Introducció

Panda Antivirus

Panda Antivirus és una solució completa i eficaç per mantenir protegit el seu ordinador enfront de qualsevol tipus de virus. S'inclouen versions Windows 95, Windows NT Workstation, Windows 3.1x, DOS i OS/2 per que estigueu protegits sigui quin sigui el sistema operatiu. Aquesta ajuda és la corresponent a **Panda Antivirus** per a Windows NT Workstation.

Estratègies de protecció

Panda Antivirus compren diverses estratègies de protecció enfront dels virus:

- **Protecció permanent:** la protecció permanent s'encarrega de protegir l'ordinador enfront dels virus en tot moment i sense necessitat d'intervenció de l'usuari. El gran avantatge d'aquesta estratègia de protecció és que permet tenir protegit l'ordinador d'una forma completament automàtica.
- **Anàlisi sota demanda:** l'anàlisi sota demanda permet analitzar qualsevol part de l'ordinador a petició de l'usuari. Heu d'escollir l'àrea a analitzar i en aquest moment començarà l'anàlisi a la recerca de virus dins de l'àrea senyalada.
- **Desinfecció:** una cop trobat el virus, es poden dur a terme algunes accions. Una d'elles és la desinfecció que consisteix a eliminar el virus de l'arxiu tot deixant aquest tal i com estava abans de la infecció.
- **Anàlisi heurística:** l'anàlisi heurística és una tècnica d'anàlisi alternativa a les que ja s'han esmentat. L'anàlisi heurística funciona sota demanda. És a dir, l'usuari ha d'indicar quina àrea de l'ordinador desitja analitzar amb aquest mètode en un moment determinat. Aquesta tècnica d'anàlisi està preparada per trobar virus desconeguts.
- **Recerca de cadenes:** a l'igual que l'anàlisi heurística, és una tècnica d'anàlisi alternativa i també funciona sota demanda de l'usuari. La seva utilitat és la recerca de nous virus a partir de dades ofertes pel suport tècnic de Panda Software.
- **Altres opcions:** sota aquest apartat s'engloben certes capacitats de l'antivirus adreçades a oferir informació o a facilitar la seva gestió. Per exemple, es compta amb un informe de resultats en què podeu veure les diferents incidències i operacions que s'han dut a terme amb l'antivirus.

Solucions antivirus Panda Software

Panda Software us ofereix les següents solucions antivirus:

- **24h-365d® Assegurança Antivirus® per a PCs Individuals**. *Llicències.*
- **24h-365d® Assegurança Antivirus® per a PCs en xarxa** (distribució automàtica des de servidors).
- **24h-365d® Assegurança Antivirus® per a Servidors de xarxa** (Novell NetWare i Windows NT Server).
- **24h-365d® Assegurança Antivirus® per a Xarxes Locals**.
- **24h-365d® Assegurança Antivirus® per a clients d'e-mail i Groupware**.
- **24h-365d® Assegurança Antivirus® per a Servidors d'e-mail i Groupware**.
- **24h-365d® Assegurança Antivirus® per a Servidors de Correu SMTP**.
- **24h-365d® Assegurança Antivirus® per a PCs connectats a Internet**.

- **24h-365d® Assegurança Antivirus® per a Servidors d'Internet (SMTP, FTP i HTTP)**.
- **24h-365d® Assegurança Antivirus® per a Proxys**.

Què és 24h-365d Assegurança Antivirus Panda Software?

24h-365d® Assegurança Antivirus® Panda Software, és un nou i revolucionari concepte de protecció antivirus que aporta encara més seguretat. **24h-365d® Assegurança Antivirus® Panda Software** és una extraordinària combinació de productes i serveis que ofereix els més alts nivells de protecció enfront dels virus. **24h-365d® Assegurança Antivirus® Panda Software** es pot contractar amb diferents temps de dret a actualitzacions i amb diferents períodes d'actualització.

El producte l'aporta **Panda Antivirus**, un antivirus que ha aconseguit els certificats més exigents en detecció de virus com ara:

- El **Certificat ICSA:** atorgat per la prestigiosa organització nord-americana ICSA als productes antivirus que detecten periòdicament el 100% de los virus *In the Wild* (els virus més estesos a cada moment) i més d'un 90% de la *Zoo Collection* (col·lecció de milers de virus menys estesos).
- El **Certificat CheckMark:** atorgat per la revista anglesa especialitzada en Seguretat Informàtica *Secure Computing*.

Si no disposeu de **24h-365d® Assegurança Antivirus® Panda Software**, la podeu trobar utilitzant l'ordre de comanda inclosa a la targeta de registre. Els serveis oferts per **24h-365d® Assegurança Antivirus® Panda Software** són els següents:

- **Hot-Line:** durant UN any solucionarem els vostres problemes tècnics per telèfon, fax, Internet o e-mail. Truqueu quan truqueu, a qualsevol hora del dia o de la nit, trobareu tècnics a l'altre costat, persones altament qualificades que són a la vostra disposició 24 hores al dia, els 365 dies de l'any. Aquest és un servei exclusiu de **Panda Software**.
- **S.O.S. Virus:** si trobeu algun virus que **Panda Antivirus** no detecta o no elimina, enviarem un missatger al vostre domicili (o recollirem la mostra sospitosa de qualsevol altre manera) i en menys de 24 hores desenvoluparem una nova versió capaç de detectar i eliminar el nou virus. Us enviarem aquesta nova versió sense cap cost.
- **Servei d'Actualitzacions amb lliurament a domicili:** el vostre antivirus estarà totalment actualitzat. Rebreu al vostre domicili actualitzacions mensuals o trimestrals en CD o en disquets si heu contractat la nostra solució **24h-365d® Assegurança Antivirus® Panda Software**. També podreu actualitzar el producte a través de la nostra WEB tantes vegades com desitgeu durant un any, tot garantint-vos com a mínim una nova actualització cada dia.
- **Servei WEB:** resolució dels dubtes més freqüents i informació sobre virus.

Instal·lació

Requisits

Per instal·lar **Panda Antivirus** per a Windows NT Workstation calen els següents elements:

- Ordinador compatible amb IBM amb processador 486 o superior.
- 16 Mb de RAM.
- 4 Mb d'espai en disc dur.
- Sistema operatiu Windows NT 3.51 o superior.
- Unitat de CD-Rom.
- Ratolí.

Procediment d'instal·lació

Hi ha dues versions de **Panda Antivirus** per a Windows NT Workstation. Una d'elles correspon a la versió 3.51 del sistema operatiu esmentat i l'altra a la versió 4.0. Cal tenir la precaució d'instal·lar la versió corresponent a cada sistema operatiu.

Ambdues versions es poden instal·lar únicament des del CD-Rom que acompanya el producte. Per instal·lar qualsevol de les dues versions, cal executar el programa CDMENU.COM. Aquest programa presenta un menú d'opcions senzill. En primer lloc, cal escollir l'idioma desitjat i tot seguit la versió que voleu instal·lar. En aquest cas cal escollir una de les dues versions de **Panda Antivirus** per a Windows NT, la 3.51 o la 4.0 en funció del sistema operatiu que tingueu instal·lat.

Per poder instal·lar la versió de **Panda Antivirus** per a Windows NT Workstation cal que tingueu els drets d'administrador sobre la vostra màquina. Això és així atesos els drets necessaris per instal·lar el driver que s'encarrega de la protecció permanent.

