UF0512 Transmissió d'informació per mitjans convencionals i informàtics

1. Connexió i funcionament operatiu de l'equipament informàtic

1.1 Maquinari

El maquinari (en anglès, hardware) d'un ordinador és el conjunt de les seves parts físiques. Es classifica principalment per situació (central o perifèric) i funció (entrada, sortida, entrada-sortida o emmagatzematge). Es considera l'element central del maquinari d'un ordinador la placa mare (de l'anglès, motherboard), que és un circuit imprès sobre el qual es connecten la resta de dispositius o la unitat central de processament (UCP, o CPU en anglès), que és el microprocessador principal que es troba muntat sobre un sòcol a la placa mare. La resta de circuits impresos són targetes (com ara la targeta de xarxa, o la targeta gràfica). A més dels components electrònics del maquinari central també hi ha elements electromecànics com el disc dur, la gravadora de CD o de DVD, la font d'alimentació, etc. Situats a l'exterior de la caixa hi ha els perifèrics d'entrada (teclat, ratolí, webcam, escànner, etc.) i sortida (impressora, monitor, altaveus, etc.).

1.2 Tipologia i classificacions

Una de les formes de classificar el maquinari és en dues categories: d'una banda, el "bàsic", que abasta el conjunt de components indispensables necessaris per atorgar una funcionalitat mínima a la computadora, i d'altra banda, el "maquinari complementari", que, com el seu nom ho indica, és l'utilitzat per realitzar funcions específiques (més enllà de les bàsiques), no estrictament necessàries per al funcionament de la computadora. Així és que: un mitjà d'entrada de dades, la unitat de processament i memòria i un mitjà de sortida de dades constitueix el "maquinari bàsic".

Els mitjans d'entrada i sortida de dades estrictament indispensables depenen de l'aplicació: des d'un punt de vista d'un usuari comú, s'hauria de disposar, almenys, d'un teclat i un monitor per a entrada i sortida d'informació, respectivament; però això no implica que no pugui haver-hi una computadora (per exemple controlant un procés) en la qual no sigui necessari teclat ni monitor, bé pot ingressar informació i treure les seves dades processades, per exemple, a través d'una placa d'adquisició/sortida de dades.

Les computadores són aparells electrònics capaces d'interpretar i executar instruccions programades i emmagatzemades en la seva memòria, elles consisteixen bàsicament en operacions aritmètic-lògiques i d'entrada/sortida. Es reben les entrades (dades), les hi processa i emmagatzema (processament), i finalment es produeixen les sortides (resultats del processament). Per tant tot sistema informàtic té, almenys, components i dispositius de maquinari dedicats a alguna de les funcions esmentades; a saber:

Elaborat per: Ramon López Data de supervisió: *febrer de 2015*

- Processament: Unitat Central de Procés o CPU.
- Emmagatzematge: Memòries
- Entrada: Perifèrics d'Entrada (E)
- Sortida: Perifèrics de sortida (S)
- Entrada/Sortida: Perifèrics mixts (E/S)

Des d'un punt de vista bàsic i general, un dispositiu d'entrada és el que proveeix el mitjà per permetre l'ingrés d'informació, dades i programes (lectura); un dispositiu de sortida brinda el mitjà per registrar la informació i dades de sortida (escriptura); la memòria atorga la capacitat d'emmagatzematge, temporal o permanent (emmagatzematge); i la CPU proveeix la capacitat de càlcul i processament de la informació ingressada (transformació).

Un perifèric mixt és aquell que pot complir funcions tant d'entrada com de sortida, l'exemple més típic és el disc rígid (ja que en ell es llegeix i es grava informació i dades).

1.3 L'ordinador. Tipus

Un ordinador (del francès ordinateur) o computadora (del llatí computare, calcular) és una màquina electrònica que rep i processa dades per a convertir-les en informació útil. Està formada per un conjunt de circuits integrats i d'altres components relacionats que pot executar amb exactitud, rapidesa i d'acord amb les instruccions que rep per part d'un usuari o d'un programa. Els ordinadors són aparells digitals en tant que es basen en l'àlgebra de Boole i el sistema binari. La principal característica que el diferencia d'altres màquines similars és que és una màquina de propòsit general, és a dir, que pot realitzar diverses tasques segons les possibilitats del llenguatge de programació i el hardware. El model en què es basen els ordinadors actuals és arquitectura de Von Neumann, és a dir, que utilitzen la memòria principal per emmagatzemar dades i instruccions alhora, característica que els permet executar programes diferents, sent per tant una màquina de propòsit general. Això els diferencia d'altres aparells com les calculadores no programables.

Tipus d'ordinadors

- Supercomputador, són els ordinadors amb més capacitat de càlcul i per tant els més cars, més voluminosos i escassos.
- Ordinador central, també anomenat mainframe: acostumen a formar part d'una xarxa amb altres ordinadors centrals, miniordinadors o microordinadors. A les empreses punteres, serveixen per a realitzar els càlculs que empren major memòria. Aquests càlculs acostumen a ser sol·licitats des de microordinadors pels usuaris de la xarxa.
- Miniordinador: Tots els usuaris es connecten al miniordinador. En desús, per la popularització de les xarxes i l'augment de capacitat dels microordinadors.

- Ordinador personal, categoria en què estan inclosos l'ordinador de sobretaula i l'ordinador portàtil.
- Microordinador un tipus d'ordinador personal enfocat al mercat domèstic. Eren els ordinadors més barats, més petits i més populars. També coneguts com a home computer, s'endollaven directament a la televisió.
- Microcontrolador, ordinador de poca potència i baix consum integrat en un sol xip, usat per rentadores, torradores, rellotges, etc.
- Estació de treball (workstation), similars que els PC però amb més potència. Per a professionals que usen aplicacions intensives com CAD, renderització 3D, etc.
- Telèfon mòbil, PDA i smartphone.
- Tauletes (Tablet PC)

1.4 Arquitectura bàsica d'un equip informàtic

L'arquitectura d'ordinadors és el disseny conceptual i l'estructura operacional fonamental d'un sistema de computador. És a dir, és un model i una descripció funcional dels requeriments i les implementacions de disseny per diverses parts d'una computadora, amb especial interès a la forma en la qual la unitat central de procés (CPU) treballa internament i accedeix a les adreces de memòria.

1.5 Components: unitat central de processament (CPU), memòria central i tipus de memòria

La unitat central de processament o CPU (per l'acrònim en anglès de central processing unit), o simplement el processador o microprocessador, és el component de l'ordinador i d'altres dispositius programables, que interpreta les instruccions contingudes en els programes i processa les dades. Els CPU proporcionen les característiques fonamentals de l'ordinador digital (la programabilitat) i són un dels components necessaris trobats a les computadores de qualsevol temps, junt amb l'emmagatzemament primari i els dispositius d'entrada/sortida. Es coneix com a microprocessador la CPU que és manufacturada amb circuits integrats. Des de mitjans dels anys 1970, els microprocessadors d'un sol xip han reemplaçat gairebé totalment tots els tipus de CPU, i avui en dia, el terme "CPU" és aplicat usualment a tots els microprocessadors.

