1. Seguretat activa

La seguretat activa inclou una sèrie d'eines, com els programes antivirus, els programes que rastregen el trànsit d'informació per mitjà de la xarxa, la configuració dels sistemes operatius i de les diferents aplicacions, la realització de còpies de seguretat tant de les dades com de la configuració del mateix sistema, les eines de control i verificació del programari i les actualitzacions corresponents, les certificacions digitals i altres utilitats.

Tots aquests elements configuren la part de la seguretat informàtica coneguda com a *seguretat activa*, que està destinada a disminuir els efectes nocius en els sistemes i a recuperar aquests sistemes de la manera més ràpida possible.

En l'apartat de la seguretat activa, la seguretat informàtica ha d'estar destinada a actuar sobre una sèrie d'elements del sistema informàtic, com el sistema operatiu, les aplicacions, els sistemes identificatius, els plans de contingència en cas de fallades de seguretat, la recuperació de dades i, d'una manera molt especial, les intrusions de virus i altres elements nocius per al sistema informàtic.

Sistema informàtic

Un sistema informàtic, com tot sistema, és el conjunt de parts interrelacionades, maquinari, programari i recursos humans.

1.1. Fallades de seguretat: plans de contingència

Els vostres sistemes informàtics estan seriosament afectats tant per l'existència dels coneguts *hackers*, *crackers*, pirates telefònics (*phreakers*) i *wannabes*, que mitjançant les intrusions en el sistema, el malmeten i hi produeixen moltes fallades de seguretat; com per l'existència de virus, cavalls de Troia, cucs, programes espia (*spyware*), pesca (*phishing*) i correu brossa (*spam*), que també malmeten el sistema d'una manera significativa.

Els atacs i les intrusions dels *hackers* poden anar des de la simple obtenció d'informació fins a la supressió de dades o l'apoderament de la màquina. Igualment, els virus i la resta de programari maliciós poden alentir el funcionament de la màquina, col·lapsar el correu o bé acabar impedint que la màquina funcioni.

Tenint en compte que la seguretat total no existeix i que sempre hi haurà algú capaç de superar totes les barreres i entrar en un sistema, cal que mantingueu la seguretat dels vostres sistemes informàtics i que sempre intenteu prevenir les situacions de risc. En aquest sentit, la vostra seguretat començarà per instal·lar i configurar correctament el sistema operatiu.

Heu de tenir en compte que, actualment, disposeu de dos tipus de sistemes operatius, els **sistemes operatius de pagament** i els sistemes operatius coneguts com a **programari lliure**. A part de la diferència que hi ha en la manera de produir cada sistema i del fet que un és de pagament i l'altre no, també hi ha diferències pel que fa a la seguretat i la quantitat de virus.

Programari lliure

El *programari lliure* (en anglès *free software*) és el programari que pot ser usat, estudiat i modificat sense restriccions. També es pot copiar i redistribuir, tant en una versió modificada com en una versió sense modificar. Tot això es pot fer sense cap restricció o amb unes restriccions mínimes per garantir que els destinataris futurs també tindran aquests drets.

Una vegada escollit el sistema operatiu i instal·lat en la màquina, caldrà configurar-lo correctament. Per fer-ho, anireu al centre de seguretat i activareu les actualitzacions del sistema perquè sempre tingui les últimes actualitzacions. Quan creeu els usuaris, només els donareu els privilegis necessaris perquè puguin fer les tasques pertinents. Igualment, escollireu com han de ser les contrasenyes per a aquests usuaris. Heu d'intentar que siguin difícils per evitar que algú que intenti desxifrar-les ho aconsegueixi.

Igualment, hi ha tot un ventall d'opcions de configuració del sistema que tindreu en compte. Per exemple, en els sistemes de propietat, podreu activar l'opció de visualitzar sempre les extensions dels arxius. D'aquesta manera, quan rebeu un correu electrònic amb un arxiu adjunt, encara que suposadament sigui d'un contacte de confiança i l'arxiu tingui una icona coneguda (com ara la d'un arxiu del processador de textos Word), abans de fer-hi un doble clic al damunt, si veieu que té una extensió *.exe*, no l'obrireu, ja que probablement conté un codi maliciós que s'executaria en el moment d'obrir-lo.

Els sistemes operatius també us ofereixen la possibilitat de crear i automatitzar les còpies de seguretat, tant per a dades guardades com per a la mateixa configuració del sistema. D'aquesta manera, podreu recuperar el vostre sistema més ràpidament i retornar-lo a la configuració personalitzada.

Una vegada instal·lat el sistema operatiu, instal·lareu les aplicacions. Una bona mesura de seguretat consisteix a instal·lar només les aplicacions que necessiteu. Les heu de tenir controlades, perquè si en algun moment detecteu una aplicació que no havíeu instal·lat, ja sabreu que es tracta d'una intrusió. Cal que us assegureu que les aplicacions que instal·leu són autèntiques i tenen la llicència corresponent. També convé que mantingueu les aplicacions actualitzades.

Seguidament, instal·lareu i mantindreu actualitzat un programa antivirus i un tallafoc.

Tallafoc

Un tallafoc (*firewall* en anglès, que originalment vol dir 'mur ignífug'), és un element de maquinari o programari utilitzat en una xarxa d'equips informàtics. Serveix per controlar les comunicacions,que permet o prohibeix segons les polítiques de xarxa que hagi definit l'organització responsable d'aquesta xarxa.

Un **antivirus** és un programa informàtic que intenta identificar, aturar i eliminar virus informàtics i altres tipus de programari maliciós (*malware*).

Els programes antivirus solen fer servir dues tècniques diferents per aconseguir l'objectiu que tenen. Són les següents:

- **Examinar (escanejar) arxius** per buscar-hi virus coneguts que s'ajustin a les definicions recopilades en un diccionari de virus.

- **Identificar comportaments sospitosos** de qualsevol programa informàtic que puguin suggerir una infecció. Aquesta anàlisi pot incloure captures de dades, monitoratge de ports i altres mètodes.

La majoria dels antivirus comercials utilitzen ambdues tècniques. Especialment, la del diccionari de virus.

Fins i tot podeu anar més enllà i controlar quins ports té oberts el vostre sistema. D'aquesta manera, podeu indicar-hi que només estiguin oberts els que realment necessiteu per treballar, cosa que dificulta l'entrada d'intrusos. Igualment, podeu posar contrasenyes a les carpetes o codificar els arxius que heu creat.

