi hagi res similar, es comença amb el procés de cerca d'alternatives, incloent el desenvolupament a mida.

Com es pot veure a la figura 5, cadascun d'aquests passos és força complex i el responsable d'informàtica, conjuntament amb l'administrador de sistemes, treballen plegats per dur a terme aquesta tasca.

Hi ha moltes solucions davant del problema d'una necessitat. Intentem buscar les que modifiquen l'estructura informàtica el mínim possible.

3.1. Metodologies àgils per al disseny i la implantació d'aplicacions

Recentment s'han modificat tècniques de desenvolupament per ser més flexibles i ràpides en l'adopció de les necessitats i solucions de clients. En especial, analitzarem les metodologies Agile i Scrum.

3.1.1. Metodologia Agile

És una metodologia que permet respostes ràpides a les valoracions que es fan del propi projecte i això és precisament el que defineix la seva naturalesa: el seu caràcter àgil.

La metodologia Agile es basa en una aproximació incremental d'entrega contínua i de validació dels resultats amb el client, de manera que el projecte «es trosseja» en petites parts que han de completar-se i lliurar-se en poques setmanes. L'objectiu és desenvolupar productes i serveis de qualitat que responguin a les necessitats dels clients, les prioritats dels quals canvien a una velocitat cada vegada major. Com que permet valorar i avaluar l'estat del projecte de forma contínua, aquest es pot anar adaptant a les necessitats del client de forma contínua.

Es fonamenta en quatre punts primordials:

1) Les persones i les interaccions sempre són la prioritat, fins i tot per sobre dels processos i les eines.

2) És més important que el producte funcioni perfectament, que una documentació extensa sobre aquest tema.

3) Sempre és preferible col·laborar amb el client, en lloc d'establir una negociació contractual.

4) El procés de treball sempre ha de respondre davant el canvi, i mai enredar-se en un pla estricte.

Aquesta nova metodologia de desenvolupament contrasta amb les metodologies de planificació de projectes en què les fases inicials corresponien a la planificació i captura de requeriments. Amb les metodologies àgils, el desenvolupament s'adapta molt més ràpid a les demandes canviants dels clients i es minimitza el risc amb validacions periòdiques.

3.1.2. Scrum

Scrum és un tipus de metodologia àgil dedicada al desenvolupament de programari, en el qual s'apliquen de manera regular un conjunt de bones pràctiques per treballar en equip i obtenir el millor resultat possible d'un projecte.

Amb Scrum es fan *sprints* en què es defineixen les entregues parcials i regulars del producte final, prioritzades pel benefici que aporten al client del projecte. La metodologia Scrum és indicada per projectes complexos en què els requisits a l'inici del projecte estan poc definits o poden canviar ràpidament amb el pas del temps. Aquesta metodologia està molt recomanada en els projectes de desenvolupament de programari, atès que amb molta freqüència (setmanalment/quinzenalment) es revisen els objectius de l'*sprint* i es van validant amb el client les funcionalitats desenvolupades.

Scrum defineix una sèrie de rols, que ajuden la metodologia a desenvolupar-se de forma correcta. Així podem citar.

- ***Product owner***: defineix l'evolució del producte, els temps i els aspectes relacionats amb l'àmbit econòmic.

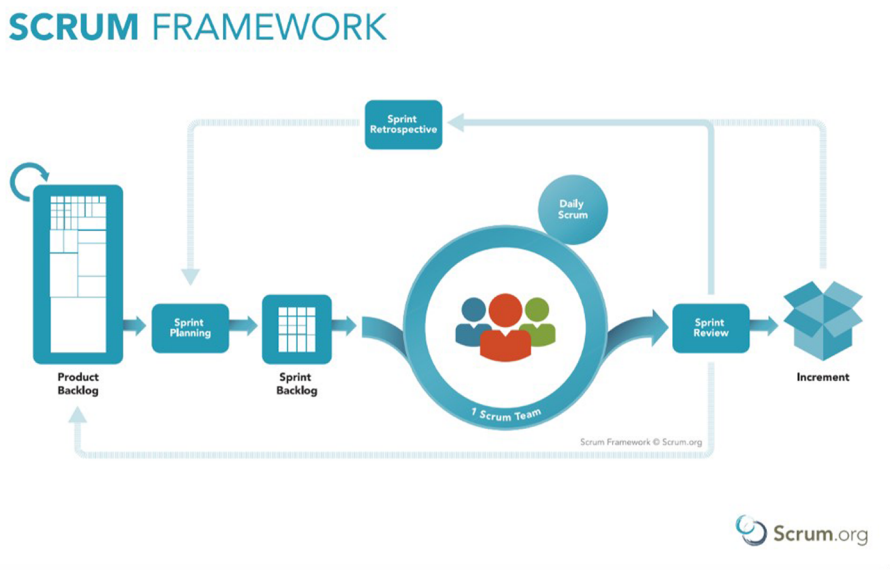
- **Equip de desenvolupament**: encarregat de dur a terme el desenvolupament d'acord amb el que defineixi el *product owner*.

