Seguretat passiva

Ivan Basart Carrillo i Carles Caño Valls

Índex

Introducció

La seguretat informàtica és una disciplina holística que engloba tots els conceptes que influeixen en la reducció i en el control dels riscos que afecten el dia a dia d'una companyia.

Quan es parla de seguretat informàtica es tendeix a pensar en tallafocs, antivirus, detectors i altres eines molt utilitzades en el món de la seguretat, però es tenen menys presents els conceptes relacionats amb la seguretat física.

En aquesta unitat veurem que, a més dels aspectes tècnics relacionats amb la seguretat informàtica, hi ha altres riscos que cal tenir en compte. Hi ha estudis de l'FBI que demostren que en els darrers anys s'ha incrementat exponencialment el robatori d'ordinadors portàtils i de butxaca, la qual cosa de vegades comporta un risc de seguretat molt important sobretot quan els propietaris són alts càrrecs d'empreses.

En l'apartat de "Seguretat passiva" s'estudien els aspectes més importants de la seguretat física per minimitzar riscos en els equips informàtics. El fet de decidir de manera encertada les característiques de la seguretat física representa tenir una base sòlida sobre la qual construir els altres elements de seguretat.

En l'apartat "Sistemes d'alimentació ininterrompuda" s'estudia com aquests elements són una peça clau de la seguretat informàtica. En un ordinador personal d'usuari, un tall de corrent pot implicar un mal menor. En un entorn corporatiu, un tall de corrent pot significar la pèrdua de dades crítiques amb les despeses econòmiques consegüents que això comporta.

En l'apartat "Seguretat lògica" s'estudien els processos de autenticació i autorització com a mesures per garantir la seguretat de la informació. Es presentaran tant les autenticacions més esteses basades en contrasenyes, com les més avançades basades en mesures biomètriques, és a dir, mesures físiques de la persona que es vol autenticar.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Aplica mesures de seguretat passiva en sistemes informàtics descrivint característiques d'entorns i relacionant-les amb les seves necessitats.
    - Descriu les diferències entre seguretat física i lògica.
    - Defineix les característiques de la ubicació física i condicions ambientals dels equips i servidors.
    - Identifica la necessitat de protegir físicament els sistemes informàtics.
    - Verifica el funcionament dels sistemes d'alimentació ininterrompuda.
    - Selecciona els punts d'aplicació dels sistemes d'alimentació ininterrompuda.
    - Esquematitza les característiques d'una política de seguretat basada en llistes de control d'accés detallant l'organització d'usuaris i grups per garantir la seguretat de la informació i funcionalitats suportades per l'equip informàtic, segons les especificacions tècniques.
    - Valora els avantatges que suposa la utilització de sistemes biomètrics i la importància d'establir una política de contrasenyes.
    - Identifica els tipus d'accés al sistema així com els mecanismes de seguretat descrivint les seves característiques principals i eines associades més comunes per garantir l'ús dels recursos del sistema.
    - Explica els procediments dels sistemes per establir permisos i drets d'usuaris, detallant la seva organització i les eines administratives associades per organitzar polítiques de seguretat, segons els procediments establerts en el programari base.
    - Comprova el registre dels usuaris i grups a l'inventari, registrant els canvis detectats.

1. Seguretat passiva

Durant les dècades de 1960 i 1970, la seguretat física dels equips informàtics era una tasca molt menys complexa que avui en dia. Els ordinadors només estaven a l'abast de grans corporacions que no n'acostumaven a tenir més d'un. El maquinari ocupava sales enormes que eren a les entranyes dels edificis de les grans corporacions i, tot i accedir-hi, molt poca gent sabia què fer-ne.

A l'actualitat gairebé tothom té un ordinador en l'anomenada *societat del primer món*. Hi ha persones que disposen de portàtils, ordinadors de butxaca i altres dispositius mòbils. Gràcies a les tecnologies sense fil es pot accedir a qualsevol equip sense tenir-hi accés físic. Protegir tots aquests dispositius contra robatoris, fraus, sabotatge, vandalisme i altres riscos és una tasca cada vegada més complexa i costosa.

La tecnologia i els entorns esdevenen més complexos amb la qual cosa apareixen nous riscos. Moltes empreses han tingut robatoris de dispositius o fugues d'informació i, en els pitjors casos, crims com ara assalts a punta de canó o tirotejos d'antics empleats ressentits.

Protegir físicament els equips informàtics és una tasca fonamental com a base de la seguretat informàtica global. Per aconseguir uns bons resultats cal aplicar una estratègia de defensa en capes. Així es desplegarà tota una sèrie de controls i mesures que combinats garanteixin uns bons nivells de seguretat.

Un exemple d'estratègia de defensa en capes seria instal·lar una tanca perimetral, seguida dels murs de les instal·lacions, llavors un accés mitjançant targeta, més una vigilància de guardes de seguretat.

Tenir uns nivells alts de seguretat física pot ser costós i impactar negativament en la productivitat. No sempre és necessari tenir una seguretat digna del Pentàgon, cal estudiar i mesurar correctament quines són les mesures de seguretat que cal instal·lar.

A l'hora d'elaborar una estratègia de protecció física dels equips informàtics, cal identificar les amenaces i els riscos que cal avaluar. Posteriorment, s'apliquen les mesures de seguretat pertinents per tal de minimitzar aquests riscos i amenaces.

1.1 Emplaçament de les instal·lacions

Quan una companyia decideix construir unes instal·lacions noves s'han de tenir en compte molts factors abans de posar la primera pedra. Naturalment, el preu del sòl, la proximitat de clients i de distribuïdors i les estratègies de màrqueting són

factors rellevants, però des del punt de vista de la seguretat també s'han de tenir en compte altres consideracions.

Algunes empreses i organitzacions que tracten amb dades d'alt secret o confidencials construeixen les instal·lacions a llocs recòndits per tal de no cridar l'atenció de possibles persones malintencionades.

Per aconseguir poca visibilitat de les instal·lacions de vegades es construeix a ubicacions que no són d'accés fàcil i, a més a més, s'evita posar-hi logos, cartells de la companyia o qualsevol tipus d'informació que doni detalls de l'activitat que es produeix dins de les instal·lacions.

Fins fa poc temps les empreses que fabricaven targetes de crèdit tenien prohibit posar cartells o logos amb el nom de la companyia

És important avaluar la proximitat de les instal·lacions respecte a les forces de seguretat i ordre, els bombers i les instal·lacions sanitàries en funció de l'activitat a què es dediqui l'empresa. Així, doncs, per a una empresa que tracti amb materials inflamables serà un requisit important la proximitat a una estació de bombers.

L'ús de xarxes sense fil, tot i que estiguin xifrades, és una de les fonts que utilitzen els intrusos per captar informació des de fora de les instal·lacions. Per tal d'evitar la captació il·legal d'informació que viatja per ones de vegades es busquen emplaçaments on les característiques de la zona facin més difícil la propagació de les ones. Com que això no sempre és possible una alternativa és construir gàbies de Faraday (que aïllen les ones electromagnètiques).

Els elements externs són un factor important que cal considerar en la ubicació de les instal·lacions. Cada cop més, la temperatura i el clima són factors que cal tenir en compte, ja que el maquinari és molt sensible a temperatures elevades i els costos de refrigeració són cada cop més importants.

La llista següent és un recull de factors que cal tenir en compte de cara a l'elecció de l'emplaçament de les instal·lacions:

- **Visibilitat**:
  - Terrenys circumdants
  - Cartells i logos de l'empresa
  - Tipus d'empreses que hi ha als voltants
  - Població de la zona
- **Factors externs**:
  - Taxes de crim i de terrorisme
  - Proximitat a estacions de policia, bombers i instal·lacions mèdiques
- **Accessibilitat**:
  - Accés per carretera
  - Trànsit
  - Proximitat a aeroports, estacions de tren i autopistes

- **Desastres naturals**:
  - Probabilitat d'inundacions, tornados, terratrèmols o huracans
  - Riscos del terreny: allaus, despreniment de roques

Emplaçaments remots d'instal·lacions

Avui en dia hi ha empreses tecnològiques de primer ordre mundial que consideren l'elecció de la ubicació de les instalacions un factor diferencial i central dins de l'estratègia de la companyia.

Per disminuir costos en refrigeració de màquines i tenir més seguretat hi ha empreses que construeixen grans parcs de servidors a mines de carbó abandonades. D'altres, en canvi, ho fan a llocs recòndits de l'estepa siberiana.

Un dels exemples més curiosos d'instal·lacions a llocs remots és el d'un dels gegants d'Internet que està desplegant parcs de servidors en vaixells a alta mar. S'aprofita el moviment produït per les onades com a font energètica i la proximitat d'aigua per a la refrigeració de les màquines. Com que la localització dels vaixells és secreta la seguretat de les màquines és molt elevada.

1.2 Condicions ambientals

No tenir uns controls adequats de les condicions ambientals pot comportar danys tant a maquinari com a persones. L'aturada de certs serveis a causa d'aquestes circumstancies pot provocar resultats desastrosos.

Tenir els sistemes elèctrics, de temperatura, de ventilació, d'aire condicionat i de prevenció d'incendis perfectament ajustats és molt important per tenir uns nivells de seguretat correctes.

Per tal de minimitzar riscos, durant la fase de construcció de les instal·lacions l'equip de seguretat s'ha d'encarregar de revisar que les canonades d'aigua i de gas estiguin dotades de vàlvules de seguretat que impedeixen la propagació en cas de fuites.

La temperatura és un element primordial que cal tenir controlat. La majoria dels equips electrònics ha de treballar en un interval de temperatures controlat per tal de funcionar correctament.

Temperatures màximes

Els components dels ordinadors i dels equips perifèrics poden resistir fins a temperatures internes de 80 C. Els bastidors de discos i equips d'emmagatzematge es poden fer malbé a partir de temperatures internes superiors a 38 C.

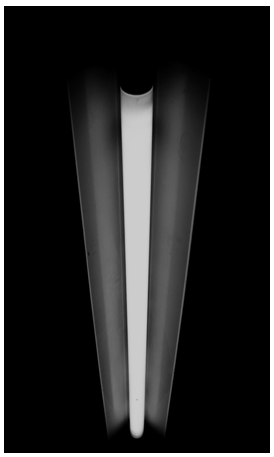
Temperatures excessives poden provocar desperfectes irreparables en els components electrònics. A més de controlar la temperatura ambiental, s'ha de revisar periòdicament el funcionament correcte dels ventiladors i d'altres components de refrigeració dels equips.

Nivells d'humitat inapropiats poden ser una font de danys en equips electrònics. Uns nivells de humitat alts produeixen corrosió en els components elèctrics, mentre que entorns massa secs provoquen massa electricitat estàtica que pot provar curtcircuits.

1.2.1 Condicions elèctriques

Podeu ampliar la informació sobre els SAI a l'apartat "Sistemes d'alimentació ininterrompuda".

Per a la majoria d'instal·lacions és necessari disposar d'un sistema d'alimentació que garanteixi la continuïtat del servei en cas de problemes externs d'alimentació. Per a això, es fan servir els sistemes d'alimentació ininterrompuda (SAI).



Els fluorescents són una de les principals fonts d'interferències de ràdio.

S'ha de controlar que no hi hagi interferències produïdes pels sistemes d'alimentació. Hi ha dos tipus d'interferències: **interferències electromagnètiques** i **interferències de ràdio**.

Si els cables utilitzats no estan aïllats degudament poden produir interferències electromagnètiques els uns amb els altres. Les vibracions produïdes per motors són una altra font comuna d'interferències electromagnètiques.

Qualsevol element que produeixi ones de ràdio és una possible font d'interferències de ràdio. La llum produïda pels fluorescents és la font més comuna d'interferència electromagnètica. Per això, s'evita passar cablejat per zones pròximes a fluorescents.

1.2.2 Ventilació

Els sistemes de ventilació tenen diversos requeriments que s'han de complir per tal de garantir un entorn segur i confortable. Per mantenir la qualitat de l'aire cal tenir un sistema d'aire condicionat de circuit tancat.

Un sistema d'aire condicionat de circuit tancat recicla l'aire que hi ha dins l'edifici un cop està filtrat degudament en comptes d'expulsar-lo a l'exterior.

L'aire condicionat és un element fonamental per mantenir la temperatura del maquinari de les instal·lacions.

Els **sistemes de ventilació** a més de tenir la funció de refrigerar també són importants per evitar l'acumulació de pols i d'altres agents contaminants.

La pols pot obstruir els ventiladors que s'encarreguen de la refrigeració interna dels equips mentre que la concentració excessiva de certs gasos pot accelerar la corrosió dels equips.

1.2.3 Mesures de prevenció d'incendis

Un incendi presenta un risc molt important de seguretat tan pel que fa a possibles destrosses de maquinari com al perill que comporta per a les vides humanes. El fum, les altes temperatures i els gasos emesos en un incendi poden crear resultats devastadors; per tant, és molt important tenir-ho en compte a l'hora d'escollir o de dissenyar unes instal·lacions.

