El sistema informàtic dins l'organització

El responsable d'informàtica

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190188

UOC
Universitat Oberta de Catalunya

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 en el futur. Ha de gestionar aspectes com el pla estratègic i el pla de seguretat informàtic, que avui dia es poden implementar amb metodologies estàndard.

També donem al mòdul alguns criteris que poden ajudar a prendre decisions, per exemple, en el moment de decidir sobre la implantació de programari, o com s'ha d'actuar davant de problemes de seguretat.

Objectius

En els materials didàctics d'aquest mòdul presentem els continguts i les eines per a 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. Conèixer el concepte de pla en una organització i conèixer-ne alguns dels que hi pot haver.

5. Conèixer els principals plans de seguretat i mètodes estàndard de gestió del risc.

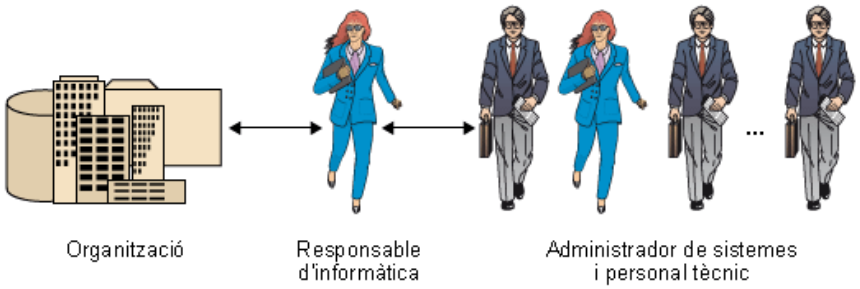
6. Saber preveure les possibles amenaces i riscos que poden posar en perill el sistema informàtic i preparar-se per a minimitzar-ne les conseqüències.

1. El responsable d'informàtica

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

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 en el gràfic, la figura del responsable d'informàtica és qui gestiona els recursos del departament (tant humans com materials). Per tant, ha de tenir un coneixement de l'organització i del departament perfecte per a aconseguir que tots dos elements es moguin com més sincronitzadament millor. Ha d'aconseguir que el departament d'informàtica s'ajusti al màxim als objectius de l'organització amb els recursos que aquesta última li dóna. En la pràctica és sempre un canal de comunicació en els dos sentits per a detectar necessitats, aconseguir recursos, ajustar objectius, etc.



El responsable d'informàtica fa de pont

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

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 a prendre moltes decisions sobre programari i maquinari. En la pràctica, la majoria de decisions tècniques es prenen amb l'ajut de l'administrador de sistemes.

Així, el responsable d'informàtica tindrà la visió més tècnica, i també les seves necessitats la visió del pla estratègic de l'empresa i, per tant, el vessant més relacionat amb la gestió de la informàtica. Molts cops no podrà accedir a les peticions d'un d'aquests grups pels requisits que tingui de l'altre grup.

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, en què s'estableix l'orientació de l'organització per a 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 a 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. El d'un departament parteix del pla estratègic de l'organització.

2.1.1. La planificació estratègica

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

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

La planificació estratègica, per a minimitzar riscos i maximitzar 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 a identificar les **oportunitats** i **amenaces**. La informació interna permet d'identificar les **fortaleses** i **debilitats** de la mateixa organització.

Vegeu també

Vegeu al subapartat 2.1.4. com es fa una 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 esmentem els components d'un pla estratègic:

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

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

- **Problema estratègic general**. Determinar factors interns o externs que poden afectar la consecució de la missió.

- **Solució estratègica general**. Donar estratègies que permetin d'assolir la missió i superin, per tant, 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 a 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.

2.1.4. L'anàlisi DAFO

En els darrers anys l'anàlisi DAFO[1] 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.

(1)DAFO és la sigla de *debilitats, amenaces, fortaleses i oportunitats*. En anglès, SWOT: *strengths, weaks, oportunities and threats*.

L'objectiu és concretar en una taula l'avaluació dels punts forts i dèbils 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 d'identificar i mesurar els **punts forts**, els **punts dèbils**, 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 què 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, fem el gràfic que recull les possibles estratègies. En aquesta matriu DAFO, en les columnes establirem l'**anàlisi de l'entorn** (1a. columna: amenaces, 2a. columna: oportunitats) i en les files, el **diagnòstic de l'organització** (1a. fila: punts forts, 2a. fila: punts dèbils). Cadascun dels quatre quadrants reflecteix les possibles estratègies que ha d'adoptar l'organització.

DAFO	Amenaces	Oportunitats
Punts forts	Estratègies defensives	Estratègies ofensives
Punts dèbils	Estratègies de supervivència	Estratègies de reorientació

L'estudi de la matriu es fa mirant aïlladament cada quadrant. Per exemple, si ens mirem el primer quadrant (1-1 punts forts-amenaces) haurem d'identificar cadascun dels punts forts que hi ha en l'organització, juntament amb cadascuna de les amenaces de l'exterior que té. Així, doncs, hem d'analitzar cada intersecció per a veure les conseqüències i les accions que se'n poden derivar.

2.2. Pla de seguretat i anàlisis de riscos

El pla de seguretat i anàlisis de riscos 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.