- ***Scrum master***: ajuda a entendre els requeriments del negoci de forma correcta i traslladar-los a l'equip de desenvolupament dins el marc de treball amb *sprints*. Igualment s'assegura d'eliminar qualsevol impediment que l'equip de desenvolupament tingui per aconseguir els objectius marcats.

El cicle d'Scrum

En la metodologia d'Scrum, es defineixen cicles curts i de durada fixa (1, 2 o 3 setmanes), on a cada cicle es realitza tot un cicle complet. En general, la figura 6 representa un cicle d'Scrum, en què cada *sprint* es revisa diàriament.

Figura 6. Scrum treballa amb *sprints* curts de forma contínua



Font: https://commons.wikimedia.org/wiki/File:Scrum_Framework.png.

La figura 7 descriu el cicle complet d'Scrum des de que el client defineix les funcionalitats, els requisits o les millores que necessita (*Product Backlog Item* –PBI–) fins que finalitza el cicle Scrum amb el producte final. A continuació, es defineixen cadascuna de les etapes del cicle:

1) El *product owner* o client defineix i prioritza els objectius en funció del valor i cost que representen els objectius marcats. Primerament, el client defineix les funcionalitats o millores que necessita (*Product Backlog Item*). Una vegada s'han definit els PBI, es crea un llistat ordenant els PBI per prioritat. Aquest llista s'anomena *product backlog* i serà la que rebrà l'equip de desenvolupadors.

2) Seguidament l'equip (*development team*) comença el procés de planificació (*Spring Planning*) i iteració amb els passos següents:

a) Selecció de requisits de l'*sprint*: es defineix amb claredat tots els dubtes i prioritats a completar dins la iteració.

b) Planificació de la iteració: es detallen la llista de tasques necessàries per al desenvolupament dels requisits seleccionats i s'estima l'esforç de cada tasca.

3) Un cop s'ha planificat comença la fase d'execució, en què normalment podem trobar:

a) Reunió de sincronització diària (*Daily Scrum*) –sol ser curta, de 15-20 minuts– en què s'analitzen les tasques i les dependències entre tasques, els objectius aconseguits i els passos planificats següents.

b) En aquesta fase el facilitador (*Scrum Master*) alinea tot l'equip per aconseguir els objectius definits en l'*sprint*, evitant interrupcions de l'exterior.

c) Igualment durant la fase d'execució el client pot refinar lleugerament els requisits (<10 %).

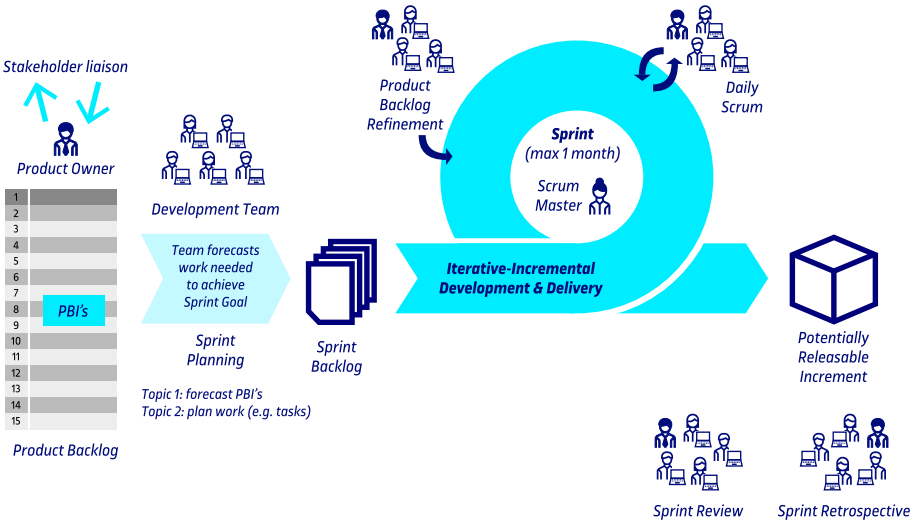
3) Finalment, l'últim dia de l'*sprint* es fa la revisió de la iteració (*Sprint Review*) amb dues parts diferenciades:

a) Revisió/demostració: l'equip mostra els objectius completats.

b) Retrospectiva: s'analitza com ha evolucionat el cicle per si s'ha de modificar alguna part per al cicle següent.

És important indicar que l'evolució d'un producte es realitza de forma cíclica i incremental.

Figura 7. Scrum alinea tot l'equip en els *sprints* de treball, focalitzant els resultats de forma incremental



Font: https://commons.wikimedia.org/wiki/File:Scrum_Framework.png.

3.2. Actualització del programari

Es tracta de veure si n'hi ha prou amb l'actualització del programari que hi ha a l'organització per solucionar la necessitat que es pretén cobrir. La tasca la farà l'administrador de sistema i la decisió sobre la viabilitat de l'actualització serà del responsable d'informàtica.

Aquesta tasca pot ser tan senzilla com valorar les característiques de l'última versió del programari via web, o tan complexa com haver de simular l'actualització en un entorn de demostració i fer una simulació per veure si s'ajusta als requisits demanats per resoldre el problema i validar que tot continua funcionant correctament.

Busquem si el programari que tenim ens serveix.

