

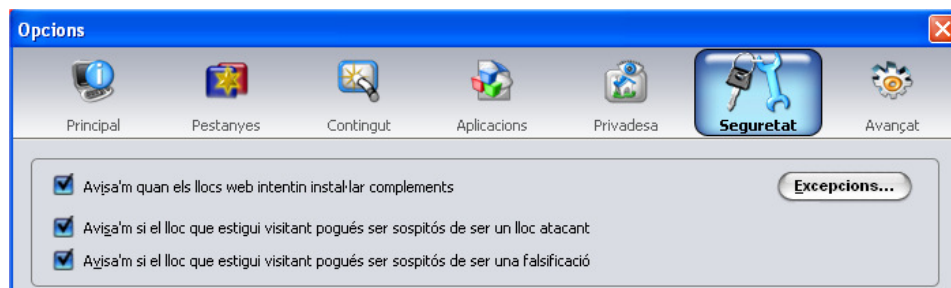
## Quins programes necessito per a que el meu ordinador sigui segur?

Tots els ordinadors haurien de tenir instal·lats dos tipus de programes, un antivirus i un antiespies. Trobareu a la secció d'*Ajudes i Manuals* de la web de celRas dos d'aquests programes gratuïts. Actualment hi ha paquets de seguretat que incorporen les dues funcionalitats com ara el *Norton Protection Center*. En la nostra opinió el millor antivirus de pagament que podeu instal·lar és el *NOD32* i el pitjor el *Panda*, el qual té la virtut de menjar-se tots els recursos de l'ordinador i alentir-lo substancialment.

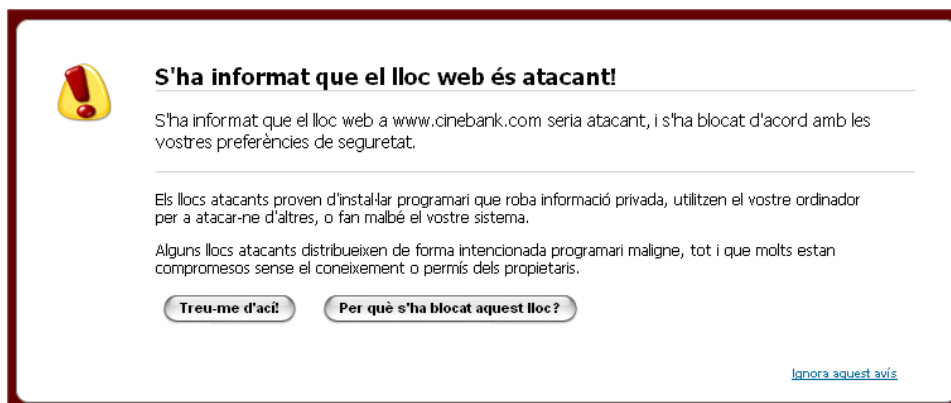


## Navegació encara més segura?

La millor manera de navegar de manera segura és utilitzar el Navegador *Firefox*, trobareu l'enllaç a la secció d'*Ajudes i Manuals* de la web de celRas. Dins a *Eines > Opcions > Seguretat* heu de marcar les opcions tal i com s'indica a la següent imatge:

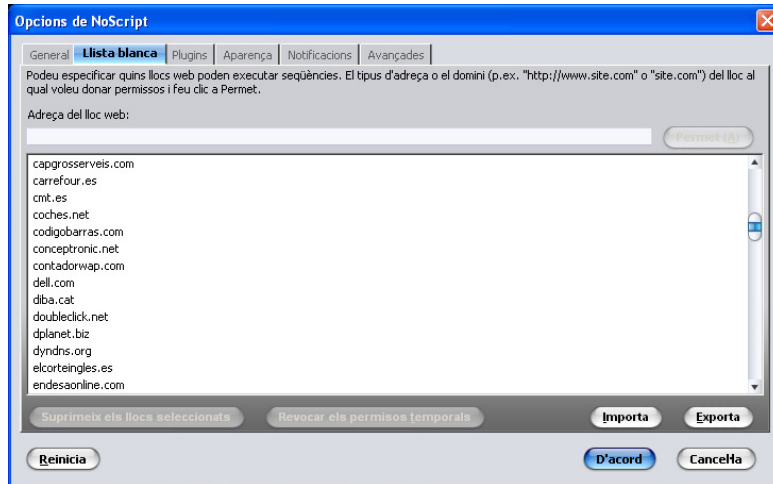


Això farà que el *Firefox* comprovi si els llocs a on esteu intentant accedir estan classificats com a llocs perillosos o no. En cas que el lloc sigui perillós us donarà un avís abans d'accedir-hi:





El Firefox és un Navegador que permet incloure extensions, és a dir petits programes que complementen les funcionalitats del propi Navegador. Una d'aquestes extensions és el *NoScript* el qual permet definir llistes blanques de llocs de confiança. **És sens dubte una extensió de seguretat imprescindible.** Per instal·lar-lo heu d'anar a *Eines > Complementos* a dins del *Firefox*.



Existeixen altres extensions de seguretat que us podeu instal·lar i que trobareu dins la secció de complementos.

## **Navego lent, per què?**

El 99% de les trucades o mails que ens parlen de lentitud en la navegació sempre tenen el mateix causant i la mateixa solució. El causant és un programa funcionant en algun dels ordinadors de l'usuari, la solució és parar o bloquejar aquest programa. Generalment aquest programa és un P2P (eMule, Azureus, Ares, etc.). Per tant, **quan vulgueu navegar més ràpidament heu de parar aquests programes.** Tingueu en compte que sortiu a Internet des de casa vostra per un únic punt (l'antena) i per tant tots els ordinadors de la casa van a buscar aquest punt. Això vol dir que tant se val quin sigui l'ordinador que té el P2P engegat perquè tots els ordinadors de la casa se'n veuran afectats.

L'usuari sol pensar que si el P2P només gasta 1 Mega i que si ell en té contractats 2, encara li queda 1 Mega per navegar. Per què no és així? Perquè aquesta no és una qüestió de sumes i restes sinó de peticions i recursos. Els programes P2P generen moltes peticions (connexions) per preguntar i intercanviar informació amb altres usuaris.



**El símil de la botiga:** Imagineu-vos una botiga on hi pot haver una cua de 100 persones. La persona del taulell pot anar despatxant a cada una d'aquestes persones i vendre-li una peça de roba. Al final del dia el calaix és ple. Però que passa si la meitat de les persones que estan a la cua només volen preguntar un preu? Al final del dia el calaix només és mig ple però la botiga ha estat funcionant igualment al 100%. Això mateix és el que passa amb els programes P2P i Internet.

Atenció, quan pareu els programes P2P fixeu-vos que no continuïn executant-se en mode ocult:



Ups! He parat l'Azureus però continua executant-se!

Tractament a part té el programa *Ares*. L'*Ares* és un programa P2P molt agressiu que continua treballant malgrat l'haguem parat. L'única manera de parar-lo és desinstal·lar-lo. No obstant, sense arribar a desinstal·lar-lo el podem bloquejar a través del *Firewall* del *Windows*. Anem a *Mi PC > Panel de Control > Firewall de Windows > Excepcions* i desmarquem l'*Ares*. D'aquesta manera l'*Ares* està bloquejat mentre volem navegar. **Des d'aquí us recomanem que no feu servir l'*Ares* en un ordinador on hi tingueu dades importants.**



Tot el que aquí s'ha dit sobre P2P i navegació és igualment aplicable al correu, xat, messenger, etc. Totes les aplicacions aniran més ràpides si en aquell moment teniu els P2P parats o bloquejats. També penseu que per terme general us haureu d'esperar uns minuts a que el Router que us fa de receptor quedi buit de tota aquesta porqueria que generen els P2P.

Des d'aquí us informem que els programes P2P s'han de fer servir segons les lleis de Propietat Intel·lectual i el Codi Penal vigent.

### **En resum, què haig de fer?**

Sempre en la nostra opinió, hauries de:

1. Instal·lar un Antivirus i Antiespies o un paquet que inclogui les dues coses.
2. Navegar amb el *Firefox* amb el *NoScript* instal·lat.
3. No utilitzar els programes P2P quan realment necessitis l'ordinador.
4. No tenir instal·lat l'*Ares* a no ser que sigui imprescindible.
5. Tenir sempre activat el *Firewall* del *Windows* i anar amb compte amb les excepcions.
6. Només redireccionar ports si és necessari (teniu un document que en parla a la web).

I recordeu que tot això no és garantia de res.