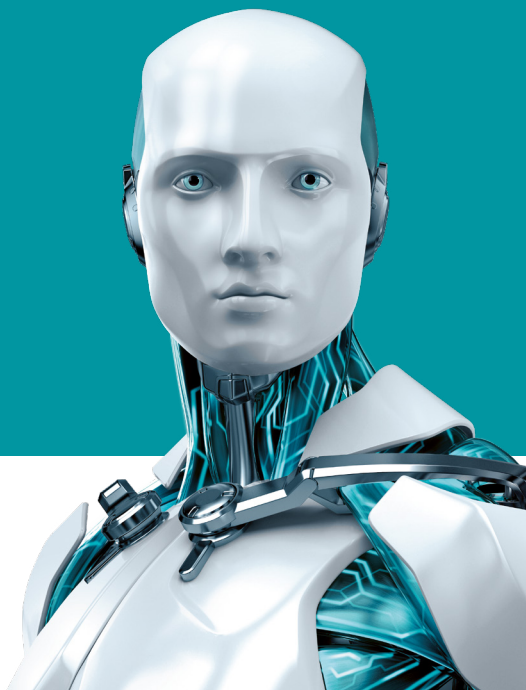
SEGURIDAD DE WINDOWS XP

Autor:
Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher, ESET



ENJOY SAFER TECHNOLOGY™

CONTENIDOS

NOTA:

El objetivo de este white paper es explicar cómo configurar Microsoft Windows XP para utilizarlo pasada la fecha de End of Life (EOL) – fin del ciclo de vida – del 8 de abril de 2014, hasta cierto momento en que pueda ser reemplazado por un sistema operativo más nuevo y seguro.

Este White paper explica cómo hacer una nueva instalación de Windows XP más segura, pero dicho consejo no debería ser interpretado como una guía para hacerlo tan seguro como las versiones más nuevas de Windows. No hay forma alguna de hacer esto más que instalar una versión de Windows más actualizada.

Ninguna solución de seguridad de terceros, sin importar su efectividad, puede ocupar el lugar de una actualización de seguridad regular lanzada por el proveedor para sus sistemas operativos y aplicaciones. El objetivo de este trabajo es explicar cómo mantener Windows XP tan seguro como sea posible hasta que pueda ser reemplazado.

INTRODUCCIÓN

Microsoft Windows XP, probablemente sea el sistema operativo más popular de Microsoft. Lanzado en 2001, tan solo un año después del lanzamiento de Microsoft Windows 2000, aspiraba a poner fin al ciclo de lanzar sistemas operativos separados para consumidores – basado en Windows 95 – y sistemas operativos lanzados para corporaciones – basado en Windows NT – con un único sistema operativo para el uso de todos. Combinando la confianza de Windows NT kernel con el subsistema multimedia de Windows 9x, podría ser igualmente útil para el trabajo y el entretenimiento.

Figura 1: Windows XP iniciándose

Entonces, ¿qué tan eficiente fue la ejecución de Microsoft en base a esta lejana visión? En abril de 2014, Windows XP fue instalado en aproximadamente el 30% de los computadores de escritorio de nuestros clientes. En marzo de 2018, Windows XP está instalado en un 5,5% de esos sistemas. Si bien esto puede parecer un pequeño porcentaje, representa 10 veces al número de computadores que ejecutan al sucesor de Windows XP, Windows Vista, que hoy suma por debajo del 1% de uso.

Una breve historia de la seguridad de Windows XP

Dada la amplia adopción de Windows XP, podría resultar difícil recordar que, originalmente, no tuvo un inicio fácil: apenas se lanzó se registraron múltiples quejas, desde críticas a su desempeño, a la falta de soporte de hardware, a reclamos sobre la relativa falta de funcionalidades nuevas comparadas con Windows 2000, hasta su costo (desde $200 dólares en adelante, según la edición, en Estados Unidos). Aun así, a pesar de todos estos conflictos, Windows XP ha disfrutada de una longevidad en PC que no se veía desde los días de Atari y Commodore, cuando se utilizaban sistemas operativos basados en ROM, durante más de una década.

Cuando en 2001 se introdujo Windows XP, Microsoft lo dio a conocer como el sistema operativo más seguro en su historia. Si bien en ese momento esto era cierto, en los años que siguieron se convirtió en el sistema operativo más emparchado de Microsoft, consecuencia no solo de su popularidad, sino también de su longevidad, en el intento por mantener el nivel de seguridad original. La respuesta de Microsoft ante la lluvia de vulnerabilidades halladas en su sistema operativo insignia para escritorio fue doble, desarrollando la iniciativa Trustworthy Computing[1, 2] (TwC –

1 Charney, Scott. "Looking Forward: Trustworthy Computing." https://cloudblogs.microsoft.com/microsoftsecure/2014/09/22/looking-forward-trustworthy-computing/.

