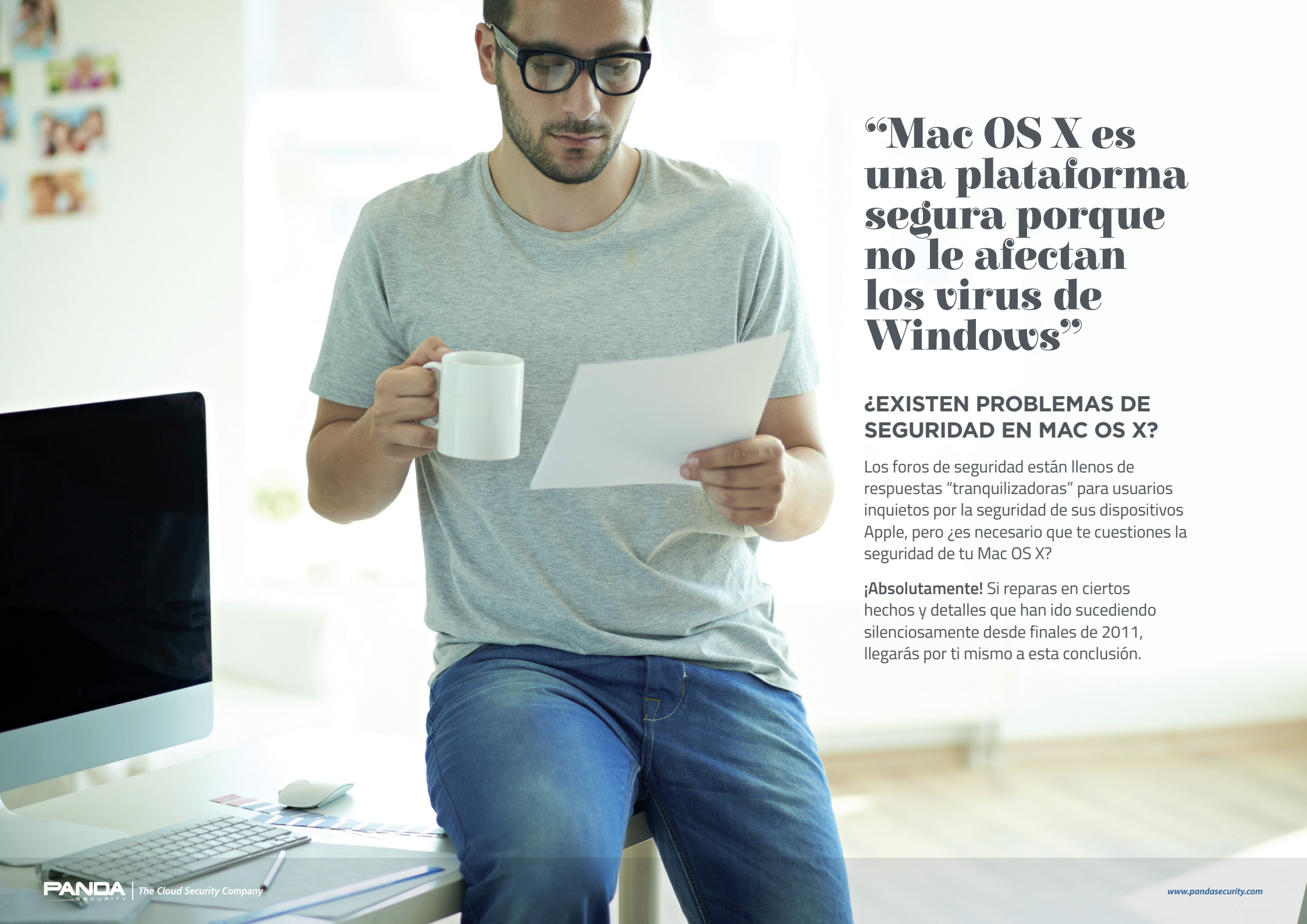
PANDA SECURITY | *The Cloud Security Company*

# CONTENIDO





# “Mac OS X es una plataforma segura porque no le afectan los virus de Windows”

## ¿EXISTEN PROBLEMAS DE SEGURIDAD EN MAC OS X?

Los foros de seguridad están llenos de respuestas “tranquilizadoras” para usuarios inquietos por la seguridad de sus dispositivos Apple, pero ¿es necesario que te cuestiones la seguridad de tu Mac OS X?

