

## El modelo de seguridad ganador

### Introducción

Corre el año 2007, y el código malicioso técnicamente ha alcanzado un nivel de sofisticación jamás visto. Muchos de nosotros hemos tenido contacto directo con programas espía, virus, gusanos y otros programas maliciosos, y sensatamente hemos decidido tomar medidas para protegernos.

El código malicioso se ha extendido tanto actualmente, que incluso aquellos pocos que no han padecido ninguna infección, deberían considerar seriamente la implementación de medidas de seguridad informática.

Se necesita una solución confiable, que abarque la mayor cantidad de áreas de riesgo posible, y que mantenga a salvo a los usuarios en línea, sin entrometerse en sus actividades.

Sin embargo, esta decisión implica una pregunta nada trivial: ¿Hacia dónde debemos encaminar nuestra búsqueda de una solución de seguridad? ¿Un antivirus, un cortafuegos, un paquete de seguridad integrado, o alguna otra opción? La respuesta será el asunto principal de este documento, donde describiremos cómo escoger la mejor combinación de herramientas para controlar las amenazas informáticas actuales.

Nuestra intención es ayudar al usuario a tomar una decisión fundamentada, enseñando mediante breves demostraciones de vídeo y descripciones simples, cómo trabajan las infecciones por código malicioso de hoy en día, y por qué esto debería guiar su proceso de toma de decisión.

### El paisaje de amenazas informáticas moderno

No es ningún secreto que en los tiempos que corren, estar en línea implica un camino lleno de peligros.

A diario aparecen nuevos tipos de amenazas, el viejo código malicioso se actualiza y sigue representando un riesgo muy grande.

Con el aumento de la cantidad de escritores de código malicioso, y su grado de profesionalismo en avance permanente, para los investigadores es más difícil que nunca perseverar en su lucha.

La brecha entre el número de desarrolladores de aplicaciones maliciosas y la cantidad de cazadores de virus es cada vez más ancha, y esta situación no puede revertirse solo con ingenio e inventiva.

Los países con muchos habitantes, como China, India y Brasil entre otros, están aportando grandes cantidades de piratas informáticos al ámbito clandestino del código malicioso de todo el mundo.

Estos individuos dominan rápidamente las habilidades necesarias para crear ataques masivos de programas dañinos.

Los métodos de investigación tradicionales contra este tipo de código, sencillamente no cuentan con los recursos humanos para examinar y crear firmas para cada una de las amenazas que producen estos ejércitos de nuevos escritores de aplicaciones maliciosas.

### La seguridad en teoría

Esencialmente, un ordenador está confiablemente protegido contra la mayoría de las amenazas informáticas si cumple con los siguientes requisitos:

#### 1. Elementos de protección proactiva.

Estos incluyen los sistemas de prevención de intrusos en ordenadores anfitriones (HIPS, *Host Intrusion Prevention Systems*), y sus parientes cercanos que controlan y restringen las actividades del sistema, analizadores de comportamiento, herramientas de protección del sistema operativo y barreras de escalada de privilegios; como así también cortafuegos y otras soluciones que desafían anticipadamente las amenazas que intentan activarse o propagarse en un ordenador.

#### 2. Elementos de protección reactiva.

Estos incluyen las soluciones antivirus y contra programas espía, así como otros productos basados en el análisis de firmas y en heurística.

#### 3. Cierta noción de las prácticas de seguridad informática de parte del usuario.

Esto debería incluir el conocimiento de las funciones clave del sistema operativo, la interacción entre archivos y programas, cómo mantener actualizadas las aplicaciones, y otras precauciones necesarias al estar en línea, ampliamente desarrolladas en los sitios de seguridad como este.

Ahora, analicemos un poco estos tres elementos fundamentales.

1. **La protección proactiva** no es, de ningún modo, una defensa infalible. Como cualquier otra medida, puede ser susceptible a ingeniosos métodos de evasión.  
Sin embargo, sí ayuda a detener el código malicioso donde este se encuentre, sin la necesidad de técnicas de identificación precisas como las que utilizan los enfoques reactivos basados en firmas.  
En la práctica, como podrán apreciar en los vídeos publicados, la protección proactiva sola es capaz de bloquear hasta un 80% de las actividades maliciosas en un ordenador.

La desventaja de esta técnica (siempre existen desventajas, la seguridad es un escenario de pujas entre la protección y la funcionalidad, en evolución permanente), es la gran cantidad de alertas y solicitudes de decisión, que podrían resultar intimidantes para un usuario con poca experiencia.

Por eso, no es sorprendente que la causa principal del fracaso en la protección proactiva, sea la respuesta incorrecta del usuario, ya sea por falta de conocimiento, o por mera displicencia ante el bombardeo de alertas que frecuentemente no indican una amenaza real.

[Outpost Firewall Pro](#) y [Outpost Security Suite Pro](#) manejan esta delicada cuestión con el sistema [ImproveNet](#), que suministra automáticamente la respuesta apropiada, basada en los datos obtenidos por experiencia real.

2. **La protección reactiva** todavía está en pie. Los programas contra programas espía antivirus continúan siendo una barrera formidable contra el código malicioso.  
Son las mejores herramientas para utilizar si es necesario eliminar una infección, o verificar la legitimidad de un archivo antes de ejecutarlo por primera vez.  
Por supuesto, también son muy confiables con respecto a la detección de amenazas existentes.  
Las limitaciones en la eficacia de estas aplicaciones más tradicionales, se deben principalmente al creciente número de amenazas nuevas. Por esta razón, mucha gente recurre al uso de múltiples soluciones diferentes, que pueden tener un impacto importante en el rendimiento del sistema, sin incrementar necesariamente el factor de detección.  
[Outpost Security Suite Pro](#) incorpora la exclusiva combinación de un motor contra programas espía y antivirus, con una técnica de análisis incremental.  
Esto minimiza la cantidad de recursos del sistema utilizados para ejecutar su tarea eficientemente.
3. Un conocimiento básico de las prácticas de seguridad informática es vital. Hay quienes afirman que la mejor herramienta de seguridad es una persona que utiliza inteligentemente su ordenador, que es consciente de los peligros existentes, y que se adhiere a los estándares seguros. Esto es absolutamente cierto.  
Sin embargo, cada trabajador necesita buenas herramientas como las descritas anteriormente para asegurar la mejor protección.

## La seguridad en la práctica

Como todo, la eficacia de las prácticas correctas de seguridad queda demostrada sólo cuando comenzamos a utilizarlas.

Por ello, hemos analizado las teorías mencionadas, en situaciones reales.

Un sistema Windows XP actualizado con todos los parches de seguridad disponibles, fue sometido a actividades típicas, como la navegación por Internet buscando novedades digitales interesantes, y la descarga y ejecución de varias aplicaciones.

También experimentamos con el manejo del correo no solicitado.

Cada actividad se realizó de dos formas diferentes: aplicando medidas de protección, y sin seguridad alguna en el ordenador.

Se pueden ver los vídeos de cada una de estas experiencias, en las siguientes páginas:

- [Video 1](#)  
[Sin protección alguna](#)
- [Video 2](#)  
[Outpost Security Suite Pro con Protección de \*host\* activada](#)
- [Video 3](#)  
[Outpost Security Suite Pro con todas las opciones de protección activadas \(Configuración por defecto\)](#)

Esperamos que sirva para ilustrar la importancia de tener una protección que sea tanto reactiva (antivirus, contra programas espía) como proactiva (protección del anfitrión).