2 Microsoft. "10 Years of Trustworthy Computing." Microsoft Corp. http://www.microsoft.com/en-us/twc/twcnext/timeline.aspx.

computación confiable), para sentar la computación segura, respaldada en la implementación de un Security Development Cycle[3] (SDL – Ciclo de desarrollo seguro) para reforzar la creación de código seguro por sus desarrolladores.

Esfuerzos como el de la iniciativa TwC, sin embargo, deben continuarse no solo con respuestas rápidas a amenazas emergentes, sino con respuestas correctas, y durante los primeros años pareció ser que los cambios hechos por Microsoft eran lentos o incompletos. Dos ejemplos conocidos:

- *Microsoft lanzó Windows XP con una funcionalidad llamada AutoPlay[4, 5], que permitía a los sistemas operativos identificar inmediatamente cuando se insertaban medios extraíbles, como un CD-ROM, en el computador. Esto se asoció con una funcionalidad relacionada llamada AutoRun[6], diseñada para ejecutar programas automáticamente desde el disco insertado. Con la idea de permitir que los dispositivos iniciaran programas tales como aplicaciones multimedia y juegos del CD-ROM, la funcionalidad nunca fue muy utilizada por los desarrolladores de software. O al menos, por desarrolladores legítimos: a medida que el precio de los USB[7] bajaba, y la oferta aumentaba, los creadores de malware comenzaron a utilizar esta tecnología para ayudar a difundir sus creaciones, como el infame gusano Conficker[8, 9, 10]. Desafortunadamente, por su mal uso, Microsoft consideró esto como una funcionalidad legítima del sistema operativo y se negó a modificarlo, hasta ocho años después, en 2009[11, 12, 13], cuando la cambiaron para prevenir comportamientos maliciosos. E incluso después, publicaron instrucciones erróneas, la primera vez[14].*
- *En el Service Pack 2, lanzado en 2004, Microsoft cambió la manera en la que los Raw Sockets de TCP/IP, un tipo de comunicación de red, eran gestionados[15, 16, 17].Esto se hizo en respuesta a una multiplicidad de ataques de gusanos que generaron tanto tráfico de red que afectaron la conectividad de Internet por completo, sin mencionar la disrupción de las redes de muchos de los grandes clientes de Microsoft. El cambio, desafortunadamente, afectó el*

3 Microsoft. "Microsoft Security Development Lifecycle." Microsoft Corp. https://www.microsoft.com/security/sdl/default.aspx.

4 Wikipedia. "AutoPlay." Wikimedia Foundation. https://en.wikipedia.org/wiki/AutoPlay.

5 St-Michel, Stephane and Aust, Brian. "Autoplay in Windows XP: Automatically Detect and React to New Devices on a System." MSDN Magazine. http://msdn.microsoft.com/en-us/magazine/cc301341.aspx.

6 Wikipedia. "AutoPlay." Wikimedia Foundation. https://en.wikipedia.org/wiki/AutoPlay.

7 Cobb, Stephen. "Are your USB flash drives an infectious malware delivery system?" WeLiveSecurity. http://www.welivesecurity.com/2012/12/11/are-your-usb-flash-drives-aninfectious-malware-delivery-system/.

8 ESET. "Virus Radar Threat Encyclopedia - Win32/Conficker." http://www.virusradar.com/en/Win32_Conficker/detail.

9 Goretsky. Aryeh. "1000 days of Conficker." WeLiveSecurity. http://www.welivesecurity.com/2011/08/17/1000-days-of-conficker/.

10 Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. http://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/.

11 Abrams, Randy. "Now You Can Fix AutoRun." WeLiveSecurity. http://www.welivesecurity.com/2009/08/25/now-you-can-fix-autorun/.

12 Microsoft. "Microsoft Security Advisory (967940): Update for Windows Autorun." Microsoft Corp. http://technet.microsoft.com/en-us/security/advisory/967940.

13 Microsoft. "How to disable the Autorun functionality in Windows." Microsoft Corp. http://support.microsoft.com/kb/967715/en-us.