El foc comença per la combustió d'algun element inflamable. Les possibles causes de l'inici d'un incendi són moltes: un curtcircuit, materials combustibles indegudament emmagatzemats, una cigarreta mal apagada, sistemes de calefacció defectuosos...

Perquè un foc es propagui calen dues coses: combustible i oxigen. El combustible pot ser paper, fusta, líquids inflamables... Com més combustible per metre quadrat hi hagi més ràpid es propagarà un incendi. Per tant, és molt important el disseny correcte de les zones d'emmagatzematge dels edificis per tal de minimitzar l'acumulació d'elements que puguin servir de combustible en un incendi.

Materials ignífugs

Hi ha certs materials que són resistents a les altes temperatures i al foc en general. Per mesurar si un component és ignífug o no ho és hi ha certs laboratoris que fan proves de resistència utilitzant configuracions específiques i valors ambientals determinats. A Amèrica del Nord existeix l'ASTM (Societat Americana del Verificació de Materials), que s'encarrega de fer aquestes anàlisis.

Detectors d'incendi

Hi ha diversos tipus de sistemes detectors d'incendi, alguns de manuals i d'altres d'automàtics. Els manuals consisteixen en activadors d'alarmes que són accionades quan algú detecta un possible incendi. Els automàtics tenen una sèrie de sensors que reaccionen davant de la presència de foc o de fum.

Els sistemes detectors d'incendi per fum són sistemes òptics que detecten la presència de fum en funció de les variacions de llum. Consisteixen en un emissor que envia un feix de llum a un receptor col·locat a una certa distància (normalment al sostre de la sala). Quan el receptor detecta una variació en la intensitat del feix de llum vol dir que hi ha partícules de fum en suspensió.

Un sistema de detecció d'incendis molt bàsic però efectiu és l'ús de sensors de temperatura. En cas que els sensors detectin un augment desmesurat de la temperatura, llavors llencen un senyal d'alarma. És molt important la col·locació correcta d'aquests sensors perquè siguin efectius.

Sistemes d'extinció

Els **sistemes inhibidors d'incendi** són els que permeten l'eradicació de focs. Poden ser elements manuals com ara extintors o mànegues d'aigua, o bé automàtics com dispersors d'aigua o de gasos que provoquen l'extinció del foc.

El CO_2 és un dels gasos utilitzats per a l'extinció d'incendis. Provoca l'eliminació de l'oxigen disponible, la qual cosa deixa el foc sense un dels elements necessaris per continuar combustionant. El problema que té és que no es pot aplicar si hi ha persones a les dependències, ja que les deixaria sense oxigen per respirar.

Hi ha certes escumes que també tenen la capacitat de deixar el foc sense oxigen per a la combustió. Són formades per aigua i certs agents que permeten que l'escuma floti sobre les substàncies que cremen, exclòs l'oxigen.

Els extintors són unes de les mesures bàsiques de prevenció de incendis. Cal que passin revisions cada cert temps perquè siguin fiables.

Gas haló

El gas haló era un dels compostos més utilitzat en els sistemes d'extinció de focs dels centres de dades per a l'eliminació d'incendis. Aquest gas té la capacitat d'interferir amb la química de la combustió, es barreja ràpidament amb l'aire i no causa cap dany en el maquinari de les instal·lacions.

Fa uns anys es va descobrir que el gas haló emetia clorofluorocarboni (CFC) que és un compost que fa malbé la capa d'ozó. Per aquest motiu, avui en dia ja no es fabriquen més sistemes d'extinció basats amb aquest compost.

Hi ha diferents tipus de foc en funció del material que està en combustió. Segons el tipus de foc, s'ha d'aplicar una mesura d'extinció d'incendi o una altra. La taula 1.1 mostra els tipus de focs i les mesures recomanades per a cada cas.

TAULA 1.1. Tipus de focs i els mètodes d'extinció

Classe	Tipus de foc	Elements de combustió	Mètodes d'extinció
A	Comú	Fusta, paper...	Aigua, escuma
B	Líquid	Petroli, carbó...	CO_2, escuma
C	Elèctric	Cables, material elèctric...	CO_2, pólvora seca
D	Metalls inflamables	Magnesi, sodi, potassi...	Pólvora seca

1.3 Riscos i amenaces

A l'hora de planificar una estratègia per protegir els nostres béns, s'han d'avaluar quines són les amenaces i els riscos que els poden afectar. S'entén per *amenaça* qualsevol vulnerabilitat que pugui ser explotada per un atacant. Un risc és la probabilitat que un atacant descobreixi una amenaça i l'exploti.

La **seguretat física** és el compendi de recursos, processos, tasques, equips i personal dedicats a protegir els recursos d'una empresa.

Les amenaces poden ser internes o externes. Una amenaça interna es pot deure a un incident fortuït, com un incendi o una fuita d'aigua, o bé ser malintencionada, produïda per un empleat de la mateixa empresa. Les amenaces internes poden ser difícils de controlar, perquè els treballadors d'una empresa tenen accés a informació i a coneixements que dificulten la protecció dels béns.

Les amenaces externes són originades per atacants aliens a l'empresa que volen o bé apoderar-se de béns i de coneixements, o bé malmetre recursos de l'empresa. Hi ha organitzacions que són més sensibles que altres a atacs. És molt important fer una anàlisi de riscos per avaluar quin nivell de seguretat és el requerit per a cada cas. El centre de dades d'una seu governamental requerirà uns nivells de seguretat diferents que el servidor d'una distribuïdora de discos.

1.4 Mesures de seguretat

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
- Dificultats en l'accés a personal no autoritzat
- Detecció d'intrusos
- Avaluació d'incidències

1.4.1 Mesures dissuasives

Moltes vegades es produeixen atacs perquè l'amenaça que es vol explotar és molt evident o simplement ho sembla. La finalitat de les mesures dissuasives és desplegar tota una sèrie d'elements visibles per a possibles atacants que els faci canviar d'opinió.

En alguns casos, n'hi ha prou de trencar una simple finestra per accedir a equips i informació aliena. Posar un sistema d'alarma contra aquest risc i un cartell que indiqui que hi ha una alarma activada pot evitar que possibles atacants tinguin males intencions.

Hi ha molts elements que es poden fer servir com a mesures dissuasives, els més comuns són senyals d'alerta visibles, disposar de guardes de seguretat, de gossos, de tanques, d'alarmes...

Tanques com a mesura dissuasiva

Les tanques a més a més de ser una barrera física important que dificulta l'accés a instal·lacions de personal no autoritzat són una barrera psicològica que fa saber a possibles atacants que l'empresa es pren seriosament les mesures de seguretat.

Segons les mesures de seguretat que es requereixin s'optarà per un tipus de tanques o per unes altres. Segons el material de la tanca, el gruix, l'alçària i la resistència s'aconsegueixen uns nivells de seguretat diferents.

Hi ha estudis que indiquen que tanques d'1 metre d'alt només serveixen de mesura disuassòria vers vianants casuals. Tanques de prop de 2 metres comporten una dificultat considerable per ser escalades amb facilitat, i tanques de més de 2 metres i mig impliquen que l'empresa es pren seriosament la seguretat.

Les tanques han de tenir una alçada determinada perquè siguin eficaces com a mesura dissuasiva contra intrusos.

Les mesures dissuasives són:

- Tanques
- Murs
- Barrots
- Guardes de seguretat
- Gossos
- Senyals d'alerta
- Il·luminació nocturna

1.4.2 Dificultats d'accés a personal no autoritzat

Una funció que ha de complir un pla de protecció física és disposar de mesures que dificultin l'accés a personal no autoritzat. L'objectiu d'aquestes mesures és guanyar temps perquè, en cas que hi hagi un possible atac, es disposi de prou temps per aplicar les contramesures que siguin convenients.

Hi ha diferents tipus de candaus segons el mecanisme intern que controla si la clau és vàlida o no.

Un dels mecanismes més econòmics i utilitzat per dificultar l'entrada d'atacants és l'ús de cadenats. Si uns atacants trenquen una finestra i entren a unes instal·lacions, el temps que necessiten per desactivar els cadenats pot ser crucial perquè arribin les forces de seguretat.

Hi ha mecanismes molt complexos per dificultar que els atacants arribin al bé que volem protegit. Instal·lacions d'alta seguretat, com agències d'investigació, segueixen estratègies que provenen del camp militar. En general, disposen de sistemes de protecció per capes, de manera que com més gran és la seguretat que es vol desplegar més capes de control s'han de superar per arribar-hi.

Mantrap

És un anglicisme que traduït literalment vol dir 'trampa per a persones'. És un mètode de control d'accés que impedeix que personal no autoritzat que entri a unes instal·lacions en pugui escapar.

Consisteix en una habitació amb dues portes. La primera porta està tancada, una persona s'identifica i és autenticada per un guarda de seguretat que li permet accés a la sala. Un cop s'accedeix a la sala, les dues portes es tanquen i per obrir la segona porta cal superar un mètode d'autenticació robust, com un control biomètric, o l'ús d'una targeta d'autenticació més contrasenya. En cas que no es pugui superar el control l'intrús queda atrapat a la sala.

Les dificultats d'accés a personal no autoritzat són:

- Cadenats
- Controls d'accés:
  - Biomètrics
  - Amb targeta intel·ligent
  - Amb teclat numèric
- Seguretat perimetral
- *Mantraps*

1.4.3 Detecció d'intrusos

Els **sistemes de detecció d'intrusos** s'utilitzen per detectar accessos no autoritzats i alertar el personal competent de l'incident. Es divideixen en dues categories: els que utilitzen sensors interns o els que utilitzen sensors externs.

El mecanisme bàsic consisteix a detectar canvis en l'ambient que són indicadors que s'està produint algun tipus d'intrusió. Els canvis en l'ambient poden ser lumínics, sonors, de moviment, electromagnètics... Així, un soroll o una ombra poden delatar un intrús.

Algunes pel·lícules ens mostren com els intrusos intenten burlar els sistemes de detecció d'intrusos.

Els SDI (sistemes de detecció d'intrusos) són cars i requereixen una intervenció humana per actuar vers les alarmes. És important que disposin d'un sistema d'alimentació propi perquè si no, deixant sense llum l'edifici, n'hi ha prou per evitar els SDI.

Els sistemes de detecció d'intrusos són:

- Sensors de detecció interns
- Sensors de detecció externs (sensors perimetrals)
- Detecció de canvis en l'ambient:
  - Lumínics
  - Acústics
  - De moviment
  - De camps electromagnètics

1.4.4 Avaluació d'incidències

És força habitual que en el nostre sistema de seguretat hi hagi falsos positius, cosa que vol dir que salten alarmes quan realment no s'està produint cap incident.

Si cada vegada que salta una alarma s'avisa les forces de seguretat això pot representar un problema.

Hi ha d'haver un protocol que permeti que cada vegada que hi hagi una incidència es pugui avaluar si realment es tracta d'un fals positiu o d'un atac real.

Normalment, la persona que monitora les alarmes és un guarda que no té més informació que un punt verd o vermell en un monitor. És recomanable redactar una sèrie de procediments que cal seguir quan apareix una alarma, i també tenir una estructura de comunicació.

L'estructura de comunicació indica a qui s'ha d'avisar per a cada incidència que es produeixi. Així, si hi ha l'alarma d'un vidre trencat pot ser suficient que un guarda vagi a inspeccionar la zona, si hi ha una alerta de foc a la sala de servidors trucar als bombers...

Els sistemes d'avaluació d'incidències són:

- Monitoratge dels sistemes d'alarmes
- Procediments per a casos d'emergència
- Estructura de comunicació

2. Sistemes d'alimentació ininterrompuda

Els pneumàtics que porta un vehicle motoritzat tenen les característiques adequades per garantir-ne la seguretat i el desplaçament. Segons les característiques que tingui un vehicle, caldrà utilitzar uns pneumàtics o uns altres. No és el mateix un turisme particular que un cotxe de competició de ral·lis. Per tant, tampoc no utilitzaran el mateix model de pneumàtics.

Cada model de pneumàtic ha de tenir una pressió concreta segons el model de cotxe. Si tenen poca pressió, la seguretat dels passatgers pot estar en perill. Quan el vehicle porta un cert sobrepès, es pot augmentar la pressió dels pneumàtics fins a un límit permès. Inflar-los fins a una pressió superior a la pressió límit també comportarà un risc per al vehicle i els ocupants.

D'una manera semblant, els sistemes d'alimentació ininterrompuda han de tenir les característiques adequades als equips a què es connectaran. No té cap sentit connectar un SAI de gamma alta a un ordinador personal d'un usuari domèstic. Tampoc no és normal utilitzar un SAI de gamma baixa en una habitació de servidors d'un centre de dades.

A més, un model de SAI té una capacitat limitada. Això vol dir que el nombre d'equips que s'hi connectin ha de consumir una potència inferior a la potència màxima que suporta el SAI. De la mateixa manera que no s'han d'inflar uns pneumàtics per sobre de la seva pressió límit, tampoc no s'ha de posar una càrrega superior a la càrrega màxima que un SAI pot gestionar.

