Pràctica 4
Programes antivirus

Introducció

Quan utilitzem un ordinador basat en Windows, cal disposar d'un programa antivirus, o *antimalware* (programari maliciós) en general. Això és a conseqüència del disseny del mateix sistema operatiu, que permet que un usuari normal pugui executar programari que malmeti el mateix sistema operatiu. Algunes persones amb finalitats poc ètiques ho aprofiten i escriuen un conjunt de programes que es propaguen sense autorització de l'usuari, malmeten fitxers, tant de l'usuari com del sistema operatiu, roben informació personal sense permís i poden fer que el sistema operatiu deixi de funcionar correctament.

Per sort, hi ha una gran varietat de programari específicament dissenyat per a entorns Windows, que ens permeten evitar la majoria dels riscos (tot i que no el cent per cent), que comporten els virus informàtics o programes espia.

Enunciat i documentació per a la realització de la pràctica

Per dur a terme la pràctica necessitem una màquina que funcioni amb el Windows; pot ser una màquina real o una màquina virtual. Si utilitzem una màquina virtual, podem emprar el programari de virtualització VirtualBox, que podem baixar des d'aquí:

http://www.virtualbox.org/wiki/Downloads

Pel que fa al programari antivirus, tot i que n'hi ha una gran varietat, per dur a terme la pràctica i sempre que sigui possible, escollirem programari que puguem utilitzar gratuïtament.

Per això, utilitzarem el programari Avast Home Edition, que és gratuït per a un ús no comercial (com és el nostre cas), està traduït al català i es pot baixar gratuïtament des de l'enllaç següent:

http://files.avast.com/iavs4pro/setupcat.exe

Un cop l'haurem baixat, fem la instal·lació del programari fent dos clics a la icona del paquet de programari. En la primera finestra que apareix hi ha un missatge de benvinguda. Tal com veiem en la figura 1, el programari està traduït al català:

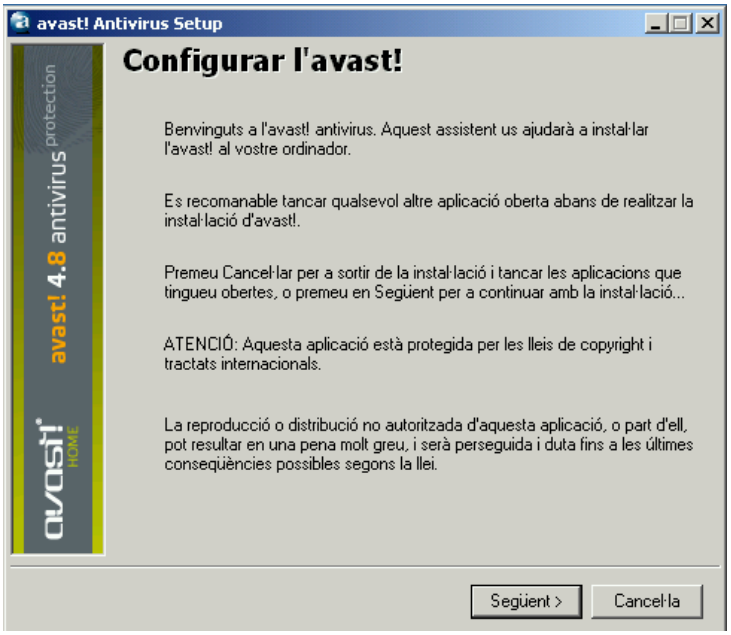

Figura1: Finestra de benvinguda al programa

Després de prémer el botó Següent >, ens surt un quadre de diàleg on podem llegir els requisits del sistema, que podem comprovar que són força baixos per a les versions més esteses del Windows, tal com mostra la figura 2:

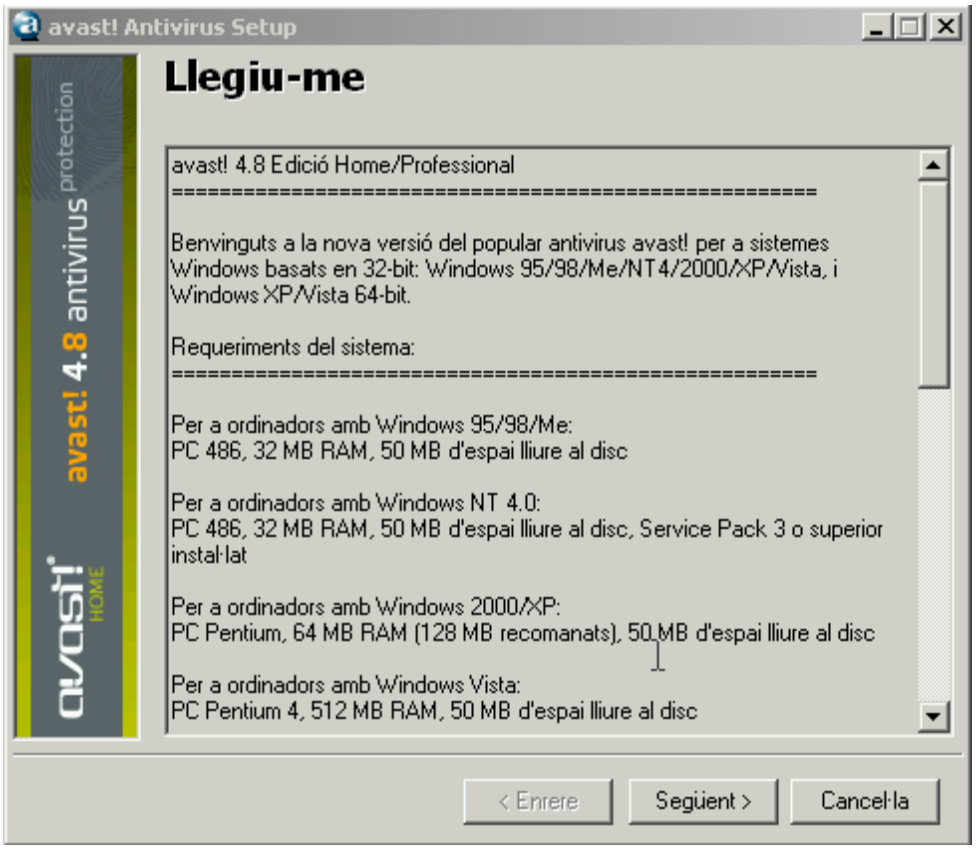

Figura 2: Requisits del sistema d'Avast Antivirus

Premem el botó Següent > i se'ns presenta una pantalla d'acceptació de la llicència d'utilització del programari, tal com veiem en la figura 3:

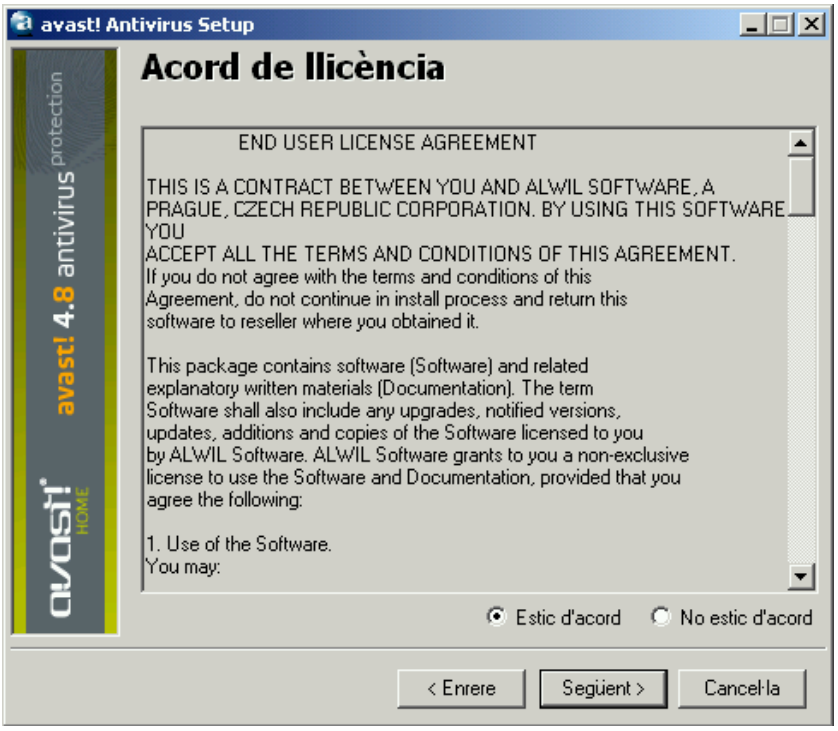

Figura 3: Pantalla d'acceptació dels termes d'ús del programari

Seleccionem el botó de radi Estic d'acord i premem el botó Següent >. Se'ns mostrarà un quadre de diàleg en què hem d'especificar el directori on volem instal·lar l'antivirus, tal com veiem en la figura 4:

