



Bisoños Usuarios de Linux de Mallorca y Alrededores | Bergantells Usuaris de Linux de Mallorca i Afegitons

¿Puedes confiar en tu PC?

Por kyle, [kyle](http://linuca.org) (<http://linuca.org>)

Creado el 27/10/2002 04:29 y modificado por última vez el 27/10/2002 04:29

Traducción al castellano del texto publicado por Richard Stallman en [NewsForge](#)⁽⁹⁾

¿Puedes confiar en tu PC?

Richard Stallman

¿De quién debería tu ordenador obedecer órdenes? La mayor parte de la gente opina que sus ordenadores sólo les deberían obedecer a ellos, y no a otros. Con un plan denominado "Trusted Computing" (Informática Fiable), las grandes compañías mediáticas (incluyendo discográficas y distribuidoras de cine) junto con Microsoft e Intel, planean hacer que tu ordenador les obedezca a ellos en lugar de a ti. Los programas propietarios han incluido características maliciosas anteriormente, pero este plan lo convertiría en universal.

"Software Propietario" significa, fundamentalmente, que tú no controlas lo que hace; no puedes estudiar su código fuente, ni cambiarlo. No es sorprendente que inteligentes hombres de negocios encuentren formas de usar su control para ponerte en desventaja. Microsoft ha hecho esto muchas veces: una versión de Windows fue diseñada para informar a Microsoft de todos los programas que tenías instalados; una reciente actualización "de seguridad" en Windows Media Player requería que los usuarios aceptaran unos nuevos términos de licencia mucho más restrictivos. Pero Microsoft no es la única empresa que hace esto: el software KaZaa para compartir música fue diseñado de tal forma que la empresa propietaria puede alquilar el uso de tu ordenador (potencia de cálculo) a sus clientes. Estas características maliciosas son habitualmente secretas, y una vez que estás alerta sobre ellas es difícil eliminarlas, dado que no tienes el código fuente.

En el pasado, estos eran incidentes aislados. "Trusted Computing" podría convertirlo en habitual. "Treacherous computing" (juego de palabras – *Informática No Fiable*) sería un término más adecuado, por que se ha diseñado este plan para asegurarse de que tu ordenador te desobedezca de forma sistemática. De hecho, está diseñado para que tu ordenador deje de actuar como un ordenador de propósito general. Cada operación puede requerir permiso explícito.

La idea técnica que subyace es que el ordenador incluye un dispositivo de firma y cifrado digital, y que las claves son secretas para el usuario. (La versión de Microsoft de esto se llama Palladium). Los sistemas operativos propietarios usarán este dispositivo para controlar qué otros programas puedes ejecutar, a qué documentos o datos puedes acceder y con qué programas. Estos programas descargarán habitualmente nuevas reglas de autorización a través de Internet, e impondrán esas políticas de forma automática en tu trabajo. Si no permites que tu ordenador se conecte a Internet para obtener estas políticas de forma periódica, algunas capacidades de estos programas dejarán de funcionar.

Por supuesto, Hollywood y las compañías discográficas planean usar esta "Informática No Fiable" para hacer DRM (Digital Rights Management – Control de Derechos Digitales) para que vídeos y música descargados solamente se puedan reproducir en un ordenador específico. Compartir ficheros será completamente imposible, al menos usando ficheros autorizados que obtendrías de esas compañías. Vosotros, el público, deberíais tener la libertad y la posibilidad de compartir estas cosas. (Espero que alguien consiga producir versiones no cifradas, y que las comparta, para que el DRM no tenga éxito completamente, pero eso no es excusa para el sistema)

Hacer que la compartición sea imposible es suficientemente malo, pero hay más cosas. Hay planes para usar la misma característica en emails y documentos – resultando que un email desaparece en dos semanas, o que los documentos solamente puedan ser leídos en ordenadores de una compañía.



Imagina que recibes un email de tu jefe diciéndote que tienes que hacer algo que tú consideras arriesgado; un mes después, cuando se demuestra que la idea salió mal, no puedes usar el mail para explicar que la decisión no fue tuya. "Tenerlo por escrito" no sirve de nada si está con tinta que desaparece

Imagina que recibes un email de tu jefe imponiendo una política que es ilegal o moralmente rechazable, como destruir las auditorías de tu compañía, o permitir que una amenaza peligrosa para tu país continúe sin ser detectada. Hoy puedes mandar esto a un periodista y exponer la actividad. Con la Informática No Fiable, el periodista no podrá leer el documento; su ordenador se negará a obedecer. La Informática No Fiable se convierte en un paraíso de la corrupción.