El procediment d'instal·lació consta dels següents passos:

1. En primer lloc es presenta una pantalla de benvinguda.
2. Seguidament es demanen les dades de l'usuari.
3. Es demana el directori on desitgeu instal·lar l'aplicació.
4. Se sol·licita el grup de programes en què es crearan les icones d'accés a l'antivirus.
5. Es dóna a escollir si voleu instal·lar la protecció permanent (driver **Sentinel**) o no.
6. Comença la còpia d'arxius al disc dur.
7. Un cop acabada la còpia d'arxius, es recomana reiniciar la màquina per que la protecció permanent entri en funcionament.

Actualització de l'antivirus

Per actualitzar una versió amb una actualització rebuda, només cal instal·lar la nova versió sobre l'antiga.

Desinstal·lació

Si es tracta de la versió per a Windows NT 3.51, la desinstal·lació de **Panda Antivirus** es realitza mitjançant el programa UNINST que es troba en el grup de programes de l'aplicació.

Si es tracta de la versió para Windows NT 4.0, la desinstal·lació de **Panda Antivirus** es realitza mitjançant l'opció *Afegir o treure programes* del *Pannell de Control*. Només cal escollir **Panda Antivirus Windows NT W/S 4.0** de la llista que es presenta en aquesta opció i prémer el botó *Afegir o Treure*. Per completar la desinstal·lació, cal reiniciar la màquina.

No heu d'intentar desinstal·lar la versió esborrant la carpeta on hagueu instal·lat l'antivirus. Desinstal·leu sempre seguint el procediment descrit.

Què és la protecció permanent

La protecció permanent és un programa que, des de l'arrencada de la màquina, intercepta totes aquelles operacions que suposen risc de contagi per verificar que cap virus no entri en el sistema.

La protecció permanent funciona de manera totalment automàtica i sense requerir cap intervenció per part de l'usuari. Tot i la vigilància constant, el rendiment del sistema no es veu afectat per la qual cosa la instal·lació de la protecció permanent és sempre aconsellable atès que augmenta considerablement la protecció de l'ordinador.

Com s'usa la protecció permanent

La protecció permanent és una de les opcions de la instal·lació. Si heu escollit instal·lar aquesta protecció, un cop s'arrenqui la màquina, la protecció permanent (**Sentinel**) estarà en funcionament.

Si el sistema operatiu és Windows NT Workstation 3.51, **Sentinel** apareixerà com una icona minimitzada a l'escriptori de Windows. Si el sistema operatiu és Windows NT Workstation 4.0, **Sentinel** apareixerà com una icona al costat del rellotge situat a la barra de tasques.

El funcionament de la protecció permanent és totalment automàtic. Si, en alguna operació, **Sentinel** detectés la presència d'un virus, avisaria d'aquesta circumstància i duria a terme l'acció pertinent.

Com es configura la protecció permanent

La protecció permanent es pot configurar per adaptar-se a les necessitats de cada usuari. Fent doble clic sobre la icona de **Sentinel**, apareix una finestra amb diverses pestanyes. Cada una d'elles fa referència a la configuració dels diferents aspectes de **Sentinel**. Les opcions de configuració són les següents:

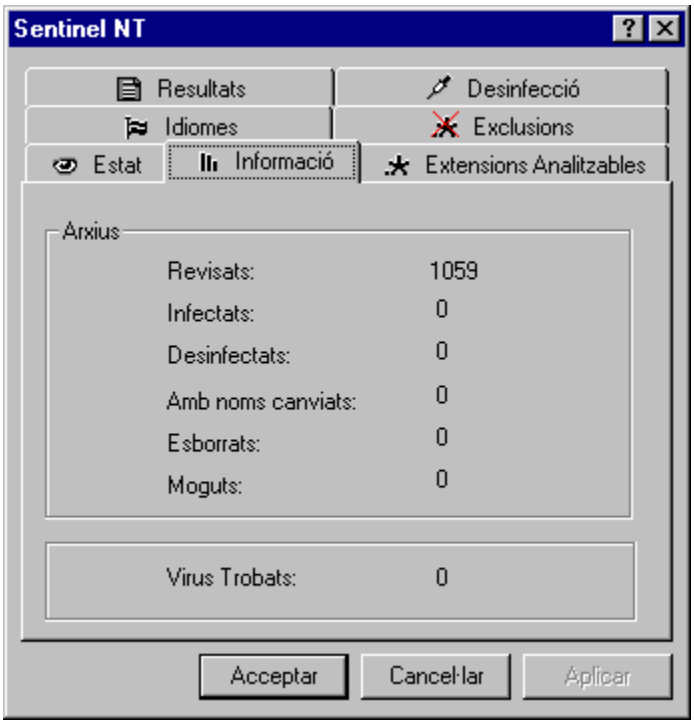
Estat

En aquesta pestanya es defineix l'estat de la protecció permanent.

- **Activat:** mitjançant aquesta opció, s'activa o desactiva la protecció permanent. Cal tenir en compte que si desactiveu la protecció permanent, l'ordinador quedarà desprotegit enfront dels virus.
- **Entrades:** amb la protecció permanent activada, aquesta opció indica que s'han d'analitzar totes aquelles entrades d'arxius a la màquina. També s'analitzaran les creacions d'arxius i les seves modificacions.
- **Sortides:** amb la protecció permanent activada, aquesta opció indica que s'han d'analitzar totes aquelles sortides d'arxius de la màquina. També s'analitzaran totes les obertures i execucions d'arxius.
- **Canvi de nom:** amb la protecció permanent activada, aquesta opció indica que s'han d'analitzar a la recerca de virus totes les operacions de canvi de nom d'arxius.
- **Xarxa Microsoft:** si la protecció permanent està activada, aquesta opció indica que s'han d'analitzar en remot totes les operacions efectuades sobre una unitat de xarxa Microsoft.
- **Xarxa Novell:** si la protecció permanent està activada, aquesta opció indica que s'analitzin en remot totes les operacions efectuades sobre una unitat de xarxa Novell.

Informació

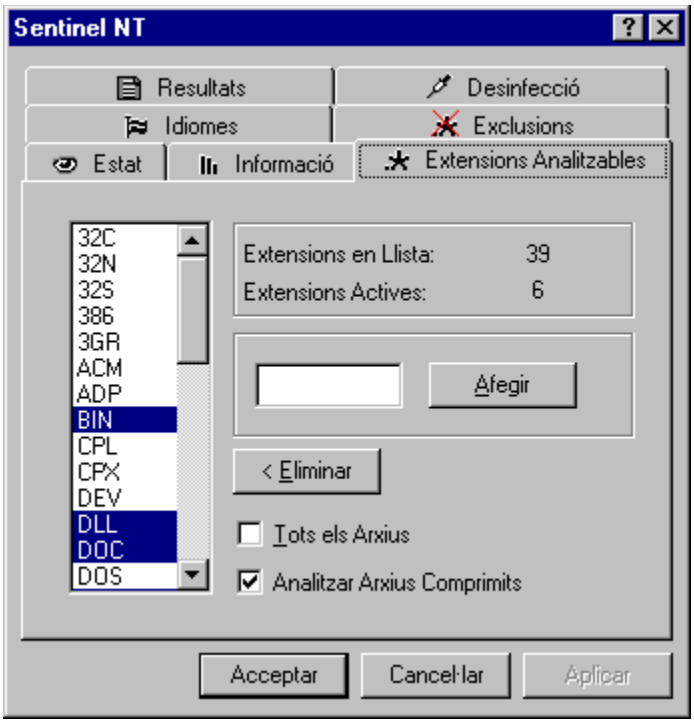
En aquesta pestanya es mostren diverses informacions referents a l'activitat de la protecció permanent.



