

Seguretat activa

Josep Pons Carrió

Seguretat informàtica

Índex

| | |
|---|-----------|
| Introducció | 5 |
| Resultats d'aprenentatge | 7 |
| 1 Seguretat activa | 9 |
| 1.1 Fallades de seguretat: plans de contingència | 9 |
| 1.1.1 Fallades de seguretat | 11 |
| 1.1.2 Plans de contingència | 12 |
| 1.2 Utilització de mecanismes per a la verificació de l'origen i l'autenticitat d'aplicacions | 16 |
| 1.3 Utilització de tècniques de recuperació de dades | 18 |
| 1.3.1 Còpies de seguretat | 18 |
| 1.3.2 Recuperació sense còpies de seguretat | 20 |
| 1.4 Sistemes d'identificació: signatura electrònica i certificat digital | 22 |
| 1.4.1 Certificat digital | 23 |
| 1.4.2 Signatura electrònica | 24 |
| 1.5 Obtenció d'identificacions electròniques, ús de signatura electrònica | 25 |
| 2 Alarmes i incidències de seguretat | 27 |
| 2.1 Detecció i resolució d'incidències | 27 |
| 2.1.1 Detecció d'incidències | 34 |
| 2.1.2 Resolució d'incidències mitjançant les instruccions pertinents | 34 |
| 2.2 Interpretació i utilització com a ajuda de documentació tècnica | 37 |
| 2.3 Documentació de les incidències de seguretat | 38 |
| 3 Protecció contra programari maliciós | 39 |
| 3.1 Virus i programes maliciosos | 40 |
| 3.1.1 Característiques comunes als diferents tipus de virus | 45 |
| 3.1.2 Grau de perillositat del programa maliciós | 45 |
| 3.1.3 Grau de propagació del programa maliciós | 46 |
| 3.1.4 Danys causats per un programa maliciós | 46 |
| 3.1.5 Mitjans i mètodes que utilitza el programari maliciós per atacar | 47 |
| 3.1.6 Situacions en què el vostre sistema corre el risc d'infectar-se | 48 |
| 3.1.7 Mètodes per evitar el programari maliciós | 49 |
| 3.2 Instal·lació, prova, utilització i automatització d'eines per a la protecció i desinfecció de programari maliciós | 52 |

Introducció

La seguretat activa és una part de la seguretat informàtica que comprèn, especialment, les parts de la seguretat que es mantenen sempre alerta i tenen un paper més important en el funcionament del dia a dia del vostre sistema informàtic.

Aquesta part de la informàtica és la que està més destinada a aturar i minimitzar els atacs que pot patir la vostra màquina. Igualment, té l'objectiu de disminuir els efectes que aquests atacs puguin produir en el vostre sistema informàtic.

Entenent que la seguretat al cent per cent no existeix, s'intentarà que sigui al més elevada possible, tant per intentar evitar un desastre en el sistema com per minimitzar-ne els efectes si es produeix.

En aquesta unitat formativa també es treballaran altres aspectes de la seguretat, com la signatura i el certificat digitals, que pretenen que la xarxa global sigui un espai més segur per fer-hi tota mena de transaccions econòmiques i dinamitzar, així, aquest sector. Alhora, faciliten fer aquest tipus d'intercanvis a l'usuari quotidià i a les petites i mitjanes empreses.

Aquestes certificacions també faciliten la comunicació del ciutadà amb les institucions, que cada vegada ofereixen més gestions a l'usuari per mitjà d'Internet.

En aquesta unitat aprendreu quines són les fallades de seguretat més corrents i com evitar-les o reduir-ne l'impacte. Igualment, coneixereu quins són els atacs més comuns i com us en podeu protegir. També aprendreu a instal·lar, configurar i mantenir actualitzat un programa antivirus per evitar, tant com sigui possible, l'entrada de programari maliciós en el vostre sistema.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Aplica mecanismes de seguretat activa, descriure'n les característiques i relacionar-les amb les necessitats d'ús del sistema informàtic.

- Segueix plans de contingència per actuar davant fallades de seguretat.
- Identifica els mecanismes de protecció del sistema contra virus i programes maliciosos per assegurar i verificar la seva actualització.
- Verifica l'origen i l'autenticitat de les aplicacions que s'instal·len en els sistemes.
- Instal·la, prova i actualitza aplicacions específiques per a la detecció i eliminació de programari maliciós, automatitzant tasques de protecció i de desinfecció.
- Aplica tècniques de recuperació de dades.
- Descriu sistemes d'identificació com la signatura electrònica, certificat digital, entre d'altres.
- Obté i utilitza sistemes d'identificació com la signatura electrònica, certificat digital, entre d'altres, amb la finalitat bàsica de la signatura de documents i de missatgeria electrònica, seguint la documentació que descriu els procediments.
- Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent al sector, i utilitzant-la d'ajuda.
- Detecta i resol les alarmes i les incidències de seguretat seguint les instruccions pertinents.
- Realitza la documentació adient sobre les incidències de seguretat, segons indicacions de l'administrador.

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.

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 impedit 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 configurarlo 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



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

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.

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 comprovar-ne 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.

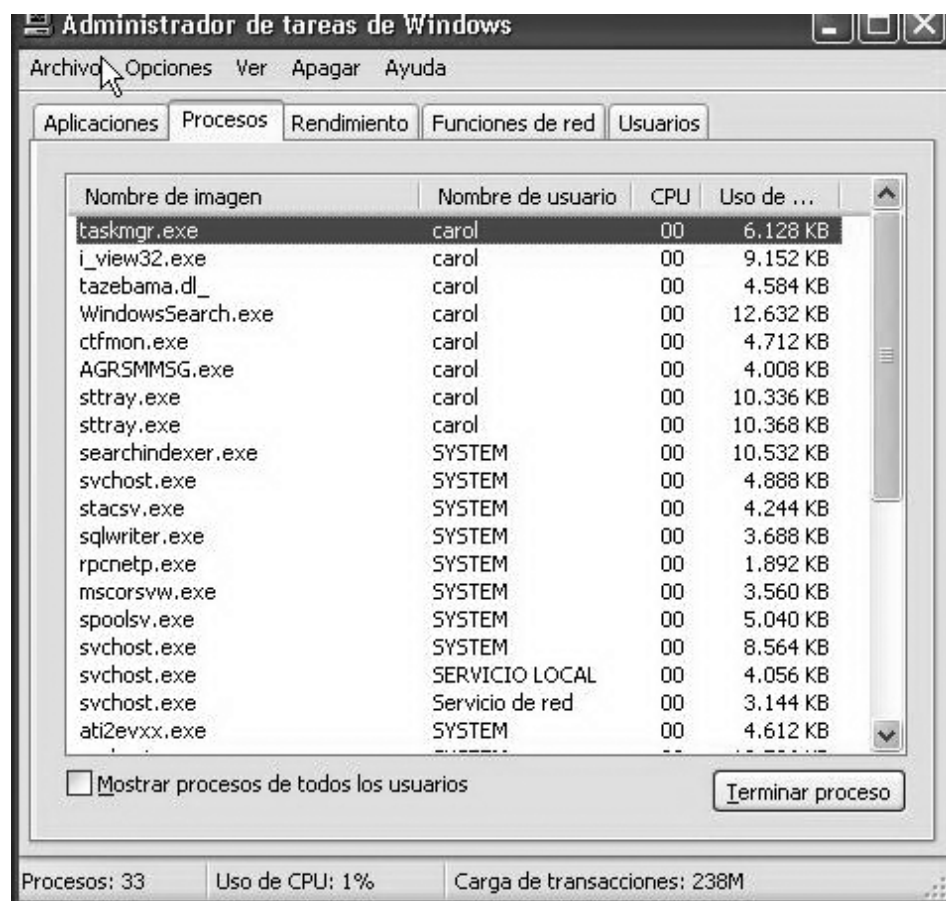
1) La primera cosa que heu de fer és **aïllar l'ordinador** per evitar que l'atacant continuï actuant. Per fer-ho, tancareu totes les aplicacions que s'estan executant en l'ordinador i **guardareu els arxius** de dades que estiguin utilitzant aquestes aplicacions.

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.

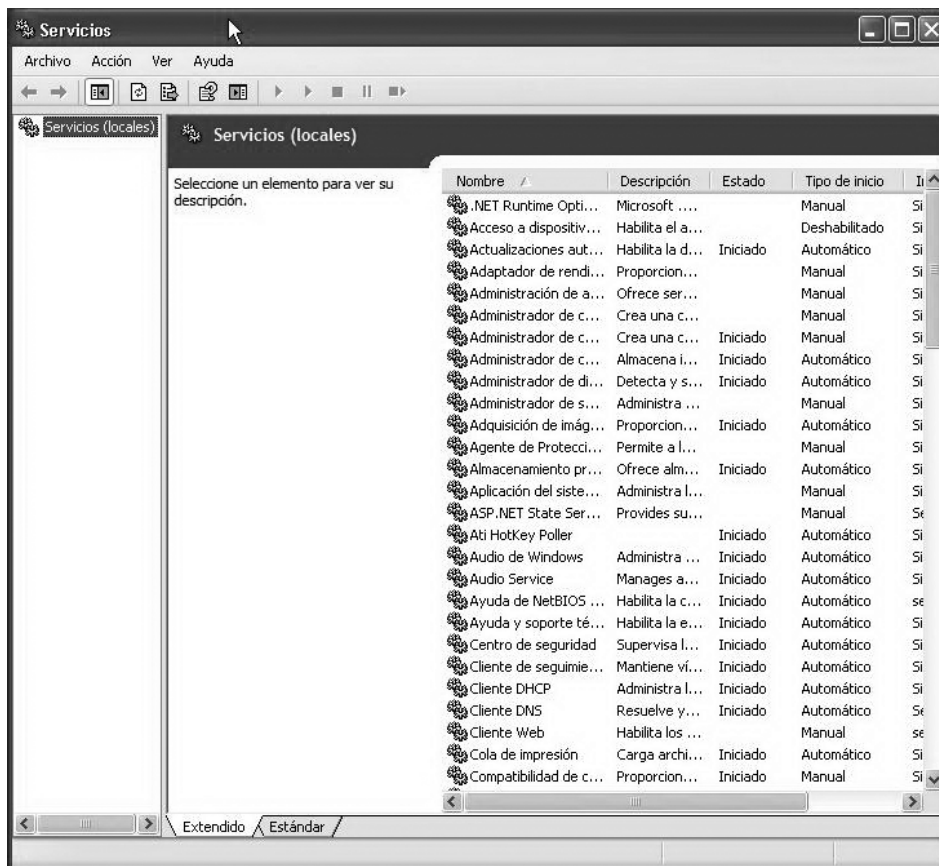
El pas següent és intentar **veure quina vulnerabilitat utilitza l'atac** per sabotejar l'ordinador. La millor manera de saber què hi passa és mirar quins programes s'hi estan executant. Abans, però, s'han de tancar tots els programes que s'estaven utilitzant. S'haurà de mirar quins són els consums de 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 1.1. En cas que es tracti de Linux, podeu fer servir el monitor del sistema.

FIGURA 1.1. 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 1.2.

FIGURA 1.2. 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, **restaurareu 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.

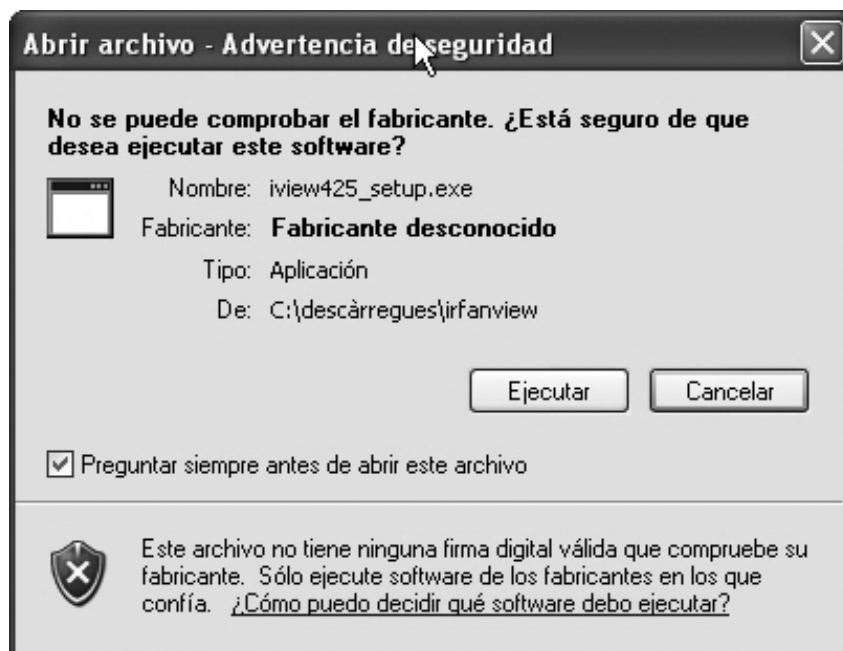
1.2 Utilització de mecanismes per a la verificació de l'origen i l'autenticitat d'aplicacions

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 1.3, en què ens ofereix la possibilitat de continuar la instal·lació sense el certificat.

FIGURA 1.3. 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 acaba 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'algorisme 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'algorisme 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 algorisme 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 demanda 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.