Totes aquestes actuacions estan destinades a impedir que els atacs externs al vostre sistema tinguin efectes nocius mínims. Però què passa si no podeu evitar els efectes del programari malintencionat o les intrusions de persones que han aconseguit saltar-se totes les barreres? Hi ha una part de la seguretat activa que actua en aquestes situacions; són els **plans de contingència**. Cal que estigueu previnguts per actuar en les situacions en què el sistema ha estat vulnerat per tal que els danys hi siguin mínims i la recuperació sigui al més ràpida possible.

1.1.1. Fallades de seguretat

Els errors en seguretat poden afectar tant la part del maquinari com la del programari. Predominantment, però, afectaran les dades que teniu guardades en el sistema, ja que seran, en la majoria dels casos, l'objectiu dels possibles atacs externs.

En el vostre sistema, la majoria d'errades de seguretat es produeixen en els navegadors, el correu electrònic, els paquets ofimàtics i les aplicacions relacionades amb la reproducció multimèdia. En els servidors, la majoria d'errades de seguretat es produeixen en els serveis d'aplicacions web, les eines d'administració dels servidors i el programari de bases de dades. Especialment, hi ha aplicacions, com les de missatgeria instantània i les de compartició d'arxius P2P, que són una font important d'entrada de virus i programes maliciosos. Això és degut a la manera com funcionen, que necessita l'obertura de determinats ports a la vostra màquina, i també al fet que són aplicacions amb un gran nombre d'usuaris.

Mantenir aquestes aplicacions degudament actualitzades amb les últimes actualitzacions de seguretat és un primer pas per millorar la seguretat del sistema. L'altre pas és instal·lar i actualitzar un antivirus i un tallafoc.

Aquestes fallades de seguretat permetran atacs en el vostre sistema. És possible que es detectin ràpidament si consisteixen, per exemple, a canviar el contingut d'una pàgina web. Contràriament, també és possible que els efectes de l'atac no es detectin fins al cap de molt de temps o, fins i tot, que no es detectin mai. És molt important detectar ràpidament un atac per tal de minimitzar-ne els efectes i restaurar el sistema com més aviat millor.

Els efectes dels atacs produïts per una fallada de seguretat poden ser de diversos tipus, des de l'apoderament d'informació fins a la instal·lació de programes nocius o la corrupció del sistema operatiu o d'algunes de les aplicacions instal·lades. Aquestes accions poden ser especialment greus si es produeixen en empreses o institucions que tinguin dades personals susceptibles. I encara més greus si intercepten les dades bancàries o les d'una targeta electrònica, ja que després les podran utilitzar.

Per tant, és molt important evitar totes aquestes errades de seguretat, ja que les conseqüències que se'n derivin poden ser molt importants. De totes maneres, no és fàcil evitar-les. Fins i tot els sistemes que tenen més seguretat, com la NASA i el Pentàgon, alguna vegada han patit atacs de *hackers* que hi han aconseguit entrar.

Els *hackers* han arribat a atacar el Pentàgon, seu del Departament de Defensa dels EEUU.

1.1.2. Plans de contingència

Quan detecteu una intrusió, el sistema mostra els efectes d'haver patit una intrusió o cau, cal que disposeu de mecanismes per minimitzar els efectes de l'atac i recuperar el sistema com més aviat millor. Per aconseguir-ho, hi ha els plans de contingència.

Aquests plans de contingència tenen la màxima utilitat en les empreses o institucions, ja que és en aquests llocs on els efectes d'un atac poden ser més importants o tenir més impacte.

Entenem per **pla de contingència** el conjunt de procediments alternatius a l'operativitat normal de cada empresa, la finalitat dels quals és permetre el funcionament de l'empresa fins i tot quan alguna de les funcions deixa d'operar a causa d'algun incident, tant intern com extern a l'organització.

El pla de contingència ha de ser un pla que permeti a l'empresa o la institució poder continuar funcionant quan hi ha alguna incidència de seguretat. Alhora, ha de donar instruccions que indiquin com s'ha de resoldre i com s'ha d'actuar. Així doncs, l'existència d'aquest pla és molt important. En cas que no hi fos, elaborar-lo hauria de ser una prioritat.

El fet de preparar un pla de contingència no implica reconèixer que la gestió de l'empresa és ineficient. Al contrari, és un gran avanç a l'hora de superar totes les situacions de risc que poden provocar pèrdues importants. Poden fer que es perdi material, però també provocar que el negoci es paralitzi durant un període de temps més o menys llarg.

Si hi ha aquest pla, cal tenir-lo a l'abast. També convé que les persones responsables de dur-lo a terme segueixin les instruccions d'una manera ràpida i precisa.

L'elaboració d'un pla de contingència consta de les fases següents:

1) Avaluació
2) Planificació
3) Proves de viabilitat
4) Execució
5) Recuperació

Les tres primeres fases de l'elaboració fan referència a la part preventiva: analitzar i avaluar els riscos del sistema en qüestió, fer una planificació de les accions que s'han de dur a terme per protegir el sistema i comprovarne l'eficàcia mitjançant les proves de viabilitat.

Les dues últimes fan referència a l'execució del pla una vegada ja ha ocorregut el sinistre en el sistema: quins passos s'han de seguir una vegada s'ha detectat un atac i com es farà la recuperació del sistema.

L'avaluació, la planificació i les proves de viabilitat dependran de cada sistema en particular. D'aquesta manera, per dur-les a terme, s'haurà de tenir en compte de quins elements consta el sistema, quines dades cal protegir, etc.

Ara veureu un exemple dels dos últims punts d'un pla de contingència en un sistema senzill, com el que podríeu tenir a casa o el que podria tenir una empresa petita. Aquests dos últims punts fan referència a les actuacions que cal seguir quan es detecta una intrusió en el sistema. La intrusió es pot detectar perquè, per exemple, l'ordinador té un comportament diferent, en desapareixen arxius, funciona amb molta lentitud, etc. Quan se sospita que hi ha algun atac que afecta el sistema, cal actuar amb rapidesa, ja que sempre val més curar-se en salut.

Els dos primers punts de l'exemple següent corresponen a l'apartat d'execució i l'últim, al de recuperació.