L'ISO defineix el risc tecnològic com la probabilitat que s'esdevingui una amenaça usant vulnerabilitats existents d'un actiu o actius generant pèrdues o danys. D'acord amb aquesta definició, hi ha diversos elements en joc (amenaces, vulnerabilitats, actius...), i per tant hi ha moltes maneres d'enfocar el risc. Nosaltres ho farem basant-nos en el pla de prevenció de riscs laborals. Es fonamenta en la idea que la seguretat és part d'un mecanisme global de tres components:

Observació

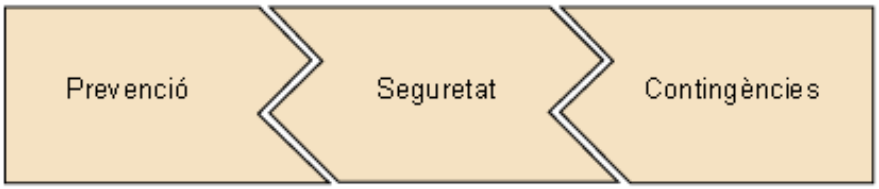
El mecanisme del pla de prevenció s'aplica a molts altres sectors amb altres noms com plans de prevenció i evacuació, plans d'emergències, etc.

1) Prevenció. L'objecte d'interès en aquest component rau en el que es desitja protegir. És necessari esbrinar què ens interessa protegir i quines solucions hi ha per protegir el nostre sistema.

2) Seguretat. En aquesta fase hem "d'implementar" la seguretat. Aquest és el pla de seguretat, és a dir com protegirem.

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

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 (en qualsevol mitjà d'emmagatzematge). Es tracta d'analitzar què pot passar i què volem protegir.

A l'**anàlisi de riscos** és necessari assegurar-se que es tenen en compte totes les possibles causes de riscos que poden provocar problemes en el sistema. Es fa una anàlisi dels riscos, que es basa a calcular la possibilitat que tinguin lloc fets problemàtics, s'obté una valoració econòmica de l'impacte d'aquests successos negatius i es contrasta el cost de la protecció amb el fet de tornar-la a crear o a comprar. Aquesta operació es repetirà amb la resta dels "actius" (equips informàtics per exemple).

- Imaginar-se què pot passar (què pot anar malament).
- Estimar el cost que comportaria per a l'organització.
- Estimar la probabilitat que es doni cadascun dels problemes possibles. Això permet de 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?
- Amb quina freqüència pot passar?
- Quines serien les conseqüències?

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

- Què s'intenta de protegir?
- Quin valor li dóna l'organització?

- De què es vol protegir?
- Quina és la probabilitat d'un atac?

El procediment per a 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 a tractar a quins riscos en seguretat informàtica ha de fer front l'organització. Una vegada s'ha fet la relació, s'ha de veure com es pot actuar per a prevenir les causes i com cal actuar per a minimitzar-ne els efectes.

Riscos de seguretat

Alguns dels riscos que una organització pot haver d'afrontar són:

- Al foc, que pot destruir equipament i informació.
- Al robatori d'equipament i arxius.
- A actes vandàlics que malmetin equipament i arxius.
- A fallades en l'equipament que fan malbé arxius.
- A errades que malmeten arxius.
- A virus, que malmeten equipament i arxius.
- A accessos no autoritzats, que comprometen la informació.

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

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

Quina probabilitat hi ha que el foc destrueixi l'equipament i informació.

- L'organització té alguna protecció contra incendis?
- Són necessaris sistemes d'aspersió automàtica?
- Calen extintors? N'hi ha?
- Són necessaris detectors de fums? N'hi ha?
- El personal té alguna formació per a actuar davant d'un incendi?

Quina probabilitat hi ha que les fallades de l'equipament malmetin la informació?

- El personal informàtic duu a terme el manteniment dels equips dins els temps previstos?
- Quines són les condicions actuals del maquinari?

3) S'ha de determinar la probabilitat per a cada risc: molt alt, alt, mitjà, baix, molt baix

4) Es fa el resum dels riscos ordenats pel factor de risc de cadascun.

Tipus de risc	Factors de risc
Robatori	Alt
Fallades en equipament	Mitjà
Acció de virus	Mitjà
Robatori de dades	Baix
Foc	Baix
Frau	Molt baix

Anàlisi dels punts dèbils 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 a accedir al sistema. Això es pot aplicar tant a portàtils com a ordinadors amb placa de xarxa (Wi-fi 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?

Es fa el tancament físic de les portes per evitar el robatori?

Es manté la porta principal sempre tancada per a evitar el vandalisme?

Respecte del 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 (*sharewa-re*), només es fan servir si provenen de llocs fiables?

La prevenció o Pla de prevenció es porta a terme a través 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.

A través 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 a través 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 deixar el sistema informàtic 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 en el 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 a assegurar que el nostre sistema es manté segur.