L'expressió "unitat central de procés" és, en termes generals, una descripció d'una certa classe de màquines lògiques que poden executar programes complexos de computador. Aquesta àmplia definició pot fàcilment ser aplicada a molts dels primers computadors que van existir molt abans que el terme "CPU" tingués l'ampli ús que té actualment. Encara que aquest terme realment ha estat utilitzat en la indústria de la informàtica des de principis dels anys 1960. La forma, el disseny i la implementació dels CPU ha canviat dràsticament des dels primer exemples, però la seva operació fonamental segueix essent similar.

Està constituïda per dues unitats funcionals: la unitat aritmetico-lògica, i la unitat de control.

Memòria

La memòria és l'espai d'entrada/sortida que permet emmagatzemar informació en un ordinador o en dispositius electrònics en general. És un dels elements del maquinari d'un ordinador.

Actualment, quan es parla de memòria a seques ens referim a la memòria d'accés aleatori (RAM), un tipus de memòria basada en els semiconductors caracteritzada per un accés ràpid però d'emmagatzemament temporal. Igualment, quan parlem d'emmagatzemament normalment ens referim a dispositius d'emmagatzemament massiu, dispositius més lents que la memòria d'accés aleatori però d'una naturalesa més permanent.

Segons el tipus d'ús:

- Primària o principal: accés ràpid però emmagatzemament temporal, mitjançant elements electrònics semiconductors (xips) memòria d'accés aleatori (RAM).
- Secundària: accés més lent que el primari però de naturalesa permanent (sense necessitat d'alimentació). La que hi ha als discs d'emmagatzemament massiu (disc dur, discs òptics, etc.).

1.6 Perifèrics: dispositius d'entrada i sortida, dispositius d'emmagatzematge i dispositius multimèdia

Entrada/Sortida

L'E/S és la manera que té l'ordinador d'enviar i rebre informació del món exterior.

Els perifèrics d'entrada típics d'un ordinador personal són el teclat, el ratolí, la palanca de control (joystick), l'escàner, el micròfon o la càmera web. I de sortida el monitor, els altaveus o la impressora. També les xarxes informàtiques són E/S.

També es considera E/S la memòria secundària, categoria de la qual formen part tota una sèrie de dispositius d'emmagatzematge com els disquets, discs durs, CD (disc compacte), DVD, cintes, memòries flash.

Ratolí

El ratolí és un perifèric d'ordinador, generalment fabricat en material plàstic, que podem considerar, al mateix temps, com a un dispositiu d'entrada de dades i de control, depenent del programari que maneja en cada moment.

Sol estar dotat de dos o tres botons de pulsació que permeten activar fent-hi clic diverses accions depenent del botó premut (esquerre, central, dret) i de l'àrea en el que es troba la puntera. Actualment la majoria de ratolins tenen una roda central que substitueix al tercer botó, això permet més comoditat en l'ús d'algunes aplicacions (com per exemple, els processadors de text o les finestres dels navegadors d'Internet) en integrar accions relacionades amb el moviment ascendent i descendent del contingut de la pantalla.

Teclat

Un teclat de computadora és un perifèric, físic o virtual (per exemple teclats de pantalla o teclats tàctils), utilitzats per a la introducció d'ordres i dades en una computadora. Té el seu origen en els teletips i les màquines d'escriure elèctriques, que es van utilitzar com a teclats dels primers ordinadors i dispositius d'emmagatzematge (gravadores de cinta de paper i targetes perforades).

Impressora

Una impressora és un perifèric d'una computadora que permet produir una còpia permanent de textos o gràfics de documents guardats en format electrònic, imprimint en paper les dades en medis físics, utilitzant carrets de tinta o tecnologia làser. Moltes impressores són utilitzades com a perifèrics, i estan permanentment unides a la computadora per un cable.

Dispositius d'emmagatzematge

Cinta magnètica

La cinta magnètica és un tipus de mitjà o suport d'emmagatzemament d'informació que es grava en pistes sobre una banda plàstica amb un material magnetitzat, generalment òxid de ferro o algun cromat. El tipus d'informació que es pot emmagatzemar en les cintes magnètiques és variat, com vídeo, àudio i dades.

Hi ha diferents tipus de cintes, tant en les seves mesures físiques, com en la seva constitució química, així com diferents formats d'enregistrament, especialitzats en el tipus d'informació que es vol gravar.

Els dispositius informàtics d'emmagatzemament massiu de dades de cinta magnètica són utilitzats principalment per a còpia de seguretat i per al procés d'informació de tipus seqüencial, com en l'elaboració de nòmines de les grans organitzacions públiques i privades.

Disquet

Un disc flexible o disquet (floppy disk) és un dispositiu d'emmagatzemament de dades format per una peça circular de material magnètic que permet la gravació i la lectura de dades. És fi, flexible i tancat en una caixa fina quadrada o rectangular de plàstic. Durant la dècada del 2000, han estat majoritàriament substituïts per discs òptics i pels dispositius de memòria flash. Han existit tres mides principals de disquets per a PC: 8 polzades, 5 ¼ polzades, 3½ polzades.

Els disquets es llegeixen i s'escriuen mitjançant un dispositiu anomenat disquetera (o FDD, de l'anglès Floppy Disk Drive). En alguns casos és un disc més petit que el CD. La disquetera és el dispositiu o unitat lectora/gravadora de disquets, i ajuda a introduir-lo per guardar la informació. Aquest tipus de dispositiu d'emmagatzematge és vulnerable a la brutícia i els camps magnètics externs, per la qual cosa, en molts casos, deixa de funcionar.

Disc dur

Un disc dur (en anglès Hard Disk Drive o HDD) és un dispositiu d'emmagatzemament no volàtil. S'hi guarden grans quantitats de dades digitals en la superfície magnetitzada dels diversos discs (platter) que conté, els quals giren a gran velocitat. Forma part del maquinari de la majoria dels ordinadors actuals. Dins els diferents tipus de memòries és classificat com a memòria secundària. L'adjectiu "dur" se'ls hi aplica en contrast amb el floppy disk o disc flexible, anteriors als discs durs. El 1956 els discs durs foren introduïts per primer cop al mercat de la mà d'IBM. Originalment foren desenvolupats per a ordinadors de propòsit general. Les característiques principals d'un disc dur són la seva capacitat d'emmagatzematge (actualment d'uns quants gigabytes (GB) a un terabyte (TB), la velocitat de transferència (throughput, en MB/s), i el temps d'accés (en ms), que alhora ve condicionat per la velocitat de rotació (rpm o rotacions per minut).

Disc òptic

Un disc compacte o CD és un disc òptic utilitzat per a l'emmagatzematge de dades. Va ser originàriament creat per a emmagatzemar àudio, però posteriorment va ser usat per a emmagatzemar dades (CD-ROM). El disc compacte va ser desenvolupat per Sony i Philips el 1980. El 1982 es va iniciar la seva producció en massa i va anar desplaçant progressivament el disc de vinil com a suport d'àudio. Posteriorment també va desplaçar els disquets d'ordinador com a suport per a la distribució de programari. L'aparició de les gravadores de CD el va convertir en una eina d'allò més útil en el món de la informàtica, per a fer còpies de seguretat i per a transportar arxius. Posteriorment aparegué el DVD, amb més capacitat gràcies a la densitat més gran de dades i a la possibilitat d'escriure fins a dues capes en la mateixa cara del disc. A inicis del 2007 aparegueren els primers aparells de Blu-Ray i HD-DVD al mercat, amb encara més capacitat d'emmagatzematge.