A més, també hi ha dispositius de SAI amb diferents funcionaments i topologies que cal conèixer per tal de poder fer una bona elecció de l'equip.

Un altre aspecte important a l'hora de l'aplicació dels SAI és la relació entre la càrrega i l'autonomia, factors determinants en l'elecció d'un model concret. També cal tenir en compte la capacitat d'un SAI i la influència del nombre d'equips que s'hi poden connectar (càrrega). Caldrà calcular la potència que consumeixen els equips per escollir el model de SAI més adient.

2.1 Alteracions del subministrament elèctric

Els ordinadors necessiten que el seu aliment, l'electricitat, els arribi de manera constant i de la manera més pura possible. Una pèrdua sobtada de corrent elèctric produeix l'acabament immediat de qualsevol activitat informàtica. Aquests talls sobtats poden malmetre el maquinari i produir pèrdues de dades amb una importància vital.

A banda de les **apagades elèctriques**, el subministrament elèctric pot presentar altres problemes que poden fer malbé els equipaments informàtics:

- **Sobretensions**: quan el voltatge de la línia és més gran del que hauria de ser.
- **Baixades de tensió**: quan el voltatge de la línia és més petit del que hauria de ser.
- **Variació de la freqüència**: quan la freqüència del senyal elèctric és diferent de la que hauria de ser (50 Hz a Europa).

2.1.1 Sobretensions

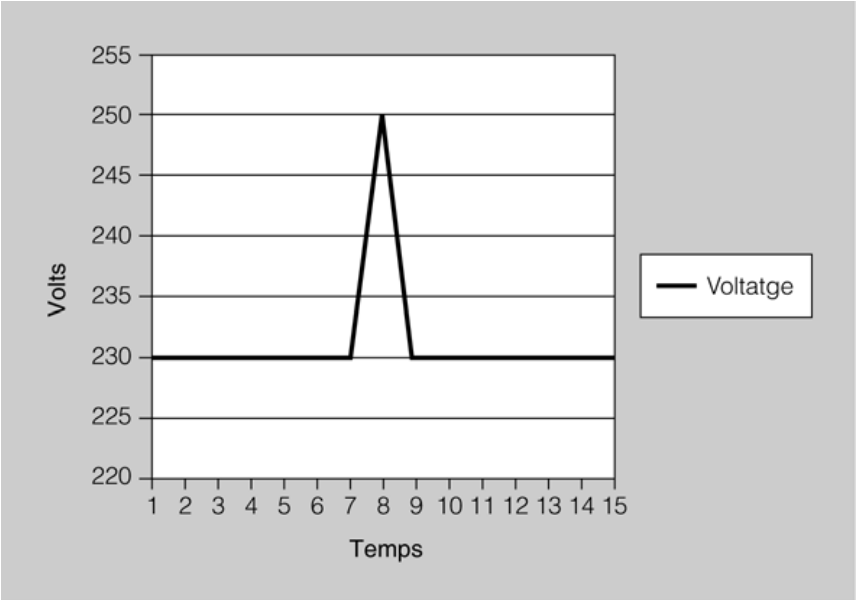
Els dispositius elèctrics i electrònics, com els ordinadors, estan dissenyats per treballar amb un **voltatge o tensió màxima** concrets. Si un dispositiu rep un voltatge superior al màxim permès, efecte conegut com a **sobretensió**, pot patir danys i desperfectes que n'impedeixin el funcionament correcte.

Per exemple, si tenim un díode electroluminescent (LED) que emet llum quan rep una tensió d'1,35 volts i suporta un màxim d'1,6 volts i el connectem directament a dues piles d'1,5 volts, el díode rebrà 3 volts de tensió elèctrica i es fondrà a l'instant. D'una manera similar, altres aparells elèctrics poden deixar de funcionar o fins i tot cremar-se si reben una **sobretensió**.

Hi ha dos tipus de sobretensions: les **permanents** i les **transitòries**, depenent de la durada que tinguin. Les més habituals són les sobretensions transitòries (figura 2.1), que duren pocs nanosegons.

Tot i la seva curta durada, una sobretensió transitòria prou elevada pot malmetre igualment un aparell elèctric.

FIGURA 2.1. Sobretensió transitòria



Les sobretensions transitòries són causades principalment per:

- Apagades elèctriques
- Llamps
- Curtcircuits
- Mals funcionaments causats per la companyia elèctrica
- Alteracions del flux de corrent de la línia elèctrica produïdes per altres equipaments (grans motors, aires condicionats...)

Un **descarregador de sobretensió** (*surge suppressor*) és un aparell que protegeix els dispositius elèctrics de les sobretensions transitòries (figura 2.2). Hi ha descarregadors de sobretensió amb **múltiples preses de corrent** que permeten connectar diversos dispositius alhora.

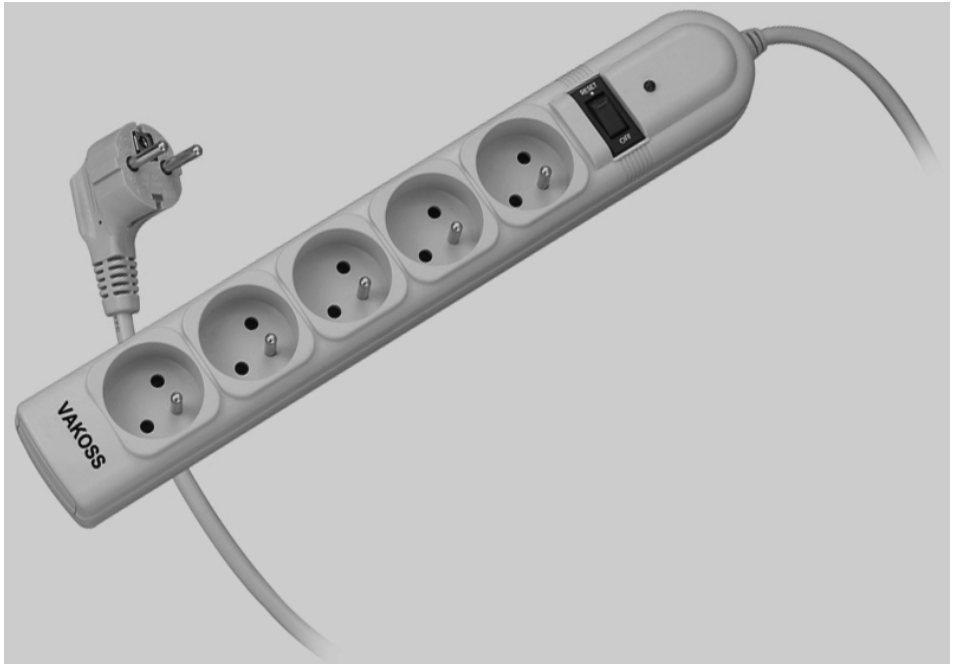
No tots els endolls amb múltiples preses de corrent porten un descarregador de sobretensió. Si no indiquen aquest tipus de protecció simplement serveixen per a subministrar el corrent elèctric.

Els descarregadors de sobretensió ofereixen una primera mesura de protecció elèctrica a un preu econòmic i, per aquest motiu, es connecten sovint a equips d'usuaris com ordinadors personals, impressores, monitors, etc. Per protegir amb més robustesa equips informàtics d'importància cabdal s'utilitzen **sistemes d'alimentació ininterrompuda** que combinen diverses mesures de protecció elèctrica.

Els llamps...

... poden provocar sobretensions tan altes que els descarregadors de sobretensió no puguin filtrar. Per tal d'augmentar-ne la protecció, els usuaris han de desendollar els ordinadors quan no s'utilitzen o en cas de tempesta.

FIGURA 2.2. Descarregador de sobretensió amb múltiples preses de corrent



Els descarregadors de sobretensió amb múltiples preses de corrent s'utilitzen com a primera mesura de protecció dels equips d'usuaris domèstics.

2.1.2 Baixades de tensió

Baixades de tensió

Per a l'equipament informàtic, les baixades de tensió són menys serioses que les sobretensions. La majoria d'equipament elèctric tolera fluctuacions de corrent més aviat grans.

Quan un gran motor s'engega consumeix una gran quantitat de corrent elèctric de cop. Això fa que es redueixi el flux elèctric per a altres dispositius connectats a la mateixa línia. Llavors es produeixen baixades de tensió momentànies.

Els **reguladors de voltatge** són circuits electrònics que mantenen un nivell de voltatge en una línia elèctrica. Eliminen sobretensions però també **baixades de tensió**. Un **mòdul regulador de voltatge** (VRM, *voltage regulator module*) és un regulador de voltatge contingut en una unitat reemplaçable.

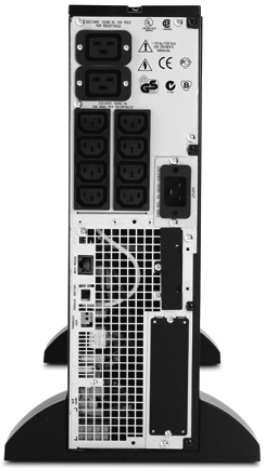
2.2 Sistemes d'alimentació ininterrompuda

Avui en dia aturar temporalment un o més servidors informàtics pot comportar fortes pèrdues econòmiques en alguns casos. Si l'aturada és causada per una apagada elèctrica, també hi ha el risc que parts del maquinari s'espatllin. En aquest darrer cas, el temps per tornar a posar a punt les màquines afectades s'incrementa encara més, ja que s'han d'aconseguir peces noves i canviar-ne les malmeses.

SAI de la companyia APC (part davantera)

Una solució al possible tall sobtat de corrent elèctric és utilitzar un o més sistemes d'alimentació ininterrompuda, coneguts com a **SAI** (*UPS* en anglès, *uninterruptible power supply*). Aquests equips asseguren una alimentació elèctrica continuada, encara que es produeixin talls de llum. A més, els SAI garanteixen una bona qualitat del corrent elèctric que arriba als aparells.

Els SAI disposen d'una o més **bateries** per subministrar l'electricitat als equips connectats. Generalment, també tenen altres elements que protegeixen de les alteracions del subministrament elèctric (sobretensions, baixades de tensió, soroll de línia, etc).



SAI de la companyia APC (part posterior)

Actualment, hi ha una gran varietat de models i fabricants de SAI, des de petits, senzills i econòmics, per a ordinadors personals; fins a grans, complexos i costosos per a **centres de processament de dades**. Depenent del fabricant i del model del SAI, s'obtindrà més o menys protecció de les alteracions del subministrament elèctric i/o una **autonomia** més gran o més petita.

Autonomia d'un SAI

En cas d'un tall de corrent, els SAI ofereixen un temps limitat de subministrament elèctric que pot oscil·lar entre els pocs minuts i algunes hores, depenent de la tecnologia del SAI i de la quantitat i de la mida de les bateries. Aquest temps extra serveix normalment per aturar les màquines d'una manera ordenada o per posar en marxa una font d'alimentació alternativa, com pot ser un **grup electrogen**.

2.2.1 Parts d'un sistema d'alimentació ininterrompuda

Per tal de poder verificar el funcionament dels sistemes d'alimentació ininterrompuda, cal conèixer les diverses parts i els components que tenen aquests aparells. En la taula 2.1 es mostren algunes de les parts principals d'un SAI que apareixen típicament en les unitats de gamma baixa o per a petits negocis. Les unitats més grans ofereixen més característiques, però no són rellevants per als usuaris d'ordinadors personals.