- **Revisats:** indica el nombre d'arxius que la protecció permanent ha revisat a la recerca de virus des de l'inici del sistema.
- **Infectats:** aquesta informació mostra el nombre d'arxius infectats que s'han trobat.
- **Desinfectats:** indica el nombre d'arxius desinfectats per la protecció permanent.
- **Canviats de nom:** aquí es mostra el nombre d'arxius el nom dels quals ha canviat la protecció permanent.
- **Esborrats:** en aquest punt es mostra el nombre d'arxius esborrats per la protecció permanent per estar contaminats amb virus.
- **Moguts:** aquí s'informa quants arxius ha mogut la protecció permanent per estar contaminats amb virus.
- **Virus trobats:** per últim, aquí s'indica quants virus s'han trobat.

Extensions analitzables

En aquest apartat es configuren les extensions que ha d'analitzar la protecció permanent.



- **Llista d'extensions:** a la llista d'extensions podeu marcar totes aquelles extensions que desitgeu analitzar. La protecció permanent sempre intercepta tots els arxius als quals s'accedeix però només analitzarà aquells arxius que tinguin una de les extensions seleccionades. Independentment, de la selecció d'extensions que feu, els arxius EXE i COM s'analitzaran sempre.
- **Extensions en llista:** aquesta dada informa del nombre d'extensions que hi ha a la llista.
- **Extensions actives:** aquesta dada informa de les extensions que heu marcat a la llista per analitzar.
- **Afegir extensió:** per afegir una extensió a la llista, heu d'escriure l'extensió a la casella a aquest efecte i prémer el botó *Afegir*.
- **Eliminar extensió:** per eliminar una extensió de la llista, heu de seleccionar a la llista l'extensió a eliminar i prémer el botó *Eliminar*.
- **Tots els arxius:** si marqueu aquesta opció, s'analitzaran tots els arxius independentment de les extensions que hagueu seleccionat.
- **Analitzar arxius comprimits:** si marqueu aquesta opció, s'analitzaran els arxius comprimits als quals s'accedeixi.

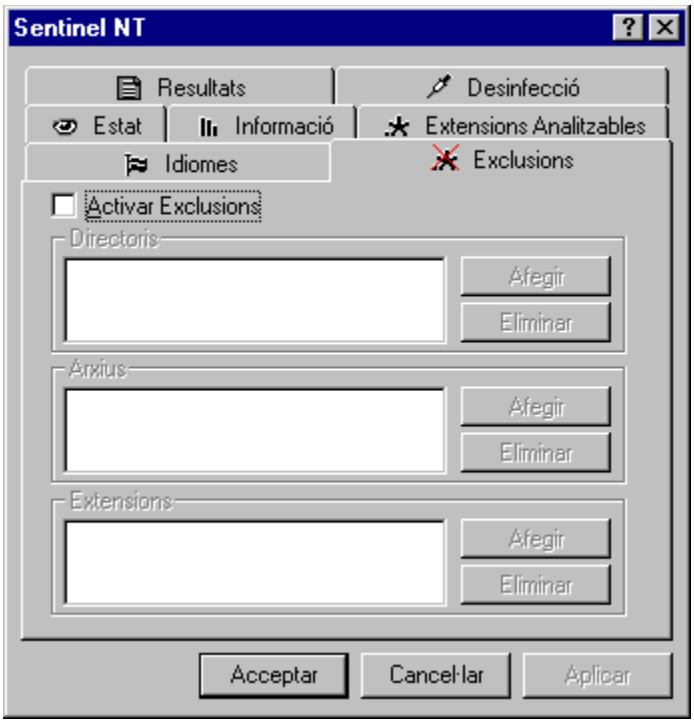
Idiomes

En aquesta pestanya podeu consultar l'idioma en el qual es troba la protecció permanent i també podeu escollir un altre idioma de la llista d'idiomes disponibles.

- **Idiomes disponibles:** es mostra una llista amb els diferents idiomes disponibles per a la protecció permanent. Per canviar d'idioma, només cal que seleccioneu l'idioma desitjat i premeu el botó *Acceptar* o el botó *Aplicar*.
- **Idioma actual:** aquí es mostra l'idioma en el que es troba en aquest moment la protecció permanent.

Exclusions

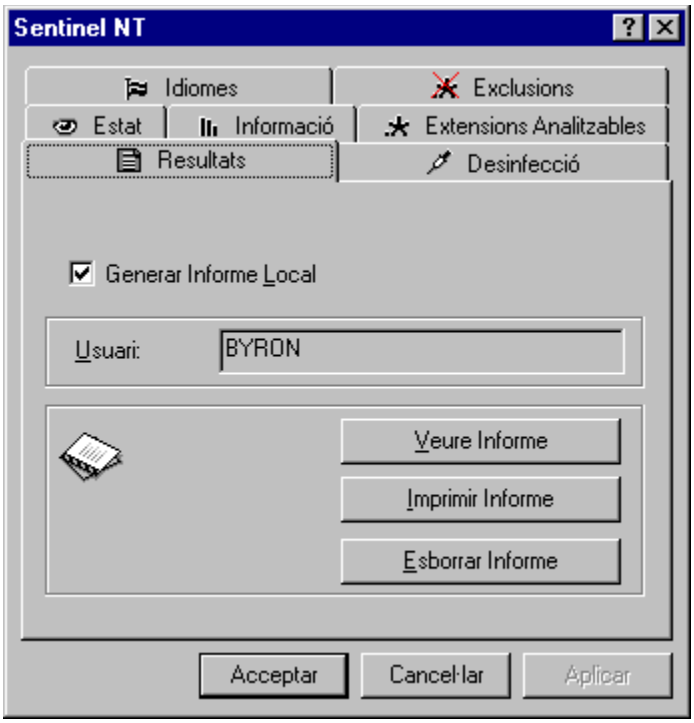
En aquesta pestanya podeu indicar aquelles àrees, arxius o extensions que no desitgeu analitzar. Independentment del que hagueu indicat a *Extensions*, totes aquelles àrees, arxius o extensions que marqueu en aquest apartat, **no s'analitzaran**.



- **Activar exclusions:** si marqueu aquesta opció s'activarà la funció d'exclusió en funció de les dades que hagueu indicat.
- **Directori:** en aquest apartat es mostra una llista amb tots aquells directoris que no s'hauran d'analitzar.
- **Afegir directori:** mitjançant aquesta opció, podeu afegir directoris que no s'analitzaran.
- **Eliminar directori:** mitjançant aquesta opció, podeu eliminar directoris de la llista de directoris que no s'analitzaran.
- **Arxiu:** en aquest apartat es mostra una llista amb els arxius que no s'han d'analitzar.
- **Afegir arxiu:** aquesta opció permet afegir un arxiu a la llista d'arxius que no s'analitzen.
- **Eliminar arxiu:** aquesta opció permet eliminar un arxiu de la llista d'arxiu que no s'analitzen.
- **Extensions:** en aquest apartat es mostra una llista de les extensions que s'han d'analitzar. Tot i que alguna d'aquestes extensions sigui a la llista d'extensions per analitzar, no s'analitzarà.
- **Afegir extensió:** gràcies a aquesta opció, podeu afegir una extensió a la llista d'extensions no analitzables.
- **Eliminar extensió:** gràcies a aquesta opció, podeu eliminar una extensió de la llista d'extensions que no s'analitzen.

