Guía de seguridad en Mac OS X 10.4 Tiger

Por Thinking different para Macuarium.com

Introducción

Como sabemos, Mac OS X es el sistema más seguro que existe, por sus raíces UNIX y su diseño, pero como cualquier sistema, si no tenemos unos mínimos cuidados puede ser vulnerable.

Esta pequeña guía no pretende ser la *Biblia* de la seguridad en Mac OS X, sino unos pequeños consejos para mantener nuestra seguridad y privacidad a buen recaudo.

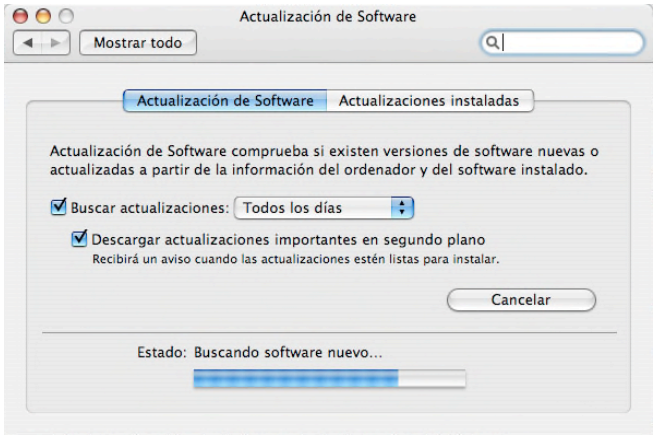
1.- Protección antivirus

Para Mac OS X apenas hay virus y los que hay suelen pedir confirmación para ejecutarse, pero aún así nuestros Macs no son invulnerables a los virus y además pueden ser un medio de transferencia para los virus pensados para Windows. Por este motivo es recomendable tener un software antivirus instalado. Aunque, a día de hoy, en Mac OS X con tener sentido común es suficiente. Además tienes que tener en cuenta que el antivirus ha de estar actualizado, sino, no sirve de nada ya que no puede detectar los virus más actuales.

Bien es verdad que muchos usuarios del Mac no hacen uso de software antivirus por la escasez de virus diseñados para nuestra plataforma y nunca les ha pasado nada, pero nunca estamos libres de nuevas apariciones de software maligno, como ocurrió hace poco tiempo con el caballo de Troya Leap-A. Por esto es necesario ser cuidadoso con los siguientes aspectos:

1.1.- Instalar siempre las actualizaciones del sistema operativo

Apple, cada cierto tiempo, proporciona actualizaciones del sistema operativo, en forma de actualizaciones mayores o actualizaciones de seguridad, que en cualquier caso, incluyen mejoras al sistema en todos los ámbitos. Ambos tipos de actualizaciones se encuentran disponibles en `Actualización de Software` de nuestro Mac (puedes encontrarlo en el menú Manzana). Para evitarte la tarea de tener que buscar periódicamente las actualizaciones, puedes activar la actualización automática en el panel `Actualización de Software` de `Preferencias del Sistema`.



1.2.- Sentido común

Esa es una parte importante para mantener un sistema seguro, el sentido común, y es que tener cuidado al abrir o descargar ficheros, leer correos o evitar navegar por páginas sospechosas son medidas más eficientes que tener el mejor antivirus instalado en nuestro sistema.

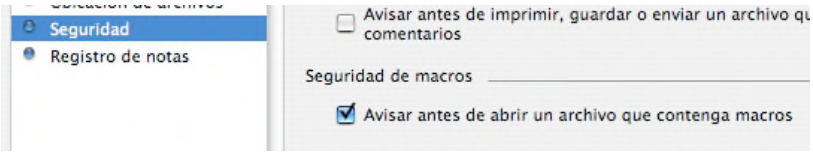
Es muy importante abrir ficheros de fuentes seguras, por ejemplo, hace no mucho tiempo apareció en las redes P2P un paquete de Microsoft Office 2004 (que pesaba 1MB, por lo que ya

debemos sospechar) que contenía un virus, confiamos en la instalación dando nuestro consentimiento con la clave de administración y... podemos ir despidiéndonos de nuestros datos.

Por ellos, este apartado es sin duda, el más importante para mantener seguro un sistema operativo. Es fundamental no confiar en ningún fichero que no nos llegue de fuente conocidas (y ni siquiera eso, porque podemos ser víctimas de virus de amigos nuestros que se propaguen por el correo, por ejemplo).