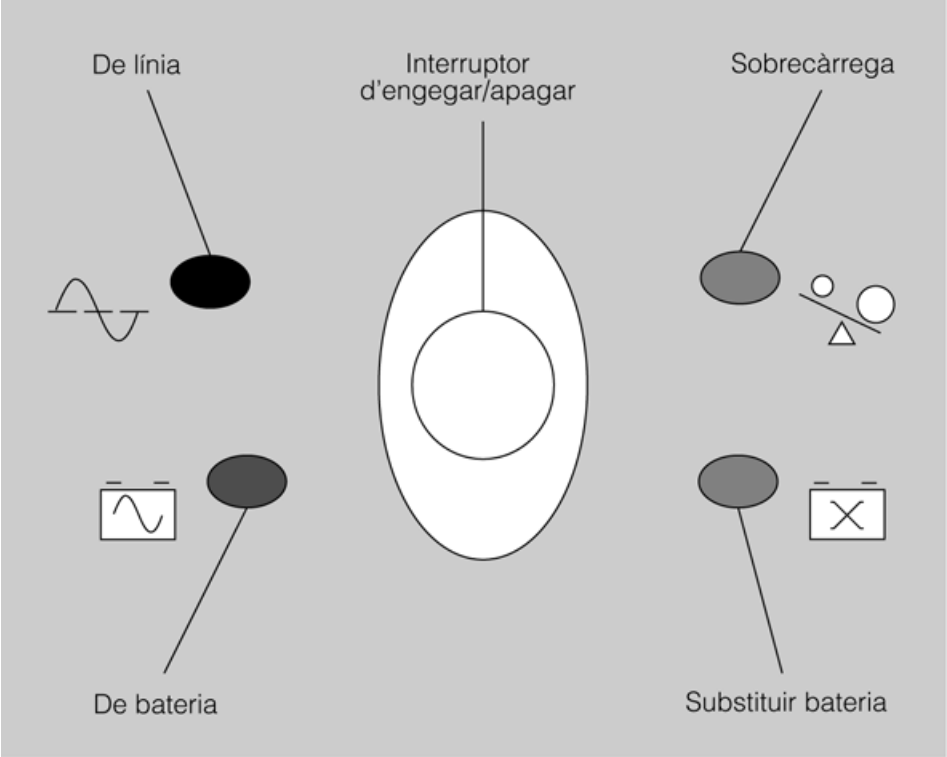
TAULA 2.1. Parts principals d'un sistema d'alimentació ininterrompuda

Component	Descripció
Circuits d'inversió i conversió	Encarregats de transformar el corrent altern de la línia principal a corrent continu per a les bateries i altre cop a corrent altern per als equips connectats. Aquests circuits es troben dins del SAI i no es veuen.
Bateria	Emmagatzema l'energia que utilitza el SAI per alimentar els equips connectats. La mida de la bateria determina, en gran part, la mida del SAI. A més, la mida de la bateria és proporcional a la quantitat d'energia que el SAI pot emmagatzemar i, per tant, de l'autonomia que tindrà.
Interruptor principal	Normalment, a la part frontal. Serveix per activar o desactivar el subministrament elèctric del SAI als equips connectats. Si s'apaga el SAI, aquests equips s'apagaran a l'instant però el SAI continuarà engegat, i carregarà la bateria mentre estigui endollat.
Connectors de corrent de sortida	Normalment, a la part posterior. Actuen com a endolls en què es connecten els equips informàtics que es volen protegir. Els SAI més cars poden tenir deu sortides d'aquest tipus o més.
Indicadors d'estat	Mostren l'estat actual del SAI. Hi ha indicadors visuals (LED) i auditius (alarmes). El nombre d'indicadors pot variar segons el model i el fabricant del SAI. Per saber què volen dir cadascun d'ells el més adient és consultar el manual corresponent.
Programes de control i monitoratge	Actualment fins i tot les unitats de gamma baixa porten programari per obtenir informació acurada de l'estat del SAI. A més del programa, cal un cable que connecti el SAI amb l'ordinador en el qual apareixeran les dades en forma gràfica.

2.2.2 Indicadors d'estat

Els indicadors d'estat d'un SAI en permeten verificar ràpidament el funcionament. En la figura 2.3 es mostren alguns dels indicadors més comuns d'un SAI.

FIGURA 2.3. Interruptor principal i indicadors lluminosos d'estat



- **De línia** (online): quan està encès indica que la unitat funciona amb corrent de la línia elèctrica. Per a un SAI de tipus *standby*, aquest és el mode normal d'operació.
- **De bateria** (on battery): si està encès indica que el SAI funciona amb l'energia de la bateria.
- **Sobrecàrrega** (overload): aquest indicador s'il·luminarà quan es connectin més equips dels que el SAI pot gestionar. Així, doncs, caldrà disminuir el nombre d'equips connectats o augmentar la capacitat del SAI, si és possible.
- **Substituir bateria** (replace battery): el SAI comprova periòdicament l'estat de la bateria. Quan la bateria estigui malament, el LED s'il·luminarà i indicarà que cal substituir-la.

Alguns SAI...

... il·luminen l'indicador de substituir la bateria quan aquesta està baixa perquè s'ha descarregat durant una apagada elèctrica. És recomanable intentar carregar la bateria endollant el SAI a la línia principal abans de concloure que s'ha de llençar la bateria.

Com que no és habitual estar mirant els indicadors lluminosos contínuament, alguns SAI disposen d'indicadors auditius per avisar de possibles problemes. El nombre de sons que es produeixen poden significar coses diverses. Consultant el manual en podrem esbrinar el significat exacte.

2.2.3 Programes de control i monitoratge

Els indicadors lluminosos d'estat donen la informació mínima necessària per detectar si tot va bé o si hi ha algun problema. Per obtenir informació extensa molts

SAI porten programes que mostren encara més dades en format gràfic mitjançant quadres de diàleg (figura 2.4).

Per obtenir tota aquesta informació cal instal·lar en un ordinador el programa que subministra el fabricant i connectar aquest ordinador al SAI amb un cable. Els SAI més antics tenien ports en sèrie, però actualment s'utilitza més sovint el port USB.

El programari de control d'un SAI varia en funció del model i del fabricant però, en general, inclou funcionalitat en les categories següents:

- **Estat**: es mostra informació de l'estat actual com la càrrega actual de la bateria, la càrrega d'equips connectats, les condicions ambientals (humitat, temperatura, etc.) i les característiques elèctriques del corrent d'entrada i de sortida.

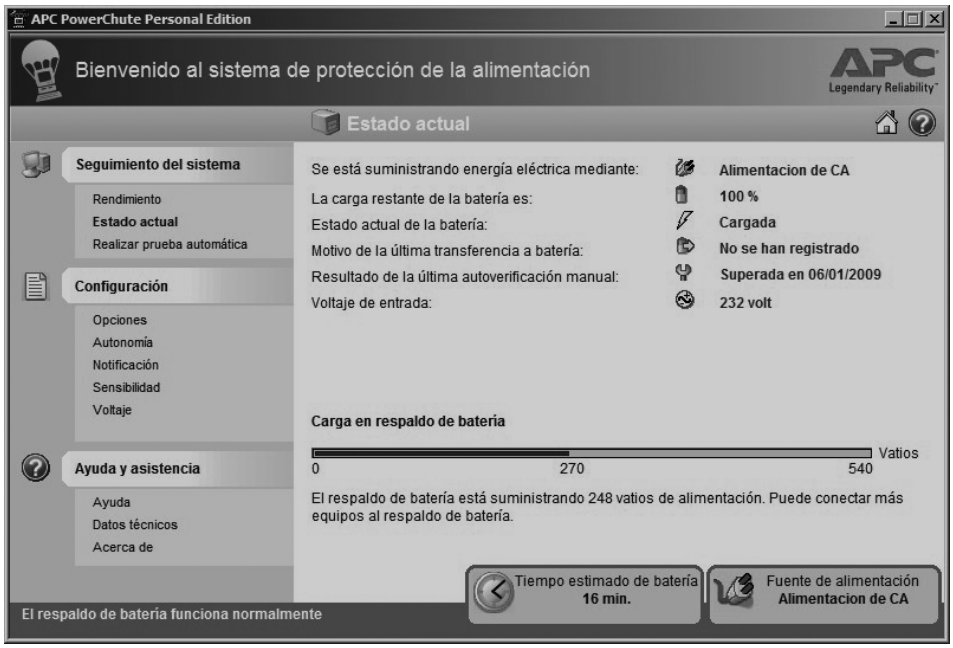
- **Registre** (logging): es manté un diari dels esdeveniments que es van donant: interrupcions de corrent, comprovacions rutinàries, etc.

- **Diagnòstic**: permet fer diverses comprovacions al SAI o planificar-les per a més endavant.

- **Alarmes PC**: permet configurar que s'enviïn notificacions a l'ordinador al qual està connectat el SAI quan apareguin problemes o que es canviï al mode en bateria.

- **Apagada automàtica**: en cas de fallada elèctrica, el SAI pot enviar les instruccions adients perquè l'ordinador es tanqui d'una manera segura, que tanqui els programes oberts i també el sistema operatiu.

FIGURA 2.4. Programa de control i monitoratge d'un SAI



2.3 Tipus de sistemes d'alimentació ininterrompuda

De manera genèrica, els SAI es classifiquen en dos tipus: els que treballen de manera continuada (*online*) i els que treballen només quan detecten un tall de corrent (*offline*). Dins de cadascuna d'aquestes categories hi ha diferents dissenys o topologies de SAI.

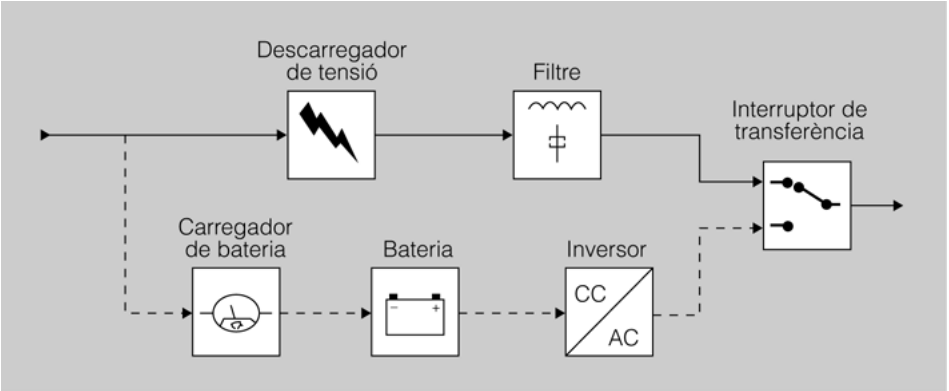
2.3.1 SAI standby

El SAI *standby* o **de reserva** és de tipus *offline* (figura 2.5). Això vol dir que, en mode normal, la bateria del SAI no subministra corrent elèctric als equips connectats, ja que aquests s'alimenten de la línia principal.

L'inversor converteix el corrent continu en corrent altern.

El **carregador de la bateria** també pren el corrent de la línia principal per carregar la bateria. La **bateria** i l'**inversor** estan a l'espera (*standby*) fins que no se'ls necessiti. Quan hi ha un tall a la línia principal, l'**interruptor de transferència** canvia i activa la font d'alimentació secundària, és a dir, la bateria. Si el subministrament elèctric principal torna, l'interruptor de transferència canvia de posició i el SAI torna a l'estat anterior.

FIGURA 2.5. Sistema SAI standby



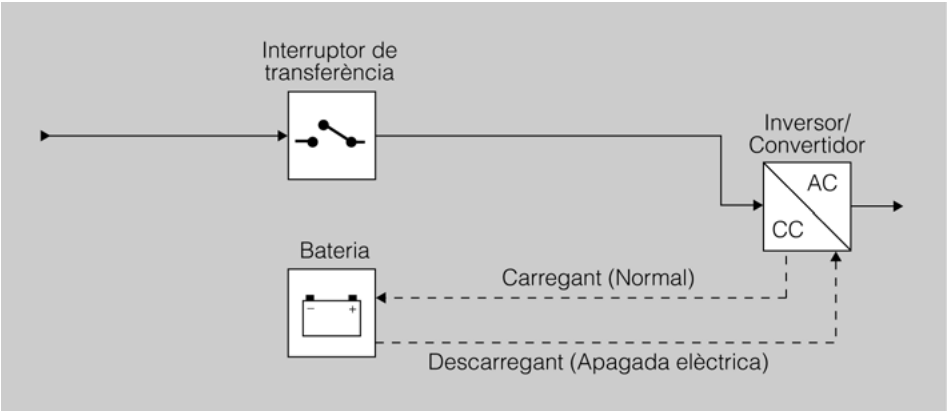
Els SAI *standby* s'utilitzen per a ordinadors personals, són de mida reduïda, tenen poca autonomia i són força econòmics.

Els SAI *standby* són de gamma baixa i tenen l'inconvenient que des que se'n va la llum fins que s'alimenta l'ordinador amb la bateria passa un interval de temps breu, de l'ordre d'una fracció de segon. Aquest temps, anomenat **temps de transferència**, és prou petit perquè no s'apagui l'ordinador connectat, però la situació ideal és aquella en què els aparells connectats reben un flux continu de corrent tant si hi ha apagades elèctriques com si no.

2.3.2 SAI interactiu de línia

Els SAI interactius de línia també són de tipus *offline*, tot i que tenen un disseny totalment diferent del dels SAI *standby* (figura 2.6). El carregador de bateria, l'inversor i el selector de la font de corrent es troben ara en l'inversor/convertidor. La línia de corrent altern és encara la font d'alimentació principal i la bateria, la secundària. Quan la línia elèctrica funciona, l'inversor/convertidor carrega la bateria, quan hi ha una apagada, aquest funciona a la inversa i obté l'energia de la bateria per alimentar els ordinadors connectats al SAI.

Figura 2.6. Sistema SAI interactiu de línia



L'avantatge principal d'aquesta topologia és que l'inversor/convertidor està sempre connectat a la sortida, alimentant l'ordinador. Això permet una resposta més ràpida en cas d'una fallada elèctrica que un SAI *standby*. Tot i això, el SAI interactiu de línia encara presenta un **temps de transferència** i no ofereix una protecció tan bona com un SAI de tipus *online*.

Els SAI interactius de línia s'utilitzen en petites empreses, servidors web i servidors de departaments.