Resultats

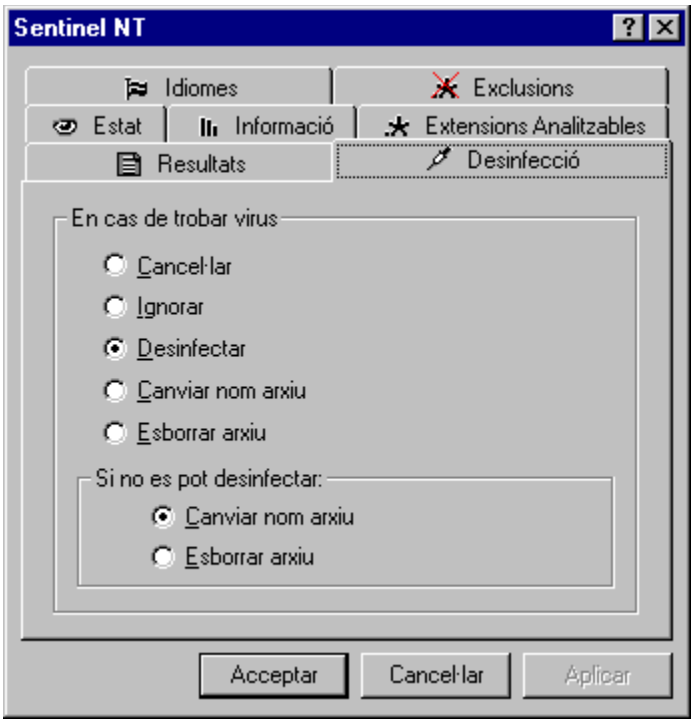
En aquesta pestanya es configura el comportament del sistema d'informes d'incidències trobades per la protecció permanent.



- **Generar informe local:** si activeu aquesta opció, es generarà un informe amb les diferents incidències que trobi la protecció permanent.
- **Usuari:** aquí es mostra el nom de l'usuari de la màquina.
- **Veure informe:** aquest botó mostra l'informe amb les incidències trobades fins al moment.
- **Imprimir informe:** gràcies a aquest botó, podeu imprimir l'informe d'incidències.
- **Esborrar informe:** mitjançant aquest botó, podeu esborrar l'informe d'incidències.

Desinfecció

En aquesta pestanya es configura el comportament de la desinfecció d'arxius contaminats per virus i detectats per la protecció permanent.

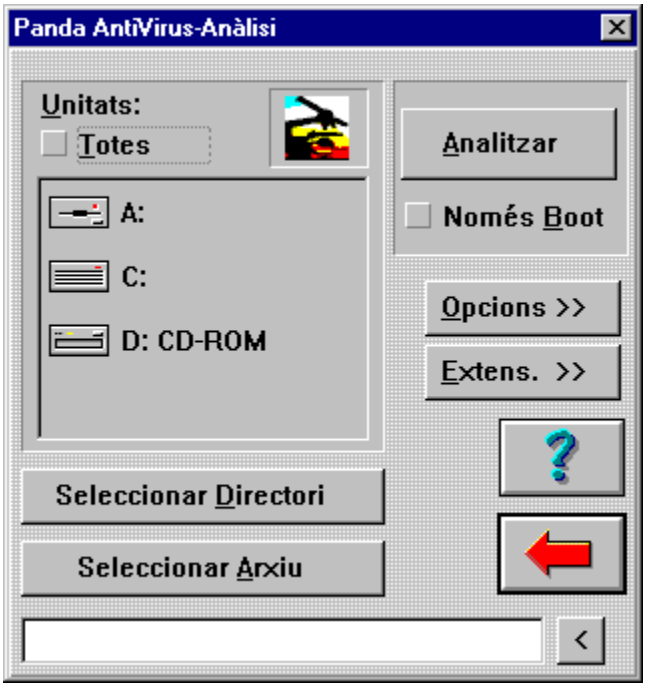


- **Cancel·lar:** si marqueu aquesta opció, l'operació en què s'hagi detectat el virus serà cancel·lada. Si, per exemple, el virus ha estat detectat en un arxiu que s'intentava executar, es cancel·larà l'execució de l'arxiu esmentat.
- **Ignorar:** amb aquesta opció marcada, malgrat es trobi un virus s'ignorarà aquest esdeveniment.
- **Desinfectar:** si marqueu aquesta opció i la protecció permanent detecta un virus, procedirà a la desinfecció tot deixant l'arxiu contaminat tal i com estava abans de la infecció.
- **Canviar nom d'arxiu:** amb aquesta opció marcada, si es detecta un virus, **Sentinel** canviarà el nom de l'arxiu per que tingui l'extensió VIR.
- **Esborrar arxiu:** si marqueu aquesta opció i **Sentinel** detecta un virus en un arxiu, es procedirà a esborrar aquest arxiu.
- **Si no es pot desinfectar, canviar nom d'arxiu:** si aquesta opció està activa, quan **Sentinel** detecti un virus i provi de desinfectar-lo, en cas de no poder realitzar aquesta operació amb èxit, l'arxiu canviarà de nom.
- **Si no es pot desinfectar, esborrar arxiu:** si aquesta opció està activa, quan **Sentinel** detecti un virus i provi de desinfectar-lo, en cas de no poder realitzar aquesta operació amb èxit, l'arxiu s'esborrarà.

Què és l’anàlisi sota demanda

L’anàlisi sota demanda us permet analitzar qualsevol àrea del vostre ordinador en el moment que desitgeu. Cada anàlisi que es realitza es pot configurar mitjançant un conjunt de senzilles opcions.

Com s'usa l'anàlisi sota demanda



Per realitzar una anàlisi sota demanda, s'han de dur a terme els següents passos:

1. **Executar l'antivirus:** per executar l'antivirus, aneu al grup de programes on s'hagin creat les icones que permetin la seva execució. Feu doble clic sobre la icona *Panda Antivirus*.
2. **Anar a l'apartat d'anàlisi:** per anar a aquest apartat, premeu el botó *Analitzar* que hi ha a la barra de botons de l'aplicació. Apareixerà una finestra per especificar què s'ha d'analitzar i com s'ha de fer.
3. **Escollir l'àrea d'anàlisi:** s'ha d'escollir l'àrea que desitgeu analitzar. En una llista es mostren les diferents unitats reconegudes en el sistema. També es pot indicar un directori o un arxiu concret mitjançant els botons corresponents.
4. **Configurar les extensions:** aquest pas és opcional. El programa guarda la configuració de les extensions que es volen analitzar. Per tant, un cop configurades, no cal repetir la configuració a cada anàlisi.
5. **Configurar les opcions d'anàlisi:** aquest pas també és opcional. El programa guarda la configuració de les opcions d'anàlisi. Per tant, un cop configurada l'anàlisi, no cal repetir la configuració a cada anàlisi. Només haureu de variar aquesta configuració quan desitgeu escollir un conjunt d'opcions diferent. Hi ha una explicació més detallada de les opcions d'anàlisi a l'apartat de configuració d'aquesta mateixa documentació.
6. **Indicar si es vol analitzar únicament el boot:** aquest pas és opcional. Si marqueu aquesta opció, només s'analitzarà el boot i no els arxius de les unitats seleccionades. Si no marqueu aquesta opció, s'analitzaran tant el boot com els arxius de totes les unitats seleccionades.
7. **Començar l'anàlisi:** el botó *Analitzar* dóna inici a l'anàlisi per buscar virus a les àrees seleccionades i amb les opcions escollides.