3.3. Programari estàndard

Aquesta possibilitat vol dir que, de moment, no volem desenvolupar programari propi i es busca un programari que estigui al mercat i que s'ajusti a les necessitats que es volen cobrir. Per tant, hem de fer una cerca completa de tots els programaris que ja existeixen, quin s'adapta a les necessitats que té l'organització, valorar els costos i la integració, etc. És una tasca que pot fer l'administrador de sistemes, però que ha de supervisar el responsable d'informàtica, ja que és qui pren la decisió final. Actualment els programaris són força parametritzables i, per tant, la tasca de valorar el programari que hi ha i com es pot adaptar a l'organització encara és més complexa.

Hi ha un últim factor molt important que cal tenir en compte. Segurament cap programari no s'adapta completament a les necessitats particulars de l'organització. Tot programari estàndard, per molt parametritzable que sigui, necessita una mica d'esforç d'adaptació per part de l'organització, és a dir, que hi ha d'haver un ajustament de l'organització envers el programari i del programari envers l'organització (això últim és, precisament, la parametrització).

Atès que normalment hi ha canvis motivats per factors externs o interns en el programari, cal estar força segurs que el proveïdor que ens el proporciona té una estabilitat prou bona per garantir-nos el manteniment del producte en noves versions i la resolució de problemes.

Una vegada s'ha pres la decisió, si optem per un programari estàndard l'hem de provar a fons i fer tot el procés d'implantació als servidors, i després implantar-lo als usuaris, formar-los, etc., perquè no sigui problemàtic.

La decisió final és del responsable d'informàtica, però la tasca de valorar els programaris que hi ha al mercat i la seva utilitat dins l'organització és, en gran part, una tasca de l'administrador de sistemes.

> Busquem un programari que ja estigui fet, tenint en compte que haurem d'implantar-lo a l'organització, amb totes les conseqüències que s'hi associen.

3.4. Programari a mida

La segona possibilitat implica posar en marxa un projecte de programari, un departament de desenvolupament del programari, una anàlisi, etc. Per tant, és força més complex i lent per obtenir al final un paquet ajustat a les necessitats de l'organització. Una vegada s'ha fet, generalment no s'acaba, necessitarà modificacions pràcticament constants, ja que l'organització és una entitat «viva». L'organització està dins d'una societat que també canvia i, per tant, el paquet de programari creat també pot necessitar manteniment. Això fa que el

departament de desenvolupament, si és de nova creació per a aquest projecte, difícilment desaparegui, ja que és possible que a part del manteniment, el paquet vagi creixent més i més amb el pas del temps.

En aquest cas, el responsable d'informàtica pren moltes decisions estratègiques, ja que ha de facilitar el marc de treball de l'aplicació. L'administrador de sistemes també ha de col·laborar a crear el marc de treball de l'aplicació i ha d'estar present al llarg de tot el procés de creació de l'aplicació. Segurament serà responsabilitat del responsable d'informàtica la decisió de qui desenvolupa el projecte, perquè depèn de si l'organització té departament de desenvolupament o no. Si no en té, la tasca de desenvolupar el programari es crea o es contracta externament. En aquest darrer cas, s'ha de negociar en un contracte la propietat de les fonts de l'aplicació.

Decidir fer una aplicació a mida és la darrera solució, la més costosa econòmicament i en temps, però s'obté un programari que s'ajusta completament a les nostres necessitats.

3.5. La responsabilitat del responsable d'informàtica

Com ja hem esmentat, el responsable d'informàtica té la funció de determinar el marc sobre el qual ha de funcionar aquest programari. Tant si la decisió és un programari estàndard com si és un programari a mida, aquí, una mica com en el disseny de l'entorn d'usuaris, tornen a aparèixer les qüestions següents:

- On hi ha d'haver l'aplicació?
- On han d'estar les dades?
- Quins usuaris hi accediran?
- Amb quins permisos?
- Sobre quina tecnologia es desenvolupa (client/servidor, etc.)?
- Des de quins punts de l'organització es farà servir el programari (dins la xarxa, intranet, extranet, etc.)?
- Quin serà el grau de sensibilitat de les dades?
- Quin nivell d'integració tindran les dades amb la resta d'aplicacions?
- S'han de fer públiques una part d'aquestes dades a la web de l'organització?
- Cal exportar les dades?

Per tant, ens hem de tornar a plantejar una taula de solucions com la que es mostra a continuació (taula 3), en què considerarem tant la ubicació de les dades com de les aplicacions:

Taula 3. Taula de solucions

		Dades	
		Local	Remot
Aplicació	Local		
	Remot		

1) Dades en remot. En aquest cas, probablement decidirem que les dades estiguin en una base de dades d'un servidor. Això facilita les còpies de seguretat, el manteniment i la implantació, especialment si a l'organització ja hi ha un servidor de bases de dades. També facilita la integració i les cerques futures dins d'aquesta nova base de dades. Si s'ha de publicar alguna cosa (fer extraccions) o controlar permisos, també és més senzill.