14 US-CERT. "Alert TA-09-020A: Microsoft Windows Does Not Disable AutoRun Properly." https://www.us-cert.gov/ncas/alerts/TA09-020A.

15 Microsoft. "Microsoft Security Bulletin MS05-019 - Critical - Vulnerabilities in TCP/IP Could Allow Remove Code Execution and Denial of Service." Microsoft Corp. http://technet.microsoft.com/en-us/security/bulletin/ms05-019.

16 Howard, Michael. "A little more info on raw sockets and Windows XP SP2." Microsoft Corp. http://blogs.msdn.com/b/michael_howard/archive/2004/08/12/213611.aspx.

17 Windows Dev Center-Desktop. "TCP/IP Raw Sockets." Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/desktop/ms740548.

> *desempeño de redes peer-to-peer (redes de pares) y aplicaciones de gestión de redes que corrían Windows XP, lo que llevó a algunos usuarios a modificar los componentes de redes de Windows para saltear las restricciones, una técnica rápidamente adoptada por los autores maliciosos. No fue hasta pasados cuatro años, en 2008, que Microsoft revirtió estos cambios.*

Si bien estas acciones llevadas a cabo por Microsoft mejoraron el estado de la seguridad de Windows XP, el sistema operativo siguió siendo atacado, y probablemente no haya sido hasta el lanzamiento de Windows Vista en 2007 que Microsoft pudo usar la experiencia ganada de su iniciativa TwC y ciclo SDL, en conjunto con la información de toda una década obtenida de patrones de ataque, para implementar grandes cambios en la seguridad de Windows kernel. Este trabajo fue refinado aún más en 2009, con el lanzamiento de Windows 7, y nuevamente en 2008, con el lanzamiento de Windows 8.

El objetivo de este document es explicar los variados métodos por los que los usuarios de Windows XP pueden impulsar su seguridad. Sin embargo, el método más seguro es simplemente actualizar a una versión más nueva y segura de Windows[18]. Si bien las medidas destacadas en este documento pueden mejorar la seguridad de Windows XP, no son capaces de arreglar las vulnerabilidades subyacentes en su código. El 8 de abril de 2014, día en que Microsoft dejó de crear nuevos parches y *hotfixes* para Windows XP para atacar los problemas de seguridad, ya ha quedado atrás en el tiempo. Si bien es verdad que Microsoft ha lanzado dos actualizaciones debido a grandes vulnerabilidades que pueden haber sido explotadas por Estados nación, dichas actualizaciones no son una práctica normal y los usuarios que siguen utilizando Windows XP deberían actualizar lo antes posible.

Sin embargo, si estás leyendo este documento, podemos apostar que no estás listo aún para decir adiós a Windows XP[19, 20]. Todavía está siendo utilizado en algún lugar de tu ecosistema informático, y continúa siendo implementado pasado el fin de su ciclo de soporte extendido de Microsoft. Podrías no tener un staff de IT dedicado a ayudarte a asegurar esos sistemas. Con esto en mente, veamos algunas de las razones por las que podrías estar usando Windows XP hoy, antes de ver cómo asegurarlo.

NOTA: Por cuestiones de facilidad de uso y brevedad, usaremos el término Windows XP para referirnos a todas las ediciones de Microsoft *Windows XP* que estuvieron disponibles a consumidores y negocios:

Edición	Descripción
Windows XP edición Hogareña	*Para usuarios hogareños, con funcionalidades de administración limitadas*
Windows XP edición Media Center	*Para PCs Home Theater con sintonizador de TV y DVD*
Windows XP edición Professional	*Para negocios, con funcionalidades de administración*
Windows XP edición Starter	*Para mercados emergentes, con hardware de bajo costo*
Windows XP edición Tablet / PC	*Para notebooks con pantalla táctil y posibilidades de digitalización*

Windows XP para Sistemas Embebidos y *Windows XP Embebbed* fueron versiones componetizadas de Windows SP disponibles únicamente para empresas y fabricantes de dispositivos, y no deben ser consideradas como cubiertas por este artículo a menos que se lo aclare. Asimismo, las ediciones 64-bit de Windows XP, como *Windows XP 64-Bit Edition for Intel® Itanium Processors* y *Windows XP Professional x64 Edition*, que se derivan de *Microsoft Windows Server 2003*, no deben tenerse en cuenta al discutir Windows XP, a menos que se lo mencione.

18 Goretsky, Aryeh. "Time to Move On From Windows XP." WeLiveSecurity. *http://www.welivesecurity.com/2014/03/25/time-to-move-on-from-windows-xp/*.