Com es configura l'anàlisi sota demanda

Tal i com s'ha esmentat, en una anàlisi cal indicar:

- Quina àrea voleu analitzar.
- Quines extensions es consideraran a l'anàlisi.
- Com es durà a terme l'anàlisi.

La configuració d'una anàlisi inclou indicar quines extensions es tindran en compte i les opcions d'anàlisi.

Extensions

Prement el botó *Extensions* apareix una finestra que permet indicar quines extensions es desitja analitzar.

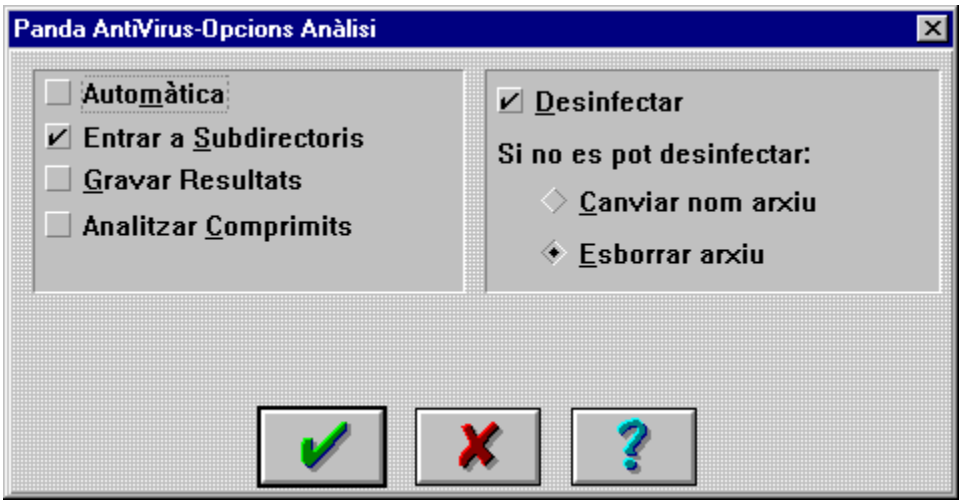
L'opció *Totes* que hi ha a la llista d'extensions indica que s'analitzaran tots els arxius amb independència de la seva extensió. Si aquesta opció no està marcada, només s'analitzaran els arxius l'extensió dels quals coincideixi amb alguna de les de la llista.

Hi ha dos botons que permeten afegir i eliminar extensions a la llista. Per defecte, es proporciona una llista amb les extensions més comunes i una selecció d'aquelles extensions susceptible d'allotjar virus.

Independentment de la selecció d'extensions que es faci, sempre s'analitzaran els arxius EXE i COM.

Opcions d'anàlisi

Prement el botó *Opcions* apareix una finestra que permet escollir les opcions d'anàlisi, que són les següents:



- **Automàtic:** si marqueu aquesta opció, el procés d'anàlisi serà completament automàtic. Si es troben virus, el procés informarà d'això però continuarà sense interrompre's. Això és especialment útil quan l'ordinador té molts arxius infectats i s'estan desinfectant.
- **Entrar a subdirectoris:** si marqueu aquesta opció, s'analitzaran els subdirectoris que es trobin a les àrees que s'estan analitzant. Si no marqueu aquesta opció, no s'analitzaran els subdirectoris que es troben amb la qual cosa si escolliu analitzar una unitat però no es marca aquesta opció, aleshores només s'analitzarà el seu directori arrel.
- **Gravar resultats:** si marqueu aquesta opció, les dades relatives a l'anàlisi corresponent es registraran a l'arxiu de resultats.
- **Analitzar comprimits:** si marqueu aquesta opció, s'analitzaran els arxius comprimits que es trobin.
- **Desinfectar:** si marqueu aquesta opció, i es troba un virus, l'antivirus provarà de desinfectar-lo.
- **Si no es pot desinfectar, canviar el nom:** si marqueu aquesta opció i l'antivirus troba un virus que no pot desinfectar, es procedirà a canviar el nom de l'arxiu en qüestió.
- **Si no es pot desinfectar, esborrar:** si marqueu aquesta opció i l'antivirus troba un virus que no pot desinfectar, es procedirà a esborrar l'arxiu en qüestió.

Què és l'anàlisi heurística

L'anàlisi heurística és una tècnica d'anàlisi addicional especialment pensada per detectar virus desconeguts.

A l'igual que l'anàlisi sota demanda, l'anàlisi heurística és immediata i a demanda de l'usuari. El mètode d'anàlisi en què es basa l'anàlisi heurística és completament diferent del mètode d'anàlisi sota demanda. Aquesta darrera es basa en intentar trobar un dels virus que l'antivirus coneix mentre que l'heurística intenta determinar si existeix un virus tot basant-se en característiques generals comunes a la majoria dels virus.

Atès que l'anàlisi heurística només pot determinar que un arxiu és sospitós d'estar infectat per un virus i que no es disposa d'informació suficient sobre el suposat virus, no es poden desinfectar aquells suposats virus detectats per l'anàlisi heurística.

És important tenir en compte que l'anàlisi heurística és un complement de l'anàlisi sota comanda.

El funcionament de l'anàlisi heurística és similar al de l'anàlisi sota demanda.

Com s'usa l'anàlisi heurística

Per realitzar una anàlisi heurística, s'ha de dur a terme els següents passos:

1. **Executar l'antivirus:** per executar l'antivirus, aneu al grup de programes on s'hagin creat les icones que permetin la seva execució. Feu doble clic sobre la icona *Panda Antivirus*.
2. **Anar a l'apartat d'anàlisi heurística:** per anar a aquest apartat, premeu el botó *Investigar* de la barra de botons de l'aplicació. Apareixerà una finestra per especificar què s'ha d'analitzar mitjançant el mètode heurístic i com s'ha de fer.
3. **Escollir l'àrea d'anàlisi:** s'ha d'escollir l'àrea que desitgeu analitzar. En una llista es mostren les diferents unitats reconegudes en el sistema. També es pot indicar un directori o un arxiu concret mitjançant els botons corresponents.
4. **Configurar les opcions de l'anàlisi heurística:** aquest pas és opcional. El programa guarda la configuració de les opcions de l'anàlisi heurística. Per tant, un cop configurada l'anàlisi heurística, no cal repetir la configuració a cada anàlisi d'aquest tipus que es dugui a terme. Només caldrà variar aquesta configuració quan es desitgi escollir un conjunt d'opcions diferent. S'ofereix una explicació més detallada sobre les opcions de l'anàlisi heurística a l'apartat de configuració d'aquesta mateixa documentació.
5. **Començar l'anàlisi:** el botó *Analitzar* dóna inici a l'anàlisi heurística per buscar virus a les àrees seleccionades i amb les opcions escollides.