1.3.- Virus de macro

Así es como se conocen a los virus que utilizan las capacidades de macro de Microsoft Office. Estos virus son especialmente peligrosos por que son multiplataforma. Microsoft, en las últimas actualizaciones de Office X y 2004, ha hecho que Office avise al abrir un documento que contiene macros. La imagen corresponde a las preferencias de Word 2004:

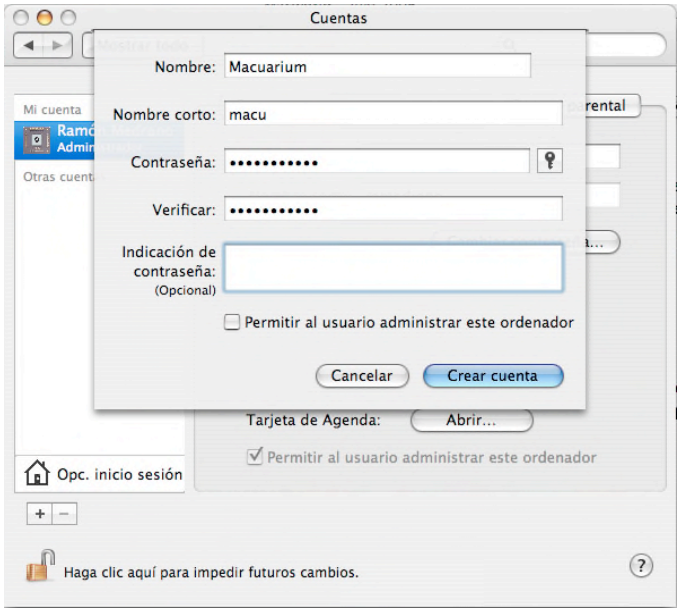


1.4.- Y Windows, ¿qué?

Desde la aparición de soluciones de emulación como Virtual PC, hasta el advenimiento de los Macs con corazón Intel con Boot Camp y soluciones de virtualización como Parallels podemos ejecutar Windows en nuestros Macs y esto, hace vulnerable a nuestro Mac ante todas las amenazas para Windows. Por ello es necesario que mantengas Windows actualizado, cuentes con un buen antivirus y uses algún firewall.

1.5.- Usa una cuenta limitada

Para el uso diario del Mac, es conveniente usar una cuenta sin privilegios de administración, esto impide que determinados programas tengan acceso a partes privilegiadas del sistema. Puedes crear una nueva cuenta en `Preferencias del Sistema / Cuentas`:



2.- Protección de la privacidad

La privacidad es algo muy importante a la hora de mantener seguro un sistema informático, métodos como el *Phishing*, *SPAM*, *Spoof* y otras variantes están muy en boga en los últimos tiempos y es necesario que nos protejamos.

Como en el caso de la protección antivirus, es muy importante tener sentido común, por ello es fundamental no abrir vínculos en mensajes de SPAM (ni el mensaje si quiera), navegar por sitios seguros y un largo etcétera.

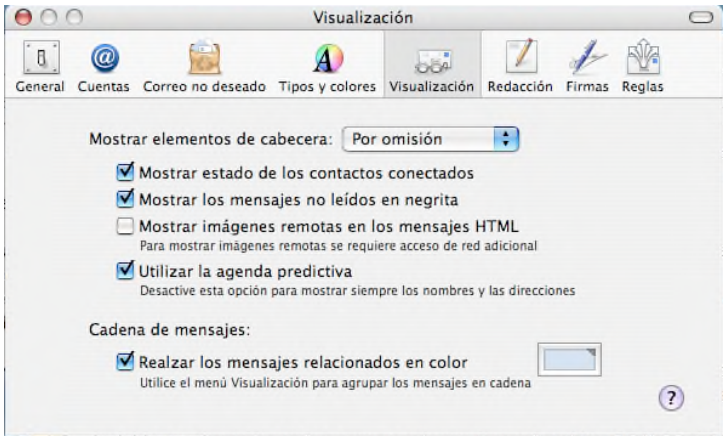
2.1.- Navegación privada

Si usas Safari 2.0 o posterior verás que existe una opción llamada `Navegación Privada` en el menú `Safari`. Esta opción te permite navegar sin que Safari registre en el historial las páginas por las que visitas ni las búsquedas en Google que hagas.

