

# Las 10 vulnerabilidades más comunes en Windows

**Autor:** Kevin Beaver, CISSP

[http://searchenterprisedesktop.techtarget.com/tip/0,289483,sid192\\_gci1331487,00.html?track=NL-1108&ad=663608&asrc=EM\\_NLT\\_4550676&uid=648659](http://searchenterprisedesktop.techtarget.com/tip/0,289483,sid192_gci1331487,00.html?track=NL-1108&ad=663608&asrc=EM_NLT_4550676&uid=648659)

**Traducción para Segu-Info:** Raúl Batista

**Fecha Publicación:** 26 de septiembre de 2008

## Las 10 vulnerabilidades más comunes en Windows

Todos sabemos que los sistemas basados en Windows tienen potencialmente muchos riesgos de seguridad. Pero, ¿son vulnerables sus sistemas?. Probablemente sí. Cualquier red está llena de vulnerabilidades de Windows. Es una ley natural y un efecto colateral de hacer negocios con redes de computadoras. Pero con los miles de vulnerabilidades que hay por allí sueltas, ¿en donde necesita enfocar *realmente* sus esfuerzos? Bien, permítame compartir con Ud. las debilidades de Windows que más estoy viendo en mi trabajo... cosas que le pueden acarrear problemas si las ignora.

**Esta es mi lista de las 10 más importantes:**

### 1. Permisos de archivos y carpetas compartidas que permiten todo a todos

Esta es fácilmente la vulnerabilidad más grande que estoy viendo en los sistemas Windows, sin importar que tipo de sistema o tipo de Windows se trate. Los usuarios que crean recursos compartidos para poner a disposición sus archivos locales a través de la red son los culpables típicos. A veces son administradores descuidados; otras son honestamente errores. Desafortunadamente, demasiado a menudo se le da acceso total al “grupo Todos” en todos y cada uno de los archivos de un sistema. En consecuencia, todo lo que queda es que un atacante interno busque palabras clave sensibles en cada archivo .pdf, .xls, .doc y otros formatos usando una herramienta de búsqueda como [Effective File Search](#) o [FileLocator Pro](#). Las posibilidades son - cerca del 100% de las veces - que el atacante se cruce con información sensible (números de seguro social, de tarjetas de crédito, lo que Ud. imagine) a la cual no debería tener acceso. En el mejor de los casos, esto resultará en un robo de identidad, en el peor, esto se convierte en una seria brecha en la seguridad que sale en los titulares de los diarios.

### 2. Falta de protección contra malware

Ya lo sé, ya lo sé, esto es algo realmente básico pero lo estoy viendo ahora más que nunca antes. He visto software antivirus y antispyware instalado y deshabilitado, y no instalado y nadie que estuviera consciente del problema.

### 3. Falta de cortafuegos personal

Este es otro control básico de seguridad que sigue sin estar habilitado en muchos sistemas Windows. Aún el Cortafuegos básico integrado de Windows (gratuito) puede impedir conexiones a los recursos compartidos IPC\$ y ADMIN\$ que a menudo están abiertos y proveen información y acceso que no debería divulgarse. Los cortafuegos personales también pueden impedir infiltraciones de malware, intrusiones inalámbricas y otras. No se me ocurre ninguna buena razón para no usar un cortafuegos personal en toda PC y en la mayoría de los servidores.

### 4. Cifrado de disco débil o inexistente

La maquinaria de marketing de cifrado de discos está haciendo su magia, pero sigo viendo que la mayoría de las organizaciones (grandes y pequeñas) no usan cifrado. Soy de la creencia que el cifrado completo del disco es el único camino. Si una máquina portátil o de escritorio es robada o se pierde, la única forma de impedir que alguien quiebre la contraseña de Windows y tenga acceso al disco rígido es cifrar todo usando frases de contraseña (passphrases) razonables. Dependiendo del Sistema de Archivos Cifrados de Windows (EFS) u otro cifrado de archivo/carpeta/volumen pone demasiado control de la seguridad en manos del usuario y es quedarse a la espera que suceda una brecha.