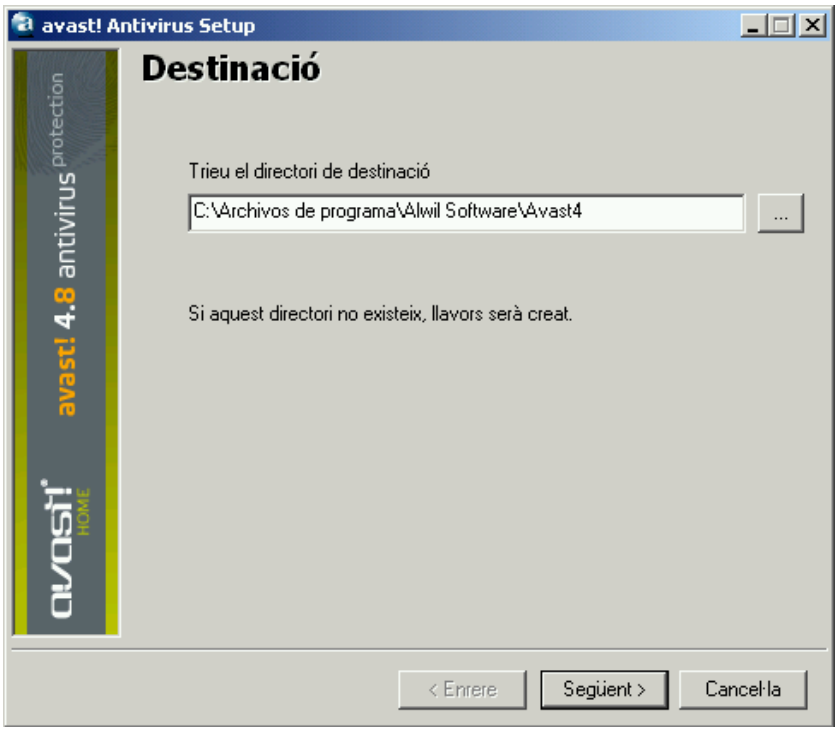

Figura 4: Quadre de diàleg de la localització de la instal·lació de l'antivirus.

Podem deixar l'opció per defecte i premem el botó Següent >, amb la qual cosa podem seleccionar els components que volem instal·lar, tal com veiem en la figura 5:

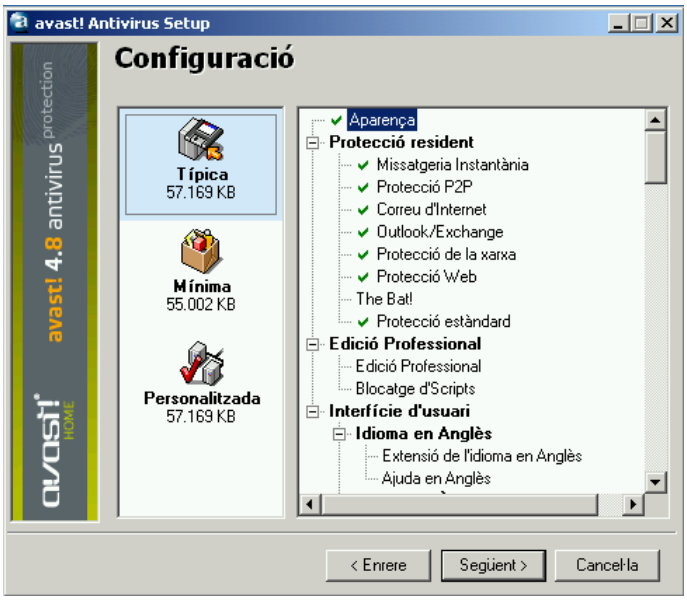

Figura 5: Opcions d'instal·lació d'Avast

En la figura 5 podem observar els tipus de protecció que ofereix aquest programari, que va més enllà dels virus tradicionals; també ens protegeix dels programes espia (*spyware*), que poden robar informació personal sense la nostra autorització, i llocs web que practiquen el *fishing*, que consisteix a simular pàgines web legítimes, per robar-nos informació confidencial (el DNI, el número de compte corrent, el número de targeta de crèdit…).

Tot i que hi ha programari específic per detectar els programes espia i els llocs web que practiquen el *fishing*, hi ha la tendència que s'acabin integrant tots en un sol programari *antimalware*, o que actua en contra del programari maliciós, localment en l'ordinador personal o mentre utilitzem una xarxa d'àrea local o Internet. En la figura 5 també podem triar una instal·lació mínima per a equips amb pocs recursos, o personalitzada si triem només els elements que volem.

Podem deixar l'opció per defecte Típica i prémer el botó Següent >, amb la qual cosa se'ns mostrarà una pantalla d'informació sobre les opcions d'instal·lació del programa, tal com veiem en la figura 6:

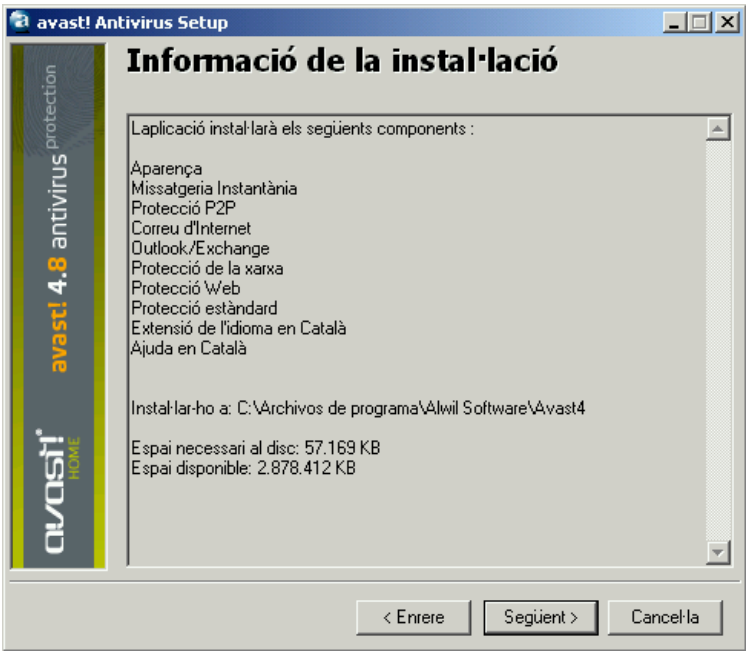

Figura 6: Finestra informativa amb les opcions de configuració de la instal·lació

Premem el botó Següent > i podem veure el procés d'instal·lació del programa, tal com veiem en la figura 7:

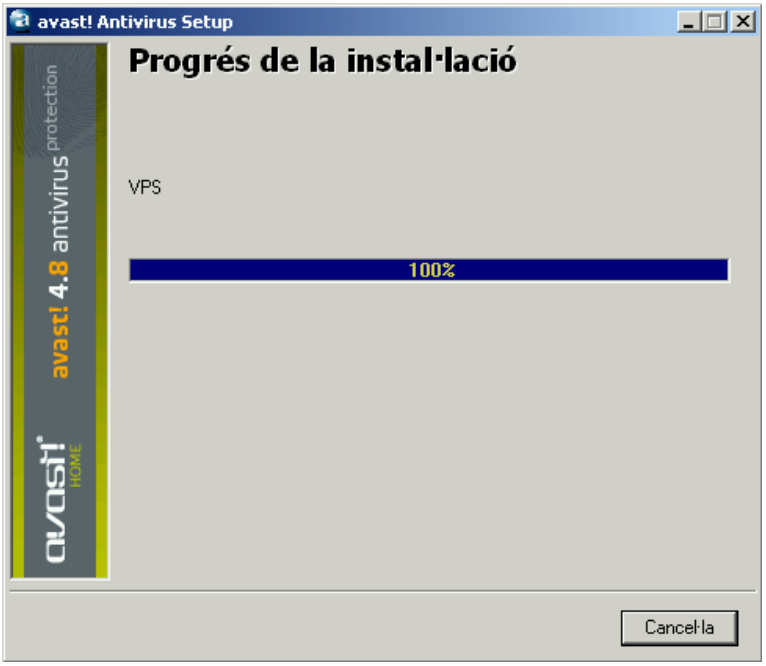

Figura 7: Procés d'instal·lació d'Avast

Un cop acabat ens apareixerà un quadre de confirmació on podem fer que el programari antivirus faci una cerca de virus i programari maliciós un cop es reinicïi el sistema després de la instal·lació, per tal d'assegurar-nos que el nostre sistema està net d'aquest tipus de programes. Ho podem veure en la figura 8:

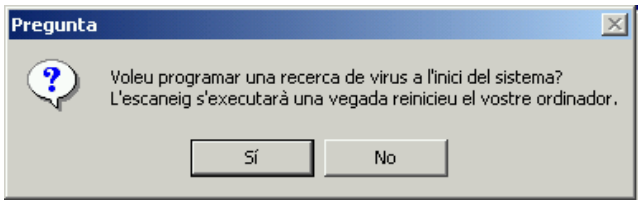

Figura 8: Quadre de confirmació d'una anàlisi del sistema després de reiniciar-lo

Si el sistema està acabat d'instal·lar podem obviar aquest pas; en cas que instal·lem l'Avast en un ordinador que fa temps que utilitzem seria aconsellable prémer Sí.

Un cop feta la selecció, el programa ens demanarà reiniciar el sistema per completar la instal·lació, tal com podem veure en la figura 9:

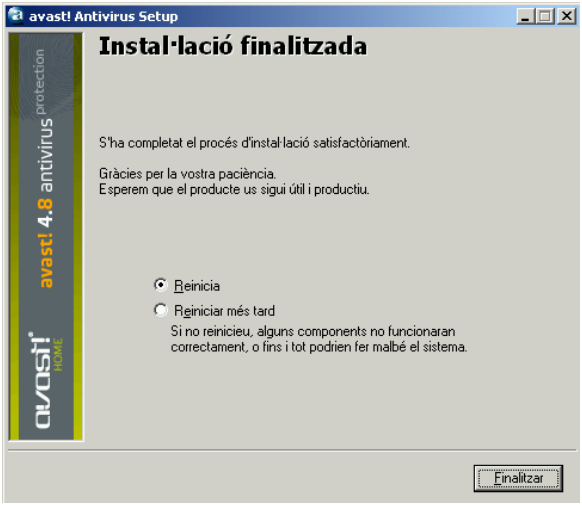

Figura 9: Quadre de diàleg de confirmació per reiniciar el sistema

Per completar la instal·lació seleccionem l'opció Reinicia. Un cop s'ha reiniciat el sistema, es mostra una pantalla informativa, on se'ns convida a fer el registre gratuït del programari. Aquesta opció evidentment és opcional, tot i que si registrem el programari podrem gaudir d'actualitzacions permanents. Ho podem veure en la figura 10:

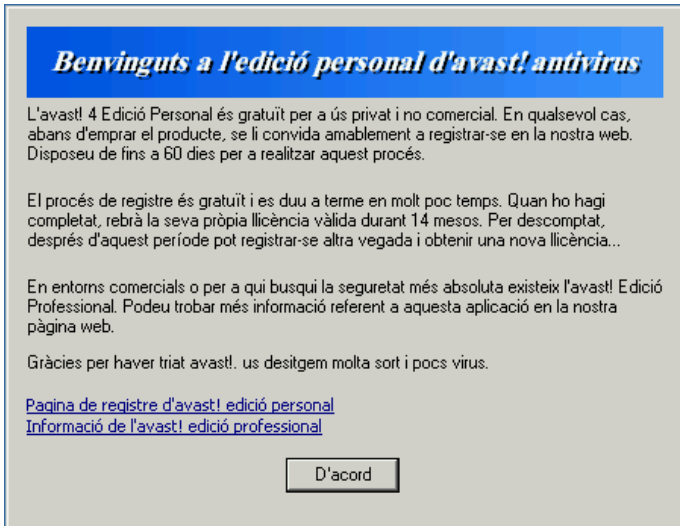

Figura 10: Finestra informativa sobre el procés de registre del programa

Premem *D'acord* i farem desaparèixer la pantalla de la figura 10. Podrem comprovar que el programa està instal·lat perquè afegeix dues icones (dues boletes blaves, l'una amb una *a* i l'altra amb una *f*), en l'àrea reservada pel sistema dins la barra de tasques. També podrem observar que el programa actualitza de manera automàtica la base de dades de virus, tal com veiem en la figura 11:

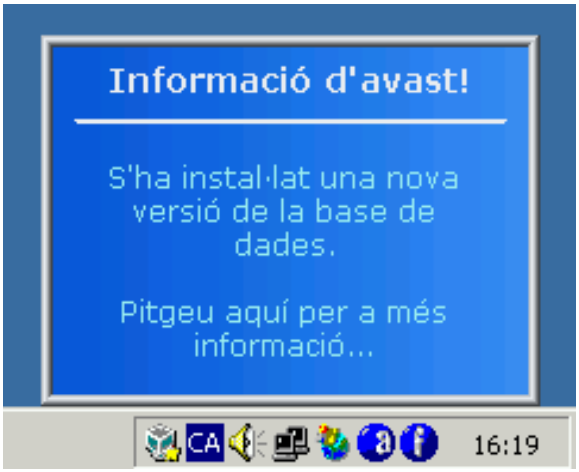

Figura 11: Àrea del sistema amb les icones d'Avast, i notificació de l'actualització del programa

Si fem dos clics a la icona en forma de bola amb la *a*, podem configurar el grau de protecció resident del programa, tal com veiem en la figura 12:

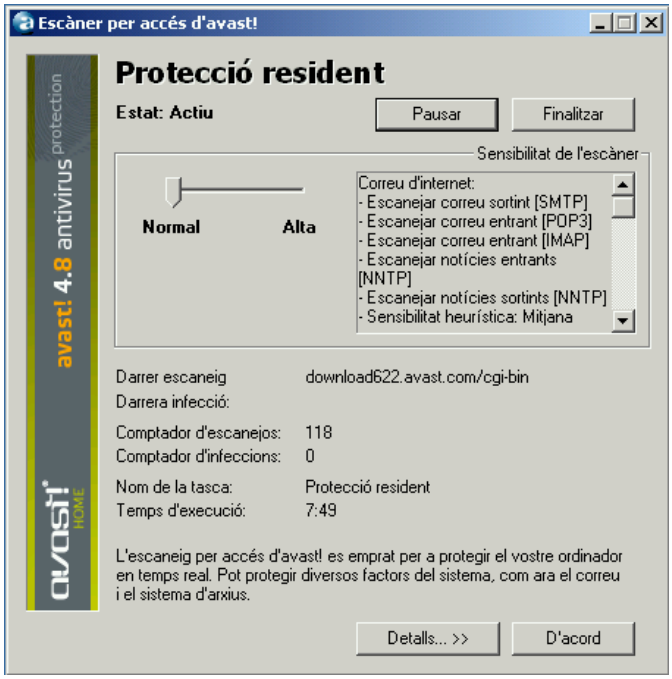

Figura 12: Configuració del grau de protecció resident d'Avast

Si premem el botó Detalls…>>, podem especificar el grau de protecció d'una manera més específica, tal com veiem en la figura 13:

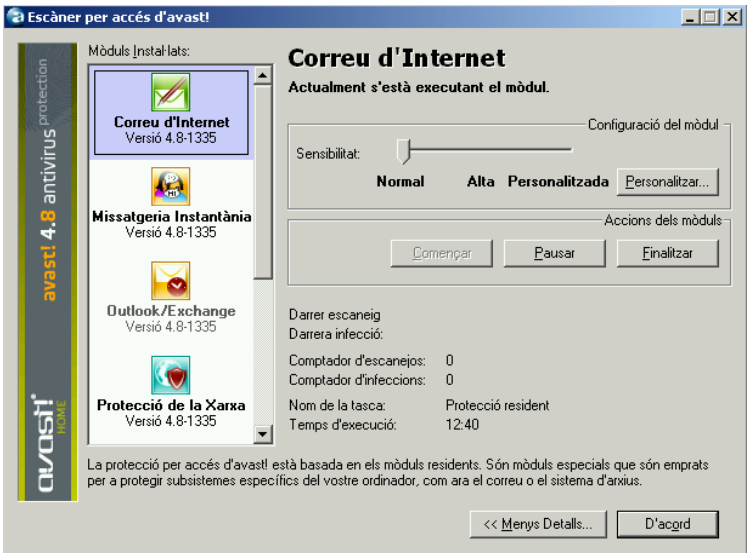

Figura 13: Grau de protecció del correu d'Internet

En aquesta primera opció podem triar el grau de protecció per al correu que consultem per mitjà d'Internet.