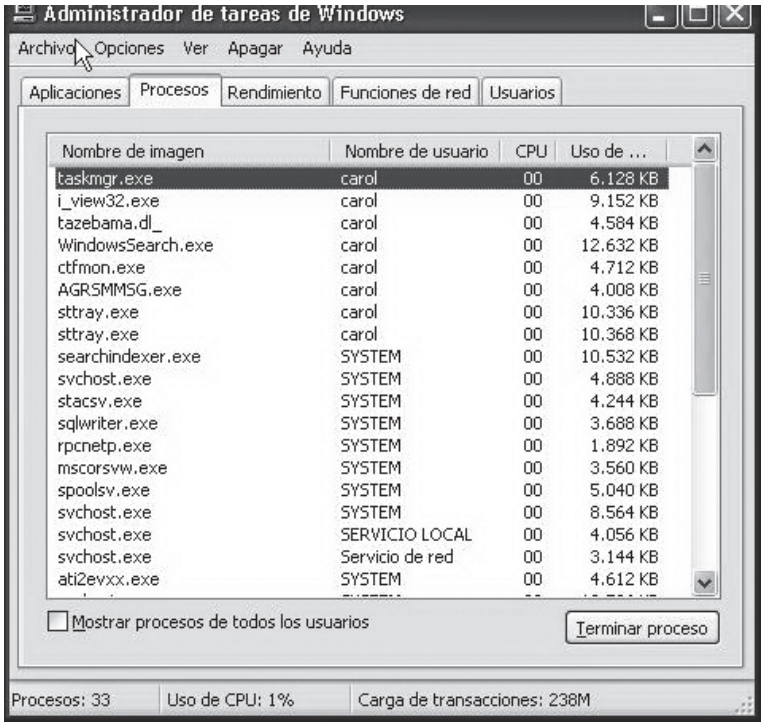
1) La primera cosa que heu de fer és **aïllar l'ordinador** per evitar que l'atacant continuï actuant. Per fer-ho, tancareu totes les aplicacions que s'estan executant en l'ordinador i **guardareu els arxius** de dades que estiguin utilitzant aquestes aplicacions.

En cas que l'ordinador actuï com a servidor, cal parar temporalment tots els serveis i recursos que s'estiguin executant. Així, evitareu que l'atac es propagui als ordinadors clients.

Per evitar que l'atac es propagui a altres ordinadors, en cas que l'ordinador infectat estigui connectat a una xarxa, és recomanable **desconnectar-lo** i, si és possible, fins i tot desconnectar-lo físicament. També és recomanable **bloquejar tots els comptes d'usuari de l'ordinador**, excepte el d'administrador. D'aquesta manera, s'evitarà que s'executin més programes a l'ordinador i que interfereixin en les tasques d'administració. Igualment, evitarà que l'atac afecti més arxius de dades i programes.

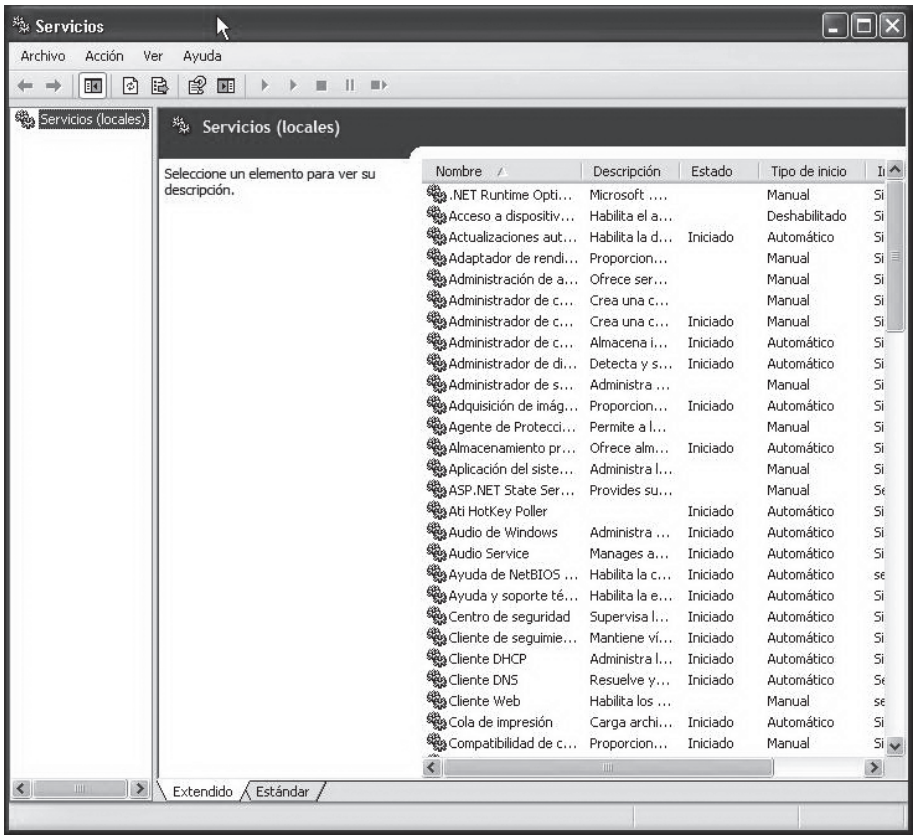
El pas següent és intentar **veure quina vulnerabilitat utilitza l'atac** per sabotejar l'ordinador. La millor manera de saber què hi passa és mirar quins programes s'hi estan executant. Abans, però, s'han de tancar tots els programes que s'estaven utilitzant. S'haurà de mirar quins són els consums de memòria i de processador de cada programa i servei que quedin en execució. Per fer-ho, si es tracta d'un sistema Windows, podeu utilitzar l'administrador de tasques, tal com podeu veure en la figura 1. En cas que es tracti de Linux, podeu fer servir el monitor del sistema.

Figura 1. Administrador de tasques d'un sistema Windows



D'aquesta manera, podrem trobar l'aplicació que paralitza el sistema i aturar-la. Convé apuntar el nom del programa i el de l'executable associat. Si ho fem, després el podrem buscar i comprovar si aquesta aplicació hauria d'estar instal·lada i si cal eliminar-la del sistema. Els serveis poden proporcionar una altra pista, tal com es pot veure en la figura 2.

Figura 2. Serveis en un sistema Windows



Quan mireu els que es troben en execució, podreu veure si hi ha algun servei que consumeix més ús de processador del compte. Si veieu que hi apareixen arxius nous amb noms i extensions estranyes, n'hauríeu de veure el contingut amb algun editor de text, com el *Bloc de notes* si parlem de Windows o l'editor *Vi* si parlem de Linux. D'aquesta manera, potser podreu saber quin tipus d'atac patiu.