Disc magnetoòptic

Un disc magnetoòptic és un tipus de disc òptic capaç d'escriure i reescriure les dades sobre si. Igual que un CD-RW, pot ser utilitzat tant per emmagatzemar dades informàtiques com pistes d'àudio. La gravació magnetoòptica és un sistema combinat que grava la informació de forma magnètica sota la incidència d'un raig làser, i la reprodueix per mitjans òptics.

No és possible alterar el contingut dels discos magnetoòptics per mitjans únicament magnètics, el que els fa resistents a aquest tipus de camps, a diferència dels disquets. Els fabricants d'aquest tipus de suports asseguren que són capaços d'emmagatzemar dades durant 30 anys sense distorsions ni pèrdues. Un exemple de disc magnetoòptic és el Minidisc.

Les unitats de gravació de discs magneto-òptics verifiquen la informació després d'escriure, de la mateixa manera que la disquetera, reintenta l'operació en cas de falla o informar el sistema operatiu si no pot efectuar-se. Això provoca una demora en l'escriptura tres vegades superior a la lectura, però fa que els discs siguin summament segurs, a diferència dels CD-R o DVD-R en què les dades són escrits sense cap verificació.

Actualment el seu ús principal és com a sistema de còpia de seguretat de ràpida disponibilitat i com a unitat NAS (Network-attached storage) per a emmagatzemar dades que solen canviar poc i

on majoritàriament s'afegeixen nous fitxers, com una base de dades documental o les digitalitzacions de catàlegs, llibres, diaris i documents.

Memòria flash

La memòria flash, és una classe de memòria EEPROM que permet esborrar posicions de memòria amb una operació programable. Amb unes altres paraules, és un xip de memòria que manté el seu contingut sense tensió d'alimentació. És molt utilitzat en càmeres digitals, ordinadors personals portàtils i PDA, telèfons, reproductors de música, videoconsoles, i més aplicacions electròniques. Tenen una gran capacitat de regravabilitat, emmagatzematge, mida petita, i compleix els requisits de medi ambient.

La memòria USB (pendrive) és un petit dispositiu de memòria flash que es pot connectar directament a un port USB. Permet desar-hi tota mena de fitxers (imatges, fotos, música, pel·lícules, programes, etc.) i fer-los servir en un ordinador, reproductor de música, de vídeo, etc.

La capacitat de magatzematge dels pendrive ha anat augmentant amb el temps, des de 32 MB dels primers models comercials fins a molts GigaBytes com tenen els d'avui dia, que poden contenir centenars de CD o desenes de DVD. Són dispositius molt corrents perquè no els cal cap instal·lació prèvia i són compatibles amb tots els sistemes operatius. Podem dir que els pendrive són com ara discs durs externs amb una capacitat ja comparable amb els de gamma baixa i s'utilitzen normalment per a guardar-hi arxius personals, programes i fins i tot sistemes operatius.

Unitat d'estat sòlid

Una unitat d'estat sòlid (de l'anglès SSD, solid state drive) és un dispositiu d'emmagatzematge persistent de dades que utilitza memòria no volàtil com la flash basada en NAND, o memòria volàtil com l'SDRAM, per a emmagatzemar dades, en lloc dels plats giratoris que es troben als discs durs convencionals. Encara que tècnicament no són "discs", molts cops es tradueix erròniament al català la D de SSD com disk encara que la paraula correcta és drive, que es tradueix com a dispositiu o unitat.

Una unitat d'estat sòlid és un dispositiu d'emmagatzematge persistent de dades, format per components electrònics d'estat sòlid. Sol utilitzar-se en ordinadors com a alternativa més ràpida al disc dur, sobretot per al sistema operatiu i àrea de memòria d'intercanvi. També és àmpliament utilitzat en portàtils, a causa del seu pes menor respecte a discs durs i la seva immunitat a vibracions, cops i sacsejades gràcies a l'absència d'elements mòbils o mecànics.

A diferència del disc dur, no conté parts mòbils o mecàniques, i la seva memòria està formada per RAM o flash.

1.7 Detecció i resolució de fallades en dispositius perifèrics

Per poder identificar les causes bàsiques d'un mal funcionament en un equip informàtic hem de seguir uns passos molt simples.

- Hem de detectar l'element que no funciona correctament.

- Hem d'assegurar-nos que l'aparell està connectat al subministrament elèctric.
- Ajustar els connectors implicats en funció del tipus de terminal.
- En tot moment hem de complir les mesures de seguretat necessàries per realitzar les operacions de connexió o desconnexió.
- Si no està al nostre abast la resolució de la incidència, hem de comunicar-ho a través dels mitjans adients a qui correspongui perquè al més aviat possible aquesta es pugui resoldre.

1.8 Normes de seguretat en la connexió/desconnexió d'equips informàtics

Els usuaris dels equips informàtics han de respectar la integritat dels recursos basats en els sistemes d'informació, evitar activitats destinades a obtenir accessos no autoritzats o suplantació d'identitat, respectar els drets de la resta d'usuaris, no acaparar els recursos compartits amb la resta d'usuaris i respectar les polítiques de llicències de programari. Aquesta normativa s'ha d'aplicar a la xarxa, a tots els equips connectats a ella i a tota la informació continguda en aquests equips.

- En tot moment s'han de complir les mesures de seguretat necessàries per realitzar les operacions de connexió i/o desconnexió del maquinari, i utilitzar els equips de protecció de riscos d'acord amb els connectors i terminals implicats.
- No s'han de moure els equips quan estan en funcionament, per tant, per moure assegura't que estigui apagat i desconnectat del corrent elèctric. En el cas d'haver de moure ordinadors desconnecta prèviament tots els perifèrics com són el ratolí, teclat, monitor, impressora, etc.
- Evita moviments bruscos o cops.
- Evita el contacte de l'ordinador o els perifèrics amb qualsevol tipus de líquid (aigua, refresc, cafè, líquids corrosius, etc.).
- No exposis els equips a la humitat, a la pols o a situacions de molta calor que puguin afectar-los.
- Utilitza els equips de protecció contra variacions de corrent o de subministrament d'alimentació ininterrompuda que eviten tant els pics de voltatge com els talls sobtats del corrent.

2. Transmissió interna personal de documentació

Els elements que s'han de donar perquè es consideri un acte de comunicació són:

Emissor. És un ens (persona, organització...) que tria i selecciona els signes adequats per a transmetre el seu missatge; és a dir, els codifica per a poder trametre de manera entenedora al receptor. En l'emissor s'inicia el procés comunicatiu. És qui emet el missatge, i pot ser o no una persona.