Podem especificar un nivell normal, un nivell alt o un nivell personalitzat.

També podem fer el mateix per a altres aspectes:

- Protecció durant la utilització de programes de missatgeria instantània (tipus *messenger*), en els quals de vegades usuaris ens poden enviar fitxers que contenen programari maliciós.
- Protecció *p2p*: ens protegeix quan baixem programari d'origen desconegut mitjançant xarxes *p2p* (per exemple, l'*emule* o el *torrent*).
- Correu d'Internet i *Outlook/exchange*: ens protegeix dels fitxers adjunts enviats mitjançant el correu electrònic que poden contenir programari maliciós.
- Protecció de la xarxa: evita que el programari maliciós envaeixi el nostre ordinador mitjançant una xarxa d'àrea local.
- Protecció web: evita que el programari maliciós envaeixi el nostre ordinador mentre estem navegant pel web.
- Protecció estàndard: ens protegeix dels virus informàtics més comuns.

A més d'aquesta protecció permanent, podem configurar altres aspectes del programa, si fem dos clics a la icona del programa sobre l'escriptori. El primer cop que fem això ens apareix un quadre de text en què podem escriure la clau de llicència del programari, que podem obtenir fent el registre gratuït a la web, tal com podem veure en la figura 14:

Figura 14: Quadre de text en què podem introduir la llicència del programa.

En cas que no ho vulguem, simplement premem el botó *Prova* i ens apareix una pantalla d'ajuda sobre les accions que podem dur a terme amb el programari Avast. Pot ser que hàgim d'aturar l'escaneig de l'ordinador. Ho podem veure en la figura 15:

Figura 15: Finestra informativa de les opcions bàsiques d'Avast

Un cop hem tancat aquesta finestra, podem accedir a la interfície del programa, tal com veiem en la figura 16:

Figura 16: Interfície principal del programa Avast

Premem el botó d'extracció situat a la part superior esquerra de la interfície i podem accedir a un menú desplegable on hi ha les opcions principals del programa.

La primera cosa que podem fer és triar quina àrea del sistema volem escanejar, especificant tots els discos durs, els mitjans extraïbles, o bé carpetes específiques. L'opció més segura és Tots els discos durs.

Ho podem veure en la figura 17:

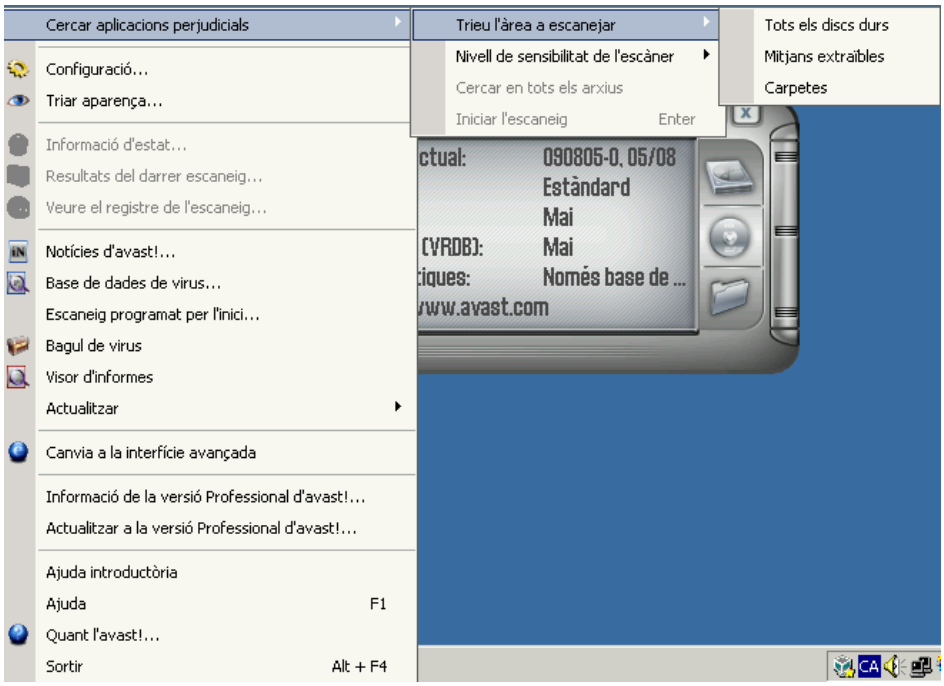

Figura 17: Selecció de les àrees que s'han d'escanejar.

En el menú desplegable hi ha diverses opcions trivials: triar l'aparença del programa, cosa que canviarà la interfície, rebre notícies sobre el programa Notícies d'avast!, obtenir ajuda, obtenir informació sobre l'aplicació i sortir del programa.

Si triem l'opció Configuració… podem triar diversos aspectes del programa, tal com podem veure en la figura 18:

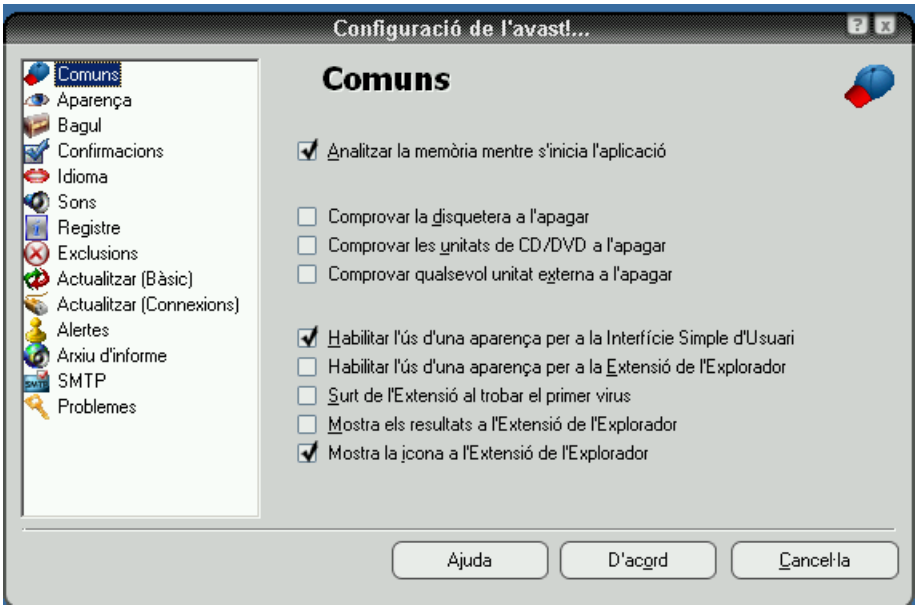

Figura 18: Aspectes comuns de la configuració del programa.

En aquest primer apartat podem especificar, clicant a l'opció corresponent, si volem analitzar la memòria quan s'inicia l'aplicació, si volem comprovar els mitjans extraïbles quan apaguem l'ordinador, si volem habilitar la interfície simplificada o si volem mostrar una extensió de l'explorador del Windows, que ens permeti escanejar un disc o carpeta, fent un clic amb el botó dret del ratolí sobre la icona corresponent en la finestra de l'explorador.