**¡Absolutamente!** Si reparas en ciertos hechos y detalles que han ido sucediendo silenciosamente desde finales de 2011, llegarás por ti mismo a esta conclusión.

Tradicionalmente, en Apple no se ha hablado de forma explícita sobre el concepto de seguridad. No es algo que surja de una preocupación clara del fabricante por proteger sus productos frente a ataques externos, se trata más de una promesa de marca o un "buen hacer".

Y lo cierto es que Apple ha disfrutado de una tradicional ausencia de problemas de seguridad, principalmente fruto de unos niveles de ventas muy inferiores en comparación a los productos con Windows. Era extraño que los hackers desarrollaran malware para una plataforma tan minoritaria, y hubiera sido más extraño aún que Apple desarrollara las medidas necesarias para evitar unas intrusiones que hasta la fecha no se habían producido de forma preocupante.

**Con una cuota de mercado mundial en escritorio en torno al 6% en el año 2012, simplemente, ni era rentable crear malware para Mac, ni lo era desarrollar los medios para defenderse de algo que casi no existía.**

Si echamos un vistazo a las recomendaciones sobre seguridad que hace tiempo Apple vertía en su página web se puede comprobar que eran bastante contundentes.

***No se contagia con virus de PC***

*"Un Mac no es sensible a los miles de virus que inundan los ordenadores basados en Windows. Esto es así gracias a las defensas incorporadas en Mac OS X que te mantendrán a salvo, sin ningún esfuerzo por tu parte".*

***Mantén a salvo tus datos. Sin hacer nada***

*"Sin esfuerzo por tu parte, OS X te defiende contra virus y otras aplicaciones maliciosas o malware. Por ejemplo, impide la entrada de los hackers a través de una técnica llamada "sandboxing" restringiendo las acciones que los programas pueden realizar en tu Mac, los ficheros que pueden acceder y los programas que pueden lanzar".*

Se hacía mención a los virus de PC como la única fuente de problemas y a las defensas incorporadas en el sistema operativo de Apple como el medio para mantener a salvo la plataforma; una plataforma tan segura que el usuario era invitado a no hacer absolutamente nada para protegerse.

Así se negaba la mayor: **el problema simplemente no existía**. Pero en Junio del 2012 el mensaje cambió significativamente.

***Construido para ser seguro***

*"Las defensas incorporadas en OS X te mantienen a salvo de las descargas inadvertidas de software malicioso en tu Mac".*

***Seguridad incorporada***

*"OS X está diseñado con tecnologías potentes y avanzadas que trabajan para mantener tu Mac a salvo. Por ejemplo impide la entrada de los hackers a través de una técnica llamada "sandboxing" restringiendo las acciones que los programas pueden realizar en tu Mac, los ficheros que pueden acceder y los programas que pueden lanzar".*

La mención a los virus de PC desapareció, es fácil de imaginar la razón: **ocultar la existencia de malware específico para Mac ya no era posible**.
Por precaución también retiró la invitación al usuario de no hacer nada para proteger su sistema.

En Junio del 2012 Apple mencionó por primera vez el malware en su keynote del Worldwide Developers Conference (WWDC) como parte de la presentación de la tecnología Gatekeeper, la cual "ayuda a mantener el sistema libre de malware".

Todo esto no hace sino demostrar lo que siempre han sido las plataformas Apple: vulnerables al malware exactamente en los mismos términos que el resto de sistemas de la competencia.