Receptor. És un ens (persona, organització...) al que es destina el missatge, realitza un procés invers al de l'emissor, ja que desxifra i interpreta el que l'emissor vol donar a conèixer. Existeixen dos tipus de receptor, el passiu que és el qui només rep el missatge, i el receptor actiu o perceptor, ja que és la persona que no només rep el missatge sinó que ho percep i ho emmagatzema. El missatge és rebut tal com l'emissor va voler dir, en aquest tipus de receptor es realitza el que comunament denominem el feed-back o retroalimentació. És qui rep la informació. Dins d'una concepció primigènia de la comunicació és conegut com a receptor, però aquest terme pertany més a l'àmbit de la teoria de la informació.

Canal. És el mitjà de comunicació (natural o artificial) que estableix una connexió entre l'emissor i el receptor. Suport material o espacial pel qual circula el missatge. Per exemple, l'aire, en el cas de la veu; el fil telefònic, en el cas d'una conversa telefònica. El canal de comunicació és el medi físic pel qual es transmet el missatge. En el cas de la viquipèdia, Internet fa possible que arribi a algú (receptor) el missatge (article de la viquipèdia).

Codi. És el conjunt de signes i la seva organització. Ha de ser el mateix per l'emissor i el receptor. És necessari també que coincideixin els subcodis que formen part del codi general. L'argot del metge pot impossibilitar la comprensió del pacient. El codi és la forma que pren la informació que s'intercanvia entre la font (l'emissor) i la destinació (el receptor) d'un llaç informàtic. Implica la comprensió o descodificació del paquet d'informació que es transfereix.

Missatge. Informació, considerada aquesta en un sentit molt ampli, tramesa entre emissor i receptor. És allò que es vol transmetre.

Situació o context. És el conjunt de circumstàncies concretes on esdevé el procés comunicatiu. Dit d'una altra manera, és la situació o entorn extralingüístic en el qual es desenvolupa l'acte comunicatiu.

2.1 L'actitud d'escolta activa en la recepció d'instruccions de treball

L'escolta activa és aquella que no només sent i percep les vibracions dels sons que emet l'emissor, sinó que li fa saber que és escoltat i que per tant l'entén. Significa realitzar una escolta en què la persona que emet el missatge, interpreta, ens interessem pel que intenta comunicar-nos. Això suposa tenir una mirada que transmet algun feedback sobre el missatge de l'altre, centrar-se pacientment, realitzar un cert buidatge de les coses pròpies i dels prejudicis i allotjar sense condicions.

Elaborat per: Ramon López Data de supervisió: *febrer de 2015*

Per a realitzar una bona escolta activa és necessari:

- Eliminar possibles distraccions.
- Establir contacte visual.
- Ús d'un to i volum adequat.
- Reforçar el missatge de l'emissor.
- No interrompre.
- Concentrar-nos en el que diuen per a poder resumir-ho
- Centrar les intervencions sobre el missatge emès.
- Controlar els silencis.
- No jutjar, ni prejutjar.
- Identificar els sentiments de l'emissor.
- Ser pacient.
- Controlar les emissions pròpies.
- Prendre notes.

2.2 Incidències en la transmissió

Podem distingir els obstacles relacionats amb l'escolta activa entre generals i específics:

- Generals
    - Propis de l'entorn: soroll, distraccions, etc.
    - Propis de l'estat físic: cansament, estat de salut.
    - Propis de l'àrea emocional: ansietat, agressivitat, temor, etc.
    - Propis de l'àrea cognitiva o mental: prejudicis morals, culturals, primeres impressions.
- Específics
    - L'ansietat.
    - La superficialitat o dificultat a l'hora d'atendre els sentiments dels altres.
    - La tendència a jutjar, imposar.
    - La impaciència i la impulsivitat .
    - La passivitat experimentada per aquells que tendeixen a donar sempre la raó.
    - La tendència a predicar.

2.3 Protocol

Un protocol de comunicació estableix una descripció formal dels formats que han de presentar els missatges per poder ser intercanviats entre diferents persones o equips. Poden incloure senyalització, autenticació i detecció d'errors i la capacitat de correcció. Un protocol descriu la sintaxi, la semàntica i la sincronització de la comunicació.

Els sistemes de comunicació utilitzen aquests formats predefinits o protocols per intercanviar missatges. Un protocol descriu tant la sintaxi i la semàntica com la sincronització de la comunicació. Un llenguatge de programació descriu el mateix per als càlculs. Es pot dir que hi ha una certa relació entre els protocols i llenguatges de programació: els protocols són per a la comunicació el mateix que els llenguatges de programació són pels càlculs.

2.4 Actitud positiva en la resolució de conflicte

Actituds positives que ajudaran a la resolució del conflicte:

- Pressuposeu bona fe: probablement no us equivocareu, evitareu malentesos i evitareu haver-vos de disculpar.
- No respongueu als atacs personals o als comentaris amb malícia. Ignoreu-los, no caigueu en la trampa de les provocacions d'un incendiari, sigueu en tot moment educat i respecteu el protocol. Concentreu-vos sobre l'assumpte que us ocupa o sobre els nous punts de vista i oblideu-vos de les persones i de les suposades motivacions de cadascú.
- Intenteu millorar abans de revertir, i eviteu una guerra. Penseu-vos-ho dos cops abans de fer qualsevol comentari, presumiblement de bona fe. Busqueu l'equilibri de tots els punts de vista. Assegureu-vos d'aportar les referències adequades en casos controvertits. Expliqueu sempre les vostres opinions.
- No us precipiteu. La majoria de situacions no són urgents. Deixeu reposar l'assumpte, que es refredi i s'assereni. Tot es pot solucionar. Més endavant ho podreu pensar amb perspectiva i mentrestant potser altres persones han contribuït a trobar una solució.
- Comenceu per identificar quins són els punts en comú. Un acord inicial bàsic pot ser el començament d'una bona col·laboració.

2.5 Lliurament de la documentació

Quan hàgim de lliurar la documentació seguirem el procediment i la forma establerts acordats prèviament. Aquest lliurament s'ha d'efectuar dins del termini acordat, seguint els principis de seguretat i confidencialitat en la transmissió, identificant el destinatari de la documentació i lliurant aquesta en el format acordat.

3. Transmissió interna informatitzada de documents

3.1 Tipus: correu electrònic i xarxa local

El correu electrònic (anomenat en anglès e-mail, o email) es refereix al sistema que permet redactar, enviar i rebre missatges o cartes utilitzant sistemes de comunicació electrònica. També s'hi poden adjuntar documents electrònics o altres fitxers. Avui en dia, la majoria de sistemes de correu electrònic utilitzen Internet per bé que també és possible el seu ús a través de la xarxa local. El correu electrònic és un dels serveis més populars d'Internet. En comparació amb el correu ordinari, té l'avantatge de ser més barat i alhora més ràpid. La majoria del correu electrònic es transmet a servidors que treballen amb el protocol SMTP (Simple Mail Transfer Protocol). Pot ser de caràcter privat, empresarial o institucional.

Una adreça de correu electrònic té la forma: usuari@domini.exemple, és l'origen i/o la destinació de missatges enviats per correu electrònic. La part abans del signe @ és la part local de la direcció, habitualment el nom d'usuari del destinatari, i la part a la dreta del signe @ és el nom de domini.