Així que hem de suposar que podem patir un incident de seguretat en qualsevol moment i hem de preparar-nos per al cas "pitjor". Per tant és necessari preveure les accions i 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 com més aviat millor i minimitzar el cost i les pèrdues en la mesura que 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 còpia de seguretat. Aquesta informació serà dins del sistema de còpies i, possiblement, dins del Pla de recuperació de desastres.
- També preveurem els incidents, com per exemple, fallades de maquinari o programari que poden deixar inutilitzat totalment o parcialment el sis-

Còpies de seguretat

Ja que les còpies de seguretat contenen informació sensible, gairebé sempre han de "complir" les polítiques de còpia que s'hagin fixat a l'organització (dins del pla de seguretat), i han de complir també la legislació vigent, en aquest cas una d'elles és la Llei orgànica de protecció de dades personals (LOPDP).

Vegeu també

Recordeu que hem estudiat la Llei orgànica de protecció de dades personals al mòdul "Administració de la seguretat".

tema informàtic, i confeccionarem els protocols a seguir davant d'aquest tipus de situacions.

2.3. Sistemes de gestió de seguretat de la informació

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

Terminologia

El sistema de gestió de la seguretat de la informació també és conegut com a projecte de gestió de la seguretat, projecte integral de seguretat, projecte de seguretat, sistema de seguretat...

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:

Observació

Sota la sigla de SGSI s'intenta recollir tant els models com els mètodes de gestió de la seguretat de la informació.

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

[(2)]SGSI és la sigla de *sistema de gestió de la seguretat de la informació.*

En els SGSI[2] 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 en l'organització i produir 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.

Model PDCA

La base per al desenvolupament, implementació i funcionament d'un SGSI es pot resumir en quatre "tasques" repetitives: planificar, fer, verificar i actuar. És l'anomenat *model PDCA* (*plan – do – check – act*). És la base dels SGSI.

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, bàsicament el MAGERIT i la metodologia que incorpora l'estàndard ISO 27001:2005.

2.3.1. MAGERIT

El MAGERIT[3] és un mètode formal per a 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.

MAGERIT consta de quatre fases:

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

2) Anàlisi de riscos. Es fa una estimació de l'impacte que tindran els riscos en 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. Se seleccionen possibles solucions per a cada risc. Són fonamentals els exercicis de simulació.

4) Selecció de salvaguardes. Es trien els mecanismes que implementaran les solucions elegides en la fase anterior.

2.3.2. ISO/IEC 27001:2005

El 15 d'octubre de 2005 neix l'estàndard ISO 27001:2005, que substitueix el BS 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 a establir, implantar, mantenir i millorar un sistema de gestió de la seguretat de la informació segons el model PDCA[4]. 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 en les organitzacions a través d'un procés formal d'auditoria.

(3)MAGERIT és acrònim de metodologia d'***a**nàlisi i **ge**stió de **ri**scos de les **a**dminis**t**racions públiques.*

Adreça recomanada

Per Internet podeu trobar i baixar [accessible en línia] la documentació sobre la metodologia MAGERIT.

Adreça recomanada

Podeu consultar la norma ISO/IEC 27001 per Internet.

(4)El model PDCA també és conegut com a Cercle de Deming.

L'ISO/IEC considera l'organització com una totalitat i té en compte tots els possibles aspectes que es poden veure afectats davant dels possibles incidents que es poden produir. L'esmentada norma està estructurada en **onze dominis de control** que cobreixen completament la gestió de la seguretat de la informació, on cada un es refereix a un aspecte de la seguretat de l'organització:

1) Política de seguretat.
2) Aspectes organitzatius per a la seguretat.
3) Classificació i control d'actius.
4) Seguretat del personal.
5) Seguretat física i de l'entorn.
6) Gestió de comunicacions i operacions.
7) Control d'accessos.
8) Desenvolupament i manteniment de sistemes.
9) Gestió d'incidents de seguretat de la informació.
10) Gestió de continuïtat del negoci.
11) Conformitat legal.

La norma pretén aportar les bases per a tenir en consideració tots els aspectes que poden suposar un incident en les activitats de l'organització.

3. Detecció de necessitats de programari en l'organització

Per què es necessita programari nou? Respondre aquesta pregunta és gairebé una qüestió filosòfica. En essència, una organització és una entitat "viva" (en un sentit ampli). Això vol dir que les seves necessitats varien al llarg del temps i, per tant, les necessitats informàtiques també. Més concretament, un programari pot tenir errors, o bé apareixen noves versions i es queda antiquat, o a alguna persona se li acuden coses noves que millorarien el rendiment o la producció, o canvia l'equip directiu o la cadena de producció, o el mètode d'administrar o les lleis, i s'han de modificar els programes comptables, o l'organització és absorbida per una altra de més important que treballa d'una manera molt diferent, o es canvia completament el departament de màrqueting i vendes, etc. I tot això són necessitats que poden motivar canvis profunds en el programari que hi ha o bé fer que s'hagi de comprar programari nou.

Veure aquesta necessitat, la importància que pot tenir per a l'organització i l'impacte que pot representar per al sistema informàtic requereix un cert temps. Bàsicament passa per les etapes següents:

1) Detecció de necessitats.

2) Concreció del problema.

3) Anàlisi de la solució del problema.

Quan la informàtica està implantada en una organització, en més o menys grau, sempre hi ha necessitats noves.