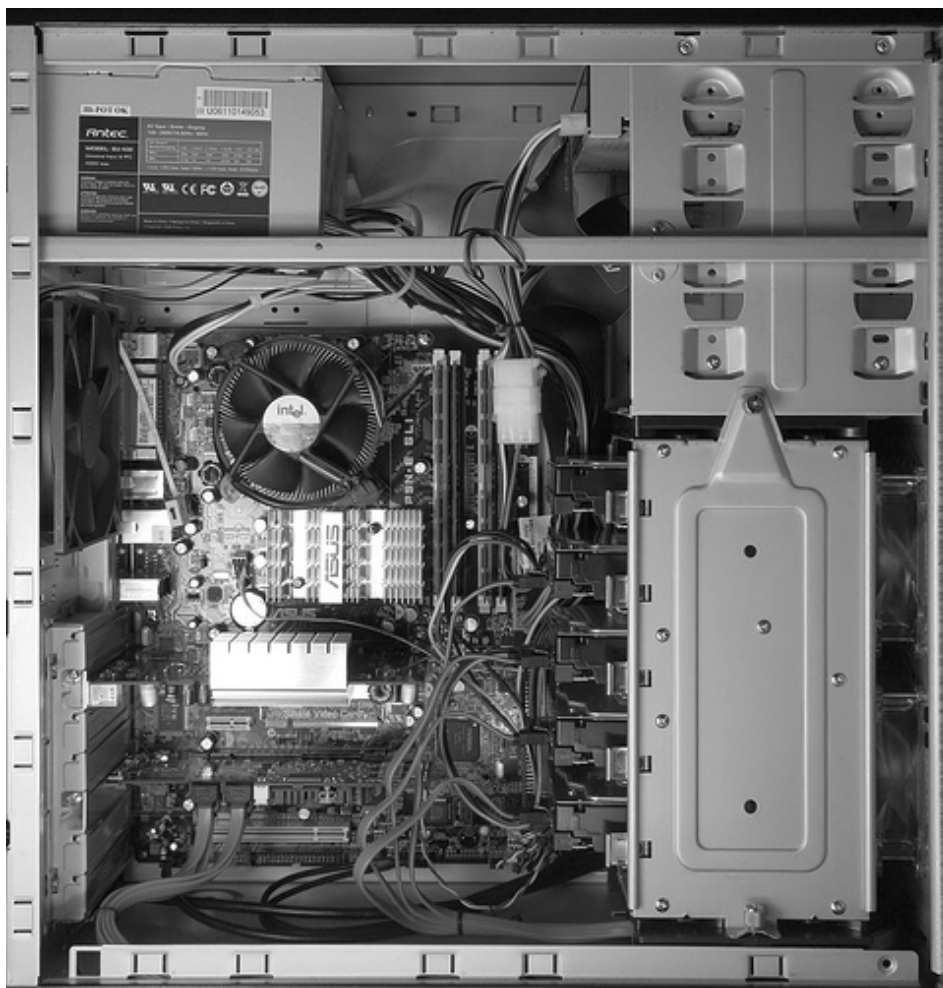
1.3.1 Còpies de seguretat

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 1.4. 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.

FIGURA 1.4. Connexió de discos en RAID



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.

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.

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.

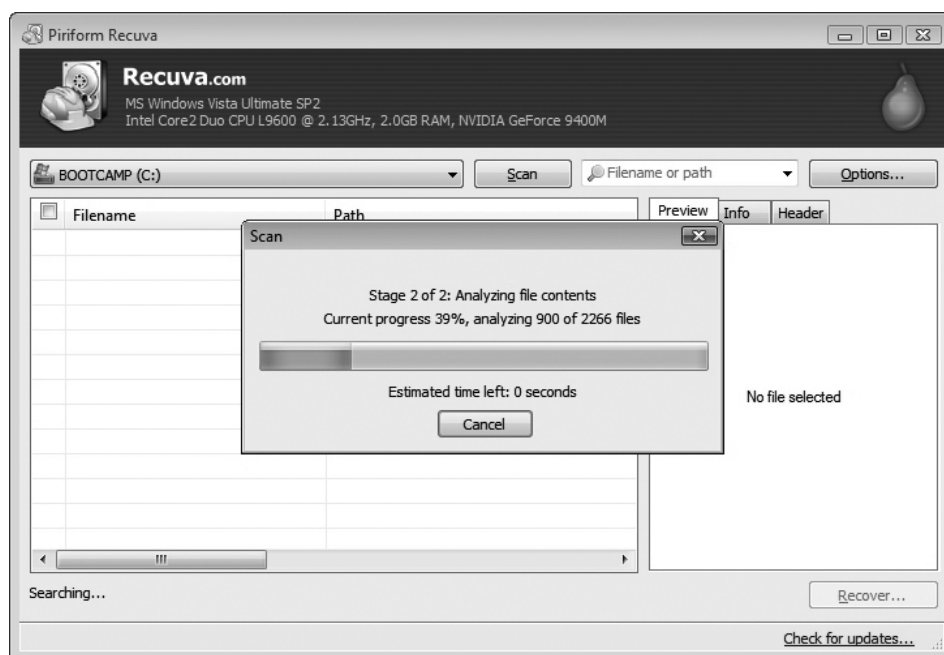
Si l'arxiu encara és a la paperera de reciclatge, n'hi ha prou amb prémer l'arxiu amb el botó dret, seleccionar *Recuperar* i arrossegar-lo fins al lloc on el volem col·locar. La paperera de reciclatge pot oferir unes quantes utilitats (corresponen a un segon nivell de protecció) que us permeten controlar 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 localitzar 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 sobre escriure. 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 1.5) o Softperfect (figura 1.6).

FIGURA 1.5. 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 diverses vegades i, aproximadament, es poden arribar a recuperar fins a set capes de dades. Com que és un treball difícil 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.

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 rebí 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 encryptar 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'encrypta 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:

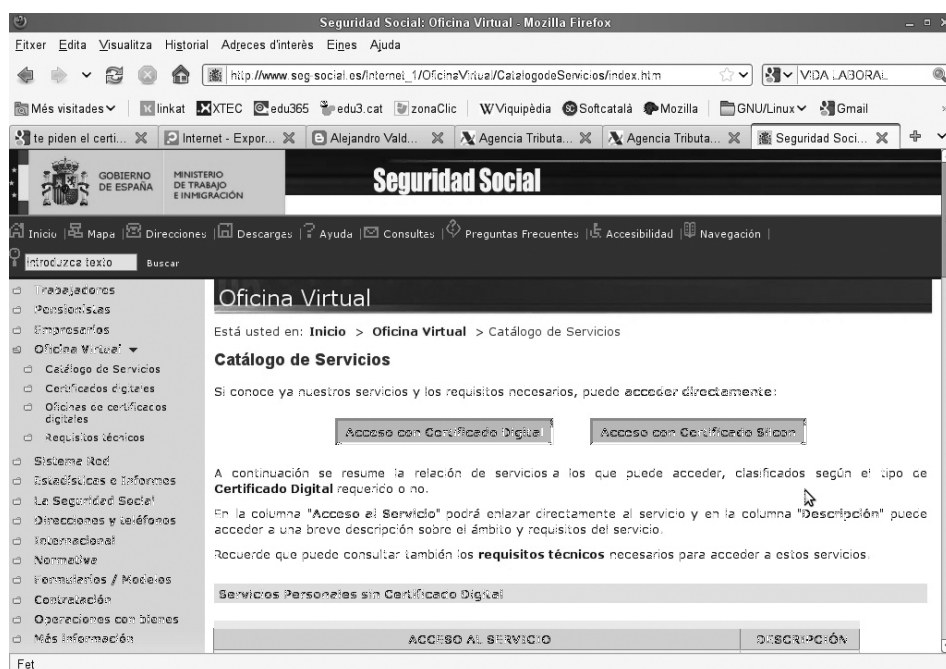
- **Simple:** inclou un mètode per identificar el firmant (autenticitat).
- **Avançada:** a més d'identificar el firmant, permet garantir la integritat del document.
- **Reconeguda:** la signatura avançada executada amb un DSCF (dispositiu segur de creació de signatures) i emparada per un certificat 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 1.7, 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 1.7. 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.

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.

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

L'agència emissora de certificats digitals us lliurarà un paquet de programari que, una vegada instal·lat en el vostre sistema informàtic, us permetrà enviar correus autenticats 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 1.8, 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 1.8. Comprovació en línia de la signatura electrònica



2. Alarmes i incidències de seguretat

En el marc de la seguretat activa, es disposa d'una sèrie d'eines, com els **IDS** (*intrusion detecting system*, sistema de detecció d'intrusos) o els **IPS** (*intrusion prevention system*, sistema de prevenció d'intrusos) entre molts altres, que us poden avisar i donar l'alarma si patiu una incidència de seguretat, sia per la detecció d'un intrús en el vostre sistema informàtic o per la detecció de qualsevol tipus de programari maliciós.

En el moment de saber que hi ha una incidència de seguretat, cal que actueu per pal·liar els efectes que pugui tenir en el vostre sistema informàtic. Aquesta actuació estarà determinada pel seguiment del **pla de contingència**. Tanmateix, en cas que no n'hi hagi o no reculli la incidència en qüestió, us haureu de cenyir a seguir les instruccions i la documentació tècnica que us proporcionaran els mateixos programes que us han donat l'alarma.

En cas que no disposeu de cap pla de contingència i el programari de seguretat no us ofereixi instruccions a seguir, sempre us quedarà l'opció de buscar informació a Internet. Hi ha nombroses pàgines sobre incidències de seguretat i múltiples fòrums en què podreu trobar les accions que heu de fer, ja que, probablement, hi ha altres persones o empreses que van patir la mateixa incidència de seguretat.

Si no es disposa d'un pla de contingència propi, cal tenir en compte que les instruccions del programari o la informació que aconseguiu a Internet poden estar en anglès, cosa que demanarà que feu un esforç per comprendre-les. Heu de recordar que a Internet també disposeu de diverses eines que us poden ajudar a traduir el material escrit en anglès.

Finalment, una vegada detectada la incidència de seguretat corresponent i resolta amb les instruccions pertinents, caldrà que documenteu la incidència. Si disposeu d'un pla de contingència i aquesta incidència no hi consta perquè no estava prevista o no s'havia produït abans, convindrà que la hi inclogueu per a incidències futures.

Pla de Contingència

Entenem per pla de contingència el conjunt d'actuacions a realitzar en cas d'haver patit una incidència de seguretat. Estan destinades a pal·liar-ne els efectes i a recuperar el sistema.

Fòrum

Els fòrums són espais a Internet destinats a la comunicació. Hi podeu deixar un missatge explicatiu i altres persones respondran a la vostra demanda.

2.1 Detecció i resolució d'incidències

Per tal de mantenir un sistema informàtic al màxim nivell de seguretat, cal disposar d'una sèrie d'eines i, a més, mantenir-les en bon estat de funcionament, cosa que inclou tenir-les al dia, actualitzades. Algunes d'aquestes eines més comunes són els antivirus, els tallafocs i les actualitzacions del sistema, sobretot pel que fa a la part dels pedaços de seguretat. També n'hi ha d'altres que no són tan conegudes, però que us poden ser de molta utilitat en cas de detectar una incidència de seguretat en el vostre sistema informàtic. El fet de tenir instal·lats programes de detecció o prevenció d'intrusos, com els IDS o els IPS i, més particularment,

els NIDS (*net intrusion detecting system*, sistema de detecció d'intrusos en xarxa) i els HIDS (*host intrusion detecting system*, sistema de detecció d'intrusos en una màquina) us permetrà detectar intrusions no desitjades en el vostre sistema i, per tant, podreu actuar.

Igualment, mantenir el vostre sistema actualitzat, sobretot pel que fa a les actualitzacions relacionades amb la seguretat, us estalviarà molts maldecaps. Moltes d'aquestes actualitzacions estan destinades a evitar l'entrada de programari maliciós o la intrusió no desitjada, ja que corregeixen possibles errades detectades en el vostre sistema.

Si treballem en un entorn Microsoft, és a dir, en un sistema operatiu Windows, cal que aneu a **Inicio\Panel de control\Centro de seguridad** per configurar-ne les actualitzacions. Una de les millors maneres de configurar aquestes actualitzacions és fer-ho automàticament. De totes maneres, heu d'activar l'opció que fa que el programa us preguntï abans d'instal·lar, tal com podeu observar en la figura 2.1.

FIGURA 2.1. Actualitzacions automàtiques sistema Windows



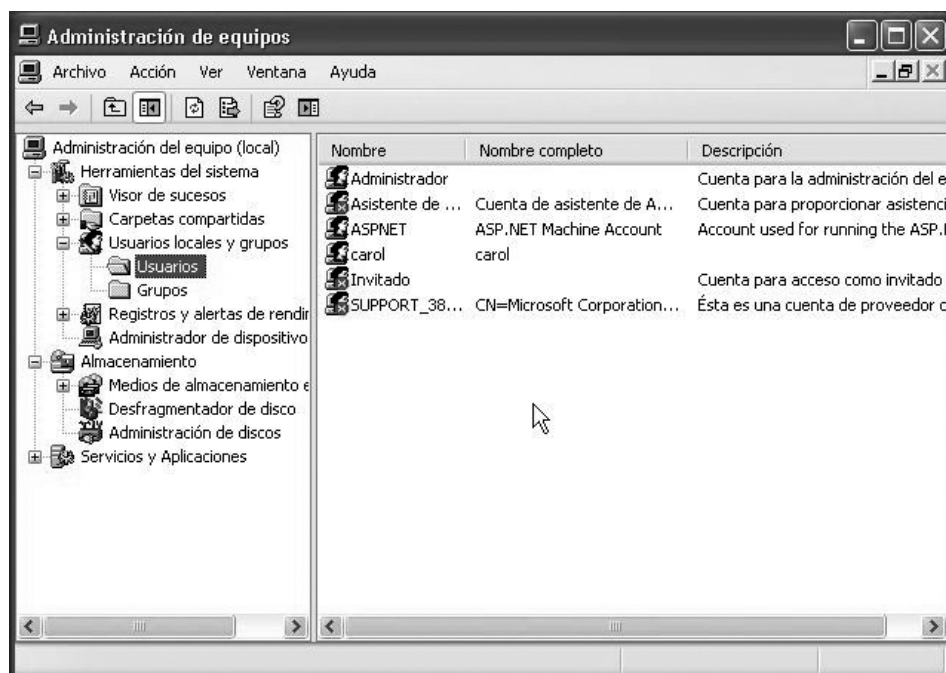
El vostre sistema buscarà automàticament les actualitzacions o els pedaços i, abans d'instal·lar-los, us preguntarà si ho voleu fer o no. En aquest moment, podreu escollir quins us cal instal·lar i quins no. De totes maneres, és convenient instal·lar els que estan relacionats amb la seguretat del vostre sistema. La resta és decisió vostra. D'aquesta manera, mantindreu el sistema actualitzat i, almenys, evitareu les possibles errades de seguretat que ja han estat detectades i corregides.