Com es configura l'anàlisi heurística

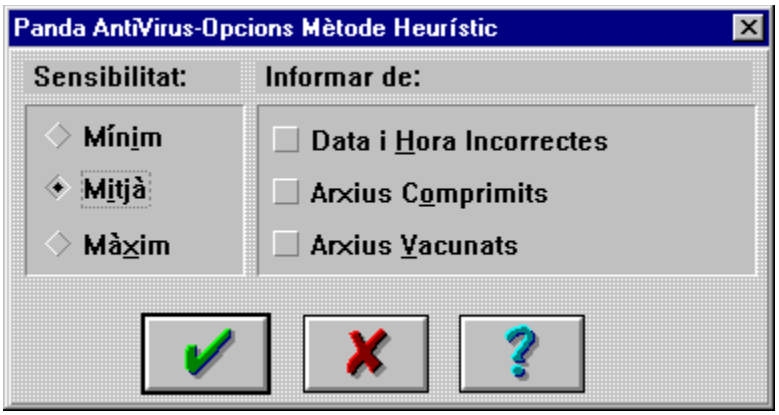
Tal i com s'ha esmentat, en una anàlisi heurística cal indicar:

- Quina àrea voleu analitzar mitjançant aquest mètode.
- Com es durà a terme l'anàlisi esmentada.

La configuració d'una anàlisi heurística consisteix en les opcions d'aquest tipus d'anàlisi.

Opcions d'anàlisi

Prement el botó *Opcions* apareix una finestra que permet escollir les opcions d'anàlisi heurística que són les següents:



- **Sensibilitat mínima:** si marqueu aquesta opció, la sensibilitat de l'anàlisi heurística serà baixa fent que només s'indiquin com a possibles arxius contaminats aquells molt sospitosos de contenir un virus.
- **Sensibilitat mitjana:** si marqueu aquesta opció, l'anàlisi heurística es durà a terme amb una sensibilitat mitjana. D'aquesta forma, només s'indicaran com a sospitosos aquells arxius amb bastant probabilitat d'estar contaminats.
- **Sensibilitat màxima:** si marqueu aquesta opció, la sensibilitat de l'anàlisi heurística serà màxima tot indicant com a sospitosos d'infecció tots aquells arxius en què es detecti alguna possibilitat de trobar-se infectats. No obstant, la possibilitat que un arxiu no infectat es mostri com a sospitós, fins i tot amb aquest nivell de sensibilitat, és mínima.
- **Informar de la data i la hora incorrectes:** si marqueu aquesta opció, s'avisarà cada cop que es trobi un arxiu amb la data o la hora incorrectes.
- **Informar d'arxius comprimits:** si marqueu aquesta opció, s'avisarà cada cop que es trobi un arxiu comprimit.
- **Informar d'arxius vacunats:** si marqueu aquesta opció, s'avisarà de tots aquells arxius vacunats que es trobin.

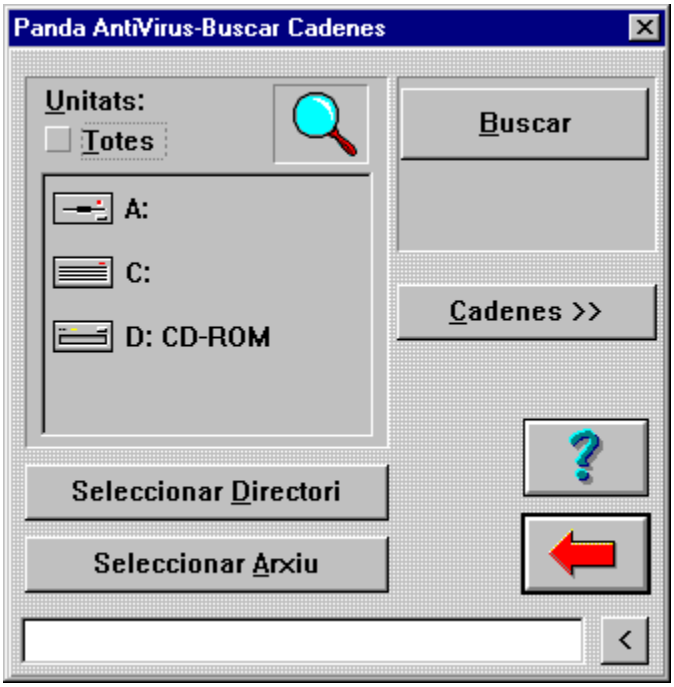
Què és la recerca de cadenes

L'anàlisi sota comanda es basa en buscar en els arxius parts dels virus que l'antivirus ja coneix. Atès que cada dia sorgeixen nous virus, l'anàlisi sota comanda es va quedant antiquat a poc a poc.

La recerca de cadenes utilitza el mateix mètode que l'anàlisi sota demanda però s'hi pot indicar una cadena (part d'un virus) per que la busqui. D'aquesta manera, el servei d'atenció al client de **Panda Software** us pot indicar una cadena corresponent a un nou virus per que l'antivirus la detecti tot i no tenir informació referent a aquest virus en el seu interior.

A l'igual que l'anàlisi sota demanda, la recerca de cadenes és immediata i a demanda de l'usuari.

Com s'usa la recerca de cadenes



Per realitzar una recerca de cadenes, s'ha de dur a terme els següents passos:

1. **Executar l'antivirus:** per executar l'antivirus, aneu al grup de programes on s'hagin creat les icones que permetin la seva execució. Feu doble clic sobre la icona *Panda Antivirus*.
2. **Anar a l'apartat de recerca de cadenes:** per anar a aquest apartat, premeu el botó *Buscar* de la barra de botons de l'aplicació. Apareixerà una finestra per especificar què s'ha d'analitzar mitjançant la recerca de cadenes i com s'ha de fer.
3. **Escollir l'àrea on es realitzarà la recerca:** s'ha d'escollir l'àrea on desitgeu buscar. En una llista es mostren les diferents unitats reconegudes en el sistema. També es pot indicar un directori o un arxiu concret mitjançant els botons corresponents.
4. **Indicar les cadenes que s'han de buscar:** heu d'escriure les cadenes que l'antivirus ha de buscar o escollir cadenes ja introduïdes d'una llista. Atès que el programa guarda les cadenes que s'hagin introduït en d'altres ocasions, si no desitgeu afegir cap cadena nova, no cal realitzar aquest pas.
5. **Començar la recerca:** el botó *Buscar* dóna inici a la recerca de les cadenes indicades a les àrees escollides.

Com es configura la recerca de cadenes

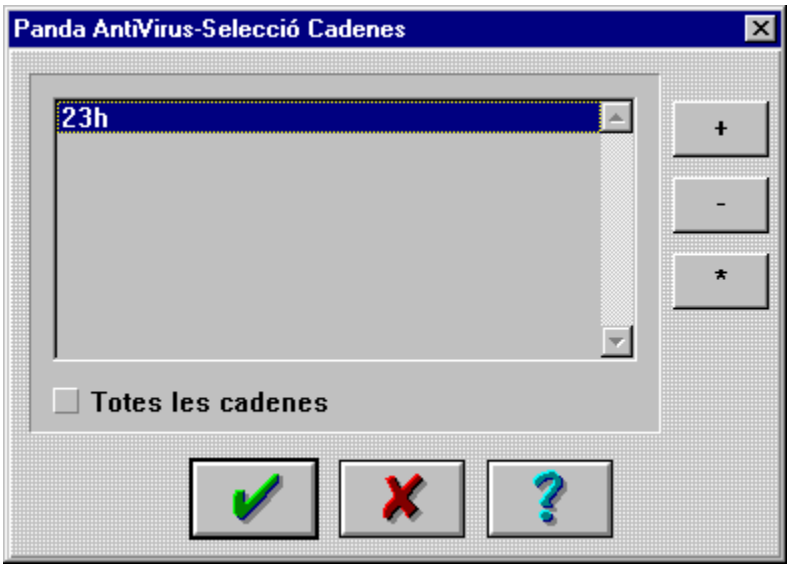
Tal i com s'ha esmentat, en una recerca de cadenes cal indicar:

- Quina àrea voleu analitzar mitjançat aquest mètode.
- Quines cadenes s'han de buscar.