3.1. Detecció de necessitats

Sovint una necessitat és molt evident, i altres vegades és molt difícil de detectar. Pot provenir de moltes fonts, algunes de les quals poden ser les següents:

- Des del centre d'atenció a l'usuari (CAU). Per tant, a partir dels usuaris que facin peticions.
- Des del centre d'atenció a l'usuari (CAU), mitjançant queixes reiterades.
- Des de qualsevol lloc de l'organització que vol alguna cosa, sense saber si és possible o no tècnicament.

- Des del mateix departament d'informàtica, per a millorar el servei.
- Des del mateix departament d'informàtica, per a millorar el rendiment.
- Des de qualsevol punt extern a l'organització, però que hi interacciona i té problemes.
- Des de la direcció, per a analitzar relacions interorganització i intraorganització.
- La mateixa organització, per a evolucionar.
- El mateix sector informàtic / de telecomunicacions, que evoluciona tecnològicament.

El més important quan s'ha detectat una necessitat és avaluar si es pot dur a terme o no. Aquesta tasca recau en el responsable d'informàtica, que depenent de la necessitat pot treballar amb l'administrador de sistemes i elaborar un informe de costos i temps per a valorar si s'engega el projecte o no. El responsable d'informàtica amb el consell directiu de l'organització, si són projectes de molta grandària, o amb l'administrador de sistemes, si són petits, decideixen la forma que se'ls ha de donar.

L'aparició d'una necessitat que ha de cobrir el departament d'informàtica pot venir per moltes vies.

3.2. Etapa de concreció

Ja s'ha detectat una necessitat. Malgrat això, moltes vegades és una qüestió difusa. La persona o les persones que l'han generat saben més o menys què volen (molt poques vegades saben exactament què volen), però a més a més, en no ser experts en informàtica, i en no tenir coneixement de l'estructura informàtica de l'organització (no n'han de tenir necessàriament), l'expressió de la seva necessitat és difusa. Tot i que l'expressen amb claredat (moltes vegades ells mateixos creuen que s'expressen clarament), la "traducció" del que diuen, del que volen, etc. en termes informàtics, i en termes de l'estructura informàtica de l'organització, no és gens evident.

Per tant, en aquesta etapa és necessària una tasca, que és responsabilitat generalment del responsable d'informàtica: la concreció de la necessitat. El responsable d'informàtica ha d'establir converses, fer reunions, etc. amb les persones que demanen la solució, perquè concretin i formalitzin el seu problema i la seva necessitat, i es pugui engegar un estudi o pla de viabilitat per part del departament d'informàtica. També és possible que en aquesta etapa hi prengui

part en algun moment alguna figura tècnica, que una vegada més acostuma a ser l'administrador de sistemes, tot i que depèn molt de la necessitat que s'hagi generat.

En aquesta etapa recollirem, a més a més, documents, papers, esquemes, etc., si és possible. Cal, però, tenir present que moltes vegades totes aquestes necessitats que apareixen costen molt de definir i de precisar, per la qual cosa és possible que tota la valoració inicial la fem sense saber gaire exactament què es vol.

És molt difícil concretar una necessitat. La comunicació amb totes les persones i departaments relacionats directament o indirectament amb la necessitat pot ser clau per a concretar el problema.

3.3. Etapa d'anàlisi

Després d'haver parlat en l'etapa anterior per a saber què es vol, en el departament d'informàtica es fa un primer estudi de viabilitat del projecte, per a determinar com pot encaixar en el sistema informàtic actual o quina seria la millor manera de solucionar el problema plantejat. Això és responsabilitat del responsable d'informàtica, sobretot pels aspectes de recursos econòmics i humans, i l'aspecte tècnic és una tasca conjunta del responsable d'informàtica i l'administrador de sistemes, o la figura tècnica que sigui necessària segons la necessitat plantejada.

Prepararem un **informe tècnic preliminar** en el qual es comentaran els aspectes de maquinari, programari, recursos humans, econòmics i de temps, d'una manera aproximada (en cas que sigui viable). Si la direcció decideix engegar-lo ja es farà una anàlisi ben feta, correcta i a fons del problema.

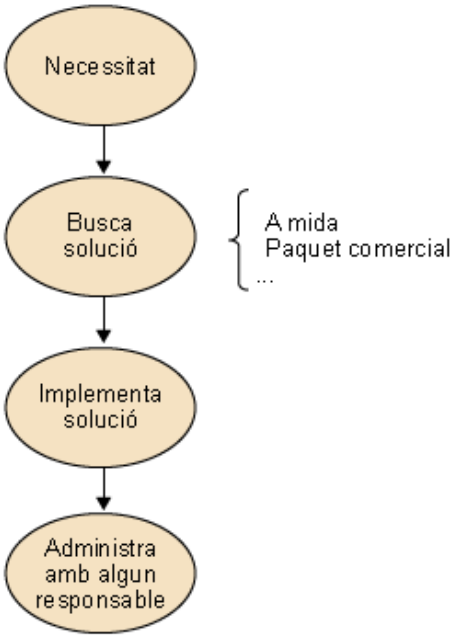
Determinar exactament una necessitat és molt important per a avaluar l'impacte que pot tenir en l'estructura informàtica i en la mateixa organització.