Cal que tingueu present que, en alguns casos, hi ha hagut programes maliciosos, virus, que s'han propagat per tot el món en qüestió d'hores. En un cas concret, per fer-ho, van utilitzar errades de seguretat dels sistemes informàtics que els dissenyadors d'aquests sistemes ja havien detectat i, per tant, ja feia mig any que havien tret el pedaç corresponent per pal·liar-ne els efectes. Per això és tan important que mantingueu els sistemes actualitzats.

Si treballeu amb programari lliure, aquestes recomanacions continuen essent vàlides. De totes maneres, convé destacar que el vostre sistema serà força més segur, ja que en aquest entorn hi ha molt poc programari maliciós. A més, el sistema de propietats i drets sobre els arxius de què disposeu, fa que sigui molt més segur en cas d'intrusions.

Per seguretat, en el cas de Windows, es recomana desactivar el compte de l'usuari *Invitado*, ja que permet l'accés a usuaris no identificats en el sistema. Per fer-ho, cal que anem a **Inicio**\Panel de control\Cuentas de usuario, escollim el compte *Invitado* i ens assegurarem que està desactivat. Ho podeu veure en la figura 2.2.

FIGURA 2.2. Desactivar compte Invitado en un sistema Windows



També convindria que féssiu un control dels ports del sistema per tal de veure quins d'aquests ports estan oberts i quines aplicacions utilitzen.

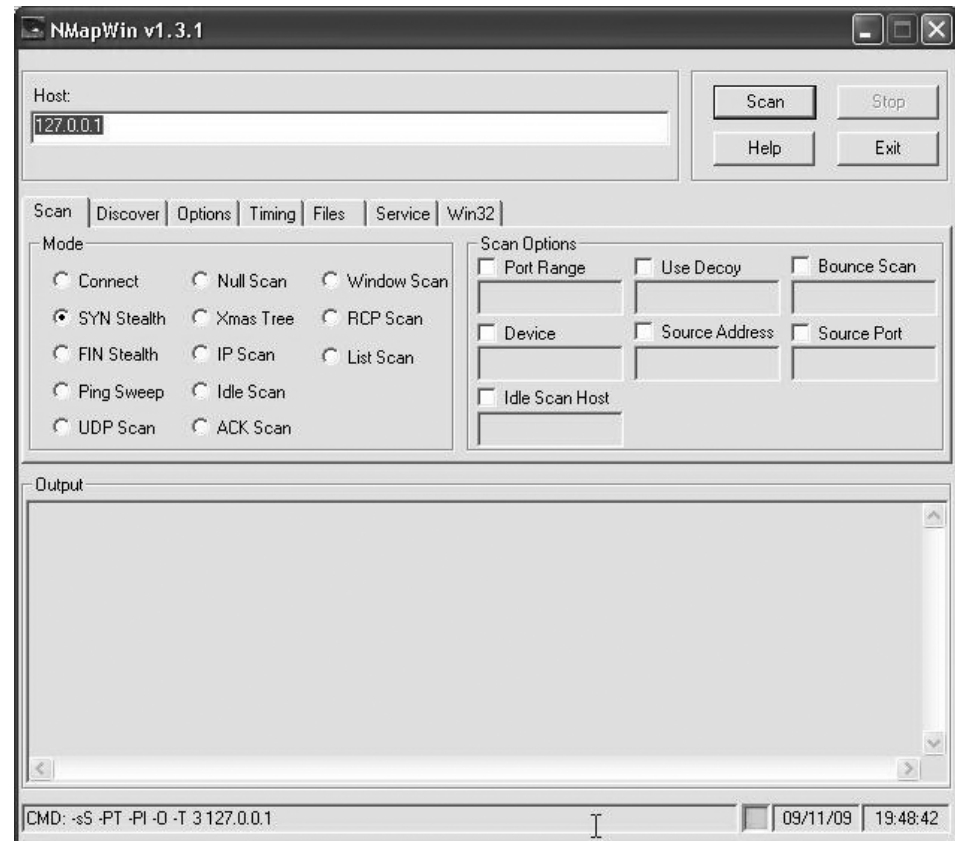
D'aquesta manera, si hi ha un port obert que no utilitza cap aplicació, cal tancar-lo. En diferents manuals de text o en algunes pàgines d'Internet, podem trobar una llista que mostra tots els ports que hi ha i indica a quina aplicació estan destinats. Podem decidir, doncs, si volem que un port determinat estigui obert perquè el pugui fer servir una aplicació determinada o, contràriament, volem que estigui tancat perquè no utilitzem l'aplicació en qüestió.

Ports

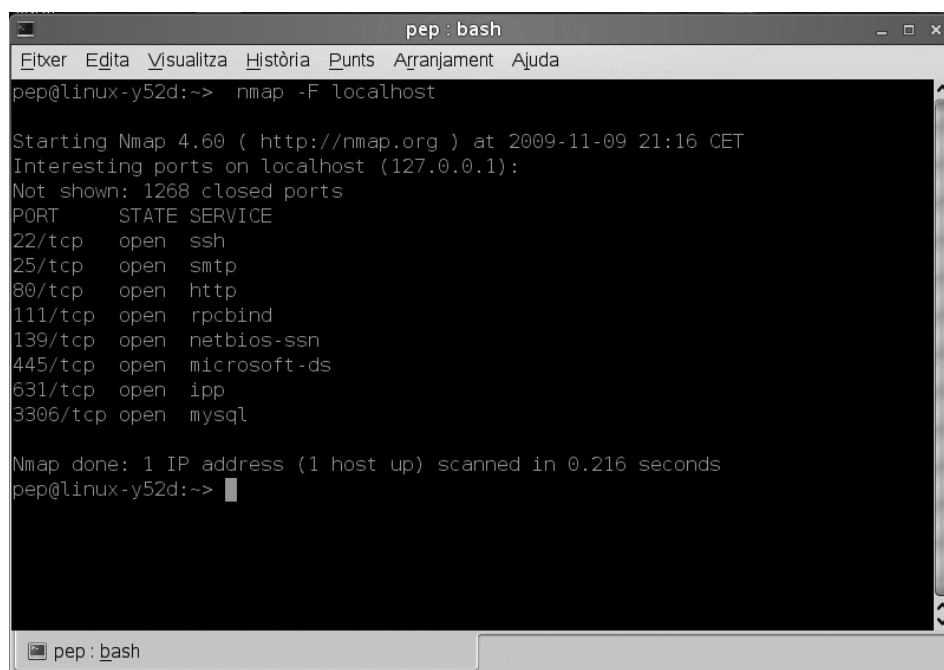
En informàtica, un port és una manera genèrica de denominar una interfície per mitjà de la qual diferents tipus de dades poden ser enviades i rebudes. Aquesta interfície pot ser física o a escala de programari (per exemple, els ports que permeten la transmissió de dades entre diferents ordinadors).

A Internet, hi ha alguns programes de programari lliure per a l'entorn Windows que permeten veure una llista dels ports que tenim. Ens indiquen quins estan oberts, quins estan escoltant i quins estan tancats. Alhora, ens permet obrir-los i tancar-los. L'**Nmap**, per exemple, és un programa de codi lliure de l'entorn Windows que ens permet fer un seguiment dels ports. L'**Nmapwin** proporciona l'entorn gràfic per no treballar en consola. El podem veure en la figura 2.3.

FIGURA 2.3. Programa per escanejar els ports en un sistema Windows



Si parlem de l'entorn Linux, hi ha diverses ordres per a la consola que permeten veure una llista dels ports i l'estat en què es troben. També permeten obrir-los i tancar-los. En podem veure un exemple en la figura 2.4.

FIGURA 2.4. Escaneig de ports en l'entorn LinuxA screenshot of a terminal window titled 'pep : bash'. The window shows the output of the command 'nmap -F localhost'. The output indicates that Nmap 4.60 was started at 2009-11-09 21:16 CET and scanned localhost (127.0.0.1). It reports 1268 closed ports and lists several open ports with their corresponding services. The terminal window has a menu bar with options like 'Fitxer', 'Edita', 'Visualitza', etc., and a status bar at the bottom showing 'pep : bash'.

```
pep@linux-y52d:~> nmap -F localhost

Starting Nmap 4.60 ( http://nmap.org ) at 2009-11-09 21:16 CET
Interesting ports on localhost (127.0.0.1):
Not shown: 1268 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql

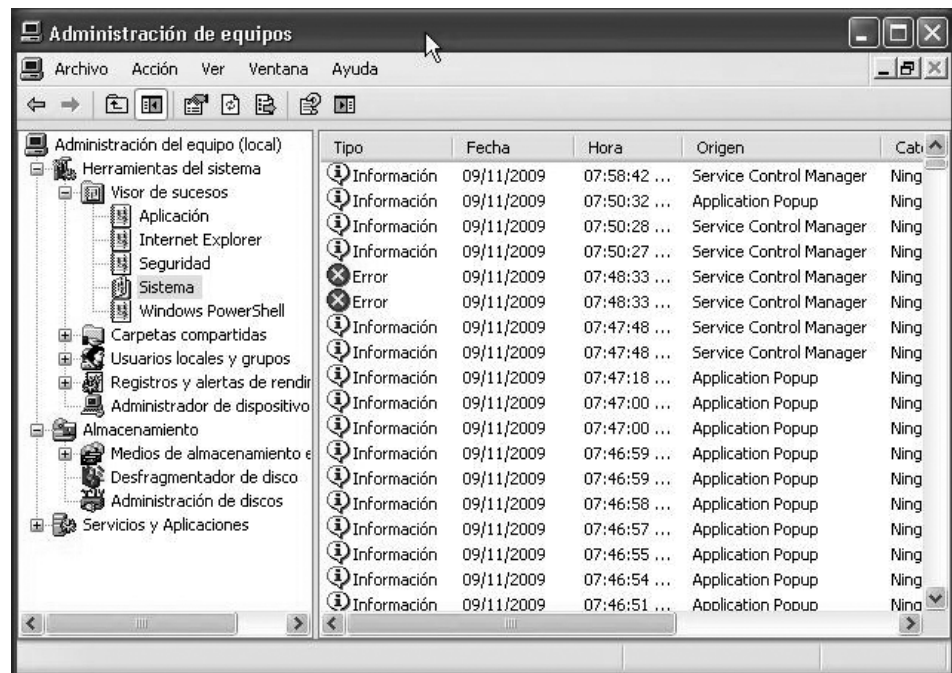
Nmap done: 1 IP address (1 host up) scanned in 0.216 seconds
pep@linux-y52d:~>
```

Especialment, cal esmentar una sèrie d'aplicacions del vostre sistema que en alguns casos poden ser molt útils. Cal tenir en compte, però, que tenen un risc potencialment alt d'intrusions. Aquestes aplicacions, són per exemple, les que estan relacionades amb el control remot del vostre sistema, com el Terminal Server, l'accés per SSH, etc. Cal valorar d'una manera especial l'ús d'aquests recursos en funció de la perillositat que comporten, ja que obren portes a possibles intrusions.

El fet de tenir instal·lats sistemes per detectar intrusions, com els IDS, representa la possibilitat de controlar-les i de rebre un avís en cas que entrin en el sistema. Bàsicament, aquesta és la funció d'aquest servei, la de detectar i avisar, però no la d'actuar o prevenir, ja que d'això, se n'encarreguen altres components. Per exemple, els anomenats *IPS*.

Els sistemes de detecció d'intrusions poden actuar instal·lats en una xarxa, els NIDS, o bé instal·lats en ordinadors individuals, els HIDS, que tenen una manera de treballar molt similar a la d'un tallafoc. Si disposeu d'un sistema en xarxa, un NIDS, la seva funció consisteix a examinar els paquets reals que viatgen per la xarxa en temps real per buscar activitats sospitoses. En canvi, un sistema instal·lat a la màquina, un HIDS, examina els arxius de registre, com el **registre d'esdeveniments** del Windows, és a dir, de sistema d'aplicacions. Aquest sistema de detecció en la màquina també examina els **registres d'esdeveniments de seguretat** i hi busca les entrades que suggereixen algun tipus d'activitat sospitosa. En la figura 2.5, podeu veure el **visor d'esdeveniments** en el quadre de diàleg d'**administració d'equips** per a un entorn Windows.

FIGURA 2.5. Visor de successos en un entorn Windows



El sistema en xarxa, NIDS, té l'avantatge de treballar en temps real. Fins i tot pot detectar un atac que no ha tingut èxit perquè sigueu conscients que s'ha produït. Alhora, també pot detectar alguns tipus d'atacs que un sistema de màquina no detectaria, ja que per identificar-los cal mirar quin és l'encapçalament dels paquets que circulen per la xarxa.

Com que un HIDS es basa en la comprovació de registres en el sistema per identificar atacs, només pot validar que un atac ha tingut èxit. En canvi, però, pot detectar intents d'accedir a arxius, de canviar-ne els permisos o de canviar els arxius importants del sistema. Es tracta d'atacs que un HIDS no detectaria.