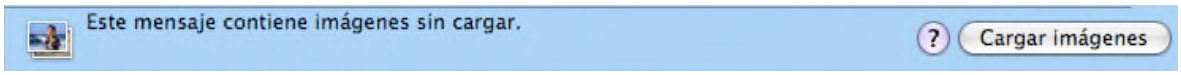
Aun así puedes navegar de manera privada creando usuarios ficticios y direcciones de correo temporales, e incluso acceder a bases de datos de nombres y contraseñas para sitios Web, como BugMeNot (www.bugmenot.com) que almacena miles de usuarios y contraseñas para acceder a sitios Web sin necesidad de registro previo.

También podemos hacer referencia en este apartado a la privacidad en los chats, es muy interesante mantener encriptadas las conversaciones porque si no nuestras palabras se enviran como texto plano por la red. Apple, en su iChat ha incluido encriptación en las conversaciones (necesitas Mac OS X 10.4.3, que incluye iChat 3.1). Aunque también puedes usar otras soluciones de terceros como ChatBarrier de Intego o PGP Desktop Home (www.pgp.com). También existen otras alternativas de mensajería segura como BitWise (www.bitwisecommunications.com) o Fire (de código abierto, http://fire.sourceforge.net).

Cuando recibimos mensajes de correo electrónico podemos ser víctimas de registros en bases de datos para luego ser bombardeados con SPAM, este método es muy común en mensajes con imágenes remotas, en las que al abrir la URL de la imagen registran nuestra información. Si usas Mail, es muy sencillo protegerse de esto, desactivando la carga automática de imágenes remotas, que podremos cargar manualmente, al recibir mensajes. Ve a las preferencias de Mail y déjalo así:



Cuanto te llega un mensaje con imágenes, Mail te mostrará esta barra:

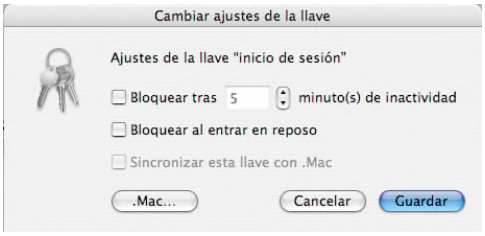


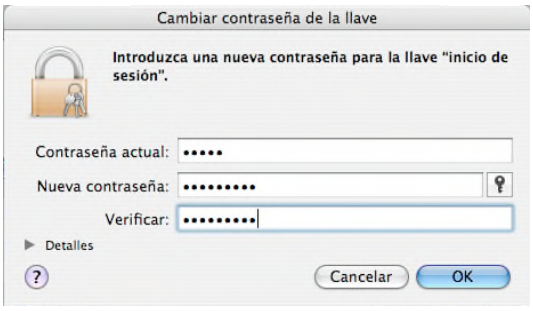
2.2.- Protección en equipos compartidos

Si compartes el equipo con varios usuarios es útil que hagas lo siguiente:

- Desactiva el inicio de sesión automático: puedes hacerlo desde el panel `Cuentas` de `Preferencias del Sistema`.
- Bloquea la pantalla cuando te vas de las cercanías del equipo: accede al panel `Seguridad` de `Preferencias del Sistema` y activa la opción `Solicitar contraseña para reactiva el equipo si está en reposo o con el salvapantallas`.

- Bloquea tu llave cuando no se esté utilizando: en el menú `Edición` > `Cambiar ajustes de la llave "xxxx"…` de `Acceso a Llaves` puedes activar el bloqueo al entrar en reposo, o tras un tiempo de inactividad.