Un missatge de correu electrònic consta de dos components principals:

- La capçalera (header) que conté de forma estructurada la informació dels següents camps:
  - From (de): L'adreça d'email, i opcionalment el nom de l'emissor.
  - To (a): L'adreça o adreces del/s receptor/s.
  - Subject (assumpte): Un resum del contingut del missatge .
  - Date (Data): data i hora del missatge.
  - Altres camps freqüents són:
  - Cc (Carbon copy): Còpia de carbó.
  - Bcc (Blind Carbon Copy): Còpia de carbó oculta.
  - Content-Type: Informació de com s'ha de mostrar el missatge, normalment de tipus MIME.
  - Reply-To: L'adreça que s'hauria d'usar per contestar al remitent.
- El cos (body) del missatge en si com a text no estructurat. De vegades conté la signatura al final.

3.2 Gestió del correu electrònic

Un client de correu electrònic és un programari d'ordinador utilitzat per llegir i enviar correus electrònics. És un programari que es connecta al servidor de correu on disposa d'un compte per, d'aquesta manera, descarregar els missatges a l'ordinador client. Una característica important d'aquests clients, és que es poden configurar per a molts servidors de correu electrònic diferents.

A més dels clients de correu electrònic també hi ha programes de correu electrònics basats en la web, anomenats webmail o correu web.

El Mozilla Thunderbird és un client de correu lliure i gratuït, d'execució ràpida i que consumeix menys recursos que altres alternatives, basat en el codi desenvolupat dins el projecte Mozilla.

El programa té gran quantitat d'opcions de personalització i incorpora les característiques més útils que pot necessitar un client de correu avui en dia: filtres de missatges, gestió del correu brossa amb autoaprenentatge, etc. Tot això juntament amb les opcions a les quals podem estar més habituats, com ara la cerca de missatges o una llibreta d'adreces personal.

Funcionalitats del client de correu Mozilla Thunderbird:

- Assistent de migració
- Auxiliar de configuració del compte de correu
- Agenda de contactes en un clic
- Recordatori de fitxers adjunts
- Gestor d'activitat
- Barra d'eines amb filtre ràpid
- Pestanyes
- Cerca
- Arxiu de missatges
- Modificació de l'aspecte i comportament
- Gestió de diversos comptes de correu
- Gestor de complements
- Retalleu la brossa
- Privadesa robusta
- Protecció contra phishing (suplantació d'identitat)
- Actualització automàtica
- Programari de codi obert

3.3 Intranet

Una intranet és una xarxa d'ordinadors d'una xarxa d'àrea local (LAN) privada empresarial o educativa que proporciona eines d'Internet, la qual té com a funció principal proveir lògica de negocis per a aplicacions de captura, consultes, etc. amb l'objectiu d'auxiliar la producció d'aquests grups de treball; és també un important medi de difusió d'informació interna a escala de grup de treball. És molt utilitzada sobretot a cases de grans dimensions.

Les intranets s'utilitzen generalment per a quatre tipus d'aplicacions:

1. Comunicació i col·laboració

2. Publicacions Web
3. Operacions comercials i gestió Processament de comandes
4. La gestió dels portals Intranet

Aquests són alguns dels seus avantatges:

- Optimitza la informació unificant-la i facilitant el seu tractament.
- Accelera el pas de la gestió de la informació a la gestió del coneixement.
- Està activa les 24 hores del dia, set dies a la setmana.
- És una eina de grup.
- Estalvi econòmic.
- Cohesió dels grups.
- Informació actualitzada, recent.
- No s'entorpeix la feina d'altres companys.
- Informació per escrit i consultable.
- Ofereix més informació, ja que és més fàcil enviar-la.
- Facilita la gestió del rumor.
- Aconsegueix que l'empleat pugui adreçar-se al cap de departament.

4. Normes de seguretat que garanteixen la confidencialitat en la transmissió

D'una manera intuïtiva, tots coneixem l'existència d'un conjunt de normes jurídiques que regulen les conductes constitutives de delicte, i també les sancions previstes en aquestes situacions (algunes poden ser fins i tot privatives de llibertat). El recull legislatiu aplicable en aquest tipus de matèria s'anomena Codi penal. Cada país disposa de les seves pròpies normes i, per tant, és possible que variïn d'un país a un altre.

És molt important conèixer l'essència de la normativa que afecta l'ús de les tecnologies, ja que, amb independència de la nostra voluntat, condiciona l'ús de les tecnologies, tant des del punt de vista del treballador tècnic, com del de l'usuari d'un ordinador d'una llar qualsevol.

El delicte informàtic no apareix explícitament definit en l'actual Codi penal (1995), ni en les reformes posteriors (Llei 15/2003) que se n'han fet i, per tant, no es podrà parlar de delicte informàtic pròpiament dit, sinó de delictes fets amb l'ajut de les noves tecnologies, en els quals l'ordinador s'usa com a mitjà d'execució del delicte (per exemple, l'enviament d'un correu electrònic amb amenaces), o bé com a objectiu d'aquesta activitat (per exemple, una intrusió en un sistema informàtic).

La legislació del nostre país encara presenta buits pel que fa als mal anomenats delictes informàtics, de manera que tan sols oferirem un seguit de directrius bàsiques, més aviat relacionades amb el sentit comú, que no pas amb la normativa complexa que es va generant entorn de l'aplicació de les noves tecnologies.

El nostre Codi penal és especialment sever amb la protecció dels drets fonamentals i les llibertats públiques, recollits en el títol I de la Constitució. Aquests drets i llibertats són inherents a la condició de persona i, per aquest motiu, gaudeixen d'una protecció tan especial.

Un dels articles de la Constitució més directament relacionat amb la pràctica informàtica (tant des del punt de vista tècnic, com del simple usuari), és l'article 18, el qual reconeix el dret a la intimitat. Han de ser objecte de protecció no sols l'àmbit íntim de l'individu, sinó també l'esfera familiar i domiciliària.

> Article 18 CE
>
> 1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la imatge pròpia.
>
> 2. El domicili és inviolable. No s'hi pot entrar ni fer-hi cap escorcoll sense el consentiment del titular o sense resolució judicial, llevat del cas de delicte flagrant.
>
> 3. **Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial**.
>
> 4. La llei limita l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

Una part molt important dels delictes produïts entorn de la informàtica s'ubica dins de la tipificació dels delictes contra la intimitat. Sovint, els autors d'aquestes conductes no són conscients de la importància dels béns protegits per la llei i no s'adonen de les conseqüències de les seves accions fins que ja és massa tard.

Els delictes contra la intimitat són recollits en l'article 197.1 de l'actual Codi penal. Com a conseqüència de l'assimilació de la intercepció del correu electrònic amb la violació de la correspondència, aquest article disposa que les conductes següents són constitutives de delicte:

- L'apoderament de papers, cartes, missatges de correu electrònic o qualsevol altre document o efectes personals.
- La intercepció de les telecomunicacions.
- La utilització d'artificis tècnics d'escolta, transmissió, gravació o reproducció de so, o de qualsevol altre senyal de comunicació.

Per ser constitutives de delicte, aquestes activitats s'han de produir sense el consentiment de la persona afectada (ni autorització judicial motivada o justificada), i amb la intenció de descobrir-ne els secrets o vulnerar-ne la intimitat.

