

## ¿Por qué Microsoft incluyó un cortafuegos en Windows Vista y qué consecuencias tendrá esto?

Tenemos que admitir que el cortafuegos de Vista brinda cierta protección básica.

El hecho de que sea gratuito (incluido dentro de otro producto) significa que no se deberían tener demasiadas expectativas en relación con su calidad.

Algo que hemos comprobado, sin lugar a dudas, cuando realizamos una [prueba exhaustiva](#) del cortafuegos *OneCare* de Microsoft a comienzos de este año.

En nuestra opinión, existen dos razones para que Microsoft incluya un cortafuegos, que se activa de manera predeterminada y se entrega de forma gratuita, en la versión de Windows Vista.

1. Para brindar un cierto grado de protección básica a los usuarios sin experiencia (es decir, buenas relaciones públicas).
2. Para capturar participación en el mercado de terceros proveedores de cortafuegos comerciales.

### ¿Qué peligros subyacen en este enfoque de Microsoft?

Todos sabemos que lo gratis es tentador.

También recordamos lo que sucedió con Netscape cuando Microsoft presentó Internet Explorer.

¿Pero durante cuánto tiempo lo gratis sigue siendo una buena opción?

Sí, Internet Explorer obtuvo 95% de participación en el mercado.

Pero después el desarrollo pareció detenerse, hasta que la participación en el mercado comenzó a dirigirse en la dirección opuesta al aparecer productos alternativos (Firefox, Opera y el regreso de Netscape).

Además, está claro que Internet Explorer tiene más agujeros de seguridad que un tamiz, tal como nos recuerdan constantemente los frecuentes anuncios de parches.

Lo que nos lleva a realizarnos una pregunta fundamental: ¿Por qué seguimos confiando en Microsoft en lo que se refiere a seguridad, cuando está claro que tiene dificultades para brindar esa seguridad en sus propios productos? Microsoft debe invertir para mantener sus productos a la altura de las expectativas de los usuarios y de los requerimientos de seguridad.

Esto es lo que les aconsejamos hacer y, quién sabe, tal vez hasta estén leyendo este artículo.

1. Escuchen lo que los terceros proveedores de seguridad comentan, y pongan a su disposición la información que estos necesitan para instalar sus propios productos y así, mejorar la seguridad de Windows Vista. Depender de Microsoft y solamente de él no va a proteger a los usuarios.
2. Pongan a disposición el código fuente de Windows, que los terceros proveedores, necesitan para poder realizar pruebas integrales de compatibilidad (es decir, verificar si el programa es compatible con otras aplicaciones). De esta forma, podrán integrarse con todos los aspectos de Vista y garantizar una seguridad efectiva y transparente para los usuarios.