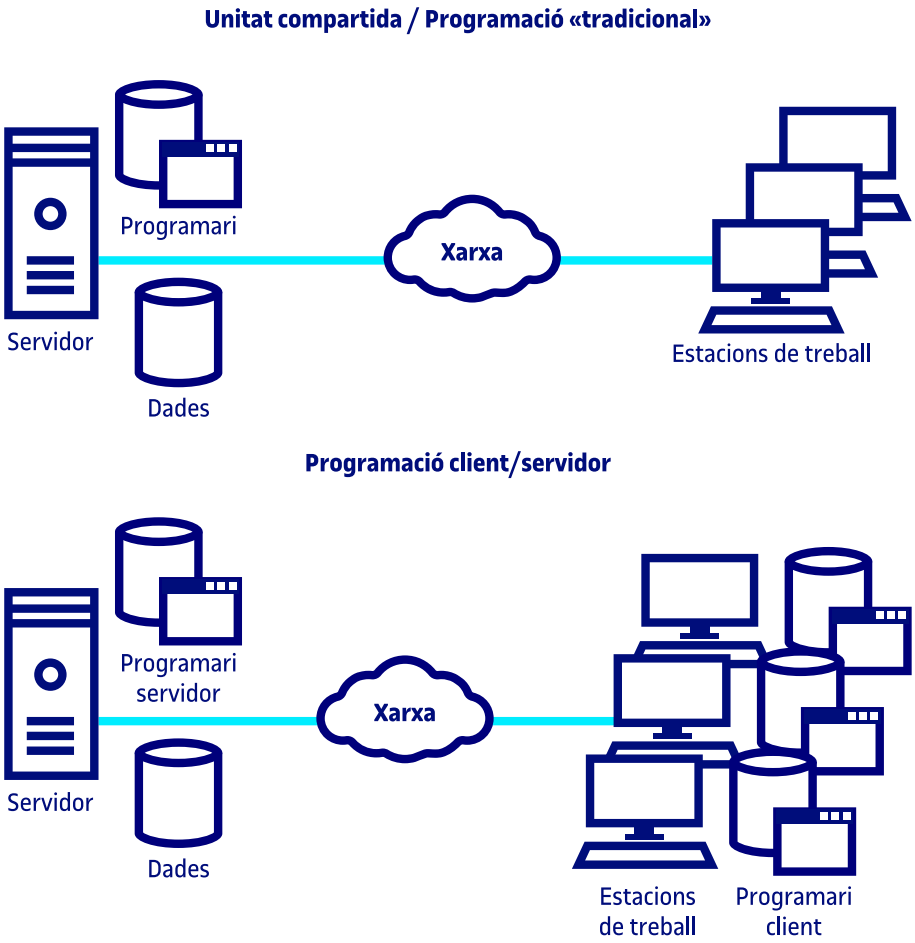
2) Programari en remot. Com mostra la figura 8, aquí estem davant de dues alternatives possibles:

a) Programa «tradicional» fet perquè pugui instal·lar-se en el client o en el servidor, o un programa amb tecnologia client/servidor que necessita una petita part instal·lada en el client.

b) Aprofitar la tecnologia client/servidor per crear una aplicació en què el programa client ja estigui instal·lat a les estacions de treball, o es pugui obrir fent servir un navegador web.

És el cas de les arquitectures en què el *front-end* (ordinador frontal) és un navegador que fa de client i el servidor allotja les bases de dades. Al mig hi ha l'aplicació servidora real.

Figura 8. Sistemes d'accés a les dades de forma remota

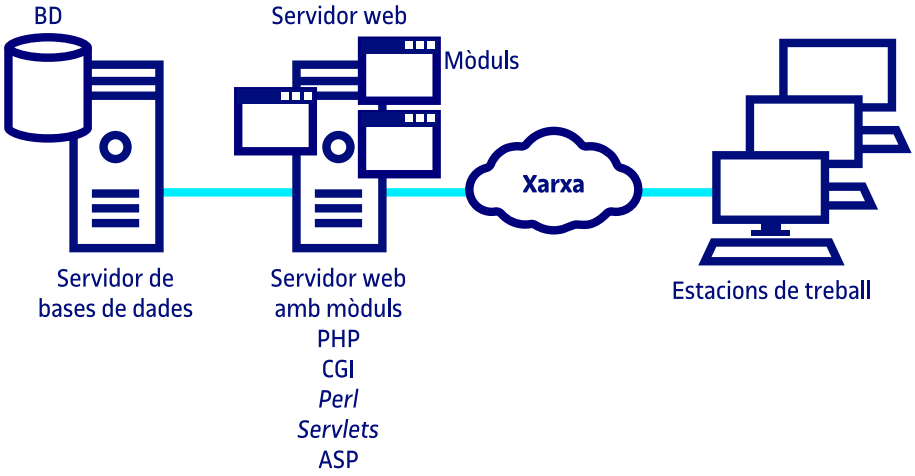


Avantatges:

- Funciona amb clients heterogenis. No cal fer una versió client per a cada plataforma.
- Funciona amb portàtils. És una bona solució per a la informàtica mòbil.
- Funciona fora de l'organització. Si hi pot haver problemes de seguretat, s'ha de posar en un servidor segur (HTTPS).
- Normalment es programa per mòduls i no monolíticament.