Los procesadores de texto como Microsoft Word podrían usar la Informática No Fiable cuando salvan tus documentos, para asegurarse de que ningún procesador de textos de la competencia pueda leerlos. Hoy en día, debemos averiguar los secretos del formato de ficheros Word a través de laborioso experimentos para poder hacer que los procesadores de texto libres puedan leer ficheros de Word. Si Word cifra los documentos usando Informática No Fiable, la comunidad del Software Libre no tendrá ninguna oportunidad de desarrollar software que los lea – y si pudiéramos, esos programas posiblemente estarían prohibidos por la Digital Millennium Copyright Act (DMCA).

Los programas que usan Informática No Fiable se descargarán de forma continua reglas de autorización a través de Internet, y las aplicarán automáticamente a tu trabajo. Si a Microsoft, o al gobierno de Los Estados Unidos, no le gusta lo que dices en un documento que has escrito, podrían dar las instrucciones para que todos los ordenadores se nieguen a leer ese documento. Cada ordenador les obedecería cuando descargue las nuevas instrucciones. Tu escrito sería susceptible de un borrado retroactivo, al estilo de 1984 (George Orwell). Puede que seas incapaz de leerlo tu mismo.

Quizá pienses que puedes averiguar qué cosas malas hace una Aplicación No Fiable, estudiar cómo de dolorosas son y decidir si aceptarla o no. Esto sería una decisión corta de miras y poco inteligente, puesto que problema es que el software estudiado cambiará inmediatamente. Una vez que dependes del uso de ese programa, estás atado y ellos lo saben; entonces ellos pueden cambiar las condiciones. Algunas aplicaciones bajarán actualizaciones automáticamente que las harán funcionar de modo diferente – y no te dejarán elegir si quieres actualizar o no.

Hoy en día, puedes evitar las restricciones del software propietario no usándolo. Si usas GNU/Linux u otro sistema operativo libre, y si puedes evitar usar aplicaciones propietarias en ello, controlarás lo que tu ordenador haga. Si un programa libre tiene una característica maliciosa, otros desarrolladores de la comunidad se lo quitarán, y podrás usar la versión corregida. También puedes ejecutar aplicaciones libres en sistemas operativos no libres; eso no te da completa libertad, pero muchos usuarios lo hacen.

La existencia de la Informática No Fiable pone en riesgo la existencia de aplicaciones y sistemas operativos Libres, por que puede impedirte que los utilices. Algunas versiones de sistemas operativos No Fiables requerirían ser específicamente autorizados por una compañía. Los sistemas operativos libres no podrían ser instalados. Todos los programas requerirían ser específicamente autorizados por el desarrollador del sistema operativo. No se podrían ejecutar aplicaciones libres en un sistema tal. Si tú descubrieras cómo hacerlo, y se lo contaras a alguien, sería un delito.

Ya hay proposiciones de ley en Los Estados Unidos que requerirían que todos los ordenadores utilicen Informática No Fiable, y que prohibirían el acceso a Internet a viejos ordenadores que no la soporten. El DBDTPA (lo llamamos "Consume But Don't Try Programming Act" – "Ley Consume–pero–no–pruebes") es una de ellas. Pero aunque no nos fueren legalmente a actualizarte, la presión para aceptarla será enorme. Hoy mucha gente usa ficheros Word para comunicarse, aunque esto cause problemas de todo tipo (lee <http://www.gnu.org/philosophy/no-word-attachments.html>⁽¹⁾). Si sólo un ordenador no fiable puede leer los últimos ficheros Word, mucha gente se cambiará a ello, si lo ven en términos de acción individual (lo tomas o lo dejas). Para oponerse a la Informática No Fiable, debemos agruparnos juntos y enfrentarnos como una elección colectiva

Para mas información sobre Informática No Fiable, lee [El FAQ de Ross Anderson](#)⁽²⁾ (Traducción a castellano en [Bulma](#)⁽³⁾).

Llegar a detener la iniciativa de "Informática No Fiable" requeriría que una gran cantidad de ciudadanos se organizaran. ¡Necesitamos tu ayuda! La Electronic Frontier Foundation (www.eff.org)⁽⁴⁾ y [Public Knowledge](#)⁽⁵⁾ llevan a cabo una campaña en contra de la "Informática No Fiable", del mismo modo que el Proyecto de Expresión Digital (Digital Speech Project – esponsorizado por la Free Software Foundation [FSF](#))⁽⁶⁾. Por favor, visita estos sitios web para unirte contra esta iniciativa.