19 Goretsky, Aryeh. "Goodbye, Windows XP!" WeLiveSecurity. *https://www.welivesecurity.com/2014/04/08/goodbye-windows-xp/.*

20 Kubovič, Andrej. "Windows XP: The zombie OS 'lives' on." WeLiveSecurity. *https://www.welivesecurity.com/2016/04/08/windows-xp-zombie-os-lives/.*

¿POR QUÉ USAR XP LUEGO DE 2014?

Hay varias razones por las que uno podría seguir utilizando Microsoft Windows XP mucho tiempo después de su origen. Debajo hay una lista de tres principales motivos por los que un negocio podría seguir utilizando Windows XP hoy:

Si bien se trata de tres casos diferentes, la razón detrás de ellos es la misma: el costo. Los ejemplos presentados se concentraron en el impacto financiero que actualizar a un nuevo sistema operativo tendrá para el negocio, pero estas razones son igual de aplicables a los consumidores finales. La familiaridad podría ser un problema aún mayor para este grupo, especialmente dada la tendencia de antropomorfizar computadores.

Descripción	Razón
Software	El computador se utiliza para ejecutar una aplicación clave que solo funciona con Microsoft Windows XP. Actualizar no resulta práctico porque el desarrollador podría ya no estar activo, el precio de la actualización estar por encima de lo permitido en cuanto a costos, o la aplicación necesitar ser reemplazada por una completamente nueva.
Hardware	El computador se utiliza para operar una pieza de hardware que funciona solo con Microsoft Windows XP. En ciertos casos, el equipamiento industrial, médico o científico podría usar una PC que ejecuta Windows XP como una clase de controlador embebido, y el costo de actualizar el sistema para admitir nuevas versiones de Microsoft Windows o reemplazarla podría exceder los costos permitidos o no ser viable por problemas de recursos.
Familiaridad	El computador se utiliza para realizar un conjunto de funciones específicas, sobre las que están entrenados los colaboradores, y con las que están familiarizados y cómodos. Si bien los dispositivos y el software que ejecuta son capaces de correr versiones más nuevas de Microsoft Windows, actualizar a una versión más moderna significa costos adicionales de entrenamiento y descenso en la productividad, hasta que los empleados estén al día con el nuevo sistema operativo y software.

WINDOWS XP, VIRTUAL

Si necesitas seguir ejecutando Microsoft Windows XP, podría ser una solución hacerlo desde un software de máquina virtual[21]. Como el nombre lo dice, una máquina virtual (VM) es un programa que emula un computador en software. La emulación es tan buena que puede ejecutar otro sistema operativo dentro suyo, y ese SO y sus programas verán la máquina virtual como si estuvieran ejecutándose en un computador

21 Wikipedia. "Virtual Machine." Wikimedia Foundation. https://en.wikipedia.org/wiki/Virtual_machine.

Figura 2: Windows XP ejecutado dentro de una máquina virtual

regular. Al utilizar la tecnología VM, un computador ejecutando un sistema operativo más moderno como Windows 7, Windows 8.1 o Windows 10, puede correr versiones viejas de Windows o incluso sistemas operativos completamente diferentes, como Linux y BSD.

El software de máquina virtual viene en varias formas, desde programas de Código Abierto, como Oracle VirtualBox[22] hasta opciones comerciales como VMware Workstation[23]. Las ediciones enfocadas en el negocio de Windows 7 (Professional, Ultimate y Enterprise) venían incluso con una máquina virtual especial para ejecutar Windows XP llamada Windows XP Mode[24, 25, 26]. Esta no está disponible para Windows Vista o Windows 8.

Utilizar una máquina virtual puede permitirte ejecutar solo esa última aplicación que requiere de Microsoft Windows XP, al menos hasta que pueda ser reemplazada. Es importante tener en mente que, si bien ejecutar Windows XP dentro de una máquina virtual puede *reducir* la superficie de ataque, cualquier vulnerabilidad presente en XP permanecerá. Sin embargo, sí facilita el manejo del computador, que puede ser importante si se trabaja con hardware más antiguo, para el que puede ser más difícil conseguir partes. Además, ejecutar Windows XP dentro de una máquina virtual en hardware moderno puede permitirte sobrepasar problemas de compatibilidad con discos duros modernos y unidades de estado sólido, algo que será discutido en detalle más adelante.