2.3.3 SAI online

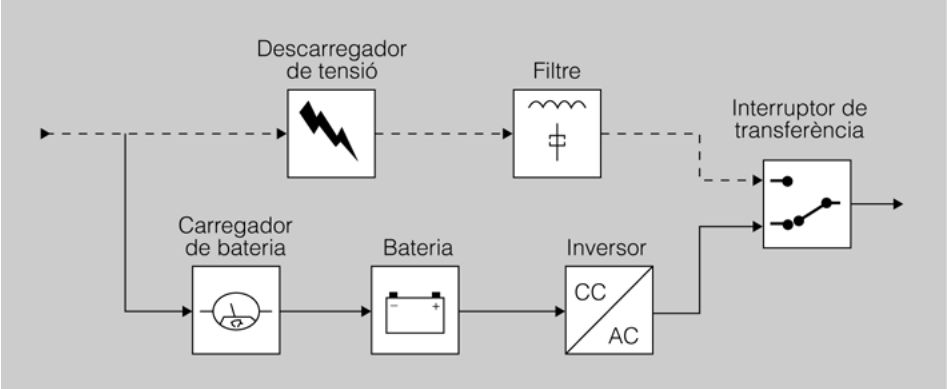
El gran avantatge dels SAI de tipus *online* és que no tenen temps de transferència en cas de fallada elèctrica (figura 2.7). L'ordinador sempre rep l'alimentació de la bateria, tant si hi ha una apagada com si no.

L'esquema del SAI *online* s'assembla al del SAI *standby* però la gran diferència és que el recorregut del corrent elèctric passa sempre per baix, de la font principal fins a l'ordinador, passant per la bateria. En el cas del SAI *standby*, el camí era per dalt. Quin sentit té, doncs, la línia discontínua de la figura 2.7? Aquesta línia secundària s'utilitza només si es produeix una fallada en l'inversor o apareix algun altre problema en la línia principal. Si no fos així es podria donar el cas que, tenint subministrament elèctric de la línia principal, els ordinadors no rebessin corrent elèctric.

Els SAI online...

... són més cars, de mida superior i amb autonomies més llargues. S'utilitzen per a grans servidors i en centres de dades.

Figura 2.7. Sistema SAI online



2.4 Aplicació dels sistemes d'alimentació ininterrompuda

Hi ha diversos factors que cal tenir en compte abans d'adquirir i d'instal·lar un SAI: la mida que té, el tipus de SAI, la càrrega que suporta, el grau de protecció contra les alteracions del subministrament elèctric, etc. Depenent del cas, escollireu un model o un altre tenint en compte el nombre i el tipus d'ordinadors que vulgueu protegir.

2.4.1 Relació entre càrrega i autonomia

Tres de les característiques més rellevants d'un SAI són la **càrrega**, l'**autonomia** i la **capacitat**, conceptes que estan relacionats entre ells.

La **càrrega** d'un SAI és el conjunt d'equips que té connectats.
L'**autonomia** d'un SAI és la quantitat de temps que podrà subministrar energia de la bateria a una càrrega concreta.
La **capacitat** d'un SAI és la potència màxima que podrà subministrar a la seva càrrega.

La capacitat de potència de sortida dels SAI s'expressa amb dos valors diferents. Per exemple, una capacitat de 330 W/700 VA per a un model concret.

La **potència aparent** és la que subministra el SAI cap a la càrrega i sempre apareix en voltamperes (VA). La **potència real** és la que consumeix realment la càrrega i sempre apareix en watts (W).

Si connecteu més ordinadors a un SAI, n'augmentareu la càrrega i disposareu, per tant, de menys autonomia. En la taula 2.2 podeu observar el quadre d'autonomies d'un SAI concret.

TAULA 2.2. Quadre d'autonomies del SAI APC Back-UPS 550VA

Càrrega (VA)	Autonomia (minuts)
80	43
160	22
320	9
480	4

Per tant, per a un mateix SAI, depenent de la càrrega que hi assigneu tindreu més o menys temps de subministrament extra. En la taula 2.2 podeu veure com amb una càrrega de 480 VA (87% de la capacitat) només tindríeu quatre minuts d'autonomia. Caldria valorar si és prou temps per dur a terme les accions posteriors pertinents.

Cal tenir en compte que la potència que necessita la càrrega no pot excedir la capacitat d'un SAI. Si fos així, el SAI patiria una sobrecàrrega i deixaria de funcionar.

2.4.2 Elecció dels SAI que cal utilitzar

Per saber quin és el SAI més adequat per a cada cas, s'han de tenir clares les qüestions següents:

- Quina serà la càrrega que haurà de suportar?
- Quanta autonomia voldrem tenir?
- De quant espai disposem per ubicar el SAI?

Càlcul de la capacitat necessària

Quan sapigueu quins equips haureu de protegir de les apagades elèctriques podreu calcular la potència real que necessiten (en watts). En la documentació respectiva o en els mateixos aparells que s'han de protegir normalment s'indica el consum en watts que tenen. Així, doncs, caldrà que sumeu els consums de tots els equips que connectareu al SAI (ordinadors, encaminadors, monitors...) i obtindreu, així, la **càrrega total necessària**.

Cal tenir en compte que haureu calculat la potència real i en cap cas no heu de confondre el valor obtingut amb la potència aparent, mesurada en voltamperes. Normalment, els fabricants indiquen les capacitats de cada SAI de les dues maneres: potència real / potència aparent.

Per exemple, un SAI amb capacitat de 300 W / 500 VA no serviria si la càrrega que necessitem és de 400 W. Aquí, l'error habitual seria prescindir de les unitats i confondre les potències per acabar concloent erròniament que, com que 400 no arriba a 500, el SAI seria vàlid per al nostre propòsit.

Autonomia volguda

Els SAI ofereixen un temps extra d'energia en cas de fallades elèctriques. Heu de tenir clar quines accions es duran a terme quan això passi. Depenent del que calgui fer, caldrà una autonomia superior o inferior.

En molts casos, amb una autonomia de pocs minuts n'hi ha prou per poder apagar els equips connectats d'una manera segura i ordenada. A més, amb el programari que ve amb la majoria dels SAI, això es pot programar per endavant i fer-se d'una manera automàtica, sense necessitat de cap intervenció humana (cosa que s'agraeix si el tall de llum es dóna a les dues de la matinada, per exemple).

En altres casos, l'autonomia haurà de ser superior per altres motius. Un possible exemple seria el de mantenir engegat un servidor que fa operacions crítiques. Si no es disposa d'un grup electrogen que subministri energia alternativa, caldrà que el SAI disposi d'una autonomia de diverses hores (la qual cosa implicarà un cost molt elevat).

2.4.3 Ubicació dels SAI

Un darrer aspecte que cal tenir en compte és on situarem el SAI en qüestió. Cal disposar d'espai a prop dels equips que s'han de protegir i amb unes condicions ambientals determinades (indicades en les especificacions de cada model).

Hi ha models de SAI que generen molta calor a causa de la càrrega continuada de les bateries i de la pèrdua energètica que es produeix en aquest procés i en altres processos elèctrics. Depenent de la quantitat de bateries o de la càrrega que tingui el SAI, la temperatura pot pujar en major o menor mesura. Si l'habitació on es troba està climatitzada com cal, s'evitaran escalfaments no volguts que poden malmetre el maquinari.

Els cables d'alimentació que es connecten al SAI han d'estar ben recollits i s'han d'evitar possibles cables enmig del pas o que pengin de qualsevol manera.

3. Seguretat lògica

La seguretat lògica és complementària respecte als elements de la seguretat passiva. El control de l'accés als equips informàtics requereix la verificació de la identitat d'una persona per tal de permetre-li l'accés a un lloc, dades i/o programes determinats. Aquestes mesures també formen part de la cadena de seguretat.

Hi ha estructures lògiques inventades per a la concreció dels drets que tindrà una persona que accedeix al sistema. Uns exemples són les matrius de control d'accés i les llistes de control d'accés. Prèviament a aplicar uns permisos determinats, però, cal autenticar la persona i la manera més habitual de fer-ho és per mitjà de contrasenyes.

Les contrasenyes poden ser molt efectives si són ben utilitzades. Amb l'aplicació d'una bona política de contrasenyes és té molt de guanyat. Cal dir que hi ha mètodes més robustos de protegir l'accés de possibles intrusos. Un dels mètodes més robustos que hi ha és l'ús de sistemes biomètrics.

3.1 Elements bàsics de control d'accés

En els sistemes informàtics, el control d'accés és una de les mesures més utilitzades per garantir la seguretat de la informació. Aquest mecanisme serveix per especificar qui o què (per exemple, un programa) pot accedir a cadascun dels recursos del sistema específic, i també el tipus d'accés que se li permet en cada cas.

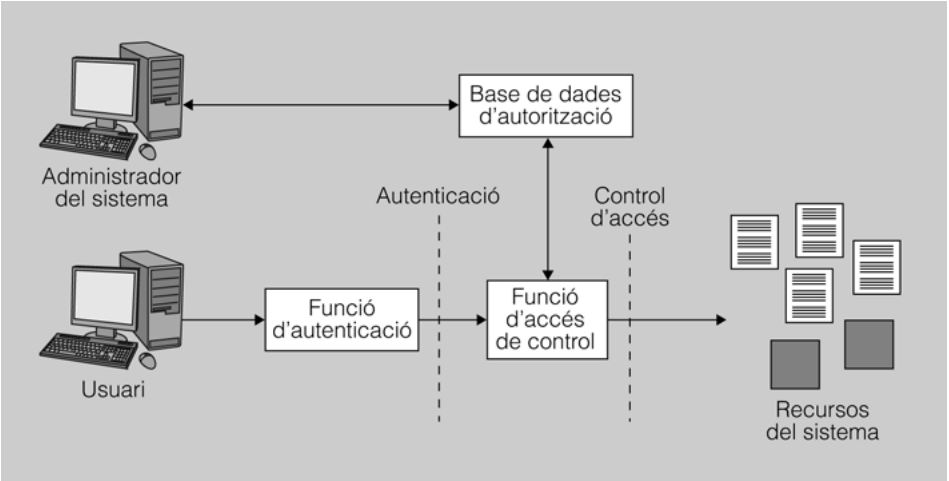
El control d'accés d'un sistema s'engloba dins d'un context més gran en què hi ha involucrades les funcions següents:

- Autenticació: verificació de la identitat d'un usuari o d'una altra entitat del sistema.
- Autorització: la concessió d'un dret o d'un permís a una entitat del sistema per accedir a un recurs del sistema.

La figura 3.1 mostra aquest esquema general en què l'usuari que vol accedir a un recurs s'ha d'autenticar primer per poder entrar al sistema. La **funció d'autenticació** determinarà si l'usuari pot passar o es queda fora. Posteriorment, la **funció de control d'accés** determinarà si l'usuari pot accedir al recurs del sistema que demana. Per fer-ho, consultarà la **base de dades d'autorització**, mantinguda per l'administrador del sistema, en què s'especifica quin tipus d'accés té cada usuari per a un recurs concret.

En la figura 3.1, la funció de control d'accés apareix com un sol mòdul. A la pràctica, això ho poden dur a terme diversos components que comparteixen aquesta funció de control.

FIGURA 3.1. Esquema del sistema d'autenticació per a l'entrada al sistema



3.1.1 Objectes, subjectes i drets d'accés

Un **objecte** és un recurs que té l'accés controlat. Normalment, un objecte és una entitat per emmagatzemar i/o rebre informació. Alguns exemples d'objecte són: registres, pàgines de memòria, fitxers, directoris i programes. Un **subjecte** és una entitat capaç d'accedir a objectes. En general, el concepte de *subjecte* va lligat al de procés. Quan un usuari o aplicació vol accedir a un objecte, en realitat ho fa per mitjà d'un procés que representa l'usuari o aplicació concrets. Tot i així, és habitual parlar d'*usuaris* com a subjectes.

Els sistemes de control d'accés bàsics normalment defineixen tres classes de subjecte, amb diferents drets d'accés per a cada classe:

- Propietari: aquest podria ser el creador d'un recurs, com un fitxer o directori.
- Grup: a més dels privilegis assignats a un propietari, un grup concret d'usuaris també pot tenir privilegis d'accés a determinats recursos. En molts casos, un usuari pot pertànyer a diversos grups.
- Altres: un nombre més petit d'accessos es concedeix a usuaris que han entrat al sistema, però que no pertanyen a la categoria de propietari o de grup per a un recurs determinat.

Un **dret d'accés** indica de quina manera un subjecte pot accedir a un objecte.

Els drets d'accés poden incloure les accions següents:

- Lectura: un usuari pot visualitzar la informació d'un recurs donat (fitxer, directori, registre...). L'accés de lectura permet copiar o imprimir recursos.
- Escriptura: un usuari pot afegir, modificar o eliminar dades d'un recurs donat.
- Execució: un usuari pot executar programes específics.
- Esborrament: un usuari pot eliminar certs recursos com fitxers o registres.
- Creació: un usuari pot crear nous fitxers, registres o directoris.