Per tant, l'un no és millor que l'altre. Cal tenir en compte que es poden utilitzar conjuntament perquè informin de tots els tipus d'atacs, cosa que no és possible si només s'utilitza un dels dos sistemes. De fet, la detecció que es basa en les signatures, és a dir, mirant l'encapçalament dels paquets d'informació que circulen per la xarxa, funciona de manera molt similar als programes contra el programari maliciós, els antivirus. Aquests programes intenten comparar l'encapçalament dels paquets (i altra informació) amb el que hi ha en una base de dades de signatures conegudes d'atacs i de codis maliciosos. El problema que hi ha amb aquest tipus de funcionament és que fins que no hi ha un atac, no és possible desenvolupar una signatura per a aquest atac. Així, cal que algú sigui atacat perquè els venedors dels sistemes de detecció o els grups de suport d'aquests sistemes puguin desenvolupar-ne la signatura corresponent. Aquesta manera de treballar fa que hi hagi un període de temps, des que es llança un atac fins que se'n rep la signatura corresponent, durant el qual no es disposa de cap classe de protecció contra aquesta amenaça.

També hi ha sistemes que utilitzen la detecció basada en les anomalies, és a dir, comparen els paquets de la xarxa amb el comportament habitual i busquen accions que no siguin normals. Per exemple, si habitualment un ordinador no fa servir un

FTP, però de cop i volta intenta iniciar una connexió FTP amb un servidor, l'IDS ho detectarà com una anormalitat i avisarà l'usuari. L'inconvenient de la detecció per anomalies és que es pot necessitar una etapa inicial en què hi pot haver molts falsos positius que es poden perdre abans no s'estableix un patró de comportament.

Totes dues tècniques de detecció tenen pros i contres, però, deixant de banda la perillositat d'una activitat determinada, la feina d'un IDS és avisar.

Un dels millors programes d'IDS és l'**Snort**, que podeu veure en la figura 2.6.

L'**Snort** és una aplicació de detecció d'intrusos en xarxa de codi obert, NIDS, gratuïta, de codi lliure. Per a aquest programa, hi ha diversos fòrums de suport i llistes de correu que podeu consultar per aprendre'n més coses o per aconseguir signatures actualitzades per a les noves amenaces. L'Snort analitza els paquets de la xarxa i pot detectar molts atacs coneguts i activitats malicioses. Hi ha altres aplicacions de codi lliure tant per a l'entorn Windows com per a l'entorn Linux, com el Wireshark.

FIGURA 2.6. Programa de codi lliure Snort



Hi ha una tecnologia més nova que també es pot encarregar de la resposta inicial. Un IPS és una cosa semblant a un híbrid entre un IDS i un tallafoc i pot funcionar juntament amb el vostre tallafoc actual. La diferència principal que hi ha entre un IDS i un IPS és que un IPS farà alguna cosa per respondre i intentarà aturar la intrusió, mentre que un IDS simplement us permetrà saber què succeeix. Un IPS controla la xarxa de la mateixa manera que ho fa un IDS i, fins i tot, utilitza les mateixes tècniques de signatures o de coincidència d'anomalies per identificar una activitat potencialment perillosa. Quan un IPS detecta que hi ha un trànsit maliciós sospitos, pot canviar les regles del tallafoc o crear-ne de noves per bloquejar tot el trànsit que passa pel port en què hi ha l'activitat sospitosa. Igualment, pot

bloquejar tot el trànsit des de la direcció IP d'origen o permetre configurar diverses respostes personalitzades.

Normalment, l'IPS es configurarà, no solament per emprendre una acció immediata que intenti evitar qualsevol activitat maliciosa posterior, sinó també per avisar l'usuari, tal com fa un IDS.

2.1.1 Detecció d'incidències

Bàsicament, hi ha dues maneres de detectar una incidència de seguretat. La primera és rebre una alarma del sistema mateix. Aquesta alarma pot provenir de qualsevol sistema de seguretat que hi hagi instal·lat: un programa antivirus, qualsevol programa de detecció d'intrusos o el tallafoc.

La segona opció és detectar una incidència de seguretat sense que el sistema n'informi. Com podeu detectar que el vostre sistema ha patit una incidència de seguretat, ha estat infectat per un programari maliciós o ha patit un atac si no hi ha cap alarma d'avís? Ho podeu detectar si noteu que el sistema informàtic actua d'una manera estranya. Per exemple, si heu vist que hi ha arxius on no n'hi solia haver o us heu adonat que hi ha arxius que han desaparegut de cop i volta. També podeu notar que el sistema va més lent del normal o que el disc dur va molt lent, fins i tot quan no esteu fent res d'especial en el sistema. Un altre indicatiu és que el sistema falli o es tanqui de cop.

Tot això són senyals potencials que indiquen que el vostre sistema informàtic podria estar infectat per alguna classe de programari maliciós o que podria haver patit alguna intrusió.

2.1.2 Resolució d'incidències mitjançant les instruccions pertinents

Una vegada heu detectat una incidència de seguretat en el vostre sistema, cal que actueu per evitar riscos i possibles danys. A l'hora d'actuar davant la incidència us podeu trobar en dues situacions. La primera és que disposeu d'un pla de contingència. Dins aquest pla hi haurà un apartat que us informará del procediment que heu de seguir en la situació en què us trobeu. El pla de contingència està preparat perquè una petita empresa o institució pugui continuar funcionant en cas d'incidència de seguretat. A més, dóna instruccions per resoldre aquesta incidència i minimitzar els riscos que hagi pogut provocar.

Aquesta és la situació més probable si us trobeu en una petita o mitjana empresa que hagi invertit recursos humans i materials en la seguretat del seu sistema informàtic. Si la situació és aquesta, només cal que seguïu les instruccions que conté el pla de contingència per minimitzar els riscos de la incidència o recuperar el sistema en cas que hagi patit alguna incidència greu.

Us podeu trobar davant el segon supòsit, sia perquè no disposeu de pla de contingència o perquè el vostre pla de contingència no recull la incidència en què us trobeu.

En cas que no disposeu d'un pla de contingència que reculli els passos que heu de seguir, convindrà que actueu pel vostre compte. Podreu seguir diverses actuacions depenent de quina sigui la incidència de seguretat.

Si no disposeu d'un pla de contingència i la incidència prové d'una alarma del vostre sistema antiprogramari maliciós, caldrà que feu el que l'antivirus us suggereixi.

En algunes ocasions, el programa antivirus neteja el programari maliciós, però en tornar a engegar la màquina, torna a aparèixer. En aquesta circumstància, podeu provar d'iniciar el sistema amb l'opció coneguda com a **mode segur** i, aleshores, eliminar-ne el virus.

Si l'antivirus no ha pogut eliminar el virus, us haureu d'assegurar que està perfectament actualitzat. Si no ho està, convindrà que l'actualitzeu amb l'última revisió de la base de dades de virus i torneu a escanejar tot el sistema. En cas que ja estigui actualitzat, caldrà una estratègia nova. A vegades, alguns venedors de programari antivirus creen eines independents gratuïtes per ajudar a detectar i eliminar amenaces difícils. Acostumen a ser eines que funcionen per mitjà d'Internet, és a dir, escanegen i desinfecten per aquesta via.

Heu de tenir present que alguns d'aquests programaris maliciosos estan fets i preparats per inutilitzar o eliminar el programari antivirus. En aquest cas, el problema pot ser més complicat i difícil de resoldre. Podeu provar diferents programes antivirus, escanejar per mitjà d'Internet o, directament, buscar informació a la xarxa sobre com resoldre la incidència. Tingueu en compte que en aquests casos la majoria d'informació que trobareu i les instruccions que haureu de seguir estaran en anglès.

Si sospiteu que passa alguna cosa en el vostre sistema, però no heu rebut cap tipus d'alarma, hauríeu de consultar, primer de tot, els **registres d'esdeveniments** de Windows. La consola del visor d'esdeveniments mostra els registres sobre la informació d'accés, execució i errors, entre altres.

El problema que hi ha amb els registres, concretament quan corresponen a la categoria d'esdeveniments de seguretat, és que el Windows només captura les dades dels registres per als esdeveniments que, segons la configuració, ha de controlar.

En la revisió del **registre de seguretat**, tant les alertes de *Correcte* com les d'*Error* us poden proporcionar informació útil depenent de quina sigui la incidència. Per exemple, podeu descobrir-hi esdeveniments d'inici de sessió de comptes correctes a una hora en què sabeu de segur que no heu utilitzat l'ordinador. Això vol dir que algú ha utilitzat el vostre nom d'usuari i contrasenya. Igualment, descobrir-hi esdeveniments d'inici de comptes erronis demostra que un atacant ha intentat accedir al vostre sistema.

Considerant la informació del registre d'esdeveniments, podríeu pensar que és interessant auditar i controlar tots els esdeveniments, els de les diverses aplicacions, el correu, els correctes, els incorrectes, etc. Cal tenir en compte, però, que controlar i registrar tots els esdeveniments afecta el processador de l'ordinador. Per fer-ho, l'ordinador necessita utilitzar recursos de memòria i això n'altera el rendiment general. Igualment, les dades dels registres ocupen espai en el disc dur. Registrar tots els esdeveniments pot fer que el vostre arxiu de dades de registre s'ompli ràpidament o que es faci més gran, cosa que us pot impedir treballar amb la facilitat d'abans.

La qüestió és trobar un bon equilibri. S'han de controlar i registrar els esdeveniments que seran més útils per identificar problemes. D'aquesta manera, no afectarà el rendiment del sistema ni s'omplirà el disc dur. Hi ha la possibilitat de limitar la mida del registre d'esdeveniments. Per fer-ho, s'ha de seleccionar l'opció *Propietats del visor d'esdeveniments* i fixar-hi una mida màxima per a aquest registre. També podeu configurar-lo perquè quan assoleixi la mida màxima, reescriui o no els esdeveniments antics. Si ordenem que no ho faci, no escriurà cap esdeveniment nou fins que els esborrem manualment.

Si no heu trobat cap activitat sospitosa o maliciosa en els registres del visor d'esdeveniments, també podeu mirar el **registre del programari del tallafoc**. Hi trobareu informació difícil d'entendre, però amb l'ajuda d'Internet podreu desxifrar i identificar quin ha estat el problema. Una vegada més, cal que tingueu en compte que, molt probablement, tota la informació que hi trobareu estarà en anglès.

Si cap de les indicacions anteriors no ha donat resultat, sempre podeu anar a veure quins processos s'estan executant en la vostra màquina. En la vista dels processos, n'hi haurà molts que no podreu identificar. Aleshores, els haureu de cercar a Internet. Pot ser que descobriu que algun correspon a un programari maliciós. Si continueu la cerca, sia en pàgines especialitzades o en fòrums, trobareu les instruccions necessàries per eliminar aquest procés que els antivirus no han pogut eliminar. En algunes ocasions, haureu d'utilitzar la consola i unes instruccions a què no esteu habituats. Seguiu-les detingudament i reinicieu el sistema quan us ho indiquin. Segurament aquesta informació també estarà en anglès.

Finalment, si cap d'aquestes opcions no us ha permès resoldre la incidència de seguretat, sempre podeu recórrer a l'opció que ofereix la majoria de sistemes operatius, la restauració del sistema a partir d'una configuració del sistema anterior a la incidència. La manera de restaurar-lo dependrà del sistema que utilitzeu. Aquesta utilitat només us servirà si disposeu de punts de restauració anteriors a la incidència, de manera que és recomanable crear-los manualment en moments en què el sistema està totalment instal·lat i funciona perfectament. Hi ha sistemes que, en detectar certs canvis, ja creen automàticament un punt de restauració.

2.2 Interpretació i utilització com a ajuda de documentació tècnica

En alguns casos, per resoldre la incidència de seguretat només caldrà que seguïu les instruccions que hi ha en el pla de contingència. Heu de tenir en compte, però, que aquestes instruccions solen ser tècniques i, consegüentment, solen utilitzar un vocabulari també tècnic relacionat amb el vostre sistema informàtic. Si en algun moment hi ha coses que no enteneu, teniu diverses opcions. Una possibilitat és utilitzar el sistema d'ajuda que incorpora el vostre sistema mateix.

El sistema d'ajuda acostuma a ser força complet. Entre altres coses, indica què és cada part del sistema i dóna les instruccions que s'han de seguir per fer diverses tasques. L'ajuda sol ser força accessible, però la ubicació depèn de cada sistema. Si teniu sistema de codi lliure, és possible que una part d'aquesta ajuda estigui en anglès.

En cas que no compreu o desconeixeu el significat d'algunes parts de les instruccions del pla de contingència, podeu consultar manuals. Si no, també podeu buscar informació a Internet. Hi podeu trobar un excés d'informació i, a més, aquesta informació pot ser dispar, cosa que pot ser un problema. És possible que moltes pàgines estiguin en anglès.

Si no disposeu d'un pla de contingència, podeu intentar seguir les instruccions que us proporcionaran les mateixes eines que han detectat la incidència de seguretat. És important que feu les tasques que us indiquen amb deteniment.

En cas que no disposeu de cap pla de contingència, que disposeu d'un pla de contingència, però no sigui útil per a la incidència en qüestió, o que simplement no tingueu cap mena d'instruccions concretes a seguir podeu recórrer a Internet. Segur que hi ha informació sobre la vostra incidència, ja que és molt probable que ja hi hagi topat algú altre. Tanmateix, tant pot ser que us costi trobar-hi aquesta informació com que n'hi trobeu massa. Per tant, si feu servir Internet, sigueu curosos a l'hora de tractar-la. Intenteu seguir instruccions de pàgines que tinguin certa credibilitat o que ja conegueu i sapigueu d'on provenen. Passa el mateix en el cas de la informació dels fòrums.