Per tant, obrir la bústia d'un correu electrònic que no sigui el nostre propi i llegir els missatges que s'hi emmagatzemen podria esdevenir una conducta constitutiva de delicte. Cal anar amb molt de compte amb aquest tipus d'accions (tècnicament solen ser molt senzilles d'efectuar, però no per això són conductes legals) i, com a norma general, mai no s'ha de llegir cap correu electrònic que no vagi adreçat a nosaltres mateixos (ni tan sols si el nostre cap, dins de l'àmbit laboral, ens ho demana).

En el cas de la intercepció del correu electrònic dins de l'àmbit empresarial, se sol argumentar que els treballadors no poden fer ús dels mitjans de l'empresa per a qüestions personals. Moltes sentències s'han pronunciat a favor de l'empresa perquè s'entén que, efectivament, els mitjans pertanyen a l'empresa i que, per tant, no és un lloc adient per enviar i rebre missatges de caràcter privat. No obstant això, davant del dubte, cal que sempre tingueu present que els correus electrònics dels treballadors de l'empresa gaudeixen de la mateixa protecció legal, pel que fa a la intimitat, que els correus electrònics personals.

Una manera útil per fer saber als usuaris d'una organització quins són els usos correctes dels mitjans de l'empresa, i les seves limitacions, consisteix en l'ús de contractes en els qual s'especifica, per exemple, quines obligacions i responsabilitats té un usuari d'un compte de correu electrònic.

Usurpació i cessió de dades reservades de caràcter personal.

Els articles 197, 198, 199 i 200 del Codi penal tipifiquen com a conductes delictives l'accés, la utilització, la modificació, la revelació, la difusió o la cessió de dades reservades de caràcter personal que es trobin emmagatzemades en fitxers, suports informàtics, electrònics o telemàtics,

sempre que aquestes conductes les facin persones no autoritzades (conductes anomenades, genèricament, abusos informàtics sobre dades personals). A més de la responsabilitat penal en què poden derivar aquests tipus d'accions, també cal considerar que les dades personals s'han d'emmagatzemar i declarar segons una normativa especificada en la Llei orgànica de protecció de dades personals (LOPDP).

Pel que fa al Codi penal, explícitament es fa esment de l'agreujant d'aquestes conductes quan les dades de l'objecte del delicte són de caràcter personal que revelin ideologia, religió, creences, salut, origen racial o vida sexual. Altres agreujants que cal tenir en compte es produeixen quan la víctima és un menor d'edat o incapacitat, o bé la persona que comet el delicte és el responsable dels fitxers que hi estan involucrats. Mereix una consideració especial l'article 199.2, en el qual es castiga la conducta del professional que, incomplint l'obligació de reserva, divulga els secrets d'una altra persona.

4.1 Gestió de la seguretat de la informació

La protecció de les dades personals implica controlar-ne l'accés, el qual només hauria de poder ser fet pels usuaris autoritzats. La primera mesura que, intuïtivament, se'ns pot ocórrer per protegir-nos dels accessos no autoritzats consisteix en el control dels accessos físics als sistemes informàtics. De fet, a més de ser la mesura més intuïtiva, també és una de les més importants i la que amb més freqüència es descuida. Penseu que una organització pot invertir molts diners en programaris que evitin i detectin els accessos informàtics no autoritzats als seus equipaments, però tota aquesta despesa no servirà de res si els recursos físics del sistema es troben a l'abast de tothom.

El maquinari sol ser l'element més car d'un sistema informàtic i, per tant, cal tenir una cura especial amb les persones que hi tenen accés material. Una persona no autoritzada que accedís al sistema podria causar pèrdues enormes: robatori d'ordinadors, introducció de programari maliciós en el servidor, destrucció de dades, etc.

4.2 Política de seguretat de l'organització

Una política de seguretat és un pla d'acció per afrontar riscos de seguretat, o un conjunt de regles per al manteniment de cert nivell de seguretat. Poden cobrir qualsevol cosa des de bones pràctiques per a la seguretat d'un sol ordinador, regles d'una empresa o edifici, fins a les directrius de seguretat d'un país sencer.

La política de seguretat és un document d'alt nivell que denota el compromís de la gerència amb la seguretat de la informació. Conté la definició de la seguretat de la informació des del punt de vista de certa entitat.

Ha de ser enriquida i compatibilitzada amb altres polítiques dependents d'aquesta, objectius de seguretat, procediments. Ha d'estar fàcilment accessible de manera que els empleats estiguin al corrent de la seva existència i entenguin el seu contingut. Pot ser també un document únic o inserit en un manual de seguretat. S'ha de designar un propietari que serà el responsable del seu manteniment i la seva actualització a qualsevol canvi que es requereixi.

Per evitar els problemes esmentats en el punt anterior es poden adoptar diverses mesures, moltes d'elles de sentit comú, com, per exemple, les següents:

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic (útil en casos de robatori).
- Protegir i aïllar el cablatge de la xarxa (tant per protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància.
- Utilitzar contrasenyes en els estalvis de pantalla.
- Utilitzar contra senyes de BIOS.
- Desactivar les opcions d'autocompletar i recordar contrasenyes dels navegadors d'Internet.
- Triar una topologia de xarxa adequada a les nostres necessitats de seguretat.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Mantenir el sistema informàtic actualitzat.
- Tenir mecanismes d'autenticació per als usuaris que volen accedir al sistema.

4.3 Identificació i classificació d'actius que cal protegir

La seguretat informàtica o seguretat de tecnologies de la informació és l'àrea de la informàtica que s'enfoca en la protecció de la infraestructura computacional i tot el relacionat amb aquesta i, especialment, la informació continguda o circulant. Per a això existeixen una sèrie d'estàndards, protocols, mètodes, regles, eines i lleis concebudes per minimitzar els possibles riscos a la infraestructura o a la informació. La seguretat informàtica comprèn programari (bases de dades, metadades, arxius), maquinari i tot el que l'organització valori (actiu) i signifiqui un risc si aquesta informació confidencial arriba a mans d'altres persones, convertint-se, per exemple, en informació privilegiada.

La definició de seguretat de la informació no ha de ser confosa amb la de "seguretat informàtica", ja que aquesta última només s'encarrega de la seguretat en el mitjà informàtic, però la informació es pot trobar a diferents mitjans o formes, i no només en mitjans informàtics.

La seguretat informàtica és la disciplina que s'ocupa de dissenyar les normes, procediments, mètodes i tècniques destinats a aconseguir un sistema d'informació segur i fiable.

La seguretat en un ambient de xarxa és l'habilitat d'identificar i eliminar vulnerabilitats. Una definició general de seguretat ha de també posar atenció a la necessitat de salvaguardar l'avantatge organitzacional, incloent-hi informació i equips físics, com ara els mateixos computadors. Ningú a càrrec de seguretat ha de determinar qui i quan es pot prendre accions apropiades sobre un ítem en específic. Quan es tracta de la seguretat d'una companyia, el que és

apropiat varia d'organització a organització. Independentment, qualsevol companyia amb una xarxa ha de tenir una política de seguretat que es dirigeixi a conveniència i coordinació.