3.2 Control d'accés discrecional

Hi ha diferents tipus de **polítiques de control d'accés**. Una política de control d'accés, que es troba plasmada en la base de dades d'autorització, determina quins tipus d'accés es permeten, en quines circumstàncies i per a qui.

El **control d'accés discrecional** (DAC*, discretionary access control*) és una política de control d'accés basada en la identitat del sol·licitant i en unes normes d'accés (autoritzacions) que indiquen el que poden o no poden fer els sol·licitants. El terme *discrecional* fa referència al fet que un subjecte pot tenir drets d'accés per donar a un altre subjecte drets d'accés per a un recurs concret.

3.2.1 Matriu de control d'accés

Una implementació del control d'accés discrecional és la **matriu de control accés** (taula 3.1). Les files d'aquesta matriu representen els subjectes del sistema, mentre que les columnes representen els objectes als quals es vol accedir. Una cel·la, és a dir, la intersecció entre una fila i una columna concretes, conté els drets d'accés per al subjecte i l'objecte que es creuen.

Taula 3.1. Matriu d'accés de control

Subjectes	**Objectes**			
	/home/albert	**/home/berta**	**/home/carme**	**/etc/passwd**
Albert	Lectura, escriptura, cd			Lectura
Berta		Lectura, escriptura, cd		Lectura
Carme	Lectura, escriptura, cd	Lectura, escriptura, cd	Lectura, escriptura, cd	Lectura, escriptura

A la pràctica, la matriu de control d'accés es descompon en estructures més senzilles i manejables per implementar en un sistema operatiu o base de dades. Hi ha dues possibles opcions:

- Descompondre la matriu en columnes i associar a cada objecte una llista de qui hi pot interactuar i com. Aquesta llista s'anomena *llista de control d'accés* (ACL, *acces control list*).
- Descompondre la matriu en files i associar a cada subjecte una llista del que pot fer. Els elements d'aquesta llista s'anomenen *capacitats*.

3.2.2 Llistes de control d'accés

Els sistemes Windows fan servir el mecanisme de llistes de control d'accés (ACL). Cada objecte del sistema: directoris, fitxers, recursos de xarxa compartits, etc., té una ACL incorporada. Aquesta ACL és una llista d'entrades que contenen un usuari o grup; una operació (com lectura o escriptura), i un permís (permetre o denegar).

Quan l'usuari provi de treballar amb un objecte, per exemple obrir un fitxer, el nucli del sistema operatiu comprovarà l'ACL de l'objecte per determinar si l'operació es permet o no. En cas que l'usuari o el grup al qual pertany no estiguin acreditats per accedir a aquell objecte, el sistema operatiu li denegarà automàticament l'accés al fitxer.

D'altra banda, els sistemes operatius de la família UNIX, com Linux i Mac OS X, utilitzen un sistema híbrid. Fan servir llistes de control d'accés perquè cada objecte porta la seva llista de permisos, però també fan servir capacitats, ja que pertànyer a un grup pot significar accedir a una sèrie de drets automàticament.

3.3 Política de contrasenyes

L'origen de les contrasenyes és molt anterior als sistemes informàtics. Es feia servir des de temps remots especialment en entorns militars per comprovar si algú pertanyia al bàndol amic o al bàndol contrari.

Quan un sentinella veia que s'acostava algun desconegut li deia una senya, que bàsicament era una pregunta o una frase. El desconegut havia de respondre una contrasenya, que era la resposta a la pregunta o frase formulada. Evidentment, calia posar molta cura perquè les contrasenyes no arribessin a orelles dels enemics.

En el món dels sistemes d'informació, la funcionalitat de les contrasenyes és bastant semblant: serveix per veure si algú que intenta accedir a una zona protegida és amic o enemic, o en lèxic informàtic *usuari autoritzat* o *no autoritzat*.

Les contrasenyes són el mètode més estès per impedir accessos no autoritzats vers sistemes o continguts dins un sistema. Són una eina que és molt econòmica i ben utilitzada pot ser molt efectiva. Ara bé, igual que succeïa en el món militar cal estar segurs que la contrasenya no arriba a orelles de possibles atacants.

Segons estudis, el mal ús de les contrasenyes és a la llista de les deu amenaces més habituals dels sistemes de seguretat. L'any 2002 una periodista es va fer famosa perquè va aconseguir accés al compte de correu de Saddam Hussein. No va necessitar grans coneixements de pirateria per accedir-hi.

Una **contrasenya** no és més que un conjunt de caràcters secrets que s'utilitzen com a procés d'autenticació.

El mal ús de les contrasenyes és una pràctica molt estesa. Els usuaris moltes vegades escullen contrasenyes fàcils de recordar, però que són alhora molt fàcils d'esbrinar. D'altres vegades, la contrasenya és molt robusta però està enganxada amb un adhesiu a la pantalla de l'ordinador.

Fer un bon ús de les contrasenyes és una tasca que implica tots els usuaris d'una organització, no solament el personal de seguretat. L'obligació del personal de seguretat és definir quines són les pautes que cal seguir mitjançant la definició d'una política de contrasenyes.

Una **política de contrasenyes** és un document que regula quines són les normes de creació de les contrasenyes, les normes de protecció de les contrasenyes i la freqüència de renovació de les contrasenyes.

3.3.1 Creació de contrasenyes correctes

Perquè una contrasenya sigui efectiva ha de ser robusta, això vol dir que ha de ser difícil d'esbrinar per un possible atacant. Contrasenyes com 1234 o el nom d'un familiar són exemples de contrasenyes dèbils.

Els responsables de seguretat han de vetllar per les contrasenyes que generin els usuaris. De vegades, es poden establir regles per impedir que un usuari generi una contrasenya dèbil com, per exemple, definir una longitud mínima.

Les contrasenyes es consideren febles si compleixen alguna d'aquestes característiques:

- Tenen menys de 10 caràcters.
- La contrasenya és una paraula que apareix en algun diccionari (sigui de l'idioma que sigui).
- La contrasenya és el nom d'algun familiar, amic, company de treball, mascota, personatge famós...

- La contrasenya és alguna dada personal com la data de naixement, adreça postal on es viu...
- La contrasenya segueix algun patró numèric o alfanumèric com aaabbb, 1234, qwerty...

Per tal que una contrasenya es consideri robusta ha de complir les característiques següents:

- Contenir tant majúscules com minúscules.
- Tenir text, valors numèrics i alfanumèrics.
- Tenir com a mínim 10 caràcters de longitud.
- No ha d'aparèixer a cap diccionari.
- No s'ha de basar en informació personal.

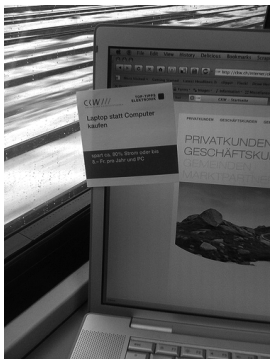
El problema que hi ha amb les contrasenyes robustes és que de vegades són difícils de recordar, amb la qual cosa acaben escrites en un tros de paper sota del teclat.

Com s'han de generar contrasenyes segures fàcils de recordar

Una tècnica per generar contrasenyes robustes és crear-les a partir d'una cançó o frase que ens sigui fàcil de recordar. Per exemple, si fem servir com a referència la frase: "Això és una manera de recordar una contrasenya" podem generar la contrasenya a partir de les inicials de cada paraula i canviar la paraula *una* pel nombre *1* i afegir-hi un caràcter alfanumèric al final: *Ae1MdR1c!*

3.3.2 Protecció de les contrasenyes

Les contrasenyes a més de ser robustes han d'estar ben protegides, ja que si arriben a mans de possibles atacants aquests poden burlar la seguretat de tot el sistema.



Perquè les contrasenyes siguin eficaces s'han de mantenir guardades en un lloc segur.

Hi ha molts mètodes pels quals els atacants poden esbrinar una contrasenya. Un mètode molt estès és el de l'enginyeria social en el qual, per exemple, un atacant truca a un usuari i li diu que és l'administrador de sistemes i li demana la contrasenya. Com que l'usuari treballa en una multinacional i no coneix en persona l'administrador de sistemes lliura la seva contrasenya a l'atacant, ja que es creu que és un administrador.

La política de contrasenyes ha d'establir de quina manera els usuaris han de protegir les contrasenyes i aplicar les regles. Les normes bàsiques de protecció de les contrasenyes són:

- No escriure mai la contrasenya en un correu electrònic.
- No dir la contrasenya per telèfon a ningú.

- No dir la contrasenya als companys d'empresa ni que siguin superiors directes.
- No parlar sobre les contrasenyes davant d'altres persones.
- No posar pistes de la contrasenya per fer-la més fàcil de recordar i alhora d'esbrinar.
- No escriure mai la contrasenya en formularis ni que siguin formularis del departament de seguretat.
- No dir la contrasenya a amics ni familiars.
- No dir a ningú la contrasenya quan es marxa de vacances.
- No escriure en cap paper la contrasenya per si de cas s'oblida.
- Canviar la contrasenya cada sis mesos com a mínim.

3.4 Sistemes biomètrics

De vegades, els requeriments quant a seguretat poden ser molt elevats com en el cas d'instal·lacions militars o governamentals. Quan la seguretat que ofereixen les contrasenyes no és suficient hi ha altres mecanismes que ofereixen més garanties com és el cas dels sistemes biomètrics.

La tecnologia que fan servir aquest tipus de dispositius és complexa i, per tant, són un mecanisme d'autenticació molt més car.

Els **sistemes biomètrics** verifiquen la identitat d'un usuari mitjançant l'anàlisi d'algun dels seus atributs físics o del seu comportament.

Un exemple de sistema biomètric basat en un atribut físic seria un lector d'empremtes dactilars. Aquests sistemes basen el seu criteri de decisió en **alguna cosa que l'usuari és**.

En canvi, una tauleta electrònica sobre la qual l'usuari escriu la seva signatura és un sistema biomètric basat en el comportament. Aquests sistemes basen el seu criteri de decisió en **alguna cosa que l'usuari fa**.

Els sistemes biomètrics que basen el criteri de decisió en algun patró de comportament tenen el problema que aquests patrons poden canviar al llarg del temps o que poden ser falsificats per atacants.

La manera de funcionar dels sistemes biomètrics és que fan un escaneig d'un patró físic o de comportament de l'usuari i el comparen amb una mostra model que tenen enregistrada. Si les dues mostres es consideren iguals llavors l'autenticació és correcta.

Els usuaris s'han de donar d'alta en els sistemes biomètrics. Durant aquest procés, el sistema biomètric recollirà una mostra del patró de l'usuari que servirà com a referència per a intents d'autenticació posteriors.

Els sistemes biomètrics, com qualsevol sistema, no són infalibles i pot ser que tinguin certs errors durant el procés d'autenticació.

Hi ha dos tipus d'errors que poden cometre els sistemes biomètrics: els falsos positius i els falsos negatius.
Un **fals positiu** es produeix quan el sistema accepta un impostor que hauria d'haver estat denegat.
Un **fals negatiu** es produeix quan el sistema denega l'accés a un usuari que hauria d'estar acceptat.

3.4.1 Tipus de sistemes biomètrics

En el mercat hi ha diferents tipus de sistemes biomètrics en funció del patró de l'usuari en el qual es basen per a l'autenticació. Els sistemes més comuns són:

- **Lectors d'empremtes dactilars**: les empremtes dactilars són formades pel relleu que es troba en els dits de la mà. Aquesta és una característica única per a cada persona.
- **Lectors del palmell de la mà**: el palmell de la mà conté informació que varia d'individu en individu. Aquesta informació inclou les empremtes dactilars i altres dades fisiològiques.
- **Lectors de retina**: aquests sistemes llegeixen el patró format pels vasos sanguinis que es troben a la retina ocular. Es fa servir una càmera que projecta un feix de llum vers l'ull i captura el patró.
- **Lectors d'iris**: l'iris és la porció de l'ull acolorida que envolta la pupil·la. L'iris conté molta informació com ara anells, colors... Aquests patrons són capturats per una càmera i es poden fer servir per identificar un usuari.
- **Lectors facials**: un sistema de reconeixement facial pot tenir en compte molts atributs com l'estructura òssia, la distància entre els ulls, la forma de la barbeta...

Els sistemes biomètrics basats en la lectura de la retina són una eina molt fiable com a mesura d'autenticació.

3.5 Autenticació d'usuaris

Perquè un usuari accedeixi a un recurs d'un sistema informàtic, prèviament cal que demostri que és qui diu que és, tingui les credencials necessàries i se li hagin donat els drets o privilegis per dur a terme les accions que demana.

La **identificació** és una manera d'assegurar-se que un subjecte (usuari o procés) és l'entitat que diu que és. La identificació pot consistir en un nom d'usuari o un número de compte. Per ser **autenticat** com cal, el subjecte també ha de proveir alguna dada addicional com, per exemple, una contrasenya, un atribut anatòmic o algun altre tipus de prova.