Si feu servir instruccions que heu trobat a Internet, és molt probable que estiguin escrites, totalment o parcialment, en anglès. És recomanable tenir un nivell d'anglès mínim, almenys pel que fa a la documentació tècnica relacionada amb la informàtica. Tanmateix, en cas que no tingueu aquest nivell d'anglès mínim, sempre podeu utilitzar Internet com a eina d'ajuda per traduir o buscar informació sobre expressions o vocabulari tècnic. Hi ha pàgines que permeten traduir documents de l'anglès. Malgrat tot, no heu d'esperar que siguin traduccions exactes de gaire qualitat. També hi ha diccionaris per buscar paraules concretes i, fins i tot, algunes aplicacions de programari per traduir textos o paraules.

Finalment, convé que recordeu que si seguïu instruccions tècniques, us heu de limitar a fer el que indiquin, ja que qualsevol canvi o modificació pot provocar situacions no desitjades. Per tant, cal que us assegureu de seguir-les al peu de la

lletra i d'utilitzar les versions del sistema i del programari que indiquin. En cas contrari, pot ser que no obtingueu els resultats que espereu.

2.3 Documentació de les incidències de seguretat

En cas que no disposeu de cap pla de contingència o que el pla no reculli la incidència en qüestió, cal que la documenteu degudament. Cal recollir i escriure quina ha estat la incidència, com s'ha detectat, quan s'ha produït, quins efectes ha tingut i, sobretot, com s'ha resolt per preparar-vos per a situacions futures. Si per resoldre la incidència s'han utilitzat materials diversos i fonts d'informació diferents, convé que quedi recollit. Tot això facilitarà enormement la resolució de futures incidències.

Aquesta documentació ha d'estar degudament recollida i s'ha de guardar en un lloc adient. És a dir, en un lloc on es pugui accedir fàcilment en cas de tornar-la a necessitar. Si en l'empresa o lloc de treball hi ha un protocol, és a dir, instruccions sobre com configurar aquesta documentació, cal seguir-lo a l'hora de documentar la incidència. Si no hi ha cap protocol, la documentació haurà d'incloure tota la informació d'una manera clara i ben estructurada. Heu de pensar que és possible que altres persones, en algun moment, llegeixin aquesta informació, de manera que és necessari que estigui ben redactada perquè sigui explícita i fàcil d'entendre i de seguir.

3. Protecció contra programari maliciós

Programari maliciós o *maligne* és la traducció del terme anglès *malicious software* o *malware*. Aquest programari, que és nociu per a l'ordinador, està dissenyat per inserir-hi virus, cavalls de Troia, cucs o programes espia, entre altres. Quan siguin dins l'ordinador, n'extrauran informació o hi compliran algun propòsit, com permetre que altres persones hi accedeixin.

Hi ha molts tipus diferents de programari maliciós. Les tècniques que utilitzen per entrar en els sistemes i les accions que hi duen a terme també són moltes i molt diverses. Per tant, vosaltres també haureu de prendre moltes precaucions diferents i, fins i tot, haureu de conjugar diversos mètodes de protecció. Sobretot, però, haureu d'instal·lar un programa antivirus a l'ordinador.

Cal tenir en compte que un ordinador, si està connectat a una xarxa, s'hi introdueixen llapis de memòria o discos extraïbles i, sobretot, està connectat a Internet, està sotmès a la perillositat del programari maliciós. Per tant, **caldrà que el vostre sistema informàtic estigui ben protegit** de tot aquest programari.

El primer que heu de fer per protegir el sistema és **instal·lar-hi correctament el sistema operatiu** amb les aplicacions i les actualitzacions corresponents, sobretot les de seguretat. També caldrà que tingueu una **bona política de còpies de seguretat**, tant pel que fa a les dades guardades com pel que fa a la configuració del sistema. D'aquesta manera, en cas que hi hagi una incidència de seguretat, la recuperació del sistema serà al més ràpida i eficaç possible.

Totes aquestes mesures, però, no serveixen de res si no s'**instal·la un programa antivirus**, que s'ha de mantenir actualitzat en tot moment. També cal reforçar la seguretat amb altres utilitats, com els tallafocs, que fins i tot es poden combinar amb programes que rastregen el trànsit d'informació per mitjà de la xarxa.

Aquestes són, a grans trets, les actuacions que cal seguir per protegir el sistema del programari maliciós. De totes maneres, s'ha d'acceptar que prendre totes les mesures de seguretat esmentades no implica tenir una seguretat total i absoluta. Per tant, la política de les còpies de la configuració del sistema i les dades són molt importants. En cas que la infecció del sistema no es pugui evitar totalment, almenys se'n garantirà al màxim la recuperació després d'una incidència de seguretat.

Especialment, cal esmentar la diferència que hi ha entre els sistemes que utilitzen programari de propietat, com els de l'entorn Microsoft, i els sistemes que utilitzen programari lliure, com els sistemes operatius de Linux. Aquests últims són molt més segurs pel que fa a la possible infecció de virus i a les intrusions. Per tant, aquest ha de ser un factor a tenir en compte a l'hora d'instal·lar un sistema determinat, ja que actualment la seguretat s'està convertint en un element important dels sistemes informàtics.

Finalment, també cal mencionar de manera especial els pirates informàtics, coneguts com a *hackers*, ja que tenen l'objectiu d'introduir-se en els sistemes informàtics amb diverses finalitats, sia només aconseguir entrar-hi o fer-hi accions perjudicials per al vostre sistema. Moltes vegades, els pirates utilitzen el que es coneix amb el nom d'*enginyeria social* o les tècniques de suplantació, més que no pas programes maliciosos que aprofiten forats en la seguretat del sistema. Aleshores, es converteix en una tasca més complicada, ja que no n'hi ha prou amb mantenir el sistema ben protegit, sinó que, a l'hora de navegar per Internet, cal anar molt alerta amb les pàgines que obriu i, sobretot, amb les dades que faciliteu.

3.1 Virus i programes maliciosos

Cal que tingueu el sistema ben protegit. Per tant, heu de tenir clar de qui us heu de protegir i què és el que voleu protegir. També heu de saber quins perills té el vostre sistema, quin és el nivell de propagació i quins són els danys que pot provocar el programari maliciós. Aquesta, doncs, és la primera tasca que cal fer.

El **programari maliciós** és tot el programari que s'instal·la en el vostre ordinador, sense el vostre consentiment ni coneixement, amb la finalitat de perjudicar-lo o d'obtenir-ne un benefici. Aquest últim cas és el més habitual, de manera que les accions del programari maliciós cada vegada són més sofisticades i difícils d'identificar.

Hi ha molts tipus de programari maliciós i, per tant, classificar-los és difícil. Malgrat tot, es poden distingir els més habituals, que són els següents:

1) Virus: es tracta d'un programa que es copia automàticament per alterar el funcionament normal del sistema, sense el permís ni el coneixement de l'usuari. Ells mateixos es repliquen i s'executen. Dins aquest apartat hi podem trobar els virus següents:

- **Virus residents:** s'executen cada vegada que engeguem l'ordinador i s'oculten en la RAM de manera permanent. D'aquesta manera, controlen totes les operacions que es fan amb l'ordinador i tenen la capacitat d'infectar tots els arxius que obrim, tanquem, copiem, executem, etc. Només s'activen quan es compleix una certa condició imposada pel creador del virus, com la data o l'execució d'una determinada acció. Fins que no es produeix, romanen ocults.
- **Virus d'acció directa:** es reproduïxen i actuen en el mateix moment que s'executen. A diferència dels residents, no són en la memòria. Normalment, només afecten els arxius que són a la mateixa carpeta/ directori o en els que es troben en el camí (*path*). Tenen l'avantatge que són més fàcils d'eliminar sense deixar cap rastre.

El Randex, el CMJ, el Meve y el MrKlunky són exemples de virus residents.

- **Virus de sobreescritura:** escriuen dins un arxiu i en canvien el contingut. L'arxiu infectat no varia de mida, ja que només se sobreescriu. Els arxius infectats per aquest virus queden inservibles i s'han d'eliminar, de manera que es perd la informació que contenen.
- **Virus de companyia:** per efectuar les operacions d'infecció, els virus de companyia poden esperar-se en la memòria fins que s'executi algun programa (virus residents) o actuar directament fent còpies d'ells mateixos (virus d'acció directa).

Contràriament als virus de sobreescritura o als virus residents, els virus de companyia no modifiquen els fitxers infectats. En algun moment, mentre el sistema operatiu està treballant (executant programes, fitxers amb extensions *.exe* i *.com*), pot haver d'executar un programa amb un nom determinat. Aleshores, si hi ha dos fitxers executables, l'un amb extensió *.exe* i l'altre amb extensió *.com*, el sistema operatiu executarà en primer lloc el d'extensió *.com*. El virus de companyia aprofita aquesta peculiaritat per crear un altre fitxer amb el mateix nom, però amb extensió *.com*, de manera que el virus que crearà la infecció serà aquest. Quan el sistema operatiu hagi de decidir quin dels dos fitxers ha d'executar, optarà pel d'extensió *.com*, que s'infectarà, i seguidament executarà el fitxer *.exe*. D'aquesta manera, l'usuari no s'adonarà de la infecció que s'acaba de produir. Aquesta manera de funcionar d'aquests virus provoca que s'estenguin d'una manera eficaç i en dificulta la detecció.

- **Virus d'arrencada o boot:** els termes *boot* o *sector d'arrencada* fan referència a una secció molt important d'un disc (tant d'un disquet com d'un disc dur). En aquesta secció es guarda la informació essencial de les característiques del disc i hi ha un programa que permet arrencar l'ordinador. Aquest virus no infecta fitxers, sinó els discos que els contenen. Actuen infectant, en primer lloc, el sector d'arrencada dels disquets, USB, CD o DVD. Quan un ordinador es posa en marxa amb un disquet, un USB, un CD o un DVD infectat, el virus de *boot* n'infecta el disc dur.
- **Virus de macro:** l'objectiu d'aquests virus és infectar els fitxers que s'han creat mitjançant determinades aplicacions que contenen *macros*: documents de Word (*.doc*), fulls de càlcul Excel (*.xls*), bases de dades (*.mdb*), presentacions en PowerPoint (*.pps*), fitxers Corel Draw, OpenOffice Writer (*.odt*), OpenOffice Calc (*.ods*), OpenOffice Base, etc.

Les macros són microprogrames associats a un fitxer que serveixen per automatitzar operacions complexes. En ser programes, les macros es poden infectar. Quan s'obri un fitxer que contingui un virus d'aquest tipus, les macros es carregaran de manera automàtica i produiran la infecció. Tot i que la majoria de les aplicacions que utilitzen les macros disposen d'una protecció antivirus i de seguretat específica, hi ha molts virus de macro que saltin aquesta protecció.

Hi ha un tipus de virus de macro diferent segons si l'eina que s'utilitza és de **Word**, d'**Excel**, d'**Access**, de **PowerPoint**, de multiprograma o d'arxius

Path

El path és el nom anglès que correspon a la ruta en què es troba un arxiu. La ruta s'expressa des del directori arrel fins al directori en què es hi ha l'arxiu. També es coneix amb aquest nom el contingut de la variable path, que correspon al directori del sistema en què es troben els executables.

El Way, el Trj.ReBoot i el Trivial.88.D són exemples de virus de sobreescritura.

El Polyboot.B i l'AntiEXE són alguns exemples de virus d'arrencada o boot.

Aquests són alguns dels exemples de virus de macro: el Relax, el Melissa.A, el Bablas o el O97M/Y2K.

RTF. De totes maneres, aquest virus pot no infectar tots els programes o eines amb macros.

- **Virus de directori o d'enllaç:** els fitxers s'ubiquen en direccions determinades (unitat de disc i directori) que el sistema operatiu coneix per poder localitzar-los i treballar-hi. Els virus d'enllaç o de directori alteren les direccions que indiquen on es troben emmagatzemats els fitxers. Així doncs, en intentar executar un programa (fitxer *.exe* o *.com*) infectat per un virus d'enllaç, el que es fa en realitat és executar el virus, ja que aquest modificarà la direcció original del programa i la reemplaçarà. Una vegada produïda la infecció, és impossible localitzar i treballar amb els fitxers originals.
- **Virus encriptats:** més que d'un tipus de virus, es tracta d'una tècnica que alguns d'aquests virus, que poden pertànyer a altres classificacions, utilitzen. Els virus s'encripten perquè els programes antivirus no els detectin. Quan volen actuar es desencripten i quan han acabat es tornen a encriptar.
- **Virus polimòrfics:** són virus que cada vegada que fan una infecció s'encripten d'una manera diferent. Per fer-ho, utilitzen diversos algorismes i claus de xifratge. Així, generen moltes còpies d'ells mateixos i impedeixen que els antivirus els localitzin per mitjà de la cerca en cadenes o signatures. Per això són difícils de detectar.
- **Virus multipartides:** són virus que poden fer moltes infeccions mitjançant la combinació de tècniques diferents. L'objectiu és qualsevol element que es pot infectar: arxius, programes, macros, discos, etc. Es consideren els més perillosos per la capacitat que tenen de combinar moltes tècniques d'infecció i pels danys que provoquen.
- **Virus web:** són virus de creació recent i apareixen quan s'entra en una pàgina web que conté **ActiveX**, **Java** o **Javascript** infectat.

Aquests són alguns exemples de virus encriptats: l'Elvira i el Trile.

L'Elkern, el Marburg, el Satan Bug i el Tuareg són exemples de virus polimòrfics.

L'Ywinz és un exemple de virus multipartides.

El PSWBugbear.B, el Lovgate.F, el Trile.C, el Sobig.D i el Mapson són alguns exemples de cucs.

2) Cucs o worms: es dupliquen com els virus, però **no modifiquen els arxius**. Es limiten a fer còpies d'ells mateixos al més ràpid possible sense tocar cap fitxer. Poden arribar a ocupar la memòria i alentir l'ordinador. A més, també poden col·lapsar per saturació les xarxes en què s'han infiltrat.