4.4 Responsabilitat personal dels documents manipulats

Confidencialitat és la propietat de la informació, per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació. La confidencialitat ha estat definida per l'Organització Internacional d'Estandardització (ISO) en la norma ISO / IEC 27002 com "garantir que la informació és accessible només per a aquells autoritzats a tenir accés" i és una de les pedres angulars de la seguretat de la informació.

La confidencialitat també es refereix a un principi ètic associat amb diverses professions; en aquest cas, es parla de secret professional. En ètica, i en Dret, concretament en judicis i altres formes de resolució de conflictes legals, com ara la mediació, alguns tipus de comunicació entre una persona i un d'aquests professionals són "privilegiats" i no poden ser discutits o divulgats a tercers. A les jurisdiccions en què la llei preveu la confidencialitat, en general hi ha sancions per la seva violació.

Confidencialitat en Informàtica

La confidencialitat s'entén en l'àmbit de la seguretat informàtica, com la protecció de dades i d'informació intercanviada entre un emissor i un o més destinataris davant de tercers. Això s'ha de fer independentment de la seguretat del sistema de comunicació utilitzat: de fet, un assumpte de gran interès és el problema de garantir la confidencialitat de la comunicació utilitzat quan el sistema és inherentment insegur.

Nosaltres, com a enregistradors de dades tenim la responsabilitat, i el deure ètic de mantenir la confidencialitat de les dades tractades, d'utilitzar les dades de forma exclusiva i amb rigor, comunicant al responsable de seguretat les possibles incidències, i/o responsabilitats davant els errors o les infraccions comesos en la manipulació de les dades.

4.5 Seguretat física

La seguretat física és el compendi de recursos, processos, tasques, equips i personal dedicats a protegir els recursos d'una empresa. La protecció física és una combinació de mecanismes que minimitzen els riscos de possibles atacs i, en cas que succeeixin, en disminueixen el dany. L'estratègia de protecció que cal seguir s'ha de decidir després de fer una anàlisi de riscos, identificar les vulnerabilitats i l'impacte que tenen.

Podem dividir les mesures de seguretat en diverses categories segons la finalitat que tenen:

- Mesures dissuasives: tanques, murs, barrots, guardes de seguretat, gossos, senyals d'alerta, il·luminació nocturna.
- Dificultats en l'accés a personal no autoritzat: cadenats, controls d'accés, seguretat perimetral.

Iniciativa d'Ocupació Juvenil
Unió Europea
Fons social europeu
L'FSE inverteix en el teu futur

- Detecció d'intrusos: sensors de detecció, detecció de canvis en l'ambient .
- Avaluació d'incidències: monitoratge dels sistemes d'alarmes, procediments per a casos d'emergència, estructura de comunicació.

4.6 Autenticació

S'anomena autenticació el procés de **verificació de la identitat** d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic.

De mecanismes d'autenticació, n'hi ha de molts tipus diferents, des del més barats i senzills (com, per exemple, un nom d'usuari i una contrasenya) fins als més cars i complexos (com, per exemple, un analitzador de retina). Com sempre, segons els objectius i el pressupost de l'organització, cal triar el que més s'ajusti a les nostres necessitats. També cal tenir en compte que molts d'aquests mecanismes són complementaris i es poden utilitzar alhora.

Mecanismes d'autenticació d'usuaris

Hi ha diversos mecanismes d'autenticació d'usuaris. Els podem classificar de la manera següent:

1. Sistemes basats en elements coneguts per l'usuari. El principal mecanisme dins d'aquest tipus d'autenticació són els sistemes basats en contrasenyes. És un dels mètodes que es fan servir més sovint per autenticar un usuari que vol accedir a un sistema. Òbviament, és el mètode més barat, però també és el més vulnerable, ja que encara que la paraula de pas o contrasenya hauria de ser personal i intransferible, sovint acaba en poder de persones no autoritzades. D'altra banda, encara que les contrasenyes s'emmagatzemin xifrades en un fitxer, és possible desxifrar-les amb múltiples tècniques.

   Tot i que l'assignació de les contrasenyes als usuaris es basa en el sentit comú, no és sobrer tenir en compte les recomanacions següents:

   - Memoritzar-la i no portar-la escrita.
   - Canviar-la periòdicament (amb caràcter mensual, per exemple).
   - No repetir la mateixa contrasenya en comptes diferents.
   - No llençar documents amb contrasenyes a la paperera.
   - Evitar utilitzar paraules de diccionari (hi ha tècniques de descobriment de contrasenyes basades en la comparació amb diccionaris sencers de paraules).
   - Evitar utilitzar dades que puguin ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el login, DNI, número de mòbil, etc.).
   - Fer servir contrasenyes d'un mínim de vuit caràcters.
   - Evitar la reutilització de contrasenyes antigues.
   - No utilitzar contrasenyes exclusivament numèriques.

- Afavorir l'aparició de caràcters especials (¡, *, ?, etc.).
- No utilitzar seqüències de teclat del tipus ”qwerty”.
- Fer servir mnemotècnics per recordar les contrasenyes.

Molts sistemes informàtics forcen els usuaris a triar contrasenyes amb un cert nivell de robustesa: obliguen a canviar la contrasenya cada cert temps, que tingui un nombre mínim de caràcters, etc.

2. Sistemes basats en elements que té l'usuari. En aquest cas, l'autenticació no es farà d'acord amb el que recorda o coneix un usuari, sinó a partir d'un dispositiu que porta al damunt (el qual també pot requerir la introducció d'una contrasenya o d'un número PIN), o bé a partir de les pròpies característiques físiques de l'usuari (sistemes biomètrics).

   a) Sistemes basats en targetes intel·ligents i testimonis (tokens) de seguretat.

   Una targeta intel·ligent (smartcard) és similar a una targeta de crèdit, però a diferència d'aquesta, les targetes intel·ligents allotgen un microprocessador (i memòria) que les dota de les característiques següents:

   - Capacitat per fer càlculs criptogràfics sobre la informació que emmagatzemen.
   - Emmagatzematge xifrat de la informació.
   - Protecció física i lògica (mitjançant una clau d'accés) a la informació emmagatzemada.
   - Capacitat per emmagatzemar claus de signatura digital i xifratge.

   És un mètode d'autenticació que cada vegada fan servir més les organitzacions, tot i el cost d'adaptació de la infraestructura als dispositius que permeten la lectura de les targetes. Un exemple de targeta intel·ligent és el DNI (document nacional d'identitat) electrònic espanyol (també anomenat DNIe).

   A més, les targetes intel·ligents poden ser de contacte (és a dir, han de ser inserides en la ranura d'un lector perquè puguin ser llegides), o sense contacte. Aquest segon tipus de targetes s'ha començat a emprar amb èxit en diversos països com a sistema de pagament en el transport públic.