Podria ser que hi apareguessin aplicacions que no heu instal·lat. En aquest cas, les haureu de desinstal·lar. També haureu de desinstal·lar les aplicacions que tinguin noms molt estranys. Sempre és millor desinstal·lar un programa i tornar-lo a instal·lar que no pas tenir-ne un d'instal·lat que perjudiqui la màquina.

2) Seguidament, s'intentarà **posar remei a la vulnerabilitat** que utilitza l'atacant. No sempre podreu saber amb exactitud quina vulnerabilitat concreta utilitza l'atac, però sí que us podreu fer una idea aproximada de la procedència d'aquest atac. El més convenient és buscar una actualització de seguretat que elimini la fallada de seguretat en l'aplicació o en el mateix sistema operatiu.

Després d'actualitzar l'ordinador, cal eliminar els serveis que es trobin actius i desinstal·lar les aplicacions dubtoses. També convindria fer una cerca exhaustiva en l'ordinador amb un antivirus actualitzat per eliminar els possibles virus que el puguin estar infectant i atacant. També seria recomanable instal·lar algun programa antiespia (***antispyware***) per eliminar els programes espia, tant d'adreces de correu com de publicitat no desitjada, que podrien estar alentint l'ordinador.

3) Finalment, caldria **reparar els danys** que pugui haver provocat l'atac. Per tal de recuperar les dades perdudes i també les que es puguin haver danyat, n'hi haurà prou amb **restaurar l'última còpia de seguretat** que tingueu de les dades. Tindreu còpies de seguretat si heu fet una bona planificació en l'apartat corresponent del pla de contingència.

És possible que hagueu de **reinstal·lar algun programa** si s'ha danyat. Una vegada fet això, és recomanable **canviar les claus d'accés** dels usuaris de l'ordinador.

Us hauríeu de **replantejar els permisos** dels usuaris. Finalment, **restaureu la connexió** de xarxa, desbloquejareu els comptes d'usuari i reiniciareu els serveis que s'havien aturat. El millor és **reiniciar l'ordinador** per tal que tots els serveis, ara que ja estan desbloquejats, es tornin a activar.

Seria molt important poder **localitzar i identificar qui ha estat l'intrús**. Per fer-ho, heu de ser capaços de trobar les pistes que ha anat deixant al llarg de l'atac, ja que l'ordinador guarda informació dels accessos que hi ha hagut. També podeu registrar les aplicacions que estan actives per cercar incidències en els arxius, tant propis com del sistema, i el trànsit que la xarxa ha mantingut. Amb aquesta informació es podrà determinar si l'atacant és un treballador de l'empresa o procedeix de la xarxa externa. També es podrà saber si utilitzava alguna tècnica de connexió il·lícita a la xarxa corporativa. De totes maneres, l'atac també pot ser culpa d'un descuit de l'usuari de l'empresa o del mal funcionament d'una aplicació en concret. La localització de l'intrús, doncs, us ajudarà a corregir l'error i a prendre les mesures necessàries per evitar-lo en un futur.

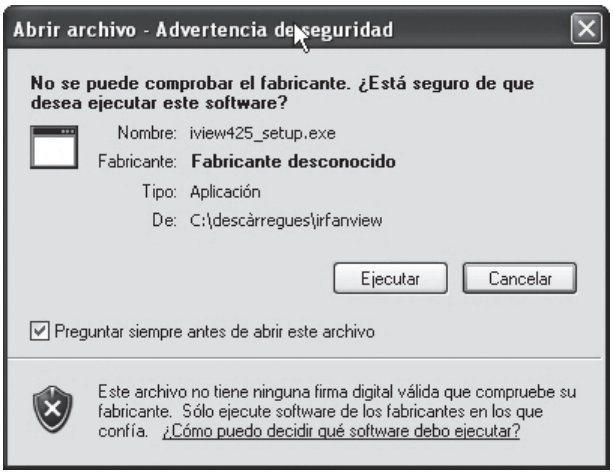
1.2. Utilització de mecanismes per a la verificació de l'origen i l'autenticitat d'aplicacions

La majoria dels fabricants de programari, especialment en cas de sistemes operatius, disposen de mecanismes de distribució d'actualitzacions de seguretat per als productes. El document analitza els mitjans de seguretat adoptats amb aquesta finalitat i posa una atenció especial en la verificació de l'autenticitat i la integritat del paquet que s'està instal·lant.

Les formes de verificació més conegudes són les següents:

- **Signatura digital del fitxer**: és la més fiable i permet verificar l'actualització fora de línia. Quan intentem instal·lar un arxiu que hem descarregat d'Internet, el sistema busca el fabricant i la signatura electrònica amb el certificat corresponent i l'origen. A més, comprova l'autenticitat i la validesa del certificat. Si troba el certificat corresponent ens avisa i ens demana si l'acceptem o no. En canvi, si no el troba ens apareix el missatge que podem veure en la figura 3, en què ens ofereix la possibilitat de continuar la instal·lació sense el certificat.

Figura 3. Certificació de programari en entorn Windows



- **WGA** (Windows Genuine Advantage, Avantatges de Windows Original) és un sistema contra la pirateria creat per Microsoft. Una vegada instal·lat, força el sistema operatiu a una validació en línia per detectar si el Windows que s'executa és genuí o no. Aquesta comprovació és necessària per accedir a Windows Update, les actualitzacions de Windows o per descarregar algun component de Windows des del centre de descàrregues de Microsoft.

  El WGA cobreix, específicament, el Windows XP i el Windows Vista. No cobreix, doncs, el Windows 2000, el Windows Server 2003 ni la família del Windows 9x.

- **OGA** (Office Genuine Advantage, Avantatges de Windows Original) és un programa de Microsoft similar al WGA que acabeu de veure. En aquest cas, però, requereix que els usuaris de Microsoft Office validin la còpia per descarregar actualitzacions no crítiques del programa i altres elements com complements, agregats, etc. Això és diferent de l'activació del producte, que és necessària per utilitzar-lo. La validació, en canvi, és necessària per descarregar arxius i actualitzacions de Microsoft Office des del web de Microsoft. La validació rebutja les claus del producte no vàlides. L'OGA cobreix l'Office XP, l'Office 2003 i l'Office 2007.