Les infeccions que produeixen aquests virus es fan per mitjà del correu electrònic, les xarxes informàtiques i els canals de xat (com l'IRC o l'ICQ) d'Internet.

3) Cavalls de Troia: no es consideren virus, perquè no infecten altres fitxers per reproduir-se ni tampoc fan còpies d'ells mateixos per propagar-se, com fan els cucs. L'objectiu bàsic que tenen és introduir i instal·lar altres programes en l'ordinador perquè es puguin controlar remotament des d'altres equips. És a dir, arriben a

l'ordinador com si fossin programes inofensius, però quan s'executen hi instal·len un segon programa, el cavall de Troia.

En general, els cavalls de Troia són programes que s'oculten en imatges o arxius multimèdia (àudio o vídeo) perquè es puguin instal·lar fàcilment.

Els efectes dels cavalls de Troia poden ser molt perillosos. Com els virus, tenen la capacitat d'eliminar fitxers o destruir la informació del disc dur. A més, però, poden capturar dades confidencials i enviar-les a una direcció externa. També poden obrir ports de comunicacions, cosa que permet que altres persones tinguin un control remot del vostre ordinador.

De les accions més comunes dels cavalls de Troia, en destacariem les següents:

- Controla remotament equips.
- Espia equips per obtenir informació.
- Obté contrasenyes del Messenger.
- Ataca els arxius del sistema.
- Assigna contrasenyes als arxius i després suborna els usuaris (víctimes) perquè paguin diners a canvi de les contrasenyes.
- Captura pantalles, similar a espiar.
- Enganya un usuari amb enginyeria social per aconseguir-ne les dades confidencials, com números bancaris, contrasenyes o noms d'usuari.

Els cavalls de Troia són tan importants que ja ocupen el primer lloc de la llista de programari maliciós, davant dels virus. El fet que a Internet hi hagi models simples per crear cavalls de Troia sense necessitat de ser cap expert en informàtica, ha fet que encara proliferessin més.

4) Bombes lògiques: estrictament, tampoc es consideren virus, ja que no es reproduïen i ni tan sols són programes independents, sinó que són segments camuflats dins altres programes.

L'objectiu que tenen és destruir les dades d'un ordinador o causar altres tipus de danys que poden arribar a ser molt destructors.

5) Falses alarmes o hoaxes: no són virus, sinó missatges de correu electrònic que enganyen. Es difonen massivament per Internet i sembren alarma sobre suposades infeccions víriques i amenaces contra els usuaris. Les falses alarmes solen guanyar-se la confiança dels usuaris, perquè aporten dades que semblen certes i proposen una sèrie d'accions a realitzar per eliminar la suposada infecció. No cal fer cas de les advertències i les instruccions, simplement s'ha d'esborrar el missatge i prou.

6) Programes espia o spyware: el programa espia és un programari, de la categoria dels programes maliciosos, que recopila informació d'un ordinador i després la transmet a una entitat externa sense el consentiment o el coneixement

L'IRC.Sx2, el Trifor o el Burglar.A són alguns exemples de cavalls de Troia.

El Good Time, el Penpal Greetings, el Join the Crew o el Win a Holiday, el Takes Guts to Say Jesus, entre altres, són algunes de les falses alarmes.

del propietari de l'ordinador. Aquest programa espia s'autoinstal·la afectant, de manera que s'executa cada vegada que l'ordinador es posa en marxa (utilitza el CPU i la memòria RAM i redueix l'estabilitat de l'ordinador). Funciona sempre i controla l'ús que es fa d'Internet, cosa que serveix a entitats externes per mostrar-vos, per exemple, anuncis relacionats amb la vostra activitat en la xarxa.

La funció més comuna que tenen aquests programes és recopilar informació sobre l'usuari i distribuir-la a empreses publicitàries o altres organitzacions interessades. Cal tenir en compte, però, que organismes oficials han utilitzat aquest programari per recopilar informació contra sospitosos de delictes, pirateria del programari, etc.

Llicència freeware i shareware

La llicència *freeware* correspon a programari de distribució gratuïta, però amb llicència d'ús restringida. Per exemple, normalment no es permet modificar el codi de l'aplicació. En canvi, la llicència *shareware* consisteix a distribuir un programari de manera gratuïta i temporal. Normalment, té funcionalitat restringida.

El programa espia es pot instal·lar en el sistema de moltes maneres diferents. Per exemple, cavalls de Troia, pàgines web que visitem i contenen determinats controls ActiveX o codis que exploten una vulnerabilitat determinada, aplicacions amb llicència de programari gratuït (*freeware*) o programari de prova (*shareware*) que descarreguem d'Internet, etc.

Atès que, normalment, el programa espia utilitza la connexió del PC a Internet per transmetre informació, consumeix amplada de banda i, per tant, afecta la velocitat de transferència de les dades.

Entre la informació que recull aquest programari, hi podem trobar missatges, contactes, adreces IP, DNS, adreces web visitades, descàrregues realitzades, números de la targeta de crèdit, contrasenyes, etc.

A banda d'aquesta enumeració de programari maliciós, cal esmentar els *hackers* i alguns dels mètodes que utilitzen de manera maliciosa, com l'enginyeria social i, dins aquest camp, la suplantació o la pesca (*phishing*).

El món dels *hackers* o pirates informàtics és molt ampli i comprèn molts tipus d'accions diferents, des d'entrar en un sistema pel simple fet de descobrir quins en són els punts febles, sense fer-hi cap acció maliciosa, fins a entrar en sistemes i apoderar-se'n per control remot o inutilitzar-los. En altres casos, es poden limitar a aconseguir contrasenyes, números de targetes de crèdit, etc.

Cal saber que els *hackers* solen ser persones amb molts coneixements de programació, xarxes i sistemes operatius. Actuen amb intencionalitats molt diverses.

Hi ha un camp, que s'anomena *enginyeria social*, que pretén aconseguir contrasenyes, números secrets o números de targeta, entre altres, per utilitzar-los amb finalitats malicioses o, directament, delictives. Per aconseguir la contrasenya d'un usuari de correu electrònic, es pot entrar en la màquina que l'usuari fa servir per connectar-se. També es pot intentar aconseguir per mitjà d'una trucada telefònica o fent-se passar per l'administrador del correu. En aquest últim cas, el *hacker* escriu un correu electrònic a la víctima i li demana la contrasenya per problemes tècnics, per exemple. Aquesta manera d'actuar, gairebé sempre sobre l'usuari, és la que es coneix com a **enginyeria social**.

Dins l'enginyeria social, hi ha una situació que es coneix amb el nom de *pesca* o *suplantació*. Són els casos en què l'estafador es fa passar per una entitat bancària

Alguns exemples de programes espia són el Gator i el Bonzo Buddy.

(la imitació de la pàgina web de l'empresa és perfecta) i demana la contrasenya de la targeta bancària. També es pot fer passar per l'administrador del correu electrònic i enviar un correu molt ben elaborat en què sol·licita la contrasenya per problemes tècnics. Evidentment, això és un delictes penat per la llei.

3.1.1 Característiques comunes als diferents tipus de virus

Tot i que hi ha molts tipus diferents de programari maliciós o maligne, podríem dir que aquest programari té tres principis bàsics. Són els següents:

1. **És nociu:** un programari maliciós sempre causa danys en el sistema que infecta. Cal aclarir, però, que el fet de fer mal no implica espatllar res del sistema. El dany pot ser implícit quan es busca destruir o alterar informació. També poden ser situacions amb efectes nocius per al sistema, com el consum de memòria principal, el temps de processador, etc.
2. **És autoreproductor:** la característica més important d'aquest tipus de programari és la capacitat que té de crear còpies d'ell mateix, cosa que no fa cap altre programa convencional.
3. **És subreptici:** això significa que utilitzarà diverses tècniques per evitar que l'usuari s'adoni que hi és. La primera mesura és tenir una mida força reduïda per poder dissimular, a primer cop d'ull, que hi és. Pot arribar a manipular el resultat d'una petició del sistema operatiu de mostrar la mida d'arxiu i, fins i tot, dels atributs que conté.

3.1.2 Grau de perillositat del programa maliciós

La perillositat del programari maliciós és el risc que corre el vostre sistema de ser infectat (per virus, cavalls de Troia, cucs, etc.). Lògicament, la perillositat del programa maliciós pot variar, pot ser baixa en un moment i molt alta en un altre, depenent de com s'estigui. Podreu diferenciar diversos tipus de perillositat:

- **Perillositat baixa:** amenaça petita, està poc estès.
- **Perillositat mitjana:** el virus està relativament estès i la infecció causa perjudicis o està poc estès, però la infecció pot causar danys importants.
- **Perillositat alta:** amenaça important, ja que el programa maliciós està molt estès i la infecció pot causar danys o grans perjudicis.
- **Perillositat molt alta:** amenaça molt important, ja que està molt estès i la infecció ha causat danys irreversibles.

3.1.3 Grau de propagació del programa maliciós

El grau de propagació que pot assolir un programa maliciós indica com d'estès està el virus. Com més estès, més probabilitats teniu de trobar-vos-el. La propagació d'un virus és determinada per la **ràtio d'infecció**, és a dir, el percentatge d'ordinadors infectats en relació amb el total d'equips explorats. En cas que es tracti d'un únic sistema, és el percentatge d'elements infectats en relació amb el total d'elements del vostre equip. Els valors que pot adoptar el grau de propagació d'un virus són els següents:

- **Epidèmia:** el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és del 10% o superior.
- **Propagació alta:** el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és superior al 7,5% i inferior al 10%.
- **Propagació mitjana:** el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és superior a l'1% i inferior al 7,5%.
- **Propagació baixa:** el percentatge d'ordinadors/elements examinats i infectats amb el *programa maliciós* és inferior a l'1%.

3.1.4 Danys causats per un programa maliciós

Els danys que provoca un programa maliciós són un indicatiu del perjudici que un virus causa en infectar un sistema informàtic. Aquests perjudicis poden ser més o menys severs: aparició de missatges a la pantalla, pèrdua o alteració d'informació, sistemes col·lapsats, impossibilitat de funcionament, etc. Els valors que el nivell de danys d'un virus pot adoptar són els següents:

- **Molt alt:** ocasiona perjudicis greus. Per exemple, destrucció o modificació d'arxius, formatació de discos durs, enviament de la informació a tercers, generació de gran trànsit en servidors, degradació del rendiment dels sistemes, obertura de la seguretat, etc.
- **Alt:** qualsevol programa maliciós, encara que sembli inofensiu, ocasiona algun perjudici a l'usuari. S'hi inclouen els que no fan accions destructives.

En la figura 3.1 hi ha un gràfic representatiu que us permet veure la relació que hi ha entre danys, propagació i perillositat.

FIGURA 3.1. Relació entre danys, propagació i perillositat dels virus

| | | | | | |
|-------|-----------|------------|---------|-----------|-----------|
| Danys | Molt alta | Mitjana | Alta | Molt alta | |
| | | Baixa | Mitjana | Alta | Molt alta |
| | Alt | Baixa | Mitjana | Alta | Epidèmia |
| | | Propagació | | | |

3.1.5 Mitjans i mètodes que utilitza el programari maliciós per atacar

A banda de saber quins són els diferents tipus de programari maliciós, quin n'és el grau de propagació i quins són els danys que pot ocasionar, també us cal saber quins són els mètodes i els mitjans que acostuma a utilitzar per arribar a un sistema.

Els mitjans que utilitza el programari maliciós per introduir-se en el vostre ordinador solen ser els següents:

- **Unitats de disc portàtils (CD, USB, etc.):** mitjans d'emmagatzematge en què es guarda informació mitjançant fitxers, documents o arxius. Amb aquest material es pot treballar en un ordinador per, posteriorment, utilitzar-lo en un altre ordinador. Si les unitats de disc estan infectades i entren en contacte amb el vostre ordinador, s'infectarà.
- **Xarxes d'ordinadors:** una xarxa és un conjunt o sistema d'ordinadors connectats entre si físicament per facilitar la feina de diferents usuaris. És a dir, hi ha connexions per transferir informació entre ells. Si hi hagués alguna informació infectada que es transferís d'un ordinador a un altre, aquest segon ordinador s'infectaria immediatament.
- **Internet:** Internet cada dia s'utilitza més per obtenir informació, enviar i rebre fitxers, rebre i publicar notícies o descarregar fitxers. Totes aquestes operacions es basen en la transferència d'informació i en la connexió de diferents ordinadors en qualsevol part del món. Per tant, qualsevol programa maliciós pot introduir-se en el vostre ordinador amb la informació que rebeu. Per mitjà d'Internet, la infecció es podria fer pels camins següents:
 - **Correu electrònic:** en un missatge es poden incloure documents o fitxers, és a dir, el que coneixem com a *fitxer adjunt*. Aquests fitxers acompanyen el missatge de text, de manera que poden estar infectats. Generalment, el destinatari no sospita que l'arxiu que ha rebut pot contenir algun tipus de programari maliciós. Tanmateix, quan després d'obrir el missatge, s'obre el fitxer, la sorpresa pot ser desagradable.
 - **Pàgines web:** les pàgines que visitem a Internet són fitxers de text o imatges escrites en un llenguatge denominat *HTML*. No obstant això,

també poden contenir **Controls ActiveX** i **Applets de Java**, que són programes. Cal anar amb compte, perquè aquests programes sí que poden estar infectats i, consegüentment, podrien infectar l'usuari que visiti la pàgina.

- **Descàrrega de fitxers (FTP):** la sigla *FTP* significa *file transfer protocol*, és a dir, protocol de transferència de fitxers. Mitjançant aquest protocol es poden col·locar documents en ordinadors que es trobin en qualsevol part del món o copiar fitxers d'aquests ordinadors al vostre (baixar o *download*). Aquests fitxers poden contenir programari maliciós que pot infectar el vostre ordinador.
- **Grups de missatges:** mitjançant els anomenats *missatges* (*news*) és possible debatre temes determinats amb qualsevol persona del món i rebre correus electrònics amb notícies noves. Aquests missatges amb notícies poden tenir documentació adjunta infectada. Aquesta documentació permet que el programari maliciós s'introdueixi en el vostre programa i s'executi en arrencar l'ordinador.