   Una altra solució per resoldre el problema de l'autenticació, força popular en el sector empresarial, consisteix en l'anomenat testimoni de seguretat (security token). Solen ser dispositius físics de mida reduïda (alguns inclouen un teclat per introduir una clau numèrica o PIN), similars a un clauer, que calculen contrasenyes d'un únic ús (canvien a cada login o bé cada cert temps). També poden emmagatzemar claus criptogràfiques, com per exemple, la signatura digital o mesures biomètriques.

   b) Sistemes biomètrics. Els sistemes biomètrics es basen en les característiques físiques de l'usuari que s'ha d'autenticar (o en patrons característics que puguin ser reconeguts com, per exemple, la signatura). Com a principal avantatge, l'usuari no ha de recordar cap

contrasenya, ni cal que porti cap testimoni o targeta al damunt. Solen ser més cars que els mètodes anteriors; per aquest motiu, encara no es fan servir gaire, tot i que alguns d'aquests mètodes ofereixen un alt nivell de seguretat a un preu econòmic molt raonable (per exemple, el reconeixement dactilar). Entre les diferents característiques que es poden utilitzar per reconèixer un usuari mitjançant mesures biomètriques destaquem les següents:

- Veu
- Olor corporal
- Escriptura
- Empremtes dactilars
- Patrons de la retina o de l'iris
- Geometria de la mà
- Estructura facial
- Traçat de les venes

4.7 Confidencialitat

Per aconseguir que la informació només sigui accessible als usuaris autoritzats i evitar que la informació en clar (és a dir, sense xifrar) que circula per una xarxa pugui ser interceptada per un espia, es poden usar diversos mètodes criptogràfics.

Una xifra o criptosistema és un mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un text xifrat o criptograma. El procés de transformar un text en clar en text xifrat s'anomena xifratge, i el procés invers, és a dir, la transformació del text xifrat en text en clar, s'anomena desxifratge. Tant el xifratge com el desxifratge són controlats per una o més claus criptogràfiques.

S'anomena criptografia la ciència i l'estudi de l'escriptura secreta. Juntament amb la criptoanàlisi (tècnica que té com a objectiu esbrinar la clau d'un criptograma a partir del text en clar i del text xifrat) formen el que es coneix amb el nom de criptologia.

Per protegir la confidencialitat de les dades (emmagatzemades o que circulen per la xarxa) es poden fer servir criptosistemes de clau privada (simètrics) o de clau pública (asimètrics).

1) Criptosistemes de clau privada o simètrics.

Els criptosistemes de clau privada o compartida (o simètrics) són aquells en els quals emissor i receptor comparteixen una única clau. És a dir, el receptor podrà desxifrar el missatge rebut si i només si coneix la clau amb la qual l'emissor ha xifrat el missatge.

2) Criptosistemes de clau pública.

A diferència dels criptosistemes de clau privada, molt intuïtius i amb força desavantatges, els de clau pública són conceptualment molt enginyosos, elegants i aporten més funcionalitats que els asimètrics. No obstant això, són força lents, comparats amb els simètrics i moltes vegades no

s'utilitzen per xifrar, sinó per intercanviar claus criptogràfiques en els protocols de comunicacions. La criptografia de clau pública va ser introduïda per Diffie i Hellman l'any 1976.

Quan un usuari A vol enviar un missatge a un usuari B, xifra el missatge fent servir la clau pública de B (que és coneguda per tots els usuaris del criptosistema). Quan el receptor rebi el missatge, únicament el podrà desxifrar ell mateix, utilitzant la seva pròpia clau privada (la qual es troba exclusivament en el seu poder).

4.8 Integritat

Un avantatge molt important del criptosistema de clau pública és que permet la incorporació de signatura digital. Cada usuari podrà signar digitalment el seu missatge amb la seva clau privada i aquesta signatura podrà ser verificada més tard, de manera que l'usuari que l'ha originat no pugui negar que s'ha produït (propietat de no-repudiació).

Certificat digital

A l'hora d'utilitzar la clau pública d'un usuari, com podem saber que és autèntica? Per resoldre aquest problema es requereix la participació d'una tercera part (anomenada autoritat de certificació) que confirmi l'autenticitat de la clau pública d'un usuari amb l'expedició d'un certificat digital. Aquest document, signat digitalment per un prestador de serveis de certificació, vincula unívocament unes dades de verificació de signatura al titular, que en confirma la identitat en qualsevol transacció telemàtica que es pugui fer.

4.9 Protecció de suports d'informació i còpies de suport

Protecció de suports.

En l'article 5 de LOPDP es defineix suport com un "[...] objecte susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar i recuperar dades".

Així doncs, és imprescindible una bona gestió dels suports, físics o informàtics, per poder dur a terme un tractament acurat de la informació. Els suports informàtics que continguin dades de caràcter personal han de complir els requisits següents:

- Els suports han d'estar clarament identificats amb una etiqueta externa, que indiqui el tipus d'informació que contenen, i també la data de creació.
- Els suports s'han d'emmagatzemar amb pany i clau, i se n'ha de restringir la utilització únicament a les persones amb accés autoritzat als fitxers.
- La sortida de suports fora dels locals (instal·lacions) on es trobin ubicats els fitxers l'haurà d'autoritzar, mitjançant la firma, el responsable del fitxer i el responsable de seguretat.

- S'ha de fer un inventari de suports que ha de contenir la informació relativa a cada suport inventariat: tipus de suport, data de creació, informació que conté i lloc on és emmagatzemat.
- En el cas de suports que s'hagin de llençar, s'ha de procedir a destruir-los o inutilitzar-los físicament, abans de la baixa en l'inventari, per impedir qualsevol recuperació posterior de la informació que contenen.
- Els suports que siguin reutilitzables s'hauran d'esborrar abans de reutilitzar-los, de manera que les dades que contenien no siguin recuperables.
- Si fos necessari que els suports surtin fora dels locals on són ubicats els fitxers com a conseqüència d'operacions de manteniment, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada.
- S'ha d'establir un sistema de registre d'entrada i de sortida de suports informàtics.
- La recepció de suports sempre ha de ser autoritzada pel responsable de seguretat.
- El responsable del fitxer ha d'arxivar els registres d'entrades i de sortides de suports.

Còpies de seguretat.

Hi ha de ser descrit i previst el procediment de còpies de seguretat i recuperació de les dades.

- Descriurem el procediment per dur a terme les còpies de seguretat i el procediment per a la recuperació de les dades, i indicarem els mitjans tècnics (dispositius, cintes, etc.) i programaris que utilitzarem per fer aquestes tasques.
- Aquests procediments hauran de garantir la reconstrucció de les dades en l'estat en el qual es trobaven en el moment de la pèrdua o destrucció.
- Indicarem la periodicitat amb què es duran a terme les còpies de seguretat, que haurà de ser com a mínim d'una còpia per setmana.

4.10 Gestió i registre d'incidències

Hem de preveure un procediment de notificació, gestió i resposta enfront de les incidències. Voldrà dir tenir un registre d'incidències en què anotarem (com a mínim), el següent:

- Les incidències que es produeixin que afectin la seguretat de les dades.
- El moment en què s'han produït.
- La persona que ha notificat la incidència i la persona a qui es comunica la incidència.
- El procediment seguit, i també les mesures adoptades com a conseqüència de la incidència produïda.

UF0512 Transmissió d'informació per mitjans convencionals i informàtics

Elaborat per: Ramon López Data de supervisió: *febrer de 2015*