- **Aplicació de l'algorismme MD5 o funcions HASH**. En el cas del programari lliure, tot aquest tema de les certificacions no té sentit, ja que és lliure, a l'abast de tothom i tothom el pot veure i modificar. Igualment, pel fet de ser lliure, no cal pagar-lo. Per totes aquestes raons, no hi ha cap fabricant amb la certificació electrònica corresponent, però sí que hi ha mecanismes de control i certificació. Si no hi haguessin mecanismes de control, com que és lliure i tothom pot modificar-ne el codi, algú podria modificar parts del codi dels paquets i redistribuir-los; fins i tot alguna part d'aquest codi podria ser maliciós. Per tal d'evitar aquestes situacions, en l'àmbit del codi lliure es **verifica la integritat del paquet** que estem instal·lant per assegurar que l'arxiu que hem descarregat no ha sofert cap modificació des que els autors el van fer disponible per descarregar-lo. En molts casos, per verificar la integritat dels paquets, s'utilitza l'algorismme MD5, que obté un número a partir de les operacions que fa sobre el contingut de l'arxiu en concret. El valor que hem obtingut d'aplicar aquest algorismme a un mateix arxiu sempre serà el mateix, de manera que els autors del programa calculen aquest número i el fan públic en la zona de descàrrega. Quan l'usuari fa la descàrrega, només ha de tornar a calcular aquest valor per comprovar que el nombre que ha obtingut i el de la web coincideixen. D'aquesta manera, s'assegura que l'arxiu que ha descarregat no s'ha corromput ni s'ha modificat i que ningú ha tret parts del codi ni n'hi ha afegit, malicioses o no. Aplicacions com el WinMD5 i l'MD5SUM fan aquest càlcul.

L'autenticitat i la integració són importants perquè molts dels servidors des dels quals es descarrega programari són molt vulnerables a atacs maliciosos que podrien reemplaçar una actualització per un virus. També podrien patir atacs del tipus *DNS spoof*, en què l'usuari es connecta a un servidor equivocat que és diferent del que ha teclejat a l'URL.

La majoria dels fabricants de programari no estan preocupats per aquest tema, probablement per falta de demanada dels mateixos clients, i no proporcionen cap mecanisme de seguretat fiable.

1.3. Utilització de tècniques de recuperació de dades

En cas de pèrdua de dades d'una petita empresa, es pot produir una situació d'angoixa, ja que això pot implicar no poder continuar l'activitat quotidiana fins al punt d'arribar a un tancament temporal de l'activitat, cosa que en alguns casos pot acabar amb el tancament definitiu.

Per evitar aquestes situacions difícils i preocupants, cal disposar de diferents tècniques de recuperació de dades. La millor opció és disposar d'una bona política preventiva amb còpies de seguretat programades. Si disposeu de còpies de seguretat, la recuperació de les dades serà més ràpida i efectiva.

1.3.1. Còpies de seguretat

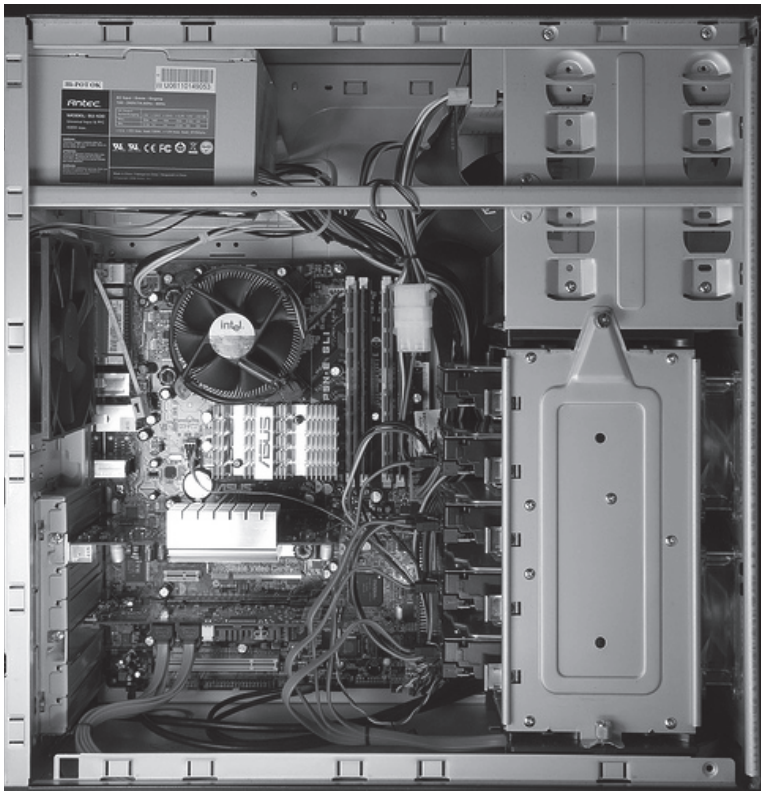
La pèrdua de dades es pot produir per diversos motius. És possible que els noms dels arxius es canviïn i, després, sigui difícil retrobar-los. També pot ser que, arran d'un accident, se sobreescriguin, s'eliminin o es perdin perquè s'ha espatllat alguna unitat o s'ha sostret algun ordinador o disc Zip.

Per recuperar les dades, el millor és tenir una política de còpies de seguretat o de creació d'imatges del disc dur. Aquestes còpies es poden fer en un altre disc dur d'un sistema RAID de discos durs, com es pot veure en la figura 4. És una bona opció per evitar pèrdues de documents a causa de la corrupció del disc dur en què es guarden. No és recomanable, però, si es tracta d'informació susceptible de ser robada. En aquest cas, la millor política és fer les còpies de seguretat en una ubicació diferent.

RAID...

... (matriu redundant de discos independents). Es tracta d'un sistema d'emmagatzematge de la informació que combina diversos discos durs que tenen la mateixa capacitat. Funcionen i es comporten com una unitat lògica.

Figura 4. Connexió de discos en RAID



En cas de perdre els arxius, si disposeu de còpies de seguretat, els podreu recuperar d'una manera ràpida, còmoda i, a més, molt efectiva, ja que només haureu perdut la informació que es va crear després de fer l'última còpia.