En l'apartat Bagul podem especificar la mida de l'espai reservat per desar fitxers que estan infectats o que són sospitosos (com una mena de quarantena). Ho podem veure en la figura 19:

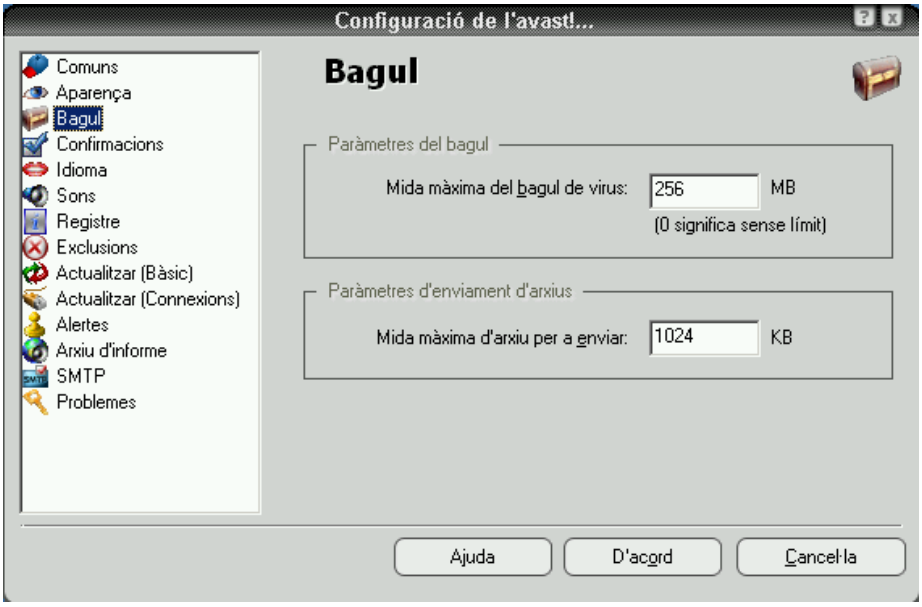

Figura 19: Quadre de diàleg en què podem especificar la mida del bagul de virus, i també la mida màxima d'arxius que podem enviar per Internet.

En l'apartat Confirmacions podem especificar en quins moments el programa ens demana confirmació per dur a terme una acció. En la figura 20 veiem que estan totes activades per defecte.

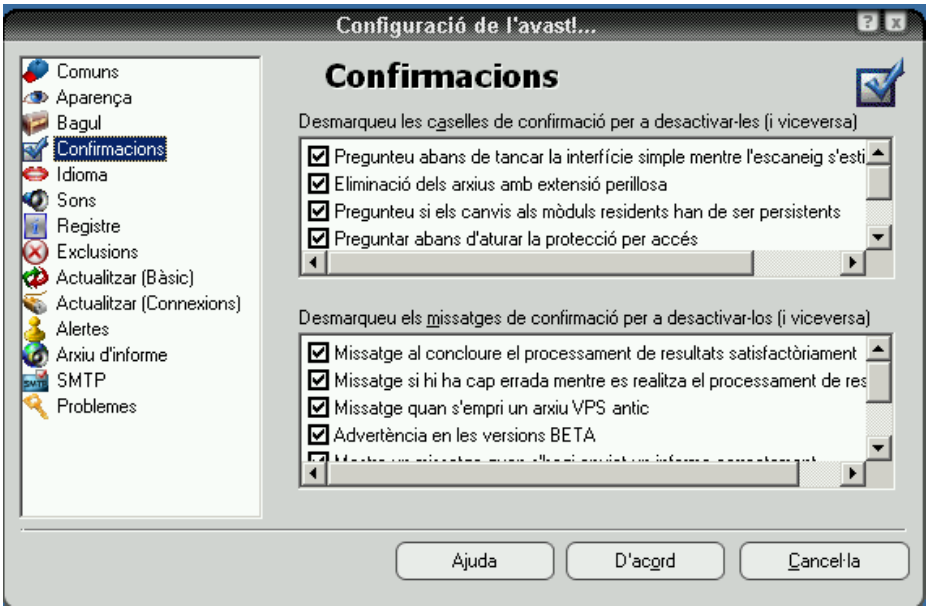

Figura 20: Opcions de confirmació

També podem desactivar els avisos sonors del programa, si els considerem molestos. Ho podem veure en la figura 21:

Figura 21: Si ho volem, podem desactivar els avisos sonors de l'Avast.

En l'opció Registre podem especificar la mida màxima dels fitxers de registre del programa, com veiem en la figura 22:

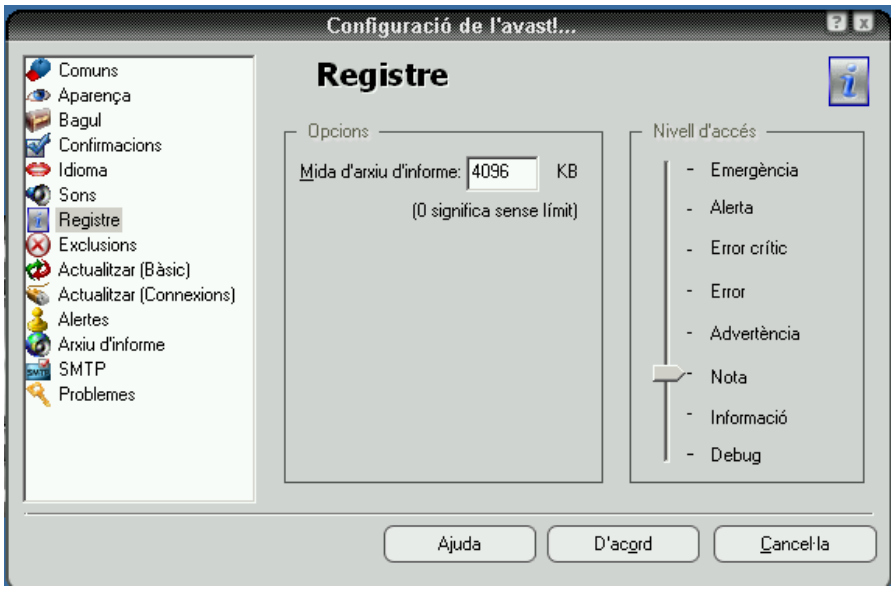

Figura 22: Mida màxima del fitxer de registre i opcions de configuració d'aquest

En l'opció Exclusions podem especificar quins fitxers, carpetes o unitats no volem que siguin analitzats en el procés d'escaneig. Ho veiem en la figura 23:

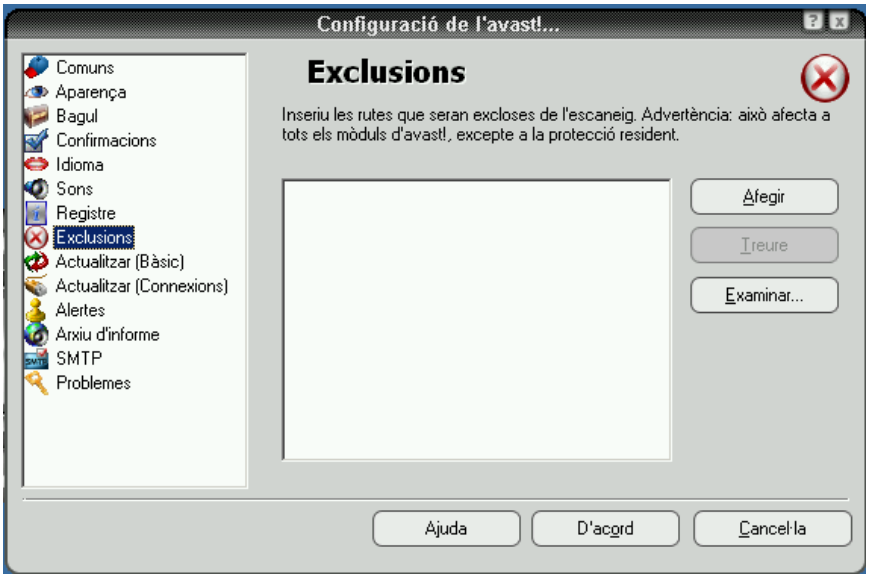

Figura 23: Opcions d'exclusió de l'anàlisi

En l'opció Actualitzar (Bàsic) podem activar o desactivar les actualitzacions automàtiques. Aquestes actualitzacions fan referència a la base de dades de virus, o bé al programa mateix.

En aquest tipus de programari és recomanable deixar activada l'actualització automàtica de la base de dades de virus, perquè així evitem que el programa no reconegui programari maliciós pel fet que disposi d'una base de dades obsoleta.