También puedes ayudar escribiendo a las oficinas de Relaciones Públicas de Intel, IBM, HP/Compaq, o cualquiera otra empresa de la que hayas comprado un ordenador, explicando que no quieres que se te obligue a comprar sistemas informáticos "fiables", así que no quieres que ellos desarrollen ninguno. Si haces esto a título individual, por favor manda copias de tus cartas a las organizaciones arriba mencionadas.

Apéndices:

1. Un comunicado anterior de los desarrolladores de Palladium afirmaba que la premisa básica que cualquiera que desarrollara o recogiera información debería tener control total de cómo tú la usas. Esto representaría un revolucionario, El Proyecto GNU distribuye GNU Privacy Guard, un programa que implementa cifrado de clave pública y firmado digital, que puedes usar para mandar correo electrónico seguro y privado. Es útil ver como GPG se diferencia de la Informática No Fiable, y ver por qué uno es útil y el otro tan peligroso.

Cuando alguien usa GPg para enviarte un documento cifrado, y tú usas GPG para descifrarlo, el resultado es un documento descodificado que tu puedes leer, reenviar, copiar e incluso volver a cifrar para mandarlo de forma segura a otras personas. Una aplicación No Fiable te permitiría leer el texto en la pantalla, pero no te permitiría producir un documento descifrado que podrías usar de otras formas. GPG, un paquete informático libre, da características de seguridad a los usuarios; ellos las usan. La Informática No Fiable está diseñada para imponer restricciones a los usuarios; les usa.

2. Microsoft presenta a Palladium como una medida de seguridad, y afirma que protegerá contra los virus, pero esta afirmación es evidentemente falsa. Una presentación realizada por Microsoft Research en Octubre de 2002 señalaba que una de las especificaciones de Palladium es que sistemas operativos y aplicaciones existentes continúen funcionando; de este modo, los virus seguirán siendo capaces de hacer las mismas cosas que hacen hoy.

Cuando Microsoft habla de "seguridad" en relación a Palladium, ellos no quieren decir lo que habitualmente significamos con esa palabra: proteger a tu ordenador de cosas no deseadas. Ellos quieren decir evitar que tus copias de datos en tu máquina sean accedidas de algún modo no planificado por ellos. Una diapositiva en la presentación listaba varios tipos de secretos para los que Palladium podría ayudar a mantener, incluyendo "secretos de terceras partes" y "secretos del usuario" – pero ponía "secretos del usuario" entre signos de interrogación, reconociendo que esto no es para lo que Palladium ha sido realmente diseñado.

La presentación hacía frecuente uso de otros términos que frecuentemente asociamos con el contexto de seguridad, como por ejemplo "ataque", "código malicioso", "spoofing" (suplantación), y "fiable". Ninguno de ellos significa lo que normalmente significa. "Ataque" no significa que alguien te intente hacer daño, sino que tú intentes copiar música. "Código Malicioso" es aquel código que tú has instalado para hacer algo que otra gente no quiere que tu ordenador haga. "Suplantación" no significa que alguien te engañe, si no que tu engañes a Palladium. Y así todo.

3. Un comunicado anterior de los desarrolladores de Palladium afirmaba que la premisa básica que cualquiera que desarrollara o recogiera información debería tener control total de cómo tú la usas. Esto representaría una revolucionaria destrucción de anteriores ideas sobre ética y del sistema legal, y crearía un sistema de control sin precedentes. Los problemas específicos de estos sistemas no son por accidente; resultan de su meta principal. Esa es la meta que debemos rechazar.

Copyright 2002 [Richard Stallman](#)⁽⁷⁾

Traducción: [Francisco García](#)⁽⁸⁾

Verbatim copying and distribution of this entire article is permitted without royalty in any medium provided this notice is preserved.

Lista de enlaces de este artículo:

1. <http://www.gnu.org/philosophy/no-word-attachments.es.html>
2. <http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>
3. <http://bulmalug.net/body.phtml?nIdNoticia=1398>
4. <http://www.eff.org/>
5. <http://www.publicknowledge/>
6. <http://www.fsf.org/>



7. <http://www.stallman.org/>
8. http://bulmalug.net/mailto:frang_AT_terra.D.O.T_es
9. <http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19>

E-mail del autor: kyle@navegalia.com

Podrás encontrar este artículo e información adicional en: <http://bulmalug.net/body.phtml?nIdNoticia=1571>