Podeu fer les còpies de seguretat des del sistema operatiu mateix o podeu utilitzar diverses aplicacions, tant de programari de propietat com de programari lliure. Aquestes aplicacions us permetran fer les còpies de seguretat, de manera automatitzada o manual, i recuperar, posteriorment, les dades que hi hagueu guardat.

1.3.2. Recuperació sense còpies de seguretat

Heu de saber que les dades guardades a l'ordinador realment no desapareixen fins que la unitat es crema o es destrueix completament. Per entendre en profunditat com es recuperen els arxius desapareguts, hauríeu de saber i entendre com s'emmagatzema la informació en el disc, però això escapa als propòsits d'aquest punt. Assenyalarem, simplement, que les plataformes Windows, Mac i Linux formaten els discos durs i hi guarden la informació de maneres diferents.

Tanmateix, independentment de com es guarden les dades en el disc dur, és a dir, de quin sistema d'arxius esteu utilitzant, heu de saber que quan s'esborra un arxiu o es llença a la paperera, el sistema operatiu realment no l'elimina del tot. En comptes d'esborrar-lo, trasllada l'entrada del directori de l'arxiu i la informació sobre la ubicació original a una carpeta oculta especial, que representa la *Paperera de reciclatge*. Per tant, els clústers de dades del disc dur no s'eliminen, ni tan sols es mouen de lloc, sinó que només es modifica la ubicació de l'entrada del directori.

Clúster

Terme que significa que correspon aproximadament als sectors aprofitables per guardar informació d'un disc d'ur.

En l'entorn Windows, quan la paperera de reciclatge s'omple, els arxius que fa més temps que hi són s'eliminen del tot. Passa el mateix quan l'usuari la buida voluntàriament.

En el cas de Macintosh, la paperera no s'omple mai, sinó que va guardant tot el que hi anem enviant fins que l'usuari, algun dia, la buida.

Tot i que si mantenim premuda la tecla *Majúscules* en Windows o la tecla *Control* en Mac podem evitar utilitzar la paperera, quan eliminem un arxiu o, fins i tot, buidem la paperera, les dades d'aquests arxius romanen en el disc dur. En tots els sistemes operatius, el nom de l'arxiu, l'entrada d'índex o el directori es modifiquen per indicar que l'usuari no hauria de poder veure l'arxiu i que l'espai que ocupava està disponible i es pot reutilitzar. Quan arribi el moment, la unitat sobreescriurà amb informació nova l'espai disponible. Per tant, hi ha la possibilitat de recuperar la informació que encara no s'ha sobreescrit.

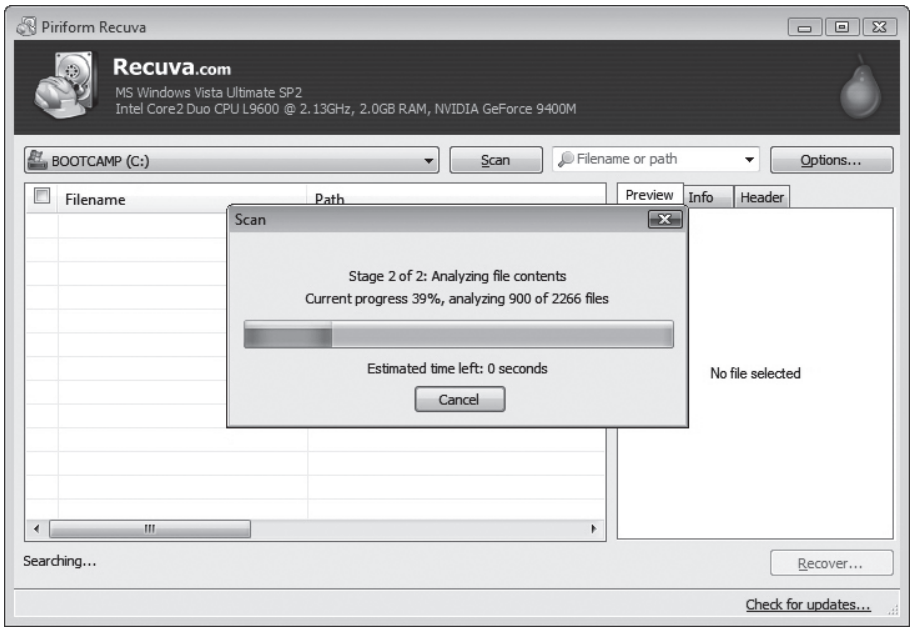
Si l'arxiu encara és a la paperera de reciclatge, n'hi ha prou amb prémer l'arxiu amb el botó dret, seleccionar *Recuperar* i arrossegar-lo fins al lloc on el volem col·locar. La paperera de reciclatge pot oferir unes quantes utilitats (corresponen a un segon nivell de protecció) que us permeten controlar els arxius que heu eliminat. Aquestes utilitats poden ser extres d'alguns paquets d'antivirus o aplicacions exclusives.

Tanmateix, quan un arxiu ja s'ha eliminat de la paperera de reciclatge i aquesta paperera no tenia incorporada cap aplicació per oferir més protecció, l'arxiu encara no ha desaparegut del disc dur i hi ha eines per localit-

zar i, després, tornar a ajuntar tots els clústers del disc dur que guardaven les dades de l'arxiu. Recordeu que només podreu reconstruir els arxius que no hagin estat sobreescrits, de manera que és molt important no fer operacions d'escriptura mentre intenteu recuperar un arxiu eliminat. Si, prèviament, no heu instal·lat cap d'aquestes eines de recuperació, no és un bon moment per fer-ho, ja que l'arxiu que intenteu recuperar es podria sobreescriure. D'aquesta manera, haureu de buscar-hi alternatives, com compartir el disc dur amb una altra màquina i intentar recuperar-lo des d'aquesta altra.

