El manteniment del vostre sistema informàtic

30/11/2015
Autor/a: José M. Pérez i Associació per a Joves TEB

El manteniment del vostre sistema informàtic

30/11/2015
Resum:
Un ordinador necessita un manteniment adequat. Existeixen diverses eines per tenir l'ordinador com si fos nou. Algunes d'aquestes eines són de programari lliure i gratuïtes.

ÍNDEX

És el nostre Sistema Operatiu infal·lible?

Per què necessito un programa antivirus?

Spyware, malware i adware

Les aplicacions

Les còpies de seguretat

És el nostre Sistema Operatiu infal·lible?

La resposta, sigui quin sigui el nostre sistema operatiu, és NO. **El Sistema Operatiu no és més que un altre programa i com a tal pot tenir errades i forats de seguretat**. Els desenvolupadors dels sistemes operatius comproven diàriament les incidències detectades i si troben que alguna pot afectar al rendiment del sistema o a la seguretat del mateix, posen un pedaç ("parche") que no és més que un nou codi que substitueix el codi erroni i soluciona la incidència.

Quan es detecta un forat de seguretat qualsevol persona malintencionada pot intentar explotar-lo en el nostre sistema. Si no hem actualitzat el nostre sistema amb el pedaç corresponent restem totalment vulnerables i, si el forat de seguretat és crític, podran controlar totalment el nostre ordinador i no podrem fer res per evitar-ho. **És per això que hem de comprovar periòdicament si hi ha pedaços de seguretat o de millora a la plana web del nostre sistema operatiu.**

Avui en dia els Sistemes Operatius més generals com Windows, OS/X i GNU/Linux, disposen d'un sistema d'avisos per actualitzar els pedaços de seguretat que van sorgint. Tal i com hem dit, és molt important que actualitzeu els pedaços de seguretat.

Per què necessito un programa antivirus?

Els programes antivirus **ens ajuden a protegir el nostre sistema** d'altres programes malintencionats "coneguts" que denominem virus. Aquests programes, els virus, fan ús de qualsevol tàctica per instal·lar-se al nostre ordinador, com per exemple adjuntar-se al correu electrònic, camuflar-se en un altre programa, explotar vulnerabilitats del sistema...

Heu de ser conscients que amb la instal·lació d'un bon programa antivirus fareu un gran salt en la seguretat del vostre sistema, però encara heu de fer més feina. El software antivirus només us protegeix dels virus coneguts i identificats fins al moment (lògicament, no ens pot protegir de coses desconegudes). Per tal que la seva protecció continuï sent eficaç és necessari **actualitzar les seves bases de dades** incorporant els nous virus apareguts i la "vacuna" contra els mateixos**.** Per sort, la majoria dels antivirus **incorporen un sistema d'actualització automàtica** que posa al dia el nostre programa sense la nostra intervenció. És molt important ser conscients d'aquesta actualització automàtica i comprovar que s'està efectuant de manera correcta, ja que si no ho fem, estarem exposats als milers de virus que surten cada setmana. La instal·lació d'un antivirus i la seva actualització diària és la millor manera de protegir el nostre sistema dels virus i d'evitar que aquests infectin més ordinadors.

Per Windows existeix Clam Free Antivirus, una eina de programari lliure que funciona molt bé i s'actualitza constantment. Una altra eina de programari lliure per Windows és Clam AV, amb un rendiment prou bo. També existeixen AVG i Avast, en versió lliure i de pagament.

Tot i que a GNU/Linux no hi han gaires virus, és molt recomenable tenir un antivirus instal·lat en el vostre sistema. Una de les propostes que us fem, és Clam AV, què és de programari lliure i està instal·lat en molts servidors. ESET NOD32, Avast i AVG, també disposen d'antivirus per GNU/Linux.

El sistema operatiu de Mac, OS/X, encara que estigui basat en un sistema UNIX, també està exposat a les amenaces dels virus. Algunes de les eines antivirus més interessants per Mac són: Avira for Mac, ClamXav2 i ESET.

Spyware, malware i adware

Què són, què fan i com els puc prevenir?
En una primera definició que englobi spyware, malware i adware podríem dir que són programes que realitzen tasques sense el nostre consentiment i fora del nostre control. Aquests programes poden **espiar les vostres dades**, mostrar publicitat no volguda, alentir el vostre sistema i realitzar canvis en la vostra configuració. A més a més, **solen ser molt difícils de desinstal.lar** del vostre sistema, per això el millor que podem fer es prevenir-los.

El **malware** o també anomenat software malintencionat són aquells programes que tenen com a objectiu infiltrar-se al vostre ordinador **amb finalitats molt diverses.** Un malware pot ser des d'un troià fins a un "spyware".

L'**adware** és qualsevol programa que automàticament i sense el vostre consentiment **executa o ens mostra publicitat** mentre fem ús del vostre ordinador. Pot aprofitar que feu qualsevol recerca per mostrar-vos publicitat relacionada amb la vostra recerca amb finalitats comercials.