La configuració d'una recerca de cadenes consisteix en les cadenes que s'han de buscar.

Cadenes

Prement el botó *Cadenes* apareix una finestra que permet escollir les cadenes que es buscaran.



En aquesta finestra es veu una llista de les cadenes introduïdes. Mitjançant els botons corresponents, podeu afegir una cadena a aquesta llista, modificar una de les cadenes ja introduïdes o eliminar una cadena de la llista.

No es buscaran totes les cadenes indicades a la llista llevat que es marqui l'opció *Totes les cadenes*. Si aquesta opció no està marcada, només es buscaran les cadenes seleccionades a la llista.

Com desinfectar amb Panda Antivirus

No existeix un apartat específic de desinfecció al **Panda Antivirus**. La desinfecció va associada a l'anàlisi sota demanda o a la protecció permanent. Si l'anàlisi sota demanda o la protecció permanent troben un virus, intentaran desinfectar-lo (si hi heu configurat així a les opcions d'aquests dos apartats).

La configuració de la desinfecció permet indicar que s'esborrin o es canviï el nom de tots aquells arxius contaminats que no es puguin desinfectar.

Un virus es pot trobar en el boot d'un disc o en arxius. En cada cas, cal procedir d'una manera lleugerament diferent. Consulteu els apartats corresponents per obtenir un procediment de desinfecció detallat.

Desinfecció d'un virus de boot

Partició FAT

Per desinfectar un virus de boot de la unitat C, cal realitzar els passos següents:

1. Apagueu el vostre ordinador. Introduïu un disquet d'arrencada net de virus (si penseu dur a terme la desinfecció des del CD-Rom, caldrà que el disquet carregui els drivers del CD) i reinicieu la vostra màquina.
2. Un cop hagi arrencat, executeu el nostre antivirus en línia de comandaments (PAVCL) d'acord amb les següents indicacions:

   - Si desitgeu executar **Pavcl** des d'un disquet, introduïu el disc 1 de **Panda Antivirus** per a DOS/Windows 3.1x i teclegeu el següent:

     ```
     PAVCL C: /CLV
     ```

   - Si desitgeu executar **Pavcl** des del nostre CD-Rom, introduïu-lo a la unitat lectora, situeu-vos en el directori DOSWIN3X i en l'idioma desitjat i tot seguit teclegeu el següent:

     ```
     PAVCL C: /CLV
     ```

     Si en qualsevol de les dues situacions us apareix un missatge indicant que la unitat escollida no és vàlida, teclegeu el següent:

     ```
     PAVCL /HD0 /CLV
     ```

Partició NTFS

Per desinfectar un virus de boot comptant amb una partició NTFS, cal saber si el virus afecta el master boot, el boot o ambdós. En cas que el virus afecti únicament el master boot, el procediment indicat per a particions FAT és igualment vàlid en aquest cas.

Si el virus afecta el boot, la manera d'eliminar el virus és reemplaçar el boot per un boot genèric mitjançant qualsevol de les eines que Windows NT proporciona a aquest efecte.

Desinfecció d'un virus present en arxius

Si ha trobat un virus en arxius, procediu a netejar el vostre sistema tot configurant l'antivirus de la següent manera:

- A *Opcions d'anàlisis* activeu *Totes les extensions*, *Desinfectar* i *Anàlisi automàtica*.
- Aneu a l'apartat d'anàlisi i escolliu l'opció corresponent a analitzar tot el sistema (totes les unitats). Segons es vagi realitzant l'anàlisi, s'aniran netejant els arxius infectats.

Desinfecció mitjançant la protecció permanent

Sentinel és capaç de desinfectar els virus que troba. Si **Sentinel** detecta un virus i està configurat per desinfectar-lo, el desinfectarà abans que es realitzi l'operació en curs i, un cop desinfectat, continuarà amb l'operació en la que s'ha detectat el virus. **Sentinel** sempre mostra una finestra tot indicant la detecció del virus.

Anàlisi en línia de comandaments

Panda Antivirus compta amb un programa anomenat **Pavcl** que s'executa des de la línia de comandaments d'MS-DOS. El nostre analitzador detecta i desinfecta des de la línia de comandaments els mateixos virus que qualsevol altra versió de **Panda Antivirus**.

Pavcl és un analitzador ràpid i que ocupa poca memòria però, per fer-lo servir, cal tenir un cert coneixement dels paràmetres que admet. **Pavcl** està disponible en el disquet número 1 de la versió DOS/Windows 3.1x o en el directori de l'idioma corresponent dintre del directori DOSWIN3X del CD-Rom.

Paràmetres de Pavcl

Tasques

`/NOM` No analitzar la memòria.

`/NOB` No analitzar el sistema d'arrencada BOOT.

`/NOF` No analitzar arxius.

`/ALL` Analitzar totes les unitats del sistema.

`/INVx` Investigar en la unitat "x" en busca de virus desconeguts.
Exemple: `/INVA` investiga en la unitat A:.

`/CLV` Eliminar els virus que s'hagin detectat.

`/LIS` Llistar els virus contemplats en aquesta versió.

`/HEU` Activar mètode de detecció Heurístic.

`/CMP` Analitzar comprimits.

`/CDR` Mostra els codis de retorn de **Pavcl**.

`/SAV` Guardar els paràmetres en un arxiu. En les següents execucions afegirà aquests paràmetres als introduïts en cada sessió.

`/IB+` Afegir vacuna Interna al BOOT.
`/IB-` Treure vacuna Interna al BOOT.
`/IB*` Verificar vacuna Interna del BOOT.

`/EB+` Afegir vacuna Externa al BOOT.

`/EB-` Treure vacuna Externa al BOOT.
`/EB*` Verificar vacuna Externa del BOOT.

`/IF+` Afegir vacuna Interna a un Arxiu.
`/IF-` Treure vacuna Interna a un Arxiu.
`/IF*` Verificar vacuna Interna d'un Arxiu.

`/EF+` Afegir vacuna Externa a un Arxiu.
`/EF-` Treure vacuna Externa a un Arxiu.
`/EF*` Verificar vacuna Externa d'un Arxiu.

`/B+` Afegir vacuna Interna i Externa al BOOT.
`/B-` Treure vacuna Interna i Externa al BOOT.
`/B*` Verificar vacuna Interna i Externa del BOOT.

`/F+` Afegir vacuna Interna i Externa a un Arxiu.
`/F-` Treure vacuna Interna i Externa d'un Arxiu.
`/F*` Verificar vacuna Interna i Externa d'un Arxiu.

Modificadors

`/NSB` No analitzar els subdirectoris de nivell inferior.

`/PTH` Analitzar els directoris continguts en la variable PATH del DOS.

`/ISO` Activar el mètode d'aïllament.