Como finalmente quedó demostrado cuando a finales de 2011 un proveedor de seguridad para sistemas Apple llamado *Intego* detectó la existencia de un troyano, al que bautizó Flashback. Este malware aprovechó una vulnerabilidad de Java para infectar a más de 600.000 Macs durante meses, 274 de ellos situados en Cupertino, California, sede del cuartel general de Apple.

Si eres usuario avanzado de Windows sabrás que muchas infecciones son visibles y se traducen en cambios en el sistema que pueden ser sintomáticos de la existencia de malware en tu equipo.

En una plataforma Mac podrías estar infectado desde hace tiempo y no ser consciente en absoluto de ello: un sistema basado en Mac OS X puede transmitir una falsa sensación de protección muy perjudicial para la seguridad de tus datos.

Los últimos avisos de Apple vienen a demostrar lo que siempre han sido sus plataformas: vulnerables al malware, como el resto de los sistemas.

# “Los virus de Mac OS X no existen”

## ¿ES CIERTO QUE NO EXISTEN VIRUS PARA MAC?

Hablar de seguridad en entornos Mac es complicado porque implica hablar de defectos y fallos y es terreno abonado para perderse entre tecnicismos y simpatías hacia la marca. Expertos en seguridad afirman que *“la mayor vulnerabilidad de Macintosh es la creencia entre sus devotos usuarios de que el sistema operativo de Apple es superior y los hacen inmunes al malware”*.

Por definición, un virus es un programa malicioso embebido dentro de otro programa o fichero que se propaga por sí mismo a otros ordenadores.

Flashback no era un virus, era un troyano que una vez instalado descargaba software específicamente diseñado para robar cuentas bancarias, contraseñas del navegador e información confidencial del equipo del usuario. Lo pertinente aquí no es hablar de virus, sino de malware.

Decir que no existen virus en Mac es muy peligroso, es un concepto que lleva a confusión y en materia de seguridad la confusión se cifra en pérdidas económicas.

A parte del ya mencionado FlashBack algunos ejemplos de malware para Mac que han tenido y tienen cierto impacto son:

## Pintsized

Es un malware que aprovecha vulnerabilidades de Java para abrir una puerta trasera en el ordenador y permitir el control remoto de tu equipo por parte del hacker.

## CoinThief

Es un malware que se hace pasar por una aplicación legitima de pagos por Internet para robar al usuario tus Bitcoins.

## Icefog

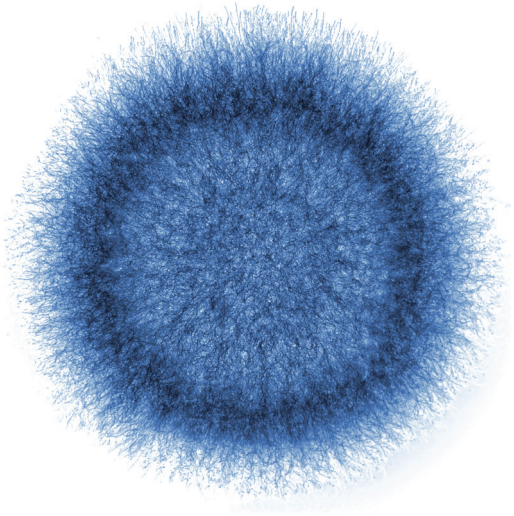
Es un malware multiplataforma muy utilizado en labores de espionaje en Asia, sobre todo Japón y Corea del Sur.

## Mac Defender

Es un falso antivirus que invita a los usuarios a registrarse y pagar por una "protección" que nunca se hace realmente efectiva.