La figura 9 mostra l'esquema de l'estructura que s'acostuma a utilitzar en aquests casos, ja que és la més segura.

Figura 9. Arquitectura de dues capes



Com que l'aplicació està en mòduls, el manteniment i el desplegament són més senzills, i atès que les dades estan en un servidor diferent del de l'aplicació és més segur, perquè si arriben a atacar el servidor web amb èxit no hi trobaran les dades, sinó que s'ha d'aconseguir arribar a un altre servidor, per la qual cosa hi ha una altra barrera de seguretat que cal traspassar. La seguretat és més elevada.

El responsable d'informàtica també s'ha de preocupar que es dugui a terme el disseny de la documentació i del pla de formació dels usuaris finals, i de proveir dels recursos necessaris per tirar endavant el projecte.

Amb la introducció del núvol, el model de desplegament remot ha canviat exponencialment, ja que tots els recursos i servidors necessaris es despleguen al núvol, únicament requerint una bona comunicació entre el client i els servidors.

El responsable d'informàtica ha de decidir el següent:

- El marc en què desenvoluparà l'aplicació.
- El disseny de la documentació.
- El pla de formació.

4. Aspectes legals

Els aspectes legals són molts i una vegada més hem d'insistir en la qüestió dels assessors legals per a consultes, ja que avui en dia la legislació és molt canviant i cada cop té més present els delictes i responsabilitats informàtiques.

4.1. Problemes de seguretat

Un dels aspectes que ha de conèixer especialment un responsable d'informàtica és què cal fer davant d'un problema de seguretat. Recordem que alguns dels problemes de seguretat que es poden donar són els següents:

- Destrucció/robatori d'informació per part de personal de l'organització.
- Destrucció/robatori d'informació externament a l'organització, per exemple per internet.
- Abús d'ús del sistema per a finalitats no corporatives.
- Negligència en l'adopció de les mesures de seguretat adients per protegir les dades i els usuaris.

Pràcticament cada cas és particular i generalitzar aquí pot ser contraproduent. Sí que és important distingir les qüestions tècniques de les decisions que cal prendre davant d'una situació. Les figures tècniques detecten els problemes i avisen que hi són. La figura del responsable pren les decisions i les figures tècniques les duen a terme. Vegem-ho amb uns exemples.

Exemple 1: abús del sistema per part del personal amb finalitats no corporatives

Si se sospita que una persona fa servir el sistema indegudament, això ho detecten normalment els administradors de sistema (figures tècniques). Ho comuniquen al responsable d'informàtica i, en aquest cas, la funció del responsable és establir els procediments legals dins l'organització a fi de poder verificar que realment aquesta persona fa un ús indegut del sistema. Una vegada posats en marxa els procediments legals, les figures tècniques poden dur a terme els mecanismes informàtics i tècnics necessaris per reunir les proves i verificar que hi ha un problema legal. Després es procedirà amb tot el sistema legal necessari, que és responsabilitat del responsable de departament, amb suport de l'administrador de sistemes, si cal.

Exemple 2: atacs a servidors web

Aquesta situació concreta és de les complexes. Segons la situació, la decisió que ha de prendre el responsable d'informàtica pot variar, perquè hi ha molts tipus d'atacs. Suposem un atac amb intenció d'obtenir informació de l'organització. El que podria passar és el següent:

L'administrador de sistemes informa el responsable d'informàtica del tipus de problema de seguretat, el qual decideix fer el següent (sempre és una orientació):

1) Que l'administrador de sistemes dugui a terme el protocol tècnic de l'equip. Parada, còpia, restauració, etc.

2) Parlar amb la direcció de l'administració sobre el problema de seguretat que hi ha hagut.

3) Al mateix temps, el responsable d'informàtica informa el cos de policia adient per denunciar el fet, concretar una data i consultar les dades o proves del sistema que puguin necessitar.

4) Els administradors de sistema elaboren un informe exhaustiu sobre el que ha passat i aporten tota la informació que considerin necessària. Aquest informe ha de contenir què ha passat, com s'ha produït la intrusió, quant ha durat, com s'ha solucionat, quin era el problema de seguretat que l'ha provocat i a quines persones/entitats s'ha sol·licitat ajut per solucionar el problema (des del punt de vista tècnic).

5) Un informe dels administradors i el responsable d'informàtica que conté els danys ocasionats al sistema i una valoració dels danys econòmics i materials que ha significat per a l'organització aquesta intrusió. Depenent de la situació real, això ho pot fer un pèrit extern a l'organització.

6) En la data fixada amb el cos de policia, hi ha la reunió en què es presenta l'informe tècnic, l'informe de danys (i el cost estimat), les evidències amb tota la informació, proves, etc., i el cos de seguretat s'encarrega de buscar la persona que ha ocasionat el dany i actua policialment, després judicialment i, finalment, si cal, penalment.

Ara bé, suposem el cas següent: l'administrador de sistemes informa el responsable d'informàtica que s'ha trobat instal·lat un servidor de pornografia infantil al servidor web. Com que aquí clarament hi ha un delicte penal, el responsable d'informàtica decideix fer el següent (sempre és una orientació):

1) No modificar res i reunir el màxim de proves possibles (fitxers de *log*, fitxers de dades, imatges, pàgines web, etc.). La finalitat és que l'intrús encara no sàpiga que nosaltres ja tenim coneixement que ha entrat al sistema. Com acabem de dir, aquesta acció la posa en marxa el responsable d'informàtica i la porten a terme els administradors de sistema.