4. Implantació/disseny d'aplicacions

En una organització, com a conseqüència de canvis interns (noves orientacions) o canvis externs, o simplement per millora del funcionament, pot aparèixer una necessitat. 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 les següents decisions:

- Modifiquem el programari que tenim (si podem)?
- Comprem programari estàndard?
- Ens creem un programari a mida?

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



Implementació de programari

Ens hem d'adonar que tots els passos els fan figures tècniques, però amb la supervisió de la figura del responsable d'informàtica, que és qui pren les decisions, en estreta coordinació amb les figures dels administradors (tècnics).

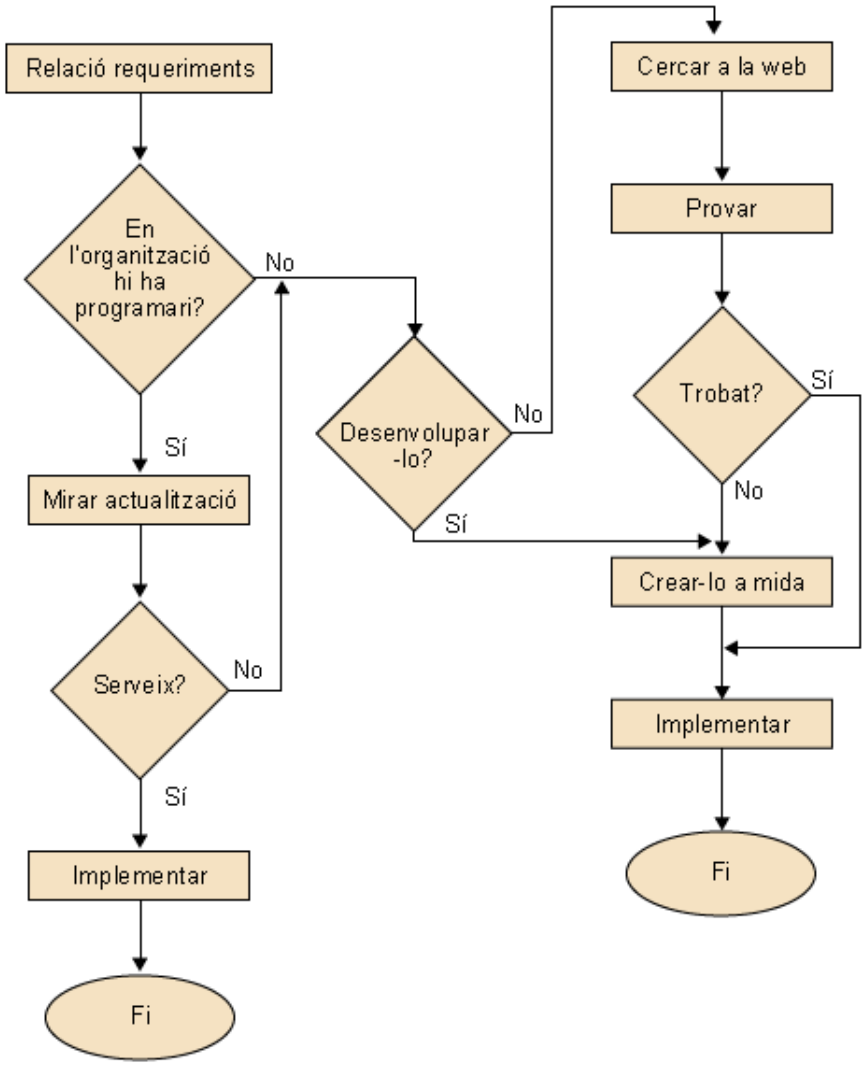
Quan es detecta una necessitat, és el responsable d'informàtica qui pren les decisions finals sobre si es pot satisfer o no. Solucionar-la té un cost i, per tant, s'ha de veure si es pot dur a terme. El responsable d'informàtica coneix el pla estratègic de l'organització, els recursos econòmics, humans, etc. de què dis-

posa. És important que el responsable d'informàtica tingui prou coneixements d'informàtica tècnica per a entendre tota la problemàtica que poden tenir els tècnics a l'hora de fer la feina de cada dia.

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

Mètode d'implantació de programari



Cadascun d'aquests passos és força complex i el responsable d'informàtica, conjuntament amb l'administrador de sistemes, treballen plegats per a dur a terme aquesta tasca.

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

4.1. Relació de requisits

La decisió la prendrà el responsable d'informàtica, però la tasca d'elaborar aquesta relació de requisits és conjunta del responsable d'informàtica i l'administrador del sistema.

Després, doncs, que l'informe tècnic preliminar hagi passat per direcció i s'hagi decidit engegar el projecte, el responsable d'informàtica, juntament amb l'administrador, marca els requisits mínims que ha de complir el programari. Els aspectes bàsics que ha d'incloure aquesta relació han de contenir:

- Els servidors actuals. Si són heterogenis, on hi ha d'haver l'aplicació. Poden canviar en un futur pròxim (plans d'actualització, pla estratègic, etc.).

- Els clients. Són o poden ser heterogenis (plans d'actualització, pla estratègic, etc.). Cada vegada més hi ha portàtils en determinats departaments. S'ha de preveure la possibilitat de clients de diferents plataformes o tipus.

- Connexions remotes/xarxa. Com i des d'on s'ha de poder accedir a l'aplicació. Qüestions associades a xarxes locals, intranets, extranets, etc.