Lo cierto es que no tienes por qué conocer esta jerga técnica. Pero la realidad es que las consecuencias del malware se traducen siempre de la misma forma, independientemente de cuál sea el tipo: virus, troyanos, ransom o rootkis. **Simplemente debes saber que ahí fuera hay malware que afecta directamente a tu Mac OS X y que lo que está en juego son, muy probablemente, pérdidas económicas.**

Afirmar que no existe malware en Mac es, cuando menos, capcioso.
La mayor vulnerabilidad de Macintosh es la creencia de sus usuarios de que el sistema operativo es superior y les hace inmunes.



# “No es necesario preocuparse por la seguridad en Mac”

## ¿QUÉ ESTÁ HACIENDO APPLE PARA PROTEGER A SUS USUARIOS?

Aunque algunos usuarios lo sigan negando, hay una guerra en curso y la prueba es que se desarrollan ataques y defensas. Una comunidad, cuya motivación crece paralelamente al aumento de las ventas de Mac OS X, está desarrollando malware con objetivos económicos y, en consecuencia, Apple desarrolla protecciones y defensas para mantener a salvo a sus usuarios, en apariencia. Pero... ¿Será suficiente?

El principal problema es que Apple ha llegado muy tarde a una arena ya muy trillada, en la que Microsoft sufrió un auténtico calvario hace años: con la llegada de Internet se generó el inicio del crecimiento exponencial del malware, y Windows 95, 2000 y XP fueron las plataformas con las que Microsoft tuvo que lidiar este desafío casi en exclusiva, ya que nunca antes se había vivido una situación similar y se "hicieron los deberes" ante la presión de millones de sistemas infectados.

El resultado de aquel aprendizaje es una compañía fuertemente comprometida con la seguridad, con un calendario claro de publicaciones de boletines de seguridad y con agilidad a la hora de liberar parches y actualizaciones de sus sistemas operativos.

El caso de Apple es totalmente distinto: solo publica actualizaciones cuando lo considera necesario y en el caso de **FlashBack tardó 6 semanas en publicar las correcciones a los errores** que propiciaban la infección, **cuando esos mismos parches ya habían sido desarrollados y publicados por Oracle**.

Lo mismo ha sucedido en otros casos. Como por ejemplo *Icefog*, cuya definición **Apple tardó 2 semanas** en incorporar al fichero de firmas de su antivirus Xprotect desde el envío de la muestra. En ese lapso de tiempo Icefog seguía infectando equipos de usuarios desconocedores del problema.

**Estas cifras dejan a Apple muy atrás con respecto a proveedores de seguridad Cloud que entregan sus actualizaciones... ¡con retrasos de minutos!**

Apple tampoco sigue una política clara a la hora de anunciar la finalización del soporte de sus productos: con la aparición de las versiones 10.9 y 10.9.1 por ejemplo se incluyeron varias correcciones que no se portaron a versiones anteriores (Lion y Mountain Lion). Sin embargo con la aparición de la versión 10.9.2 la compañía sí publicó las correcciones de seguridad que protegían del malware a los usuarios de las versiones Lion y Mountain Lion. Aquí Snow Leopard (10.6) es el gran olvidado. **¡Si tu sistema es un 10.6 actualízalo cuanto antes!**

El resultado de todo esto es que **el usuario no sabe cuándo se publican las correcciones** ni si le cubrirán en el caso de que no tenga instalada la última versión del sistema operativo.

Verdaderamente el compromiso de Apple en materia de seguridad no está a la altura: el oscurantismo es su principal baza y quizá la razón de esta actitud se pueda encontrar en que **le está costando renunciar a la etiqueta de "plataforma invulnerable" que tan buenos réditos le ha dado en el pasado**.

Los "anticuerpos" de Mac OS X van apareciendo paulatinamente, estableciendo un avance en la seguridad de la plataforma, pero esta oferta forma parte de la instalación básica del sistema operativo y es tenida en cuenta por los creadores de malware.

No obstante, a partir del 2009 Apple ha ido introduciendo progresivamente modificaciones sustanciales en sus sistemas operativos orientadas a reforzar la seguridad de su sistema. Un pequeño resumen podría ser el siguiente:

- **Leopard (10.5)**
  SandBox, Quarantine de ficheros y Firewall de aplicaciones.
- **Snow Leopard (10.6)**
  Antivirus Xprotect.
- **Mountain Lion (10.7)**
  Gatekeeper.