### 5. Sin estándares mínimos de seguridad

Los usuarios con redes inalámbricas, necesitan cumplir políticas de seguridad de la compañía en sus hogares, tales como requerir SSL para el Acceso Web a Outlook (OWA), una conexión VPN PPTP para la conectividad de red remota, o WPA-PSK con una frase de contraseña fuerte para ayudar que todo esté seguro y sólido. Se puede forzar esto sin necesidad de un IDS/IPS inalámbrico instalado en la PC (componente típico de sistemas inalámbricos de administración empresarial) o un sistema de Control de Acceso a la Red (NAC) bien configurado. No obstante, hágalo parte de su política e impóngalo cuando sea posible.

### 6. Parches faltantes en Windows y en software de terceros

Parches tales como VNC, RealPlayer y otros. Este es un [gran problema que a menudo es pasado por alto](#). No digo que deba buscar y encontrar ese tipo de agujeros, solo señalo que los parches que no se aplican. Usando [Metasploit](#) o sus alternativas comerciales [CANVAS](#) y [CORE IMPACT](#), muchos parches olvidados pueden ser explotados por un pícaro atacante interno o por un atacante externo que se metió en su red de alguna forma. ¿Acceso remoto para todos?

## 7. Configuración débil de políticas de seguridad de Windows

Algunos ejemplos de esto incluyen los registros de auditoria no configurados para eventos fallidos; salvapantallas sin protección de contraseña; no requerir Ctrl+Alt+Del para ingresar; no requerir contraseñas complejas; y mostrar el ultimo usuario que ingresó al sistema. Las políticas para controlar estas cosas son fáciles de implementar localmente en cada sistema Windows en una instalación pequeña que no utilice Directorio Activo. Es aún más sencillo para compañías grandes mediante Políticas de Grupo de Directorio Activo (GPO).

## 8. Sistemas ignorados para correr servicios desconocidos y no administrados, tales como IIS y SQL Server Express

A menudo estos son [sistemas Windows heredados](#) que no están en la visión de la seguridad y conformidad de la compañía. A veces, ni siquiera son soportados por los sistemas de seguridad de terceros y entonces son dejados de lado. Estos sistemas (típicamente Windows 98, NT y 2000) a menudo están des-asegurados y no emparchados y están a la espera de ser explotados. Inevitablemente también habrán algún sistema usado para entrenamiento o pruebas y olvidado por todos. Pero sistemas como esos son los que necesita alguien con malas intenciones para meterse en la red y hacer cosas malas.

## 9. Contraseñas débiles o inexistentes

No puedo decirle cuantos sistemas (especialmente portátiles Windows) he visto que no tenían una contraseña asignada a la cuenta del administrador o que la cuenta del usuario por defecto es igual al nombre del usuario. El problema de la contraseña ha estado por allí desde el comienzo de los tiempos, así que no hay excusa para esto.

## 10. Windows Mobile y otras debilidades de dispositivos móviles

En el mundo móvil de hoy no debo dejar de mencionar las vulnerabilidades asociadas con Windows Mobile y otros dispositivos móviles parecidos. Es esencial tener en el rada algunos temas específicos de los dispositivos móviles. En un consejo llamado [Seguridad Windows mobile security: Manténgalo cerrado](#), he descripto varias cosas para tener en cuenta..

Para encontrar estas vulnerabilidades, necesitará buenas herramientas, incluyendo escáner de puertos y herramientas de enumeración de sistemas, tales como [SuperScan](#) o, idealmente, escáneres de vulnerabilidades que hacen todo en una sola vez, tal como [QualysGuard](#). Un analizador de red fácil de usar como [OmniPeek](#) o [CommView](#) son necesarios, tanto como un buen [editor hexadecimal](#). Por ultimo, pero no menos importante, deberá usar su propia habilidad para analizar manualmente sus sistemas para buscar puntos débiles. Es fácil verificar cuando está instalada una protección contra malware, pero no es tan sencillo determinar cuan débiles son los permisos en archivos, Políticas de grupo que faltan o cosas similares que pueden ser explotadas.

Ahora que sabe en que enfocarse, puede empezar a ver que es cada cosa. El balance final es conocer *que* hay en sus sistemas y *que se puede hacer* con sus sistemas. Esta es la receta para un entorno Windows seguro.