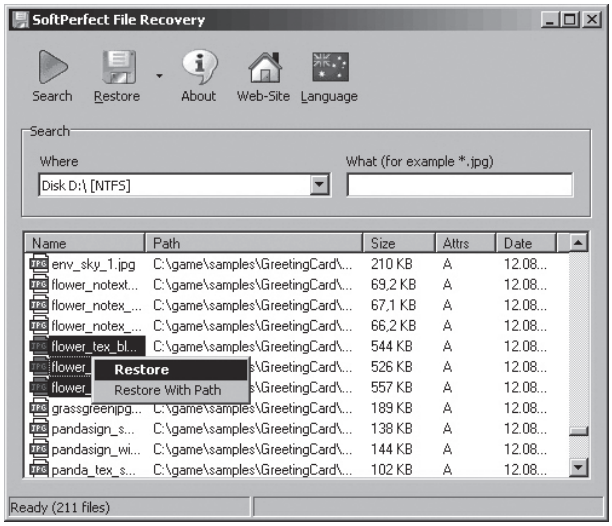
En el cas de Windows, la millor eina de recuperació és *Undelete*. Amb aquesta eina, els arxius eliminats no s'eliminen realment, sinó que el programa intercepta les peticions d'eliminació i els arxius eliminats s'emmagatzemen en una altra ubicació anomenada *Paperera de recuperació*. L'eina també ofereix la possibilitat de recuperar un arxiu que s'ha eliminat realment. Per fer-ho, fa una cerca pels clústers del disc dur. Hi ha altres eines de programari lliure que fan aquesta funció, com (Recuva, figura 5) o Softperfect (figura 6).

Figura 5. Programa Recuva



Els clústers del disc que estaven ocupats per l'arxiu eliminat s'han sobreescrit amb dades noves. En principi, les dades anteriors es perden, però també és possible que encara siguin en el suport magnètic, en forma de contorns en les ones que representen les dades. Els equips d'alta tecnologia permeten recuperar-les seguint un procés molt complex. Aquest procés difícil i costós es pot repetir vàries vegades i, aproximadament, es poden arribar a recuperar fins a set capes de dades. Com que és un treball dificultós i car que només poden fer els experts, aquest sistema només s'utilitza en casos en què el valor de les dades perdudes és molt important.

Figura 6. Programa Softperfect



1.4. Sistemes d'identificació: signatura electrònica i certificat digital

Internet i el seu ús creixent han contribuït de manera significativa a la globalització, fet que ha provocat que es converteixi en una eina molt important i, en alguns casos, imprescindible per a moltes empreses. Tanmateix, aquesta eina nova tan potent, que és a l'abast de les empreses que hi veuen una oportunitat de negoci nova o, simplement, una eina per millorar la productivitat, comporta un problema afegit, la seguretat.

La connexió a Internet porta implícita un risc de seguretat pel sistema informàtic de l'empresa. Això ha fet que els administradors de xarxa tinguin la necessitat de crear polítiques de seguretat que consisteixen a crear connexions segures, enviar i rebre informació encriptada, filtrar accessos i informació, etc.

Dins aquest problema de seguretat hi ha la **privacitat** de les dades. Fins ara, no hi havia cap protecció real que garantís que els missatges que s'envien o es reben no fossin interceptats, llegits o, fins i tot, alterats per algun desconegut, ja que, realment, no hi ha ningú que dirigeixi o controli la xarxa d'Internet.

Aquest fet provoca que es plantegin preguntes com les següents: com sabeu si una persona té, efectivament, un compte vàlid? o com sabeu si es pot confiar en un comerciant que no heu vist mai?

Per tal que la privacitat i la seguretat tinguin una rellevància important a Internet, cada entitat necessita tenir una manera de poder verificar la identitat de les altres i poder-hi establir, així, un nivell de confiança.

El **certificat digital** i la **signatura electrònica** són algunes de les eines que permetran establir connexions segures entre les persones i les administracions. També oferiran la possibilitat de fer transaccions comercials.

1.4.1. Certificat digital

Els certificats digitals representen el punt més important en les transaccions electròniques segures. Aquests certificats permeten una manera convenient i fàcil d'assegurar que els participants en una transacció electrònica puguin confiar l'un en l'altre. Aquesta confiança s'estableix a partir de tercers. Són les **autoritats certificadores**. Primer, doncs, cal que aneu a una autoritat certificadora. Us haureu d'identificar correctament i, tot seguit, ells certificaran que sou qui dieu ser i us donaran el certificat digital corresponent. Aleshores, quan envieu missatges que vulgueu que us identifiquin davant altres persones, només caldrà que hi afegiu una còpia pública del vostre certificat digital. D'aquesta manera, la persona que rebi el missatge sabrà de segur que l'emissor del missatge és qui diu ser, garanteix altres persones, entitats, o administracions públiques quina és la vostra identitat.

Dit d'una manera senzilla, un certificat digital garanteix que dues computadores que es comuniquen puguin fer transaccions electròniques amb èxit. Aquests certificats digitals es basen en la tecnologia de codis secrets o **encriptació**. L'encriptació garanteix la confidencialitat, la integritat i l'autenticitat de la informació que es vol transmetre, que té una importància vital per a la persona o l'empresa.

El procés d'encriptació és senzill. Un missatge pot passar per un procés de conversió o d'encriptació, que el transforma en codi mitjançant una clau. És, doncs, la manera de traduir els signes d'un missatge a un altre sistema de signes, la lectura del qual no té cap sentit per a una persona que l'intercepti. Això es coneix com a *procés d'encriptació* d'un missatge. Un sistema senzill d'una clau pot consistir a canviar cada lletra del missatge per la lletra de l'abecedari que la segueix. D'aquesta manera, la paraula *hola* es converteix en *ipmb*. Per poder desxifrar el missatge o desfer l'encriptació, la persona que el rep necessita saber la clau secreta, és a dir, el certificat digital. Actualment, els certificats digitals que hi ha són els següents:

- Certificats de servidor (SSL)
- Microsoft Server Gated Cryptography Certificates (Certificats de CGC –una extensió del protocol SSL– que ofereix Microsoft)
- Certificats canalitzadors
- Certificats de correu electrònic
- Certificats de valoració de pàgines web
- Certificats de segell, data i hora

L'encriptació amb **clau secreta**, tot i tenir moltes limitacions significatives, és útil en molts casos. No és gaire pràctic que una gran corporació intercanviï claus amb milers o, fins i tot, milions de persones, cosa que limita el potencial de les transaccions electròniques.

La solució a la seguretat en la xarxa oberta és una forma de codificació més nova i sofisticada. Es va desenvolupar a la dècada dels anys setanta i es coneix amb el nom de *clau pública*. Funciona amb un sistema en què cada participant té dues claus, una de pública i una de privada. Les dues claus funcionen conjuntament, és a dir, si es vol enviar un missatge a un amic i no es vol que ningú més el llegeixi, es busca la clau pública de l'amic i s'utilitza per encriptar el text del missatge. Aleshores, quan l'amic el rep, ha d'utilitzar la seva clau privada per desfer l'encriptació. D'aquesta manera, si un tercer intercepta el missatge, no el podrà desxifrar perquè no disposarà de la clau privada d'aquest amic.

