

## Expertos dudan de los planes de Microsoft con respecto a la criptografía.

**A tres semanas de que Microsoft detalle oficialmente sus planes para crear un sistema seguro de criptografía para los ordenadores personales que funcionen bajo Windows, dos expertos criptógrafos han lanzado la voz de alarma contra la estrategia del gigante del software.**

Whitfield Diffie, ingeniero de Sun Microsystems Laboratories y co-inventor del sistema de clave pública, advirtió que la llegada de un sistema de seguridad en ordenadores que integre al máximo los servicios de seguridad es inevitable, pero que el enfoque de Microsoft es fallido, pues no permite a los usuarios un control total sobre sus claves de seguridad personales. [Ronald Rivest](#), profesor en el MIT (Instituto Tecnológico de Massachusetts) y fundador de RSA Security, abogó por la necesidad de un amplio debate público sobre las pretensiones de la empresa de Bill Gates.

Según Diffie, Microsoft "pretende dominar el mercado, alejando al propio usuario del control de su ordenador. Esto va a causar problemas que ensombrecerán cualquier otro debate similar mantenido durante la pasada década. Definitivamente, tenemos que tener el control de nuestras propias claves", añadió, "y para ello, es necesario un estándar, no competir por el control de la tecnología propietaria". Diffie ya advirtió en su día [de los problemas de la universalidad del sistema .NET de Microsoft](#).

Rivest, por su parte, añadió que "hay que verlo como si se añadiera un dispositivo virtual dentro de nuestro PC que no controlamos del todo. Esencialmente estamos alquilando una parte de nuestro ordenador a gente en la que definitivamente no confiamos".

Sun ya consideró en su día realizar un ordenador que no funcionaría sin la presencia de un sistema operativo firmado digitalmente. El proceso de venta hubiese sido similar a una transacción criptográfica en la que se adjudican claves de seguridad a los usuarios finales. Finalmente se descartó la idea.

En el nuevo proyecto de Microsoft, los usuarios tendrían que evocar un sistema seguro que estaría deshabilitado por defecto. Instrucciones nuevas en la CPU así como cambios en el controlador de memoria ayudarían a crear un espacio en la RAM necesario para cargar un pequeño y seguro kernel de sistema. Un módulo de memoria flash ayuda en las funciones de identificación y autenticación, basadas en claves almacenadas y valores hash. La idea también requiere canales seguros entre el teclado y la memoria principal, así como entre la interfaz gráfica.

Microsoft nos dejó una primera prueba de sus planes hace ya un año, con un proyecto cuyo nombre clave es [Palladium](#). El sistema se supone diseñado para mejorar sustancialmente la habilidad de proteger la información personal y corporativa de cualquier ordenador. Mario Juárez, product manager de Palladium, afirma que no sólo resolverá problemas, sino que explorará nuevas posibilidades que cambiarán la manera que tienen hoy día las personas de relacionarse con los ordenadores. Este nuevo sistema se muestra como una combinación de hardware y software que sellará información de los atacantes, bloqueará virus y gusanos, y hasta eliminará el spam. Todo esto se ha dado en llamar [Next-Generation Secure Computing Base](#) (NGSCB, pronunciado "enscub").

Microsoft ha desvelado sus planes a treinta socios, y pretende hacer público el resto de detalles técnicos en el [Windows Hardware Engineering Conference](#) a principios de mayo.

Artículo original en: <http://www.eetimes.com/story/OEG20030415S0013>

Sergio de los Santos

[www.forzis.com](http://www.forzis.com)

s.delossantos@forzis.com

**Fecha artículo: 2003-04-16 15:19:44 - url artículo: <http://www.internautas.org/html/118.html>**

**Logos y marcas propiedad de sus respectivos autores.**

**Los comentarios son propiedad y responsabilidad de cada autor.**

**© 1998-2009 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)