Els mètodes que un virus té per entrar en un sistema solen ser els següents:

- Iniciar-se juntament amb un programa que l'usuari sí que instal·la voluntàriament.
- Incrustar-se en un programa **sa**, no infectat, per activar-se quan l'usuari engegui aquest programa.
- Aprofitar el sector d'arrencada d'un disquet, un llapis de memòria o un disc dur extraïble. S'executa quan l'usuari engega l'ordinador amb aquest dispositiu posat.

3.1.6 Situacions en què el vostre sistema corre el risc d'infectar-se

Es poden enumerar unes quantes situacions en què el vostre sistema corre el risc de contagiar-se d'algun virus. Són les següents:

- Quan instal·leu programes de pagament sense utilitzar els discos originals del fabricant o quan són disquets gravables que han estat desprotegits en algun moment i algun virus s'hi ha pogut gravar.
- Quan engegueu programes que provenen d'un altre equip, sense tenir la certesa absoluta que tot l'equip d'origen està ben net de virus.
- Quan engegueu programes que descarregueu d'Internet o us envien per correu electrònic, sense tenir la certesa absoluta que la font dels programes és fiable i està neta de virus.
- Quan engegueu l'ordinador amb un disquet, un llapis de memòria o un disc extraïble posat i aquest dispositiu no està gravat i protegit de fàbrica.

- Quan, amb un navegador, obriu pàgines d'Internet que tenen components **ActiveX** programats i no podeu controlar la fiabilitat d'aquests components. Alguns navegadors en la configuració us donen l'opció d'habilitar o no aquests i altres programes en la vostra navegació. És un risc tenir-los sempre activats sense que el mateix navegador, quan una pàgina disposa d'aquests programes, us avisi perquè pugueu escollir si accepteu executar-los o no.

En canvi, també es poden enumerar situacions en què el vostre sistema no corre cap risc nou. Són les següents:

- Quan instal·leu o utilitzeu discos comprats juntament amb revistes, comprats en una botiga o de regal, sempre i que l'empresa o entitat que produeix aquest programari s'hi identifiqui.
- Quan engegueu programes del sistema mateix.
- Quan engegueu l'ordinador amb un disquet, un llapis de memòria o un disc extraïble posat i heu formatat aquest dispositiu amb el mateix sistema que formateu l'ordinador.
- Quan descarregueu programes d'Internet que provenen de les pàgines oficials de l'empresa o entitat productora, que estigui perfectament identificada legalment.

Formatar

La formatació és un procés lògic que consisteix a implantar un sistema d'arxius que assigna sectors a arxius. Per tenir diferents sistemes d'arxius en un disc dur, primer cal fer-hi particions.

3.1.7 Mètodes per evitar el programari maliciós

Hi ha algunes actuacions, o mètodes, que podeu portar a terme per tal d'evitar el programari maliciós com poden ser:

- La instal·lació del sistema operatiu i dels programes posteriors ha de partir d'un **sistema net** (discos durs en blanc, CMOS de fàbrica). Es pot fer en comprar un equip nou.
- Per instal·lar el sistema operatiu, **només s'han d'utilitzar discos originals del fabricant**. No poden haver estat mai desprotegits contra gravació. Una altra opció és que es tracti d'una còpia **de disc a disc** dels discos originals. Ha d'haver estat feta en un entorn completament net.
- No s'ha de deixar mai cap disquet, llapis de memòria o disc extraïble connectat quan s'apaga o s'engega l'equip, excepte que s'hi vulgui iniciar el sistema (des del dispositiu net).
- No s'haurien de descarregar mai, sense conèixer-ne realment la procedència, arxius executables (amb extensions *.exe*, *.com*, *.dll*, *.bat*, *.pif*, *.cmd*, *.vbs* i altres) d'Internet. Tampoc s'haurien d'obrir quan són arxius adjunts d'un missatge de correu electrònic.

- No s'han d'obrir mai arxius executables (amb extensions *.exe*, *.com*, *.dll*, *.bat*, *.pif*, *.cmd*, *.vbs* i altres) d'un dispositiu que hagi gravat algú amb un altre equip, sense que tingui la garantia d'una empresa o entitat productora de programari.
- Mai no s'ha de donar accés, des de l'exterior, al disc dur o als dispositius propis quan s'està connectat a Internet o a alguna xarxa amb equips que no són propis. Un sistema eficaç és connectar-se a Internet amb un encaminador (*router*) que disposi de tallafoc.
- No s'ha de deixar que altres persones (per exemple nens) utilitzin programes externs sense assegurar-ne la fiabilitat.
- El sistema informàtic sempre l'ha d'utilitzar una única persona i sempre ha d'estar clar a qui cal consultar abans de resoldre qualsevol situació. És essencial preguntar a l'administrador del sistema sempre que hi hagi un dubte.

Que estiguen connectats a Internet i navegueu per pàgines web no significa que us hagueu d'infectar, si no és que algun *hacker* o pirata s'entesta a infectar-vos. No obstant això, cal que seguiu una sèrie de consells per impedir la infecció. Són els següents:

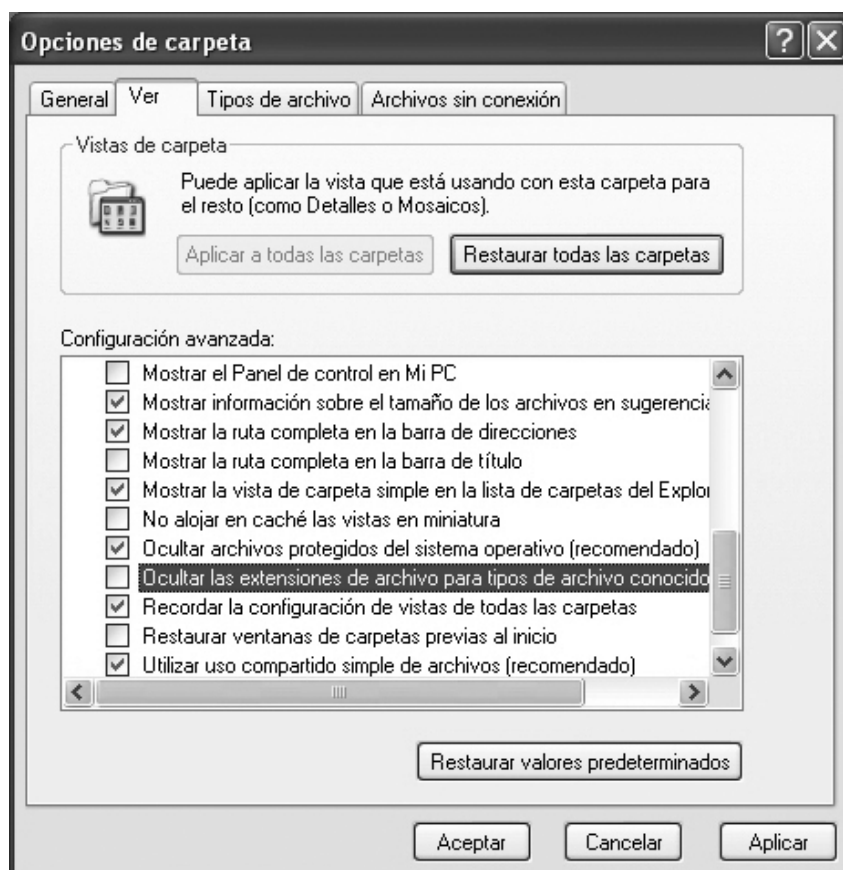
1. El primer consell és **crear còpies de seguretat regularment** en elements externs, com CD, altres dispositius o altres ordinadors.
2. El segon consell és **instal·lar un programa antivirus**, ja que molt freqüentment utilitzem fitxers que tenim guardats en llapis de memòria, obrim un fitxer adjunt en el nostre correu electrònic, etc. Per poder utilitzar aquesta informació amb més seguretat, hem de disposar d'un antivirus que sigui capaç d'analitzar els fitxers i buscar-hi virus. Els antivirus seran millors si faciliten aquesta anàlisi i, consegüentment, s'integren en les eines del correu, el processador de textos i el sistema operatiu.
3. El tercer consell consisteix a **actualitzar freqüentment** el sistema antivirus un cop instal·lat. Aquest procés pot ser cansat si el fem manualment i, fins i tot, us en podeu oblidar. Per tant, és aconsellable que activeu l'opció de fer les actualitzacions de manera automàtica.

Per evitar tipus de virus determinats, heu de seguir tàctiques concretes. Últimament, han aparegut desenes d'i-worms nous que tenen el potencial d'infectar molt ràpidament per mitjà de correu electrònic. Alguns d'aquests virus populars tenen noms que també són molt populars i suggerents com, per exemple, *Nadal*, *Hybris*, *Music*, *BeBla*, etc. N'hi ha molts que tenen el potencial d'infectar molt ràpidament. En alguns casos poden infectar en regions específiques (localment) i en altres, a escala global, cosa més perillosa. Generalment, arriben per correu electrònic.

Tenir un antivirus instal·lat i actualitzat és la millor manera de protegir-se dels *i-worms* i altres tipus de virus. De totes maneres, també hi ha altres mesures que els usuaris han de prendre per evitar problemes i mantenir els sistemes nets. Són les següents:

- Un virus del tipus cuc acostuma a utilitzar l'Outlook Express o el Microsoft Outlook per difondre's. Microsoft ofereix de manera gratuïta els últims pedaços de seguretat a Internet. Aquests pedaços no substitueixen un programa antivirus, però posen barreres per evitar el contagi d'una gran majoria de virus.
- És convenient **evitar els fitxers adjunts del correu**, sobretot quan són fitxers estranys o desconeguts. Moltes vegades aquests fitxers els enviarà un amic nostre, però el missatge estarà en anglès o serà estrany.
- Cal que configurem el Windows perquè ens mostri les extensions dels fitxers. D'aquesta manera, sabrem si es tracta d'un fitxer *.doc* del Word, d'un fitxer de text *.txt* o d'un programa *.exe* o *.com*. Les extensions *.vbx*, *.pif* o *.shs* són les que tenen més probabilitats de ser un virus. Per configurar el Windows d'aquesta manera, ho fareu per mitjà de les *Herramientas\Opciones de carpeta\Ver*. Desmarcareu l'opció *Ocultar las extensiones per a tipos de archivos desconocidos*, tal com es mostra en la figura 3.2. També veureu clarament que es tracta d'un virus quan trobeu fitxers amb dobles extensions com, per exemple, *.txt.exe*.

FIGURA 3.2. Configuració extensions per a un entorn Windows



- És millor esborrar els correus publicitaris directament, especialment si inclouen dades adjuntes.
- Els correus amb arxius de caràcter sexual tenen moltes probabilitats d'estar infectats. Fitxers com *sex.exe* són una bomba potencial.
- Els fitxers adjunts en xats, fòrums o grups de missatges també són poc recomanables, si no és que coneixem la persona que ens els envia.
- Finalment, és recomanable fer servir sistemes de correu web com el Hotmail, el Gmail o el Yahoo! Mail, ja que solen passar programes antivirus a tots els fitxers adjunts i, evidentment, controlen l'actualització amb les últimes versions.

Els **virus de tipus macro** s'acostumen a transmetre dins de documents Word, però també en qualsevol altre format de document que admeti macros avançades (l'Excel, el Corel Draw, etc.). En el moment en què s'obre el document, la macro es copia en la plantilla genèrica de Word (*Normal.dot*) i es replica en cada document que s'obre. L'estratègia que s'ha de seguir per evitar el contagi d'aquest tipus de virus és la següent:

- El problema principal a l'hora de comprovar si hi ha un virus dins un document i eliminar-lo és que per fer-ho fa falta ser dins el Word, fins i tot per saber simplement si hi ha cap macro en el document. A partir d'aquest moment, qualsevol cosa que aparegui, o no aparegui, a la pantalla és potencialment falsa i no fiable, perquè és possible que el virus ja hagi actuat i estigui modificant tot el que es veu. No obstant això, si no disposem d'un programa antivirus, és recomanable obrir el submenú *Macro*, en el menú principal d'*Eines*, i si a la pantalla apareix algun nom estrany, el millor és esborrar-lo directament.
- Si sospiteu que hi ha un virus, una altra cosa que podeu fer és esborrar la plantilla *Normal.dot*. El Word continuarà funcionant correctament.
- Com a norma habitual, el més convenient és no permetre que s'executin macros en arxius que no coneixem. En aquest sentit, el Word i l'Excel sempre us adverteixen, amb una finestra, que el fitxer incorpora macros i us demanen el vistiplau per obrir-les.

3.2 Instal·lació, prova, utilització i automatització d'eines per a la protecció i desinfecció de programari maliciós

L'existència de virus o programari maliciós, amb les conseqüències que pot tenir en el vostre sistema, requereix que hi feu atenció. Si disposeu d'un sistema informàtic, probablement correrà el risc de patir infeccions per part d'aquest programari. D'aquesta manera, heu de prendre mesures per pal·liar-ne els efectes possibles.

Podeu establir tota una sèrie de mesures per evitar i pal·liar els efectes del programari maliciós, però cap d'aquestes mesures no invalida o fa innecessària la presència d'un programa antivirus en el vostre sistema informàtic.

La instal·lació, la configuració posterior i l'establiment d'actualitzacions són passos fonamentals per establir mesures de seguretat importants davant l'amenaça, cada vegada més present, de programari maliciós.