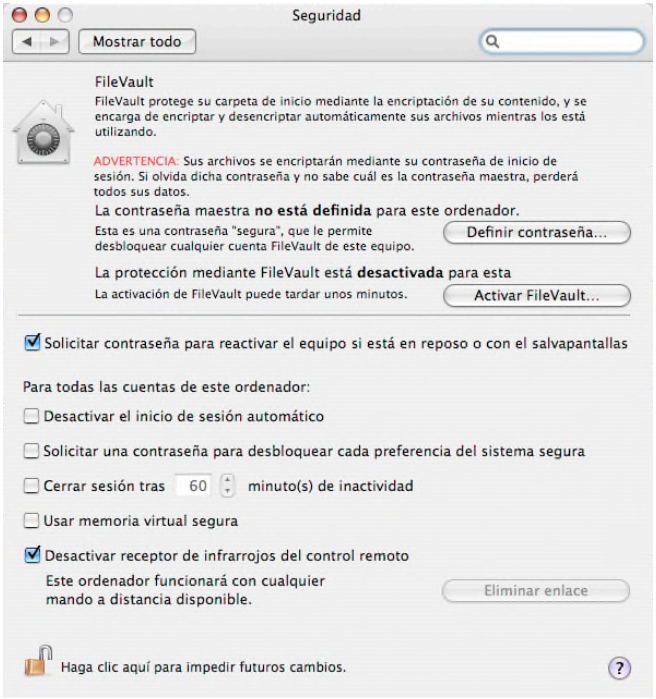




- Cambia la contraseña de tu llave por otra distinta de la de tu cuenta: en el menú `Edición` > `Cambiar contraseña de la llave "xxxx"…` de `Acceso a Llaves` puedes realizar el cambio. Si quieres también puedes desactivar el desbloqueo automático de las llaves al iniciar sesión (mira en el menú `Preferencias…` de `Acceso a Llaves`).

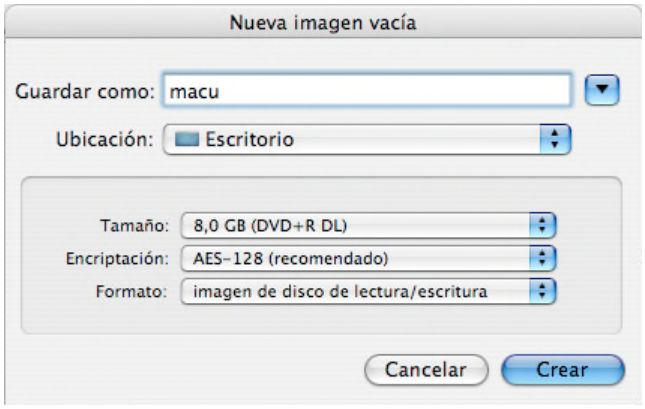
2.3.- Protección en equipos públicos

Si usas un equipo público, es necesario, que además de las medidas anteriores, protejas aún más tus ficheros. Mac OS X (10.3 o superior) te ofrece una forma muy sencilla para proteger tus ficheros, encriptándolos automáticamente, llamada FileVault. Esta opción encripta de manera automática y transparente tus ficheros (los de tu carpeta de usuario) y los descifra del mismo modo.



Para activarlo, puedes acceder a la opción `Seguridad` de `Preferencias del Sistema`. Tienes que definir una contraseña maestra para poder desbloquear cualquier cuenta FileVault (si se olvida una contraseña por ejemplo, o para fines administrativos) y a continuación, hacer clic en `Activar FileVault`.

Si la opción de FileVault te parece excesiva, puedes crear una imagen de disco encriptada y almacenar allí tus ficheros. Para hecerlo, puedes usar la aplicación Utilidad de Discos. Usa el menú Archivo > Nueva > Imagen de disco vacía... A continuación selecciona un nombre, tamaño y en el campo encriptación escoge AES-128. Tendrás que establecer una contraseña.



2.4.- Protección de redes inalámbricas

Las redes inalámbricas son un punto donde potencialmente se puede vulnerar nuestra privacidad. Cualquier persona con un software apropiado puede ver el tráfico de nuestra red. Esto no lo podemos evitar, porque repartimos la información a los cuatro vientos, pero podemos usar técnicas criptográficas para evitar que esa información tenga sentido ante una lectura por terceras partes.

En Mac OS X, podemos hacer uso con facilidad de estas técnicas, configurando las conexiones inalámbricas con protección WEP, WPA o WPA2 (cada cual más segura que la anterior). La forma de hacerlo depende de tu hardware de red, pero si tienes un punto de acceso AirPort de Apple, deberás usar la `Utilidad de Administración AirPort` en la carpeta `Utilidades`. Recuerda actualizar el software de tu estación y que las estaciones AirPort originales no soportaban WPA o WPA2. Cuando más larga sea la clave que uses y más “aleatoria”, mejor.