2) Al mateix temps, el responsable d'informàtica informa el cos de policia adient per denunciar el fet, concretar una data i consultar les dades o proves del sistema que puguin necessitar (per exemple, poden decidir clonar el disc o discs durs del servidor i restaurar el sistema –així s'evita que el delicte es continuï produint–).

3) Amb tota la informació extreta del sistema, amb la denúncia i la consulta feta al cos de policia sobre la informació que cal extreure, els administradors de sistema poden procedir de la manera següent:

- Restaurar el sistema.
- Recuperar la informació de còpies de seguretat.
- Assegurar el sistema, si cal. Això significa afegir pedaços del sistema operatiu o d'aplicació destinats a tapar el forat de seguretat que pugui haver ocasionat l'entrada il·legal de l'intrús.

Aquestes operacions destrueixen pràcticament totes les proves, pistes/traces que hagi pogut deixar l'intrús al sistema. Per això, és molt important haver extret abans tota la informació de proves i haver-ho fet en coordinació amb el cos de seguretat de l'Estat, a fi d'estar segurs de no perdre cap prova important. D'aquesta manera el servidor afectat torna a estar operatiu al més aviat possible.

4) Els administradors de sistema elaboren un informe exhaustiu sobre el que ha passat i aporten tota la informació que considerin necessària. Aquest informe ha de contenir què ha passat, com s'ha produït la intrusió, quant ha durat, com s'ha solucionat, quin era el problema de seguretat que l'ha provocat, a quines persones/entitats s'ha sol·licitat ajut per solucionar el problema (des del punt de vista tècnic).

5) Un informe fet pels administradors i el responsable d'informàtica que conté els danys ocasionats al sistema i una valoració dels danys econòmics i materials que ha significat per a l'organització aquesta intrusió. Depenent de la situació real, això ho pot fer un pèrit extern a l'organització.

6) En la data fixada amb el cos de policia, hi ha la reunió en què es presenta l'informe tècnic, l'informe de danys (i el cost estimat), les evidències amb tota la informació, pro-

ves, etc., i el cos de seguretat s'encarrega de buscar la persona que ha ocasionat el dany i actua policialment i després judicialment i, finalment, si cal, penalment.

Totes dues maneres d'actuar són molt semblants, però depenent de cada cas hi ha variacions. No hi ha, doncs, regles fixes en la manera d'actuar davant de situacions irregulars.

4.2. Aspectes legals del programari a mida

Moltes vegades el programari a mida es contracta a companyies alienes a la mateixa organització. Aquestes companyies desenvolupen el programari i l'implanten, però cal aclarir en el contracte, amb els assessors legals corresponents, els termes de propietat del codi font i fins on arriba aquest codi font (llibreries, entre d'altres).

S'han donat molts casos de companyies que han canviat l'orientació, han discontinuat el producte i, per tant, han deixat de donar suport al programari que han fabricat, de manera que l'organització que ha demanat el programari a mida en realitat no té res, perquè ningú, ni la mateixa organització contractant programadors, no serà capaç de fer el manteniment de l'aplicació. La companyia té un element conegut com a *know-how*, que és el coneixement que ha desenvolupat i que aplica als programes, que no ha de donar necessàriament a l'organització, però és bo arribar a algun tipus d'acord abans de començar el projecte perquè hi hagi alguna via per poder mantenir l'aplicació en cas que no ho faci la companyia que l'ha creat.

Per evitar aquest risc, és habitual incloure en els contractes una clàusula *escrow* o dipòsit del codi font a un tercer, que, en cas de bancarrota de la companyia subministradora, es pot executar per poder obtenir el codi font.

El problema legal de la propietat del codi font (o d'alguna part d'aquest codi) s'ha de negociar abans de començar el projecte.

5. Tasques del responsable d'informàtica

Una relació aproximada de les tasques o responsabilitats del responsable d'informàtica és la següent:

- Elaboració de la part del pla estratègic del departament, subordinat al pla estratègic de l'organització, i vetllar-lo.
- Detecció de les necessitats.
- Concreció de les necessitats amb el personal de l'organització.
- Decisió d'implantar les necessitats i la manera de fer-ho.
- Plans d'actualització informàtica.
- Pla de contingències.
- Determinació dels permisos dels usuaris en els programaris.
- Supervisió dels projectes de programari.
- Actuació i resposta davant de situacions que comprometin la seguretat del sistema.
- Decisió davant de situacions legals.
- Gestió de la seguretat.

Reflexió

Considereu que falta alguna responsabilitat important? Comenteu-ho al fòrum de l'assignatura.

Resum

El responsable d'informàtica és la figura que pren les decisions estratègiques que afecten el departament. Ha de tenir la visió de futur de com serà la informàtica.

Amb els plans s'intenta preveure què pot passar a fi de prendre mesures per minimitzar-ne les conseqüències, des de com evolucionarà la informàtica per adaptar-se fins a com cal reaccionar davant d'un desastre.