- Informació pública/privada
  - Cal fer parcialment visible l'aplicació?
  - És necessari extreure (exportar) dades per a fer-les públiques o per a introduir-les en altres programaris de l'organització?

- Qüestions de seguretat associades a la xarxa, la informació, l'aplicació.

- Com i quins usuaris poden accedir a l'aplicació? Els usuaris tenen nivells de seguretat o veuen tota l'aplicació quan han entrat? Poden modificar qualsevol informació? Poden imprimir qualsevol llistat?

- També és convenient plantejar-se la qüestió de configuració/parametrització, especialment en llistats. El temps fa que sigui necessari canviar elements com, per exemple, el "logo" de l'organització.

Programari ajustat a les necessitats

Aquí hem parlat d'un programari multiusuari, en servidor, amb usuaris configurables, amb propietats per a les xarxes i facilitats per a extreure'n dades, possiblement multiplataforma en la part client, etc. I segurament per a una organització d'una certa mida és el que cal. Ara bé, si la nostra organització és de cinc persones (per exemple, un taller mecànic o una botiga), moltes d'aquestes característiques no són necessàries. Segurament amb un programari monousuari que funcioni sobre una sola màquina (si té usuaris millor), amb llistats configurables, que pugui funcionar en una xarxa, però només amb un usuari

simultani, i que funcioni correctament, és suficient per a resoldre el problema. L'altre estaria totalment sobredimensionat a les necessitats reals de l'organització, i tindria un cost massa elevat. Els mateixos fabricants de programari fan moltes vegades el mateix programa en diferents "mides" i preus, segons l'organització a què es destina.

Amb la relació de requisits, ens hem de plantejar la qüestió de si dins l'organització hi ha un programari que faci més o menys el que es necessita funcionalment.

Saber què cal tècnicament per a resoldre el problema i per a integrar-lo en l'estructura de l'organització és el primer pas.

4.2. L'actualització

Es tracta que veiem si actualitzant algun programari del que hi ha en l'organització n'hi ha prou per a 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 mirar les característiques de l'última versió del programari en paper o via web, o tan complexa com haver de demanar un CD-ROM de demostració i necessitar un ordinador de prova per a instal·lar i fer una simulació per a veure si s'ajusta als requisits demanats per a resoldre el problema.

Busquem si algun programari del que tenim ens serveix.

4.3. Programari estàndard

L'opció del programari estàndard representa que de moment no volem desenvolupar programari propi, i es busca un programari que ja hi sigui i que s'ajusti a les necessitats que es volen cobrir. Per tant, hem de mirar, de tots els programaris que hi ha en el mercat, quin s'adapta a les necessitats que té l'organització. És una tasca que pot fer l'administrador de sistemes, però que ha de supervisar força el responsable d'informàtica, ja que és qui pren la decisió final. Actualment els programaris són força parametritzables i, per tant, la tasca de veure 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 bastant segur que el proveïdor que ens el proporciona té una estabilitat prou bona per a 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 en servidors, i després implantar-lo en els usuaris, formar-los, etc. perquè no sigui problemàtic.

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

Busquem programari que ja està fet, tenint en compte que haurem de posar programari nou dins l'organització, amb totes les conseqüències que s'hi associen.

4.4. Programari a mida

La segona possibilitat implica posar en marxa un projecte de programari, un departament de desenvolupament de programari, una anàlisi, etc. Per tant, és força més complex per a obtenir al final un paquet ajustat a les necessitats de l'organització. Una vegada s'ha fet, generalment no s'acaba, ja que com que l'organització és una entitat "viva", necessita modificacions pràcticament constants. 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 de 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 donar 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 de ser present en tot el procés de creació de l'aplicació. Segurament el responsable d'informàtica és qui haurà de prendre 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.

4.5. 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 de ser 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.).
- Grau de sensibilitat de les dades.
- Nivell d'integració de les dades amb la resta d'aplicacions.
- S'han de fer públiques part d'aquestes dades en el web de l'organització?
- Cal exportar dades?

Per tant, ens hem de tornar a plantejar una taula de solucions.