L'actualització del programa no es fa de manera automàtica per defecte, sinó que s'informa a l'usuari quan surt una versió nova, i se li dóna la possibilitat d'actualitzar. Ho podem observar en la figura 24:

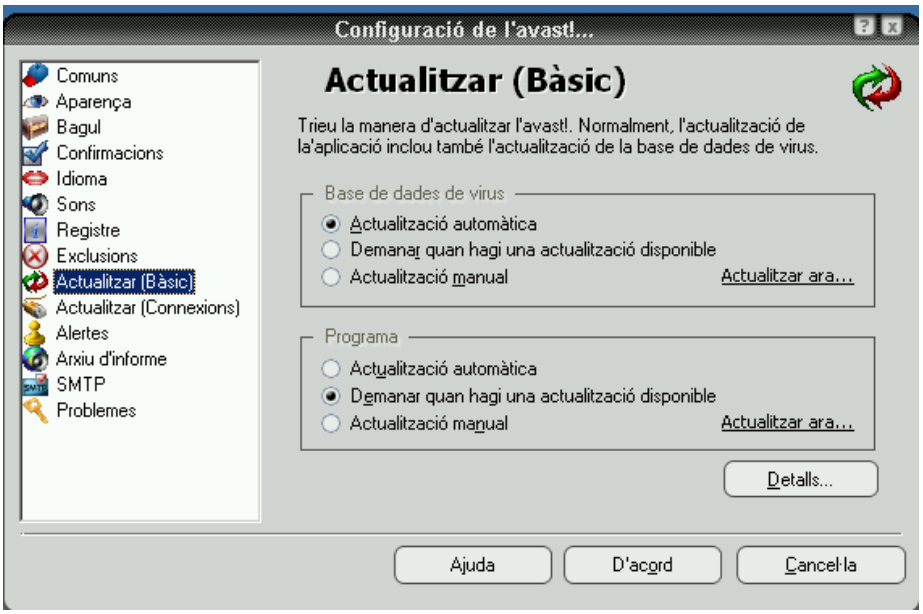

Figura 24: Opcions d'actualització del programa i la base de dades de virus

En l'opció Actualitzar (Connexions) podem especificar si ens connectem a Internet mitjançant un mòdem i podem configurar un servidor intermediari o *proxy* en cas que el fem servir. Ho mostra la figura 25:

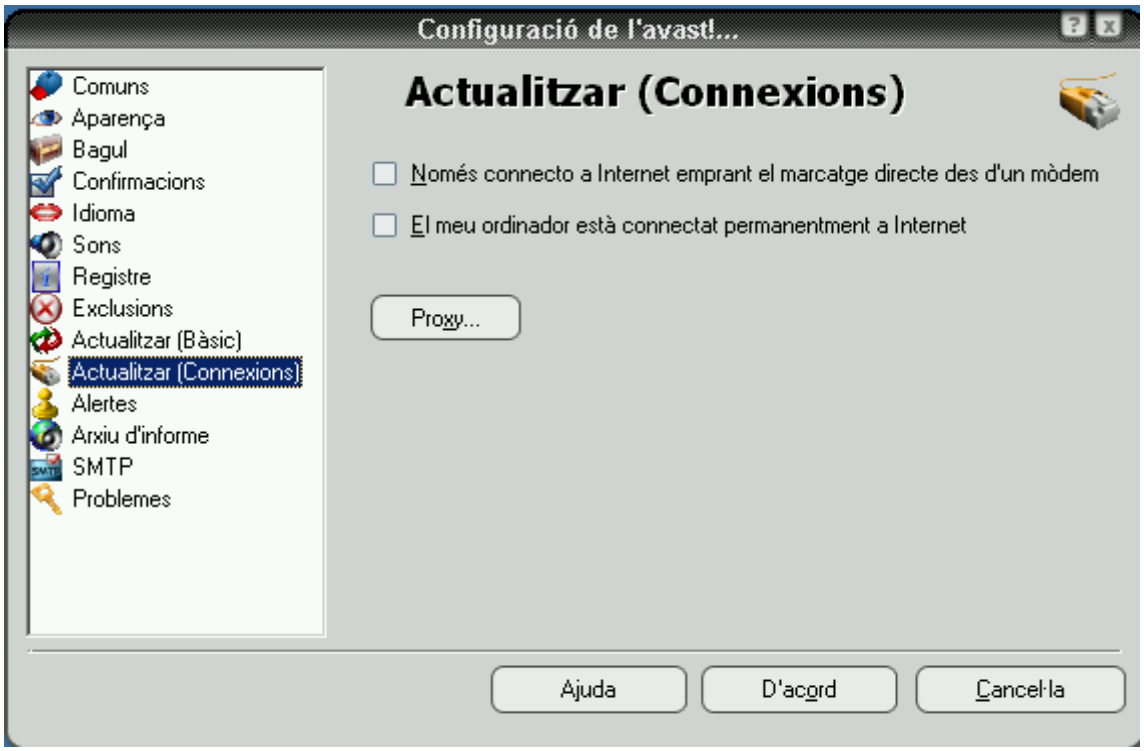

Figura 25: Opcions de configuració de la connexió a Internet per poder actualitzar el programa

En l'opció Alertes podem configurar com s'informarà a l'usuari que s'ha detectat un virus. Ho podem veure en la figura 26:

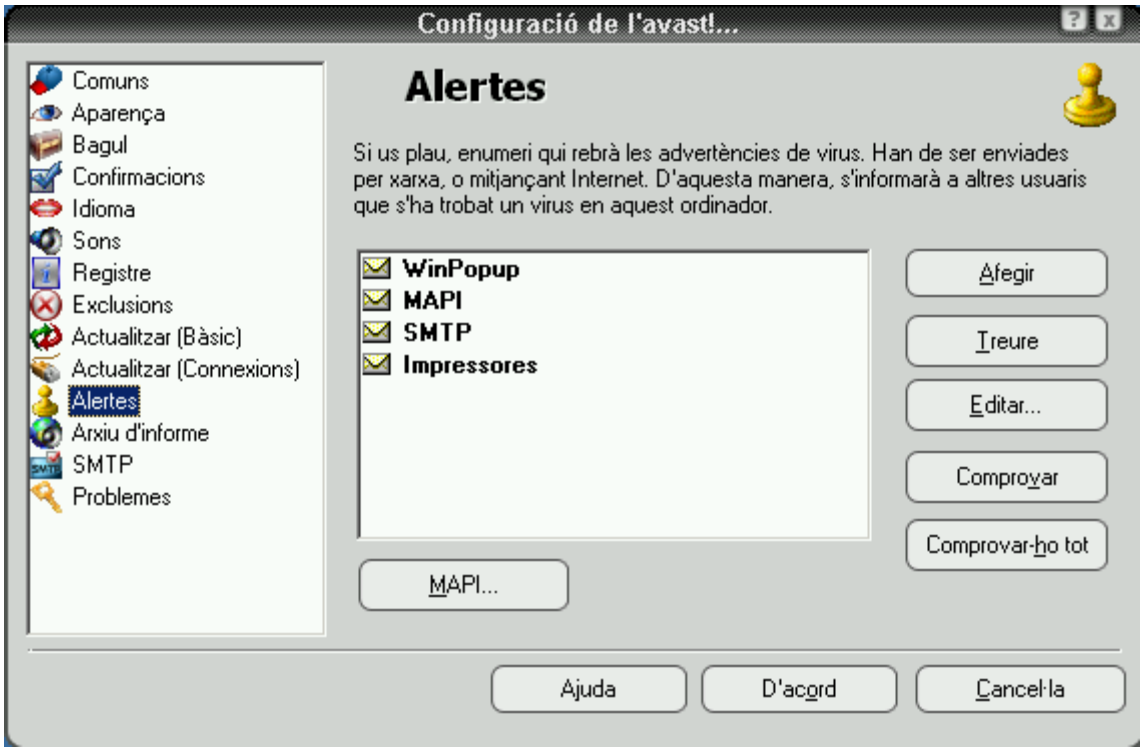

Figura 26: Configuració de l'enviament d'alertes de detecció de virus a l'usuari

Veiem que, per defecte, s'envia una alerta a l'usuari mitjançant una finestra emergent, i també podem configurar el programa perquè enviï alertes mitjançant correu o informes a la impressora.
En l'opció Arxiu d'informe podem activar la creació d'un arxiu on es desen els informes generats per l'aplicació activant l'opció corresponent. També podem canviar el format dels informes, que pot ser text (per defecte), o es poden generar fitxers XML, tal com mostra la figura 27:

Figura 27: Opcions de creació d'arxius d'informe

En l'opció SMTP podem configurar els paràmetres del servidor de correu mitjançant el qual enviem correus electrònics. Vegem-ho en la figura 28:

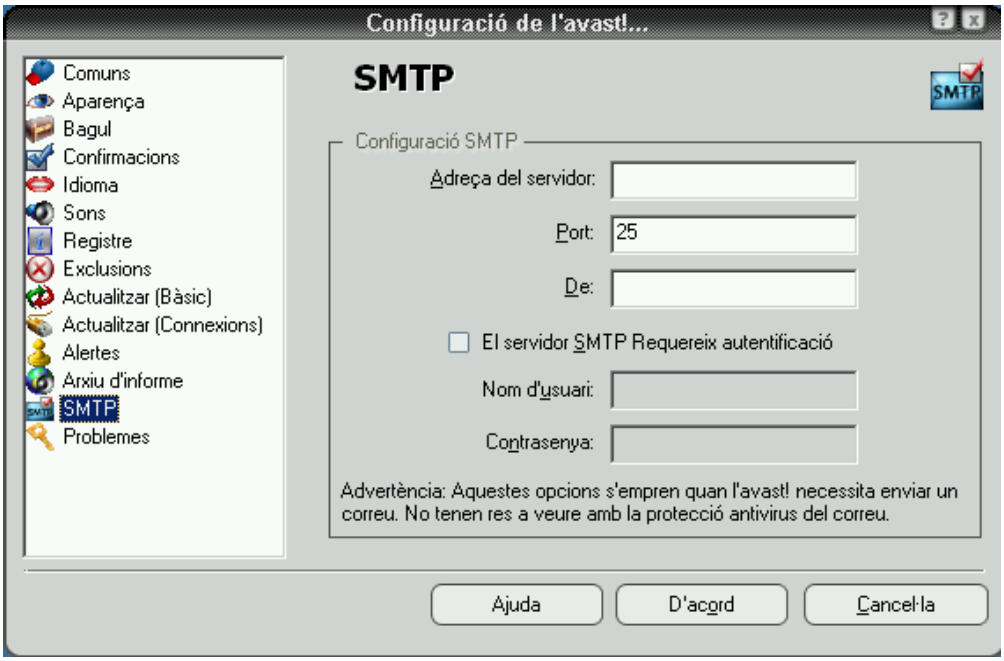

Figura 28: Opcions de configuració del servidor de sortida del correu electrònic

Finalment, en l'opció Problemes podem activar o desactivar opcions que ens permeten evitar problemes a causa de l'execució del programa, tal com veiem en la figura 29:

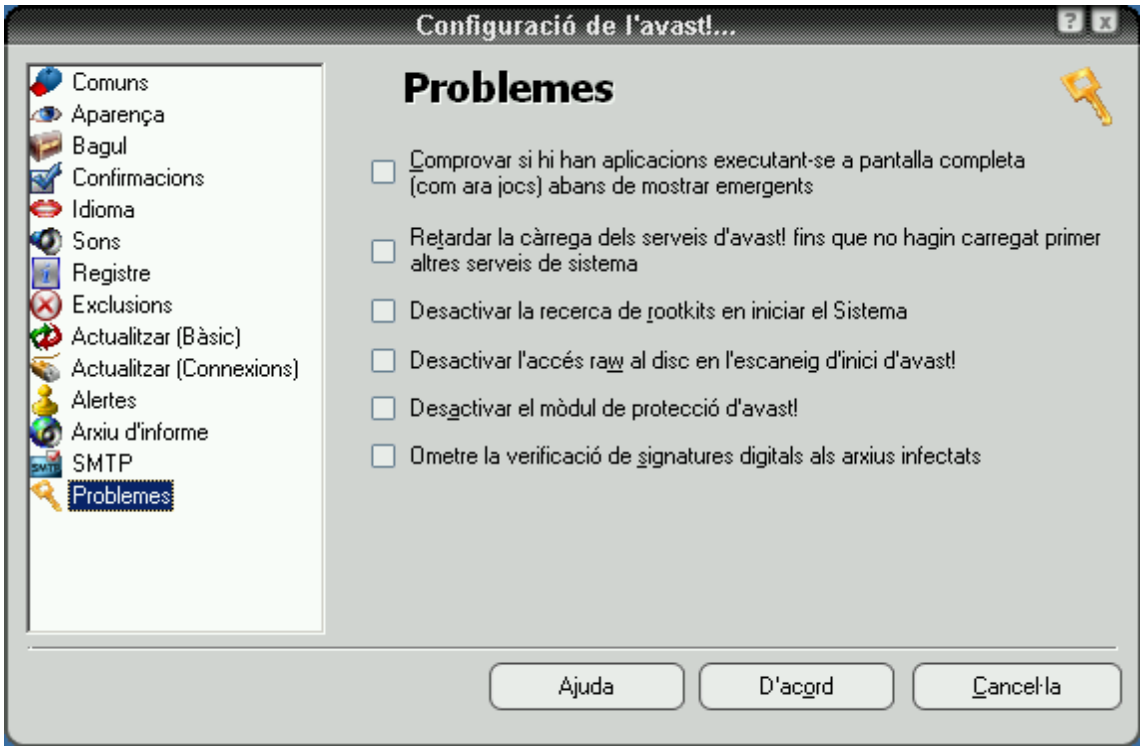

Figura 29: Opcions de configuració de l'Avast per evitar problemes en la seva execució

Un cop haurem configurat totes les opcions, i després de configurar les carpetes que volem analitzar, podem fer una anàlisi del sistema, prement el botó *play* de la interfície principal. Podem veure el procés en la figura 30:

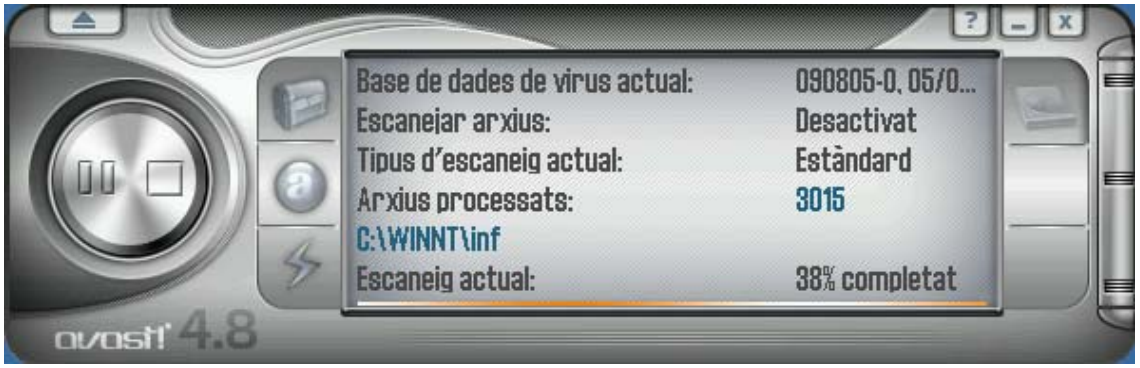

Figura 30: Procés d'anàlisi del sistema

Després d'haver acabat el procés d'anàlisi, si fem un clic al text Veure l'informe del darrer escaneig, dins de la interfície principal del programa, ens mostrarà una pantalla informativa del resultat del procés. Ho podem veure en la figura 31:

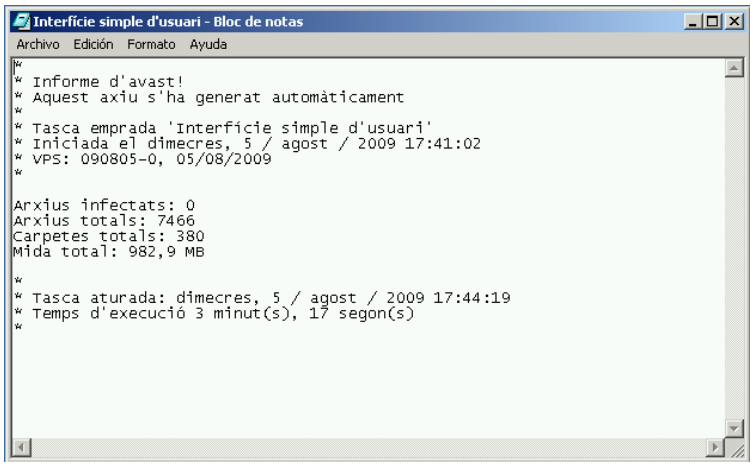

Figura 31: Informe de l'anàlisi del sistema

Si en la interfície principal del programa premem el botó Bagul de virus, podrem obrir la carpeta en què l'Avast guarda tots els fitxers infectats. En cas que n'hi hagi, ens permetrà eliminar-los. Ho veiem en la figura 32:

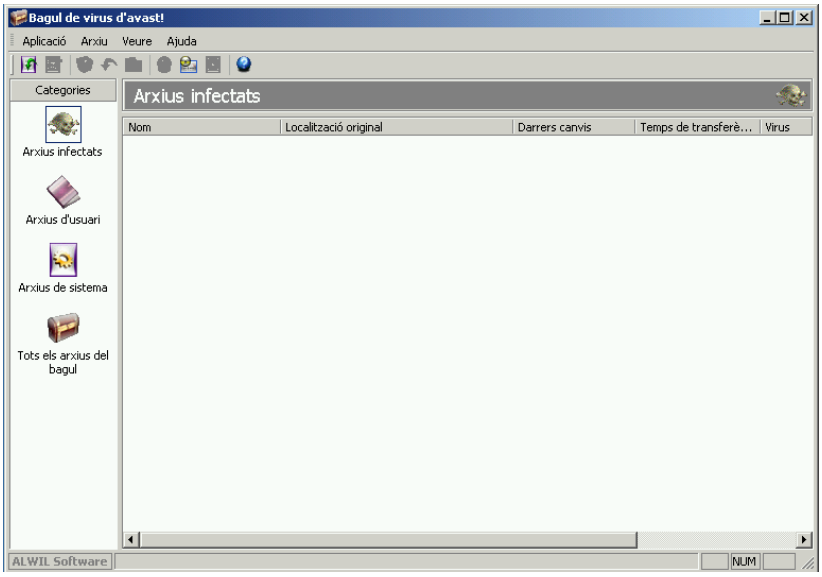

Figura 32: Bagul de virus, lloc on l'Avast desa els arxius infectats perquè no afectin la resta del sistema.

En la interfície principal, si premem el botó amb la *a* dins de la boleta, podrem configurar el grau de protecció que proporciona l'antivirus. Ho veiem en la figura 33:

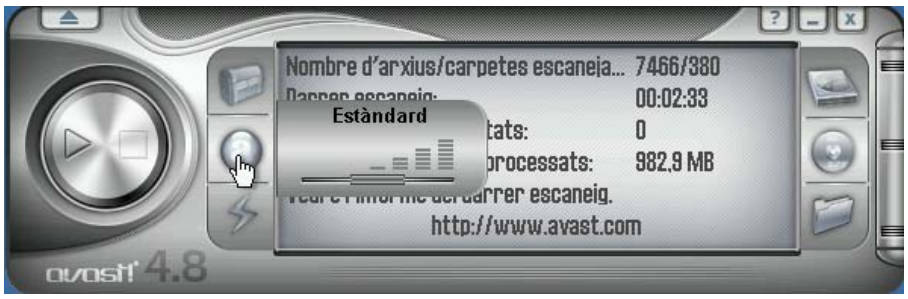

Figura 33: Grau de protecció de l'antivirus

Si premem el botó en forma de llamp (a sota del marcat en la figura 33), s'actualitzarà l'antivirus, i quan acabi se'ns mostrarà una pantalla informativa del procés d'actualització. Vegem-ho en la figura 34:

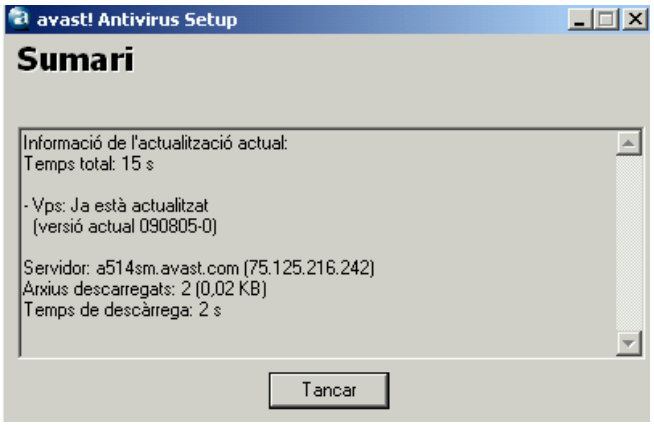

Figura 34: Resum del procés d'actualització de l'antivirus

Si premem el botó del disc dur, podem configurar el grau d'anàlisi dels discos durs, com veiem en la figura 35:

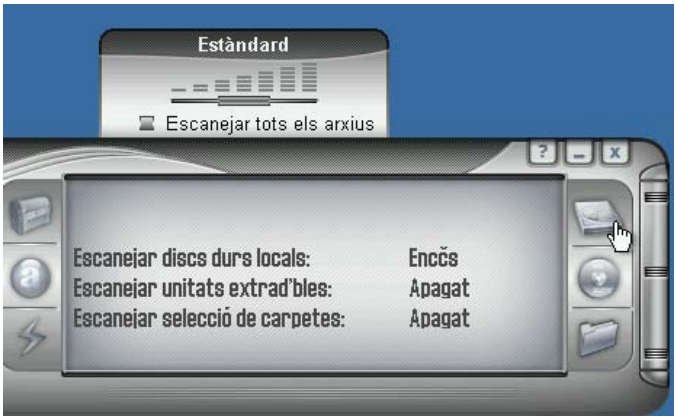

Figura 35: Grau d'anàlisi dels discos durs del sistema.

Prement el botó de sota, en forma de CD, podem activar l'anàlisi de disquets i CD o DVD, tal com podem veure en la figura 36:

Figura 36: Configuració de l'anàlisi dels disquets i les unitats òptiques

Finalment, si premem el botó en forma de carpeta, s'obre un quadre de diàleg en què podem seleccionar les carpetes que volem analitzar fent un clic en el quadre corresponent a la unitat. Ho veiem en la figura 37:

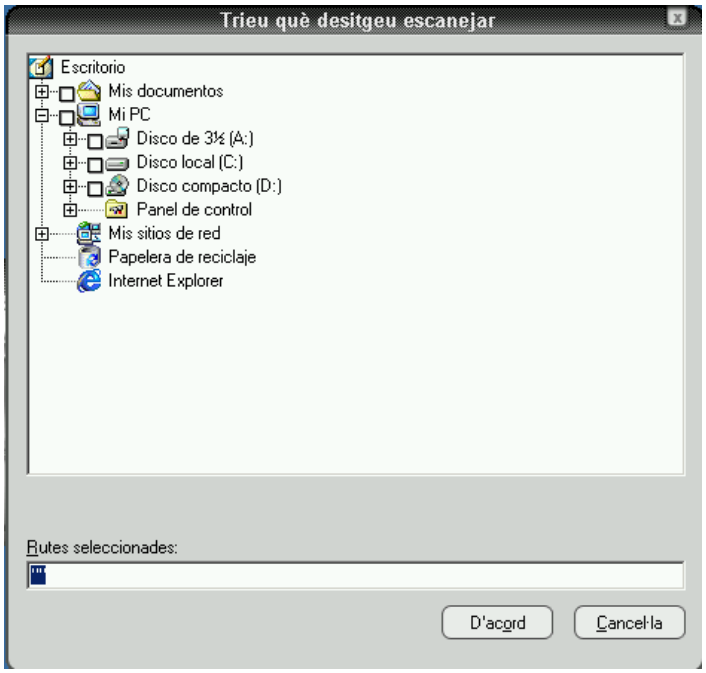

Figura 37: Selecció de les carpetes i unitats que volem analitzar.

Exercicis que ha de fer l'estudiant

- Instal·leu i configureu l'Avast de manera que faci una anàlisi de tots els discos durs del sistema. Adjunteu en un fitxer de text l'informe creat a partir d'aquesta anàlisi.

- Cerqueu informació a Internet sobre un altre programa Antivirus, si pot ser, gratuït, i analitzeu-ne les característiques i funcionalitats més importants i les diferències que té amb l'Avast.

Adreces d'interès

http://www.avast.com

Pàgina d'Avast Antivirus.