En aquest sentit, cal distingir dos tipus de programari antivirus, el programari de propietat i el programari lliure. El primers els creen les empreses, que determinen les condicions sota les quals es pot utilitzar. El paquet corresponent, que s'ha de comprar, ofereix suport per a aquest programari i actualitzacions de la base de virus, almenys durant un període de temps determinat.

Els antivirus de programari lliure són totalment gratuïts i només solen requerir que us registreu amb les vostres dades per facilitar-vos l'accés a les actualitzacions de la base de virus.

Seguidament, s'ofereix un exemple d'una instal·lació i una configuració d'un antivirus de programari lliure. Qualsevol altra instal·lació d'un altre antivirus de programari lliure s'hi assemblarà molt. Per a aquest exemple, s'ha escollit un antivirus en concret, però podria ser qualsevol altre i el procés seria molt similar a aquest. Si coneixeu el procés per baixar, instal·lar i configurar l'antivirus d'aquest exemple, sabreu fer-ho en el cas d'un altre antivirus diferent.

En la figura 3.3, teniu una captura de pantalla d'un exemple d'una possible descàrrega d'un antivirus de programari lliure.

FIGURA 3.3. Descàrrega d'un antivirus de programari lliure

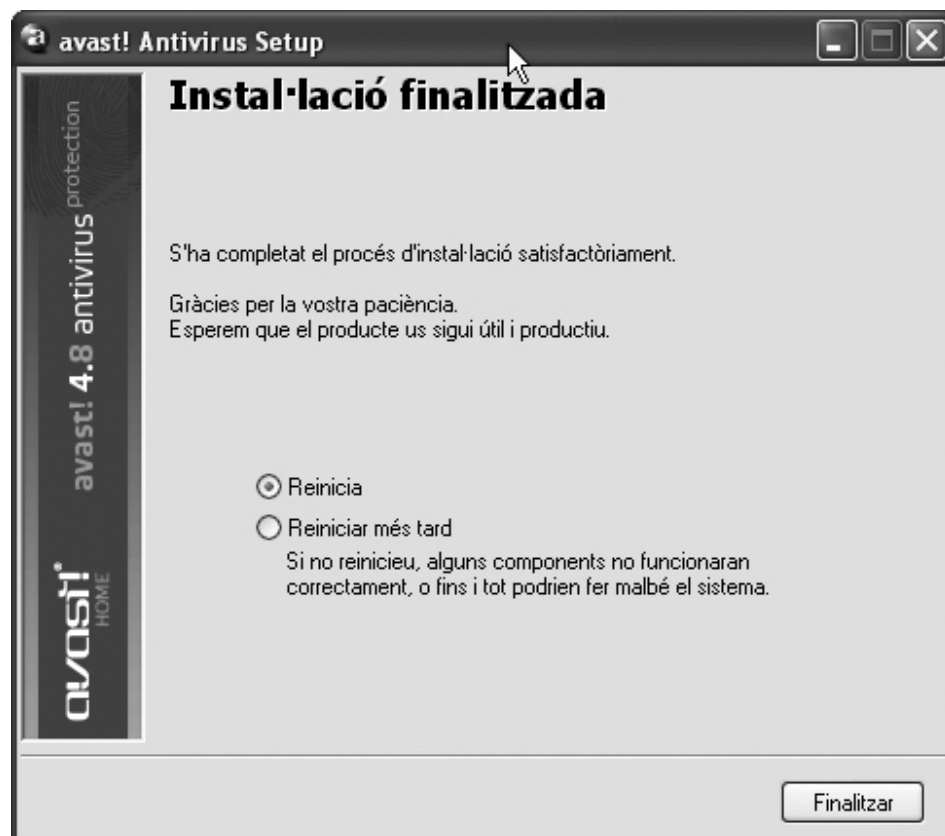


Repositori

:offset:10 Un repositori informàtic és un espai en què normalment accediu per Internet. S'hi emmagatzemen i mantenen paquets de programari. Són fonts de programari.

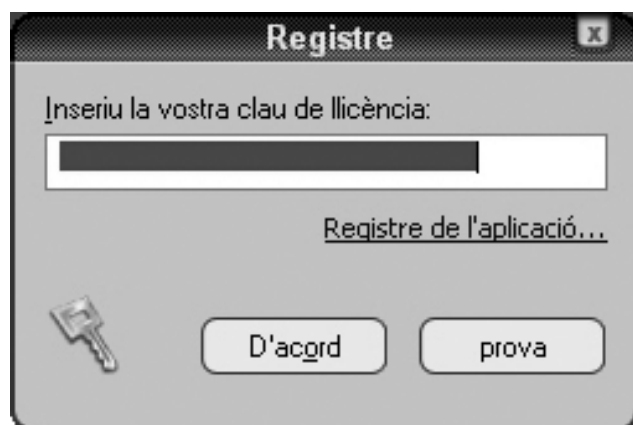
Quan ja disposeu d'un programa antivirus, sia comprat en una botiga, en línia o descarregat d'una pàgina repositori de programari lliure, cal que l'instal·leu en el sistema. Aquest procés normalment requereix poca atenció i acostuma a ser un "següent". És sistemàtic si no és que voleu canviar el directori d'instal·lació o escolliu l'opció personalitzada per instal·lar només una part de les utilitats del programari. Una vegada acabada la instal·lació, us demanarà si voleu fer un escaneig quan reinicieu el sistema. Podeu escollir que no. Seguidament, us demanarà que reinicieu el sistema, tal com podeu veure en la figura 3.4. Feu-ho.

FIGURA 3.4. Final del procés d'instal·lació



Quan la instal·lació finalitzi i obriu el programa, us sol·licitarà la clau de llicència, que podeu aconseguir si us hi registreu. Per registrar-vos-hi, només cal que entreu a Internet per mitjà de l'enllaç que apareix en la pantalla del registre i aleshores haureu d'emplenar un petit formulari amb les vostres dades. En finalitzar aquest procés obtindreu la llicència corresponent i ja la podreu introduir en la finestra del programa que us l'ha sol·licitat. Ho podeu veure en la figura 3.5.

FIGURA 3.5. Inserir la llicència



Una vegada realitzada la instal·lació i el registre corresponent, convindrà que proveu si el vostre programa antivirus funciona correctament. Tal com podeu veure en la figura 3.6, l'antivirus, en obrir-se, ja fa un escaneig de la memòria. Durant aquest procés, ja pot trobar algun virus.

FIGURA 3.6. Virus trobat



Intenteu fer un escaneig en alguna part del sistema. És preferible que no sigui en tot el disc dur, ja que només es tracta de fer una prova. L'escaneig total del sistema ja el fareu quan hagueu actualitzat el vostre sistema antivirus.

Si el programa funciona correctament, cal que l'actualitzeu. Concretament, és recomanable que actualitzeu la base de signatures de virus, que us permetrà disposar d'un registre dels virus més actuals. Podeu veure aquesta actualització en la figura 3.7.

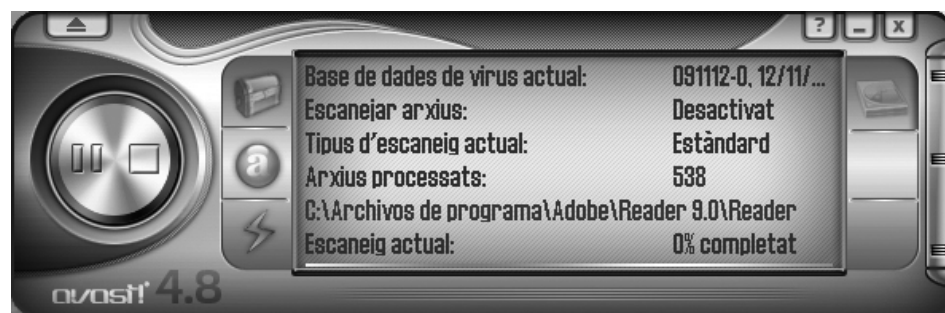
FIGURA 3.7. Actualització de la base de signatures de virus



Alguns programes antivirus disposen de diverses eines, com els escanejors en diferents parts del sistema, el control de l'execució de programes, l'obertura d'arxius, la comprovació dels fitxers adjunts en el correu, etc. D'altres, inclouen una eina específica per controlar l'ús d'Internet. Si és així, primer cal configurar el sistema antivirus per efectuar correctament el control de la connexió i el trànsit d'Internet. Després ja podreu connectar-vos i fer l'actualització.

Una vegada actualitzat el programa antivirus amb les noves signatures de virus, cal que feu un escaneig complet de tot el vostre sistema per buscar-n'hi, sobretot els que són més actuals. Ho podeu veure en la figura 3.8.

FIGURA 3.8. Fent escaneig del sistema

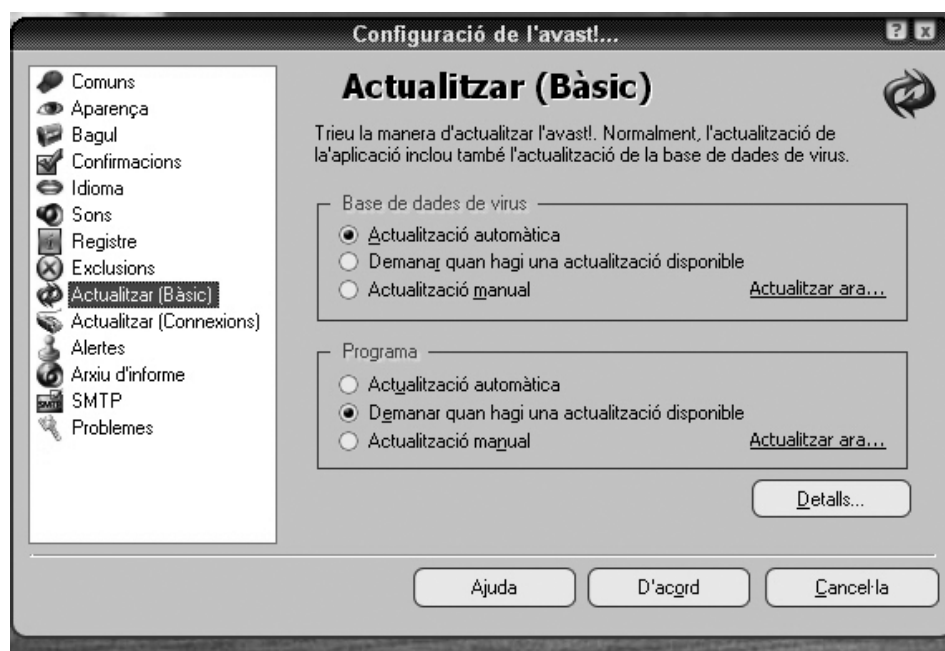


També és aconsellable fer un rastreig de tots els dispositius extraïbles de què disposeu per eliminar-ne els virus. Aquesta part del procés, la de rastrejar tot el vostre sistema, pot trigar força depenent de la quantitat de memòria de què disposeu, la quantitat de dades guardades i les aplicacions instal·lades. Per tant, possiblement us permetrà deixar que el programa escanegi una bona estona.

Quan hagueu instal·lat el programa antivirus, l'hagueu actualitzat i hagueu fet un rastreig de tot el sistema, caldrà que el configureu correctament. Haureu de decidir cada quant de temps ha de fer aquests escanejos complets del sistema, tant si els estableix automàticament com manualment. En aquest últim cas, cal que ho tingueu present i no deixeu passar gaire temps entre un escaneig i l'altre.

Una altra cosa important que cal configurar és l'actualització de la base de dades de signatures de virus nous. És aconsellable que ho faci diàriament i de manera automatitzada. Així, descarteu la possibilitat d'oblidar-vos d'actualitzar-lo manualment i, consegüentment, deixar més temps el vostre sistema desprotegit dels virus més nous que van apareixent gairebé diàriament. Podeu veure part de la configuració en la figura 3.9.

FIGURA 3.9. Configuració de l'antivirus



En la configuració també podeu indicar al programa què ha de fer quan trobi un virus i on l'ha de guardar, en cas que el guardi. Igualment, li podeu ordenar que l'elimini sempre que pugui o que us avisi o no quan en trobi un. La configuració també us ofereix la possibilitat d'automatitzar les tasques. De totes maneres, si no ho acabeu de veure clar, podeu deixar les opcions de configuració tal com s'han instal·lat. El programa funcionarà correctament.

Això a part, també hi sol haver la possibilitat d'actualitzar el mateix programa antivirus (no la base de dades dels virus que van apareixent). És aconsellable que el mantingueu actualitzat, ja que així tindreu les utilitats noves de què disposi.

Una vegada fet tot aquest procés, ja teniu instal·lat, actualitzat i configurat el vostre antivirus. Tanmateix, cal tenir en compte que aquesta eina, que és molt important per mantenir el sistema protegit, no invalida l'ús d'altres mesures protectores. D'aquesta manera, també podeu instal·lar tallafocs, actualitzar periòdicament els pedaços del sistema operatiu o fer altres actualitzacions, sobretot les que estan relacionades amb la seguretat.

Encara que tenir un programa antivirus instal·lat i configurat correctament és una mesura molt important per protegir el sistema i les dades que hi ha guardades, cal tenir present que la seguretat total i absoluta no existeix. Per tant, és aconsellable combinar l'antivirus amb altres mesures de seguretat.

Finalment, cal destacar el fet que la majoria dels programes antivirus, de pagament o de programari lliure, estan destinats a sistemes operatius privatis, és a dir, a l'entorn Windows. D'aquesta manera, n'hi ha molt pocs per als sistemes operatius de programari lliure. La raó és que aquests sistemes són molt menys vulnerables als virus i, a més, no en tenen tants. Per això és important que, a l'hora d'instal·lar un sistema o un altre, us plantegeu quina en serà la utilitat i fins a quin punt la seguretat hi serà important. Es tracta d'un factor de pes que s'ha de tenir en compte perquè pot ser determinant.