La gestió de la seguretat, per mitjà d'alguna de les metodologies existents, ha esdevingut fonamental per garantir un bon funcionament del sistema informàtic.

Detectar, valorar o, fins i tot, preveure necessitats de l'organització és una mica un art. Concretar la necessitat és una tasca de comunicació i fer-ne una anàlisi i un informe és un tasca tècnica.

Quan es necessita programari nou, intentem recórrer a la via més conservadora, ja que en un primer moment sembla la via menys traumàtica per a l'organització. El responsable d'informàtica pren les decisions, malgrat que hi ha molta feina tècnica a fer.

Ser **un bon cap d'informàtica** vol dir tenir totes les facetes esmentades anteriorment, és a dir, ser un bon tècnic, un bon dialogant, un bon cap, tenir visió de futur, tenir capacitat de previsió i moltes altres qualitats més que estan fora de l'abast d'aquests materials.

Exercicis d'autoavaluació

1. Han entrat al vostre servidor web i us n'han canviat la pàgina inicial. La primera vegada la restaureu, però al llarg d'una setmana passa tres vegades. Què faríeu?

2. Quines d'aquestes frases són certes i quines són falses?

a) Les necessitats sempre provenen del CAU.
b) És millor fer un programa a mida, ja que el podrem modificar quan vulguem.
c) El responsable d'informàtica només gestiona recursos, no ha de tenir necessàriament grans coneixements tècnics.
d) Sempre és millor un programari multiplataforma i multiusuari corrent al servidor, perquè no se sap mai com creixerà l'organització.

3. Quina d'aquestes frases sobre la implantació de les aplicacions és falsa?

a) L'últim pas és la implementació del programari escollit.
b) Només ens plantejarem crear-lo a mida si no en trobem cap d'estàndard.
c) Si l'actualització serveix, la utilitzarem de base per crear-nos el programari a mida.
d) La relació de requisits ens serveix en tot el procés.

4. Uneix el concepte amb la seva definició correcta.

Concepte	Definició
Conjunt de propostes realistes per fixar objectius de l'organització	DAFO
Definir el marc d'una aplicació nova	Detecció de necessitats
Eina de diagnòstic dins la direcció estratégica	Pla estratègic
Analitzar els riscos als quals pot estar exposat l'equip informàtic	Pla de contingències
Relació de requeriments	Responsabilitats del cap

5. Una d'aquestes tasques no és responsabilitat del responsable d'informàtica.

a) Donar accés a les aplicacions corporatives.
b) Elaborar la part del pla estratègic del departament, subordinat al pla estratègic de l'organització, i vetllar-lo.
c) Detecció de les necessitats.
d) Concreció de les necessitats amb el personal de l'organització.
e) Supervisió dels projectes de programari.
f) Actuar i respondre davant de situacions que comprometin la seguretat del sistema.

Solucionari

Exercicis d'autoavaluació

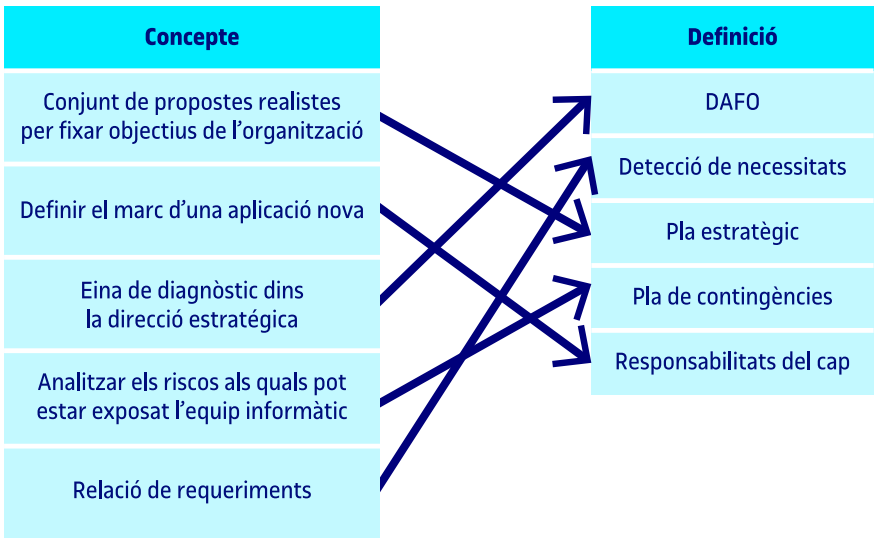
1. És habitual entre els intrusos intentar entrar a servidors web. Quan ho han aconseguit una vegada es donen per satisfets i no ho intenten més. Per tant, el millor seria restaurar la pàgina inicial, mirar els fitxers de *log* i fer una recerca al sistema per comprovar que no han canviat res més, i finalment buscar el forat de seguretat i tapar-lo. Aquesta acció pot comportar diversos dies de feina. Com que sembla que mentre es fa això es torna a atacar el servidor per segona vegada, possiblement intenten provocar l'administrador, però ja no és clar què busquen, perquè no és el procediment habitual. Per tant, possiblement el millor, en aquest cas, és tornar a posar la pàgina inicial, però paral·lelament començar a buscar els fitxers de *log*, registrar les accions, activar elements que registrin les accions i veure què passa. Quan els intrusos ataquen per tercera vegada, és molt clar que busquen alguna cosa. Segurament creuen que hi ha informació sensible com, per exemple, números de targetes de crèdit o qüestions similars i, per tant, és possible que l'atac no estigui limitat a la substitució de la pàgina inicial del servidor, sinó que pretenguin anar més lluny. En aquest punt, com que ja estarem previnguts, registrarem les seves accions fins on vulguem, ja que ara es tracta que ells no sàpiguen que nosaltres sí que sabem que són dins la màquina, i posarem en marxa tot el dispositiu de registre d'accions. Quan tanquem i assegurem el servidor és perquè tenim tota la informació del que fan que considerem necessària per poder-los localitzar. Quan es torni a obrir el servidor, ja estarà arreglat i assegurat. Ells ja sabran que nosaltres tenim coneixement que han entrat i, possiblement, no ho tornin a provar. Si ho fan, serà per un altre lloc o per alguna porta amagada que hagin deixat abans, però no pel mateix lloc. Però nosaltres ja tindrem informació suficient per actuar davant la policia en contra seva (i ells no ho saben).