Un cop l'usuari ha estat identificat i autenticat, el sistema ha de comprovar si té drets per accedir al recurs que demana. Per fer això, el sistema utilitzarà algun mecanisme de control, com ara una matriu de control d'accessos. Si el sistema determina que el subjecte té accés al recurs, **autoritzarà** el subjecte; en cas contrari, li denegarà l'accés.

3.5.1 Identificació

Determinar la identitat en seguretat informàtica té tres aspectes clau:

- **Unicitat**: en un sistema cada individu ha de tenir un identificador únic. L'empremta digital o l'escaneig de la retina es poden considerar elements únics per determinar la identitat d'un subjecte.
- **No descriptiva**: cap part de la credencial no ha d'indicar la finalitat del compte. Per exemple, un identificador d'usuari no hauria de ser **webadmin**, **superusuari** o **gerent**.
- **Expedició**: els elements proveïts per una altra autoritat reconeguda per demostrar la identitat d'un subjecte. El document nacional d'identitat és un tipus d'element de seguretat que es consideraria una forma d'expedició d'identificació.

A més, en un sistema concret és recomanable establir un sistema d'identificadors estàndard. Per exemple, els noms d'usuari sempre tindran de la forma següent: de primer, el nom, després, un punt i, a continuació, el primer cognom, sense caràcters ASCII estès (accents, enyes...).

3.5.2 Autenticació

Un cop el subjecte s'ha identificat, cal que s'autentiqui, és a dir, cal que demostri que és qui diu que és. Hi ha tres factors que s'utilitzen per a l'autenticació: alguna cosa que una persona sap (autenticació per coneixement), alguna cosa que una persona té (autenticació per possessió) i alguna cosa que una persona és o fa (autenticació per característica).

- L'**autenticació per coneixement**, com una contrasenya o una combinació de caixa forta, normalment és la manera més econòmica d'implementar

l'autenticació. L'inconvenient principal és que persones no autoritzades puguin esbrinar la informació secreta i accedir igualment al sistema.

- L'**autenticació per possessió**, com una clau o targeta d'accés, s'utilitza sovint per accedir a instal·lacions, però també pot ser útil per autenticar sistemes. El problema apareix quan algú perd la seva propietat o la hi roben, cosa que es podria convertir en un accés no autoritzat.

- L'**autenticació per característica** es basa en un dels atributs físics d'una persona. Els sistemes biomètrics estàtics utilitzen atributs físics únics, com l'empremta digital o la retina per autenticar els usuaris (alguna cosa que l'usuari és). Els sistemes biomètrics dinàmics reconeixen els usuaris per la veu, les característiques de l'escriptura (alguna cosa que l'usuari fa).

- Una **autenticació multifactor** utilitza dos o tres factors d'autenticació i assegura un nivell més alt de seguretat. En general, el tipus d'autenticació multifactor més utilitzada és l'**autenticació de dos factors**. Un exemple seria aquest: un usuari vol accedir a un sistema i per fer-ho ha d'indicar alguna cosa que sap (contrasenya) i utilitzar alguna cosa que té (targeta magnètica). Una altra possibilitat podria ser una contrasenya més un atribut físic (escaneig de la retina).

3.6 Autorització

El mecanisme d'autenticació permet comprovar la identificació d'un usuari perquè accedeixi al sistema o a un recurs concret. Un cop dins, però, l'usuari només podrà fer determinades accions o accedir als recursos als quals se li ha donat permís.

L'administrador del sistema autoritza els usuaris a fer determinades tasques. Així, l'administrador té el màxim control possible del sistema i restringeix l'accés a certs recursos i limita allò que pot fer cada tipus d'usuari. Suposeu que l'usuari Joan s'ha identificat i autenticat correctament i ja és dins del sistema, accedeix a un fitxer de text i prova d'obrir el document. Abans que li aparegui per pantalla, el sistema comprovarà que l'usuari Joan té autorització per accedir al fitxer que demana. Si té aquesta autorització, podrà veure el contingut de l'arxiu; en cas contrari, se li mostrarà un missatge d'error que digui que no hi té accés.

3.6.1 Criteris d'accés

Per facilitar a l'administrador del sistema la tasca d'autoritzar l'accés als recursos, es poden establir diferents criteris d'accés mitjançant l'ús de rols, grups, localitzacions, hores d'accés i tipus de transaccions.

S'utilitzen els **rols** quan es volen donar permisos a un tipus d'usuari que fa una tasca concreta. Aquest rol es basa en un tipus de feina o funció. Per exemple, un

treballador que faci d'auditor en una empresa només requerirà accés de lectura a qualsevol transacció que es faci. Aquest rol no necessitarà privilegis per modificar o esborrar dades.

Els **grups** van bé quan es tenen diversos usuaris amb característiques semblants que requereixen l'accés a certs recursos i a certes dades. Ajuntar aquests usuaris en un únic grup i donar-los els permisos d'accés corresponents al grup és més senzill i efectiu que fer-ho individu per individu. En el cas d'un institut, es poden crear dos grups diferents: alumnat i professorat. Els directoris i els fitxers de les assignatures seran accessibles en mode lectura per als dos grups, mentre que només el grup de professors tindrà privilegis per modificar o esborrar dades.

La **localització** de l'usuari que vol accedir a un recurs és un altra manera eficaç de controlar l'accés al sistema. Aquesta localització pot ser **física**, només es pot accedir a un recurs si físicament ens trobem al mateix lloc, o **lògica**, normalment tenint en compte l'adreça de l'ordinador des d'on s'accedeix. Un exemple de localització lògica podria ser el següent: configureu un dels servidors de bases de dades de tal manera que només es poden fer consultes des de les adreces IP dels ordinadors de l'empresa.

L'**hora d'accés** és un altre mecanisme de seguretat adient per controlar l'accés al sistema. Aquest criteri permet establir les franges horàries en què es pot accedir a un recurs concret. Suposeu que teniu un servidor web per fer tràmits administratius mitjançant formularis. Es podrien configurar unes hores d'accés de vuit del matí a vuit del vespre per poder-los utilitzar. Fora d'aquest horari, no seria possible introduir cap més dada. D'aquesta manera, es podrien evitar possibles atacs que es produïssin fora de l'horari administratiu en dies feiners.

Finalment, les **restriccions per tipus de transacció** permeten controlar les dades a les quals s'accedeix durant un certs tipus de funcions i quines accions es poden dur a terme amb les dades. Quan accediu al vostre compte bancari via web, podreu veure el saldo que us queda però no podreu fer cap transferència mentre no passeu un segon nivell de seguretat.

3.7 Control d'accés als recursos i d'execució de tasques

Per garantir la seguretat d'un sistema informàtic, els usuaris s'han d'identificar i d'autenticar correctament per poder-hi accedir. Un cop dins, però, els usuaris només podran accedir als recursos per als quals se'ls ha donat permís, és a dir, els que estan autoritzats a utilitzar. D'una manera semblant, els usuaris només les tasques per a les quals se'ls ha donat dret.

3.7.1 Permisos

L'administrador del sistema pot decidir i configurar l'entorn perquè determinats usuaris no puguin veure, modificar o eliminar certs arxius o directoris, per exemple. També hi ha la possibilitat de donar certs permisos a grups d'usuaris amb característiques similars. Així, l'administrador del sistema s'estalviarà temps en donar els mateixos permisos a tot un conjunt d'usuaris (grup) en comptes de fer-ho un per un (usuari).

Hi ha diversos mecanismes per controlar qui està autoritzat a utilitzar un recurs i qui no. En general, el sistema operatiu emmagatzema per a cada recurs els usuaris i els grups que el poden fer servir i en quines condicions (lectura, escriptura, execució...). Un mecanisme per controlar els accessos consisteix a utilitzar llistes de control d'accés (ACL).

3.7.2 Els permisos en entorns tipus UNIX

Quan feu una llista en format llarg del contingut d'un directori en un sistema de tipus UNIX, podeu veure els permisos de cada fitxer o subdirectori.

```
1 > ls –l
2 total 80
3 –rw–rw–r–– 1 joan profes 31744 Feb 21 17:56 seguretat.doc
4 –rw–rw–r–– 1 joan profes 41472 Feb 21 17:56 freebsd.pdf
5 drwxrwxr–x 2 joan profes 4096 Feb 25 11:50 materials
```

Cada línia correspon a un arxiu o subdirectori, el primer caràcter indica el tipus d'objecte: arxiu normal (-), directori (d), enllaç simbòlic (l), etc.

Tot seguit hi ha nou caràcters que representen els permisos d'accés a l'arxiu o al directori en qüestió:

- Tres caràcters per a l'usuari propietari de l'arxiu o directori (*user*).
- Tres caràcters per al grup d'usuaris de l'arxiu o directori (*group*).
- Tres caràcters per a la resta d'usuaris, és a dir, que no són ni l'usuari propietari ni pertanyen al grup de l'arxiu o directori (*others*).

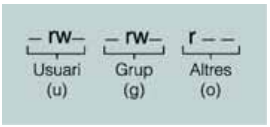
En cada grup de tres caràcters, el primer correspon al permís de **lectura** (*r*, *read*), el segon al permís d'**escriptura** (*w*, *write*) i el tercer al permís d'**execució** (*x*, *execution*). Si un caràcter conté un guió significa que no es té el permís corresponent activat.

Després dels permisos, hi ha un nombre enter que representa el nombre d'enllaços forts a l'arxiu o directori. Seguidament trobem l'usuari i el grup propietaris de l'arxiu o directori.

En la línia següent podeu veure que l'arxiu seguretat.doc pertany a l'usuari Joan, del grup profes.

```
rw-rw-r-- 1 joan profes 31744 Feb 21 17:56 seguretat.doc
```

Si observeu amb detall els permisos, veureu que l'usuari Joan té permís de lectura (r) i d'escriptura (w) sobre l'arxiu. Els usuaris que pertanyen al grup profes també tenen permís de lectura (r) i d'escriptura (w). La resta d'usuaris només disposa de permís de lectura (r). En canvi, ningú no té permís d'execució sobre l'arxiu (en ser un document tampoc no té sentit que estigui activat aquest permís).



El permís d'execució en directoris es fa servir per permetre-hi o impedir-hi l'accés. Si traieu el permís d'execució a un directori per a tots els usuaris, ningú no hi podrà entrar.

Els permisos bàsics que pot tenir un arxiu són tres: **lectura**, **escriptura** i **execució** (rwx). Aquests permisos són definits per a cadascuna de les categories d'usuaris: **usuari** propietari, **grup** i **la resta**. Per tant, cada arxiu disposa de nou permisos definits: tres per a l'usuari, tres per al grup i tres per a la resta.

L'ordre chmod

Per poder canviar els permisos en sistemes tipus UNIX s'utilitza l'ordre **chmod** (*change mode*). En general, permet indicar quins permisos voleu afegir a un arxiu o directori concrets o treure'n. Hi ha diverses maneres d'utilitzar l'ordre chmod. Per obtenir-ne una ajuda completa podeu consultar la pàgina d'ajuda corresponent (*man chmod*).

La manera més bàsica d'utilitzar chmod consisteix a indicar primer el subjecte afectat (usuari, grup o altres) seguit dels permisos que es volen afegir o restringir. Finalment, s'indica l'arxiu o directori al qual es volen canviar els permisos.

```
> chmod u=rwx freebsd.pdf
```

Afegeix tots els permisos (=rwx) a l'usuari propietari (u) de l'arxiu freebsd.pdf.

```
> chmod ugo-r materials
```

Treu el permís de lectura (-r) a tots els usuaris (ugo: *user*, *group*, *others*) del directori materials.

```
> chmod o+w freebsd.pdf
```

Afegeix el permís d'escriptura (+w) per a la resta d'usuaris (o) a l'arxiu freebsd.pdf.

Només l'administrador del sistema o l'usuari propietari pot modificar els permisos d'un arxiu o directori.

L'ordre chown

Quan es crea un arxiu, s'hi assigna automàticament un usuari i un grup propietaris. L'usuari és el que ha creat l'arxiu i el grup és el grup principal al qual pertany.

Per motius pràctics, us pot interessar canviar l'usuari propietari d'un arxiu o directori. Potser heu creat l'arxiu com a administrador del sistema (usuari *root*), però voleu que estigui disponible per a algun usuari o grup concrets.

Suposeu que heu creat l'arxiu qualificacions.doc com a usuari *root* i en voleu canviar el propietari.

- rw-rw-r– 1 root root 4292 Mar 11 22:46 qualificacions.doc

Amb l'ordre **chown** (*change owner*) ho podeu fer. El primer paràmetre és l'usuari que voleu com a nou propietari i el segon paràmetre és el nom de l'arxiu o directori en qüestió.

```
> chown joan qualificacions.doc
> ls –l
–rw–rw–r–– 1 joan root 4292 Mar 11 22:46 qualificacions.doc
```

Cal tenir en compte que només el propietari d'un arxiu pot configurar un propietari diferent (a més de l'administrador).