		Dades	
		Local	**Remot**
Aplicació	**Local**		
	Remot		

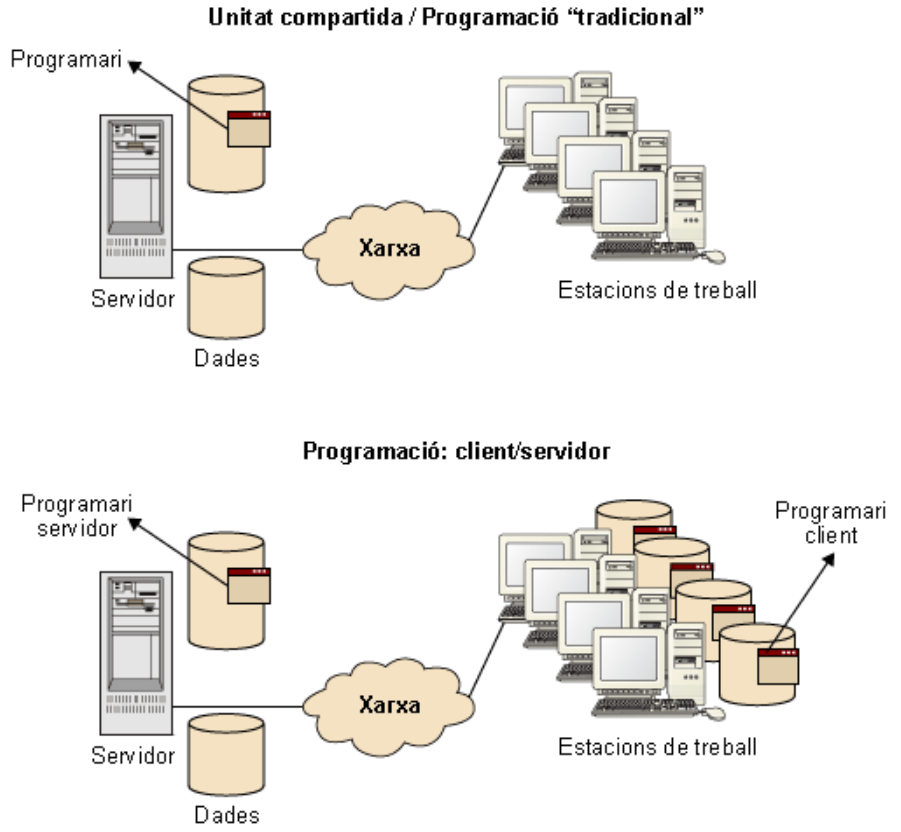
En el cas de les **dades en remot** probablement decidirem que les dades siguin en una base de dades en un servidor. Això facilita les còpies de seguretat, el manteniment i la implantació, especialment si a l'organització ja hi ha un servidor de bases de dades. També facilita la integració i les cerques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

En el cas del **programari en remot** estem davant de dues alternatives possibles:

1) Implantar un programa "tradicional" fet perquè pugui córrer en el client o en el servidor, o un programa amb tecnologia client/servidor que necessita una petita part instal·lada en el client.

2) Aprofitar la tecnologia client/servidor per a crear una aplicació en què el programa client ja estigui instal·lat en les estacions de treball, per exemple, un navegador. És el cas de les arquitectures en què el *front-end* (ordinador frontal) és un navegador que fa de client i el servidor web ataca les bases de dades. Al mig hi ha l'aplicació servidora real.

Tipus de programari remot

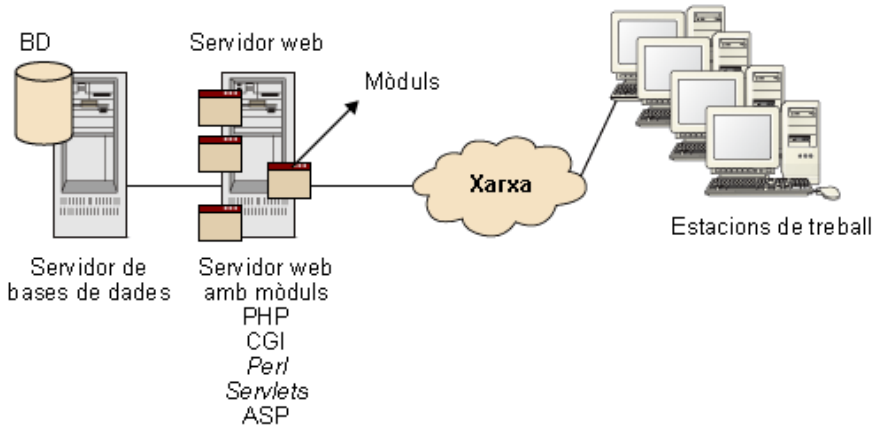


Els avantatges del programari en remot són:

- 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 sobre un servidor segur (HTTPS).
- Normalment es programa per mòduls i no monolíticament.

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

Esquema d'estructura de programari remot



Com que l'aplicació està en mòduls, el manteniment i el creixement són més senzills, i atès que les dades són 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 per a traspassar. La seguretat és més elevada.

Vegeu també

Vegeu els mòduls "Administració del web" i "Administració de la seguretat".

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 de recursos per a tirar endavant el projecte.

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.

5. Aspectes legals de l'administració de xarxes

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.

5.1. 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.

Cada cas pràcticament 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 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.

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 per a poder verificar que realment aquesta persona fa un ús indegut del sistema. Una vegada engegats els procediments legals, les figures tècniques poden dur a terme els mecanismes informàtics i tècnics necessaris per a 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.

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-:

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

Vegeu també

Vegeu en el mòdul "Administració de la seguretat" quins són els passos.

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

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

- Els administradors de sistema elaboren un informe exhaustiu sobre el que ha passat i aporten tota la informació que considerin necessària en format CD-ROM. Aquest informe ha de contenir què ha passat, com s'ha donat 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 a solucionar el problema (des del punt de vista tècnic).

- Un informe dels administradors i el responsable d'informàtica que conté els danys ocasionats en el 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.

- 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), el CD-ROM 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 és necessari, penalment.

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

- 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 en el sistema. Com acabem de dir, aquesta acció l'engega el responsable d'informàtica i la porten a terme els administradors de sistema. Aquests passos estan descrits en l'apartat "Administració de la seguretat".