`/NOS` Desactivar el so.

`/AEX` Analitzar tots els arxius, independentment de la seva extensió.

`/AUT` Exploració sense la intervenció de l'usuari.

`/OVR` Sobreescriure abans d'esborrar.

`/NOR` No generar arxiu de resultats.

`/DEL` Esborra els arxius infectats encara que es puguin desinfectar.

`/LOC` Analitza totes les unitats locals.

`/NBR` No permet cancel·lar el procés d'anàlisi.

`/ITW` **Pavcl** només analitzarà buscant els virus *In The Wild*. Aquest paràmetre només s'ha

d'utilitzar en condicions especials.

Addicionalment disposa de l'switch "/?" estandarditzat en el DOS, per tenir accés a una llista dels switches disponibles. En aquesta també s'inclouen aquells corresponents als idiomes suportats per la versió de **Pavcl**.

Les tasques per defecte són:

- Analitzar Memòria.
- Analitzar Boot.
- Analitzar Arxius.

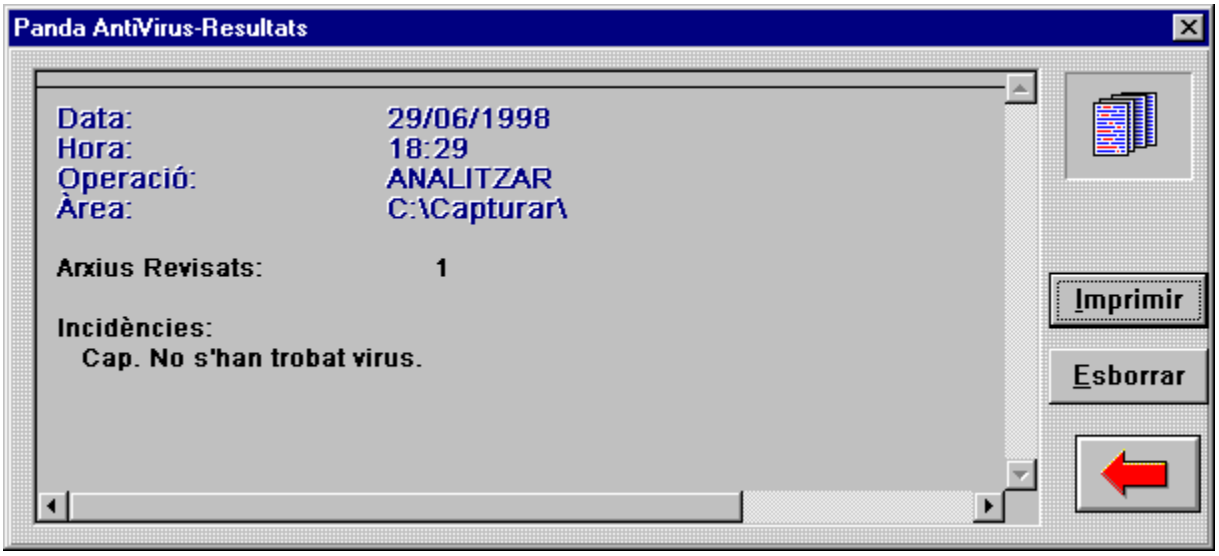
i els modificadors per defecte són:

- Analitzar subdirectoris.
- No desinfectar.
- Efectes de so activats.
- Analitzar només extensions executables.
- Generar arxiu de resultats.

Les tasques /?, /LIS, /INVx són exclusives, és a dir, quan se seleccionen no es realitza cap de les altres tasques. Un cop finalitzades, es torna al DOS. El camí o camins que es volen analitzar s'especifica com és habitual en el DOS:

[Unitat:][Camí][NomArxiu]

Informe de resultats



L'informe de resultats va guardant les diferents operacions que es van realitzant amb l'antivirus com també les diferents incidències que es produeixin.

La informació continguda a l'informe de resultats es conserva de sessió en sessió. Per tant, és útil per consultar, en qualsevol moment, l'activitat que s'ha dut a terme amb l'antivirus.

Per cada operació realitzada, es guarden les següents dades:

- Data i hora.
- Tipus d'operació.
- Àrea sobre la que s'ha dut a terme l'operació.
- Nombre d'arxius revisats.
- Totes les incidències que hi ha hagut relacionades amb els virus.

Per tal que es vagin emmagatzemant les dades a l'informe de resultats, cal activar l'opció *Gravar resultats* de la finestra d'*Opcions d'Anàlisi*.

Podeu imprimir el contingut de l'informe de resultats per tal de facilitar la seva consulta. També podeu esborrar el contingut de l'informe de resultats en qualsevol moment per evitar que adquireixi una mida massa gran.

Llista de virus

La llista de virus presenta una llista amb els virus que **Panda Antivirus** és capaç de detectar. A la llista de virus s'indica el nom i la mida de cada virus.

Juntament amb la llista, s'indica el nombre de virus reconeguts en aquesta versió de **Panda Antivirus**. També s'indica la data de l'arxiu de virus per saber, d'aquesta manera, el nivell d'actualització o desactualització de l'antivirus.

Podeu indicar el nom del virus a la casella destinada a aquest efecte per així trobar un virus concret amb major facilitat. Per això, la llista de virus es presenta ordenada alfabèticament.

Una vegada escollit el virus, si premeu el botó *Info*, apareix una finestra amb una sèrie de dades d'interès com ara:

- Nom.
- Origen.
- Mida.
- Alies.
- Data en què fou detectat per primera vegada.
- Si es pot desinfectar o no.
- Àrees de la màquina que es poden veure afectades pel virus.
- Característiques de comportament del virus.

Tot seguit, es detalla una explicació de les diferents característiques amb què pot comptar un virus:

- **Resident:** quan s'executa, el virus reserva una petita part de la memòria i s'instal·la dins d'ella per anar contagiant-se des d'allà.
- **Stealth:** és una tècnica que usen alguns dels virus residents. Aquesta tècnica consisteix a camuflar els canvis que el virus fa sobre els arxius que infecta. Quan algú intenta mirar una de las característiques de l'arxiu que el virus ha modificat, el virus, que està resident a la memòria, intercepta la consulta i ofereix les dades anteriors a la modificació.
- **Encriptat:** els virus que posseeixen aquesta característica són capaços d'encriptar-se de manera diferent cada cop que infecten un arxiu. D'aquesta forma, no es pot intentar buscar el virus mitjançant una cadena.
- **Sobreescriptura:** els virus de sobreescriptura, que poden ser residents o no, sobreescriuen l'arxiu que infecten. Aquest arxiu queda, per tant, inservible. La mida de l'arxiu no varia llevat que la mida del virus sigui més gran que la de l'arxiu. L'única forma d'eliminar aquests virus és esborrant l'arxiu infectat i posant en el seu lloc una còpia sense infectar.
- **Polimòrfic:** els virus polimòrfics són versions avançades dels virus encriptats. Els polimòrfics són capaços de canviar el mètodes d'encriptació de generació en generació. D'aquesta forma, no hi ha cap part del virus que romangui inalterada.

Funcionament general

Panda Antivirus per a Windows NT presenta un interface còmode i fàcil d'usar. A la finestra principal del programa, les opcions més comunes estan disponibles a través d'uns botons grans.

Prement sobre aquests botons accediu a les diferents parts del programa. Consulteu l'apartat corresponent per obtenir una explicació de funcionament detallada.