Els **programes espia o spyware** són els més perillosos de tots, ja que a banda de fer tasques no desitjades i d'alentir el nostre sistema, **recopilen informació personal** o sobre les vostres accions i l'envien a tercers. Aquesta acció, enviar la vostra informació personal, posa en perill la vostra seguretat ja que pot enviar configuracions, contrasenyes de sistema, del correu electrònic i, fins i tot, bancàries i el mateix enviament fa ús del vostre ample de banda amb la qual cosa es pot veure afectada la velocitat de connexió a Internet.

La majoria dels antivirus detecten i eliminen els programes més perillosos d'aquest tipus, però no tots. Existeixen programes específics destinats a la recerca i destrucció de malware, spyware i adware.

Per sistemes Windows disposeu del Search and Destroy Spybot, un programa bastant complet i fàcil de fer funcionar. També recomanem el CCleaner, que us facilitarà la neteja de malware, spyware i també **d'arxius temporals i programes** que fa temps que no feu servir.

Per a sistemes GNU/Linux, el mateix sistema ja impossibilita que el «malware» pugui desenvolupar-se. Això és degut a què el sistema de permisos de GNU/Linux **està molt més desenvolupat que Windows**, i per això no permet l'expansió d'un «malware». De totes formes, els mateixos paquetsESET NOD32, Avast i AVG per GNU/Linux, afegeixen una capa de seguretat contra els programes malware.

Tot i que els sistemes Mac, tenen una base UNIX, malauradament pateixen de programes «malware». Però per sort, també existeixen programes que eliminen aquests programes maliciosos. Alguns d'aquests programes ja venen inclosos en paquets antivirus com Avira. Altres programes, com «MalwareBytes for Mac», compleixen amb l'objectiu d'eliminar arxius «malware».

Les aplicacions

També és molt important pel rendiment del nostre ordinador **mantenir les nostres aplicacions al dia.**

Ara que ja tenim el nostre Sistema Operatiu actualitzat i els nostres detectors de virus, spyware, malware i adware també actualitzats, hem de fer un pas més: mantenir les nostres aplicacions al dia. La primera cosa que hem de tenir clar és que si no fem servir algunes aplicacions o aquestes han quedat obsoletes les hem de desinstal·lar del nostre ordinador. Només ocupen espai i fan el sistema més vulnerable. Una fallada d'una aplicació obsoleta i/o deficient pot fer molt mal al nostre sistema.

Una vegada sabem que comptem amb les aplicacions que necessitem, hem d'assegurar-nos periòdicament que les tenim actualitzades. La raó és ben senzilla:

1.- Si tenim les aplicacions actualitzades estarem gaudint dels últims avanços que els desenvolupadors han incorporat.

2.- S'hauran corregit totes les deficiències o bugs detectats fins al moment.

3.- També s'hauran corregit els forats de seguretat que l'aplicació pogués tenir.

No hem de confondre actualitzar amb comprar o adquirir nous programes. Si el fabricant treu una nova aplicació més completa però que té un cost afegit, haurem d'estudiar si realment la necessitem o si amb la que tenim instal.lada ja en tenim prou. No obstant, encara que treguin noves versions, els desenvolupadors estan obligats a mantenir durant un cert temps les seves aplicacions anteriors, sobretot si es troben bugs i/o forats de seguretat.

Les còpies de seguretat

El pas més important és **fer còpies de seguretat!**

No n'hi ha prou amb tenir el nostre sistema al dia, és totalment necessari que fem còpies de seguretat regularment. Pensem que si hem seguit totes les indicacions anteriors tenim el nostre sistema protegit contra les amenaces conegudes però cada dia en surten de noves i, encara que les actualitzacions surten molt ràpidament, no existeix un sistema cent per cent protegit. A més de les amenaces, també hem de prevenir altres possibles incidències com ara avaries del hardware, accidents i, evidentment, les nostres pròpies accions que, per error, ens poden fer perdre els nostres arxius més importants.

En fer les còpies de seguretat hem de decidir si únicament fem còpia dels arxius que nosaltres hem generat (documents, fulls de càlcul, fotos, etc.) o si bé fem còpia de tot el sistema (programes, configuració, sistema operatiu, etc.). **Existeixen diferents tipus de còpia de seguretat que ens permeten estalviar temps i espai (còpia completa, incremental, diferencial) i també disposem de diferents sistemes per fer la nostra còpia, entre ells, cintes, DVD, cartutxos i, fins i tot, còpies de seguretat online.**

És molt recomanable fer una còpia de tot el nostre sistema almenys una vegada al mes, així si hem de recuperar el nostre ordinador després d'un accident ho aconseguirem en un termini raonable de temps. El que sí és IMPRESCINDIBLE és fer còpia de seguretat de les nostres dades almenys una vegada a la setmana (idealment l¿hauríem de fer diàriament), perquè si patim un accident i no tenim una còpia, haurem perdut totes les dades i en conseqüència tot el nostre treball.

Per últim, hem de recordar que les organitzacions que treballen amb dades de caràcter personal (pràcticament totes) estan obligades per la Llei Orgànica de Protecció de Dades a fer còpies de seguretat.

Etiquetes: programari lliure

URL d'origen: https://xarxanet.org/informatic/recursos/el-manteniment-del-nostre-sistema