Apple está introduciendo modificaciones en sus sistemas operativos para reforzar la seguridad, después de los últimos problemas detectados.

Los "anticuerpos" de Mac OS X van apareciendo como si de un organismo biológico se tratara, y aunque es un claro avance en la seguridad de la plataforma se reproduce el mismo efecto que se comprobó en sistemas Windows con Security Essentials: la oferta de seguridad de Apple forma parte de la instalación básica del sistema operativo y los creadores de malware ya saben de su existencia y focalizan sus esfuerzos en desarrollar medidas para sortear estas protecciones.

**Es por esta razón que el usuario debería completar la oferta de seguridad básica de Apple con un buen antivirus de terceros**.

## ¿QUÉ PUEDE HACER PARA MINIMIZAR RIESGOS DE INFECCIÓN?

El sentido común y la sensatez son los puntos clave para evitar infecciones: ser consciente de que nuestro sistema es vulnerable, prudencia a la hora de salvaguardar la información que manejamos en nuestros dispositivos, instalar un buen antivirus y mantenerlo actualizado, y descartar aquellos ficheros y webs que nos resulten sospechosos.

Retrocediendo al año 2011, veíamos como Apple anunciaba orgullosa en web que su sistema era inmune a los virus de PC. Y era bastante cierto: en líneas generales un virus escrito para sistemas Windows no funciona en Mac OS X.

Con la aparición de malware para Mac OS X el propio de Windows continúa siendo una potencial fuente de problemas en entornos mixtos o en lo referido a la imagen de empresa: imagínate enviando una propuesta comercial a un cliente con un fichero adjunto infectado con virus de PC; según estadísticas externas, el 43% del malware encontrado en sistemas Mac OS X es malware nativo de Windows.

Ya sea para proteger tu sistema, el de los ordenadores Windows que te rodean o tu propia imagen, podrás dotar a tu Mac de un más que razonable nivel de seguridad con unas pequeñas medidas generales fácilmente aplicables.

Facebook y otras redes sociales
son, a menudo, una fuente de malware
muy importante.
Maneje solo ficheros que provengan
de una fuente fiable.

## 1. Tu Mac no es invulnerable

Interioriza esta verdad absoluta: el sistema Mac no es invulnerable. Es posible que tu equipo esté infectado y el sistema, lejos de ayudarte a descubrirlo, puede llegar a trabajar en tu contra haciéndote creer que los virus simplemente "no funcionan".

## 2. Hazte con un buen antivirus de un proveedor externo

Ganarás enteros en protección, independientemente de la versión de Mac OS X que utilices. En la actualidad, el malware en circulación intentará sortear las protecciones de Apple, cuantos más antivirus haya en el mercado el esfuerzo de los hackers tenderá a diluirse más y más y las probabilidades de infección serán mucho menores que si hay un "monopolio de la seguridad de facto".

## 3. Instala todas las actualizaciones

Instala todas las actualizaciones del sistema operativo y del software de terceros que tengas instalado tan pronto como se publiquen.

## 4. Debes ser extremadamente cuidadoso con los ficheros que ejecutes

Sitios como Facebook y similares son una fuente de malware de presuntos "amigos".

Ficheros adjuntados por email de remitentes desconocidos y ficheros descargados de programas P2P caen en el mismo saco. Por tanto, descarga y ejecuta ficheros solo de fuentes confiables.

## 5. Desactiva el software especialmente problemático

Java y Flash son dos tecnologías con una larga tradición de bugs y exploits.

Ve al Panel de Seguridad en las preferencias de tu navegador Safari y desactiva el módulo Java o haz clic en "Gestionar ajustes de sitios web" según sea la versión del navegador.