1.4.2. Signatura electrònica

La signatura electrònica forma part del certificat digital, és un dels seus components juntament amb les dades de l'usuari i la clau pública. Un certificat digital permet garantir que l'autor del missatge és, realment, qui diu ser. És a dir, garanteix que el receptor pugui verificar que el document ha estat enviat per l'autor, que l'autor no pot negar la realització del document i que el receptor no pot alterar-ne el contingut.

Per exemple, quan un usuari A genera un missatge per a un usuari B, l'encripta juntament amb el seu certificat. Opcionalment, el pot protegir amb la clau pública de l'usuari B. Això s'anomena *signar digitalment* o construir el que es coneix com a *sobre electrònic* o *signatura digital*.

Ningú pot modificar el contingut del missatge sense destruir el certificat de l'emissor, cosa que garanteix la inviolabilitat del missatge.

Les signatures electròniques són blocs de dades que han estat codificades amb una clau secreta i que es poden descodificar amb una clau pública. Principalment, s'utilitzen per verificar l'autenticitat del missatge o la d'una clau pública.

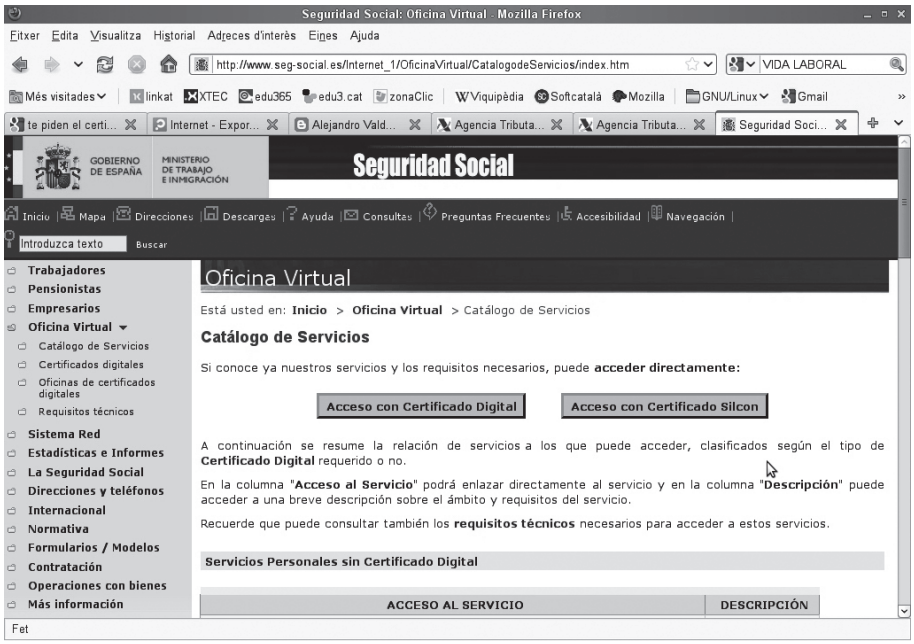
A Espanya hi ha la Llei 59/2003 de signatura electrònica, que defineix tres tipus de signatures:

- **Simple**: inclou un mètode per identificar el firmant (autenticitat).
- **Avançada**: a més d'identificar el firmant, permet garantir la integritat del document.
- **Reconeguda**: la signatura avançada executada amb un DSCF (dispositiu segur de creació de signatures) i emparada per un certificat reconegut (certificat que s'atorga després de la verificació presencial de la identitat del firmant). A vegades, aquesta firma es coneix com a *qualificada* per la traducció del terme *qualified* de la Directiva europea de signatura electrònica.

1.5. Obtenció d'identificacions electròniques, ús de signatura electrònica

Els certificats digitals i les signatures electròniques permeten fer transaccions segures per mitjà d'Internet. Igualment, també permeten identificar les persones tal com podeu veure en la figura 7, en què apareix una captura de pantalla de la pàgina d'Hisenda. En aquesta pàgina, hi ha la possibilitat d'identificar-se amb el certificat digital corresponent. Si es fa, tot seguit permet efectuar, per mitjà d'Internet, una sèrie d'accions que no és possible fer sense la identificació.

Figura 7. Entrada al web d'Hisenda amb certificat digital



Aquesta identificació és possible perquè, prèviament, cada persona s'ha personat en un organisme que emet les certificacions electròniques i contrasta que la persona és qui diu ser.

En el nostre país, us podeu adreçar a una sèrie d'organismes per aconseguir un certificat digital. Són, entre altres, l'**Agència Catalana de Certificació** o algunes delegacions del **Ministeri d'Hisenda**.

Per obtenir més informació sobre els certificats digitals, consulteu la secció "Adreces d'interès" del web.

Quan aneu personalment a un d'aquest centres emissors de certificats digitals i us hi identifiquem correctament, us proporcionaran un programari determinat que després haureu d'instal·lar en el vostre sistema. Aquest programari tindrà unes especificacions de maquinari i programari que necessitareu tenir per poder-lo executar. La majoria d'aquest programari només s'executa en entorn Windows. De totes maneres, actualment l'agència catalana treballa per treure una versió per a programari lliure.

L'agència emissora de certificats digitals us lliurarà un paquet de programari que, una vegada instal·lat en el vostre sistema informàtic, us perme-

trà enviar correus autentificats per certificació electrònica o per signatura electrònica. Juntament amb el programari, l'organisme emissor us entregarà els manuals amb les instruccions, tant per instal·lar el programari com per utilitzar-lo posteriorment en el vostre gestor de correu electrònic.

Aquestes certificacions electròniques us permetran identificar-vos davant les administracions públiques per fer tota una sèrie de tràmits per mitjà d'Internet que abans calia fer personalment, com els canvis en les dades personals, canvis d'adreces, petició de certificats, declaració de la renda i un llarg etcètera de gestions que cada dia es va ampliant.

Pel que fa a la utilització de la signatura electrònica, hi ha eines, com la pàgina web que apareix en la figura 8, que permeten comprovar-ne la validesa i l'efectivitat. Aquesta pàgina web fa una comprovació en línia de la vostra signatura electrònica per assegurar que és correcta i donar-vos la seguretat que podeu utilitzar-la en els vostres documents.

Figura 8. Comprovació en línia de la signatura electrònica