L'ordre chgrp

Per canviar el grup propietari d'un arxiu o directori disposeu de l'ordre **chgrp** (*change group*). El seu funcionament és semblant al de l'ordre chown, però aquest cop cal indicar primer el nou grup al qual pertanyerà l'arxiu.

```
> chgrp profes qualificacions.doc
> ls –l
–rw–rw–r–– 1 joan profes 4292 Mar 11 22:46 qualificacions.doc
```

Novament, només l'administrador del sistema i el propietari de l'arxiu poden especificar un nou grup propietari.

3.7.3 Execució de tasques mitjançant drets d'usuari

Així com els permisos permeten accedir a diferents recursos, els drets d'usuari permeten dur a terme determinades tasques. Gràcies als permisos podreu evitar que certs usuaris modifiquin o eliminin un arxiu. Amb els drets d'usuari us assegurareu que només les persones adequades poden reiniciar el sistema, canviar l'hora i data del sistema o donar de baixa usuaris, per exemple.

L'administrador d'un sistema informàtic acostuma a tenir tots els drets d'usuari activats i, per tant, pot fer qualsevol acció o tasca. Precisament, és l'administrador qui assigna els drets d'usuari a altres usuaris i grups donats d'alta.

Lògicament, cada sistema operatiu gestiona els drets d'usuari a la seva manera. En sistemes Windows, es poden consultar i modificar des de les **Eines administratives**: s'ha d'escollir primer l'opció **Directives locals** i després l'opció **Assignació de drets d'usuari**. En la taula 3.2 podeu veure alguns dels drets d'usuari que s'utilitzen en un sistema Windows 2003.

Taula 3.2. Drets d'usuari locals

Dret d'usuari	Descripció
Accedir a aquest ordinador des de la Xarxa.	Connectar mitjançant la Xarxa a un ordinador.
Fer còpies de seguretat de fitxers i directoris.	Fer còpies de seguretat del sistema. Aquest dret d'usuari està per sobre dels possibles permisos dels recursos. És a dir, tot i no tenir permís de lectura, es podran llegir els arxius per fer-ne una còpia de seguretat.
Canviar l'hora del sistema.	Configurar l'hora i/o la data del rellotge intern de l'ordinador.
Depurar programes.	Depurar aplicacions per trobar possibles errades de programació.
Forçar apagat des d'un sistema remot.	Permet que un ordinador sigui apagat o reiniciat des d'un sistema remot.
Apagar el sistema.	Permet apagar localment el servidor de Windows 2003.
Prendre propietat de fitxers o d'altres objectes.	Pren propietat de fitxers, directoris i altres objectes que no són propietat d'altres usuaris.

3.8 Registres d'usuaris, incidències i alarmes

Hi ha molts tipus de registres que poden contenir tot tipus d'informació. Normalment, la majoria d'aplicacions amb un mínim de complexitat guarda registres per poder tenir informació en casos de fallida.

En aquest punt ens interessa conèixer els registres que tenen relació amb la seguretat informàtica. Revisar el registre de l'aplicació "calculadora" pot resultar molt entretingut, però no aporta gaire informació des del punt de vista de la seguretat.

La primera tasca que cal tenir en compte és identificar quines són les aplicacions crítiques que cal avaluar en els nostres sistemes d'anàlisi de registres. Tenir un volum excessiu de registres pot ser problemàtic perquè processar la informació és una tasca molt laboriosa.

Guardar informació de registres que no es revisa és tan poc útil com no guardar-la. Les polítiques de seguretat defineixen qui és el responsable de validar la informació i amb quina freqüència ha de fer-ho.

Des del punt de vista de la seguretat, els registres que tenen més rellevància són:

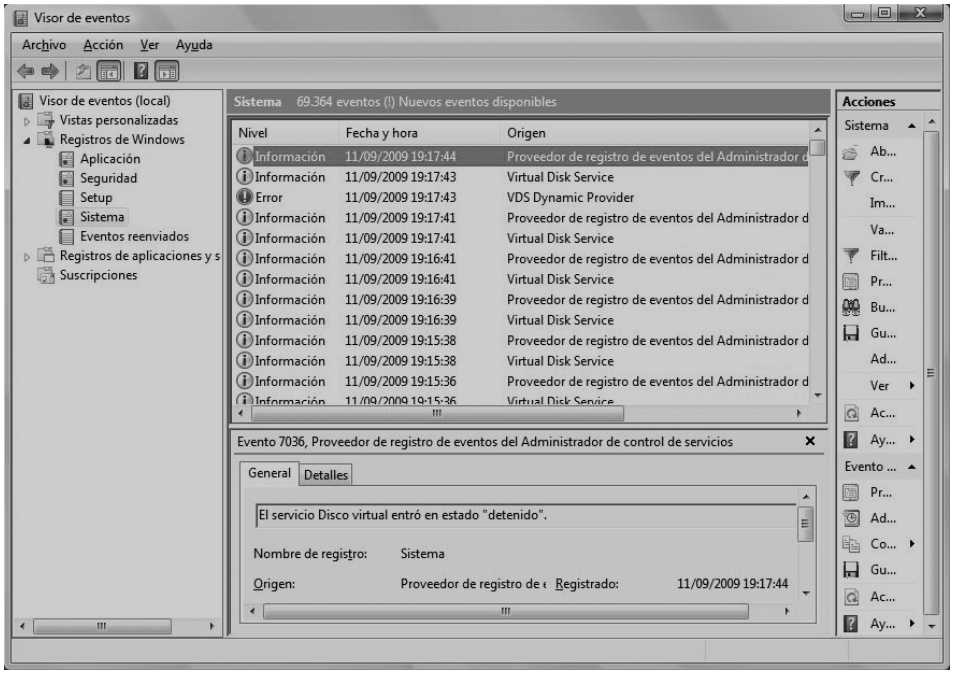
- Registres dels sistemes operatius
- Registres del programari de seguretat

3.8.1 Registres dels sistemes operatius

Hi ha gran varietat de sistemes operatius depenent del dispositiu per al qual estan destinats. Hi ha sistemes operatius per a servidors, per a equips de client, per a estacions de treball, per a dispositius de xarxa (encaminadors, commutadors...).

La gran majoria de sistemes operatius guarda registres dels esdeveniments que succeeixen sobre el sistema en què operen (figura 3.2). La informació que registren es pot dividir en dues classes: esdeveniments del sistema i esdeveniments de l'usuari.

FIGURA 3.2. Visor d'esdeveniments de Windows



Els **esdeveniments del sistema** són accions o operacions produïdes pels components del mateix sistema operatiu com, per exemple, apagar el sistema o iniciar un servei. Normalment, totes les accions que produeixen errors són enregistrades. En canvi, els **esdeveniments d'usuari** són conseqüència d'accions produïdes per un usuari.

Tot i que la informació que es registra depèn de la configuració del sistema operatiu que ha fet l'administrador, la llista següent mostra els esdeveniments que hi són típicament recollits:

- Rendiment del sistema
- Intents d'accés al sistema (fallits i satisfactoris)
- Identitat dels usuaris que han accedit al sistema
- Bloqueig d'usuaris (després d'un nombre repetit d'intents d'accés fallits)

- Data i temps dels intents d'accés al sistema
- Utilització d'eines d'administració del sistema
- Dispositius utilitzats
- Peticions d'alteració de fitxers de configuració

Aquesta informació pot resultar molt valuosa per analitzar si un sistema està sent atacat. Així, doncs, per exemple, un decrement molt accentuat del rendiment pot ser un indicador que hi ha algun virus o cavall de Troia.

Sintaxi dels registres

La manera com es mostra la informació pot variar molt d'un sistema operatiu a un altre. Cal un cert coneixement del sistema operatiu per poder interpretar la informació que apareix en el registre. A continuació, es mostra un exemple de registre de Windows:

```
Event Type: Success Audit Event Source: Security
Event Category: (1)
Event ID: 517
Date: 362009PM
Time: 2:56:40
User: Admin\SYSTEM
Computer: KENT
Description: The audit log was cleared
Primary User Name: SYSTEM
Primary Domain: Admin
Primary Logon ID: (0x0,0x3F7)
Client User Name: userk
Client Domain: KENT
Client Logon ID: (0x0,0x28BFD)
```

3.8.2 Registres del programari de seguretat

Cada vegada hi ha més programari per protegir la seguretat dels sistemes informàtics. Aquest tipus de programari enregistra qualsevol informació que pugui ser d'utilitat.

La majoria de programari de seguretat es configura perquè si es produeixen certs tipus d'esdeveniments a més a més d'enregistrar-los es dispari una alarma que enviï un correu electrònic a l'administrador del sistema.

Entre el programari de seguretat que pot generar registres cal fer menció especial a:

- **Antivirus**: guarden registre de virus, cavall de Troia i altre programari maliciós detectats. També enregistra desinfeccions de fitxers i quarantenes (bloquejar el fitxer) aplicades. De vegades, també enregistra quan es produeixen actualitzacions de les bases de dades de virus i escanejos del sistema.
- **Encaminadors**: són dispositius de xarxa encarregats de fer arribar la informació a diferents equips. Normalment, es configuren per permetre o

A l'actualitat molts usuaris tenen encaminadors a les xarxes domèstiques perquè diversos equips pugin connectar-se a Internet.

bloquejar determinats tipus de tràfic de dades. Cada vegada que es bloqueja tràfic de xarxa que pugui ser perillós s'enregistra l'esdeveniment.

- **Tallafocs**: de la mateixa manera que els encaminadors, permeten o bloquegen determinats tipus d'accions basats en una política de decisió. Els tallafocs guarden registre de tota l'activitat que monitoren.

- **Servidors intermediaris (** *proxies* **)**: són servidors intermediaris mitjançant els quals s'accedeix als llocs web. Els usuaris en comptes de fer peticions directament, el servidor intermediari les fa per ells. Es poden configurar per bloquejar l'accés a determinades pàgines web que puguin ser perilloses. Es guarda registre de totes les peticions que arriben al servidor intermediari.

- **Programari d'accés remot**: de vegades hi ha empreses que permeten accedir als sistemes des de fora de les instal·lacions mitjançant l'ús de programari d'accés remot. Els atacants poden intentar fer servir aquesta porta d'entrada per accedir als sistemes informàtics. El programari d'accés remot enregistra tots els intents d'accés per poder detectar si usuaris no autoritzats intenten accedir al sistema.

3.9 Gestió de registres

Gestionar correctament els registres és clau per poder extreure la informació necessària, sobretot quan ens enfrontem a grans volums d'informació.

Per tal que la feina de gestió dels registres sigui més senzilla és necessari que els administradors configurin correctament els sistemes. Per a una gestió i configuració correctes dels registres cal tenir en compte el següent:

- **Evitar tenir massa fonts de registres**: si hi ha massa registres dispersos en servidors per tota l'organització la gestió es dificulta.

- **Inconsistència de les dades**: de vegades per augmentar l'eficiència només s'enregistren les dades més rellevants. Això pot representar un problema a l'hora de rastrejar incidents si les dades no són consistents. Un exemple seria que un registre emmagatzemi la IP però no el nom d'usuari. mentre que un altre enregistri el nom d'usuari però no la IP.

- **Inconsistència temporal**: una de les dades importants que s'ha d'enregistrar és la data i l'hora de quan succeeix un esdeveniment. La majoria de vegades la font horària que es fa servir és l'hora del servidor en què es troba el registre. Si tots els sistemes no estan sincronitzats temporalment això pot crear confusions en analitzar els registres.

- **Inconsistència de formats**: la informació que es desa als registres es pot trobar en formats molt diferents. De vegades, en XML, d'altres, en valors

separats per comes, d'altres, en bases de dades... Tenir massa formats diferents augmenta molt la complexitat de la gestió dels registres.

- **Informació sensible**: a l'hora de configurar quina informació s'enregistra no és pot ometre la informació especialment sensible com l'activitat dels comptes amb privilegis de *root* o administrador.
- **Utilitzar eines de gestió de registres**: analitzar els fitxers de registre (*logos*) manualment és una tasca que requereix molt temps. De vegades, resulta rendible adquirir una eina de gestió de registres.

3.9.1 Protecció dels registres

Si un atacant atracador accedeix a la caixa forta d'un banc un cop perpetri el robatori farà tot el possible per eliminar les pistes del crim. El mateix s'aplica per als fraus informàtics, l'atacant intentarà esborrar qualsevol registre que el pugui incriminar. Sense la informació dels registres no és possible adonar-se que s'ha produït un atac.

La informació que hi ha als registres ha d'estar protegida. Només certes persones (administradors o personal de seguretat) ha de poder veure, modificar o esborrar la informació dels registres.

La integritat s'ha d'assegurar mitjançant mètodes criptogràfics, de manera que si algú altera les dades del registre es pugui detectar.

De vegades, pot ser convenient xifrar la informació dels registres per tal de garantir-ne la confidencialitat. També es pot enregistrar aquesta informació en discos de CD-ROM per evitar la pèrdua o l'alteració de les dades enregistrades.