Vegeu també

Vegeu en el mòdul "Administració de la seguretat" quins són els passos.

- Al mateix temps, el responsable d'informàtica informa el cos de policia adient per a 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).

- 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 al següent:
  - Restaurar el sistema.
  - Recuperar la informació de còpies de seguretat.
  - Assegurar el sistema, si és necessari. Això significa afegir pedaços de 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 en el 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, per a estar segurs de no perdre cap prova important. D'aquesta manera el servidor afectat torna a estar operatiu com més aviat millor.

- Els administradors de sistema elaboren un informe exhaustiu sobre el que ha passat i aporten tota la informació que considerin necessària en format CD-ROM. Aquest informe ha de contenir què ha passat, com ha estat 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 a solucionar el problema (des del punt de vista tècnic).

- Un informe fet pels administradors i el responsable d'informàtica que conté els danys ocasionats en el 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.

- 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), el CD-ROM 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 i després judicialment i, finalment, si és necessari, penalment.

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

5.2. Aspectes legals del programari a mida

Moltes vegades el programari a mida es contracta a companyies que no pertanyen a la mateixa organització. Aquestes companyies fabriquen 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 "saber fer[5]", 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 un projecte perquè hi hagi alguna via per a poder mantenir l'aplicació en cas que no ho faci la companyia que l'ha creat.

[5]En anglès, *know-how.*

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.

6. Tasques del responsable d'informàtica

Una relació aproximada de les tasques/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-la.
- Detecció de necessitats.
- Concreció de necessitats amb el personal de l'organització.
- Decisió d'implantar 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.

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 de preveure què pot passar per a prendre mesures per a minimitzar-ne les conseqüències. Des de com evolucionarà la informàtica per a adaptar-se fins a com cal reaccionar davant d'un desastre.

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

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

Quan es necessita programari nou, intentem d'anar per 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 dialogador, un bon cap, tenir visió de futur, tenir capacitat de previsió i moltes altres qualitats més que cauen fora de l'abast d'aquests materials.

Exercicis d'autoavaluació

1. Han entrat en el 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 en servidor, perquè no se sap mai com creixerà l'organització.

3. Quina d'aquestes frases sobre la implantació d'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 a crear-nos el programari a mida.
d) La relació de requisits ens serveix en tot el procés.

4. Relacioneu el concepte amb la definició.

Definició
Conjunt de propostes realistes per a fixar objectius de l'organització
Definir el marc d'una aplicació nova
Eina de diagnòstic dins la direcció estratègica
Analitzar riscs als quals pot estar exposat l'equipament informàtic.
Relació de requeriments

Concepte
DAFO
Detecció de necessitats
Pla estratègic
Pla de contingències
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-la.
c) Detecció de necessitats.
d) Concreció de 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 corrent entre els intrusos intentar d'entrar en 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 en el sistema per a 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 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 a 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 a actuar policíacament en contra seva (i ells no ho saben).

2. Argumentem-ho una mica:

a) Fals. Moltes sí que vénen del CAU, però no totes. Per exemple, hi ha necessitats generades per la direcció.

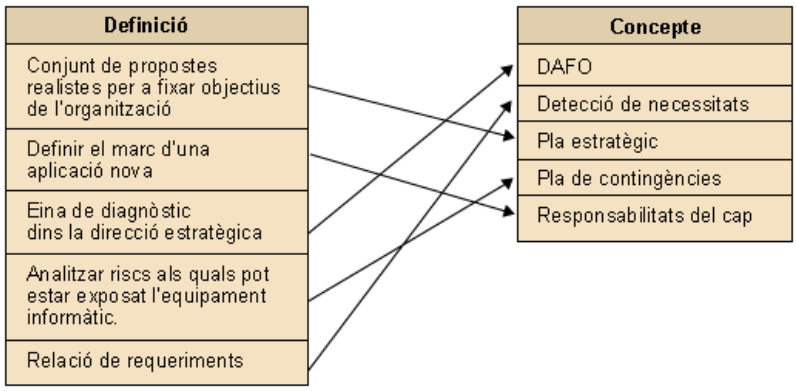
b) Fals amb condicions. Sempre que parlem d'una aplicació gran. Un programa a mida té un cost elevat respecte a un programa estàndard. El temps de fer-lo també és molt gran. La qüestió de la facilitat de modificació és una qüestió negociada. Podria ser cert si l'organització del departament té un desenvolupament 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 mida de l'organització i del seu pla estratègic. El programari ha d'estar dimensionat en 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 en l'organització i produir danys o pèrdues materials o immaterials en els seus actius.

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

debilitats, amenaces, fortaleses, oportunitats *f* Tècnica de diagnòstic per a l'anàlisi interna d'una organització. Són les sigles que es posen en una matriu 2x2.
sigla: **DAFO**.

logo *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 és en un servidor ni on es guarden les dades).

multiplataforma *adj* Dit del programari estàndard que pot funcionar sobre 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 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* L'ISO defineix el risc tecnològic com la probabilitat que s'esdevingui una amenaça usant vulnerabilitats existents d'un actiu o actius que poden generar 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. ISBN 84-340-0960-9

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

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

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