2. Argumentem-ho una mica.

a) Fals. Moltes sí que venen del CAU, però no totes. Per exemple, hi ha necessitats generades per la direcció.
b) Fals amb condicions. Sempre que parlem d'una aplicació gran. Un programa a mida té un cost elevat respecte a un programa estàndard. El temps de fer-lo també és molt gran. La qüestió de la facilitat de modificació és una qüestió negociada. Podria ser cert si l'organització té un departament de desenvolupament propi, de manera que llavors és un projecte intern de la mateixa organització.
c) Fals. Per exemple, en el cas d'un projecte informàtic, s'estableix el marc sobre el qual es farà l'aplicació. En la definició de necessitats també fa d'interlocutor amb les persones implicades. Ha de tenir grans coneixements tècnics.
d) Fals. Sempre depèn de la grandària de l'organització i del seu pla estratègic. El programari ha d'estar dimensionat per a l'organització i les seves expectatives futures. En principi, és informació que posseeix el responsable d'informàtica.

3. c

4.



5. a

Glossari

actiu *m* Recurs del sistema d'informació o relacionat amb aquest, necessari perquè l'organització funcioni correctament i assoleixi els objectius proposats per la direcció.

amenaça *f* Esdeveniment que pot desencadenar un incident a l'organització, produint danys o pèrdues materials o immaterials en els seus actius.

DAFO *f* Vegeu **debilitats, amenaces, fortaleses, oportunitats**.

debilitats, amenaces, fortaleses, oportunitats *f pl* Tècnica de diagnòstic per a l'anàlisi interna d'una organització. Són les sigles que es posen en una matriu 2 × 2.
sigla: DAFO

logotip *m* Imatge corporativa que identifica una organització. Des del punt de vista informàtic, normalment és un fitxer gràfic.

monousuari *adj* Dit del programari en què només pot treballar un usuari cada vegada. Aquest adjectiu no indica res sobre la tecnologia del programari (com està fet, si està en un servidor, ni on es guarden les dades).

multiplataforma *adj* Dit del programari estàndard que pot funcionar en arquitectures diferents.

multiusuari *adj* Dit del programari en què poden treballar diversos usuaris a la vegada. Aquest adjectiu no indica res sobre la tecnologia del programari, malgrat que sembla clar que les dades estan centralitzades en algun lloc comú al qual accedeixen tots els usuaris quan treballen concurrentment.

parametrització *f* Acció d'ajustar un programari estàndard a les necessitats particulars de l'organització mitjançant una configuració, que pot ser per mitjà de fitxers, finestres, un programa, etc.

PDCA *m* Model PDCA (*plan-do-check-act*). Planificar, fer, verificar, actuar. És la base dels SGSI.

risc tecnològic *m* La ISO defineix el risc tecnològic com la probabilitat que esdevingui una amenaça usant vulnerabilitats existents d'un actiu o actius i generant pèrdues o danys.

risc *m* Possibilitat que una amenaça es materialitzi.

Bibliografia

Barcelo García, M.; Pastor i Collado, J. (1999). *Gestió d'una organització informàtica*. Barcelona: Universitat Oberta de Catalunya.

Microsoft Corporation (1997). *Windows NT 4.0 Workstation Kit de Recursos*. Madrid: Mc Graw Hill.

Ministerio de Administraciones Públicas (2006). *Metodología de Análisis y Gestión de Riesgos MAGERIT*. Madrid: BOE.

Pfleeger, C. (1997). *Security in Computing*. Estats Units: Prentice Hall.

Piattini, M.; Calvo-Manzano, J.; Cervera, J.; Fernández, L. (1996). *Análisis y diseño detallado de Aplicaciones Informáticas de Gestión*. Madrid: Ra-Ma.

Tena Millán, J. (1989). *Organización de la empresa: Teoría y aplicaciones*. Barcelona: EADA.