22 Oracle. "VirtualBox." Oracle. *https://www.virtualbox.org/*.

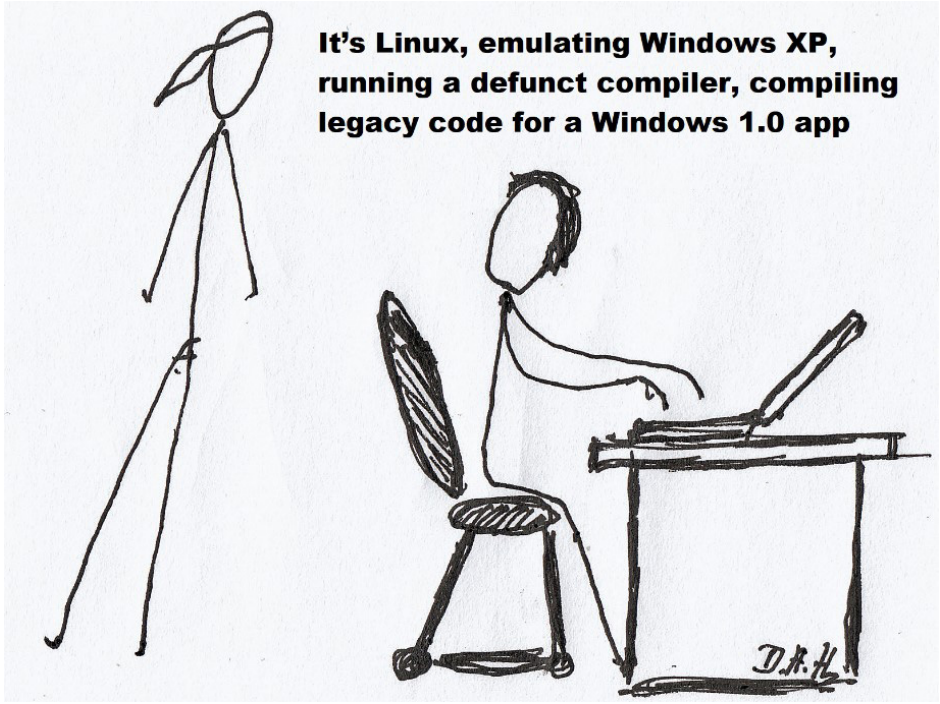
23 VMware. "VMware Workstation." VMware, Inc. *http://www.vmware.com/products/workstation/*.

24 Microsoft. "Windows XP Mode." Microsoft Corp. *http://windows.microsoft.com/en-us/windows7/products/features/windows-xp-mode*.

25 Microsoft. "Install and use Windows XP Mode in Windows 7." Microsoft Corp. *http://windows.microsoft.com/en-us/windows7/install-and-use-windows-xp-mode-in-windows-7*.

26 Microsoft. "Microsoft Download Center – Windows XP Mode." Microsoft Corp. *http://www.microsoft.com/en-us/download/details.aspx?id=8002*.

Si existe alguna pregunta sobre si usar o no una máquina virtual para seguir ejecutando Microsoft Windows XP, esa pregunta debería ser "¿Puedo?" Si *puedes*, **deberías** hacerlo para evitar costos asociados con el mantenimiento de hardware viejo necesario para ejecutar Windows XP. Sin embargo, puede suceder que tu uso de Windows XP dependa de algún software o hardware que no funcione como corresponde dentro de una máquina virtual. Si ese es el caso, deberás mantener el hardware "nativo". Tocaremos este asunto en detalle más adelante.



UNA NOTA SOBRE LA PRIVACIDAD

Mientras investigábamos la resistencia de los consumidores por abandonar Microsoft Windows XP, una cuestión recurrente que surgía era la piratería de software: una minoría significativa de personas con las que se habló está ejecutando una copia pirata de su sistema operativo, y en ocasiones, también aplicaciones. En algunos casos, el computador venía originalmente con una versión licenciada de Windows XP, pero fue reemplazada en algún momento con una copia pirata durante una actualización de hardware, o como resultado de la rotura de un disco, o debido al deseo de evitar el software preinstalado del fabricante del equipo, o por alguna otra desgracia. Esto no solo los privó de actualizar legalmente a un nuevo sistema operativo usando ediciones renovadas gratuitas, significa también que suelen evitar la instalación de parches de seguridad y mejoras, con el miedo de que alguna de ellas deshabilite sus copias piratas de Windows.

Esta paranoia no se vio beneficiada con el lanzamiento de Windows Genuine Advantage[27] (WGA) de Microsoft. WGA es una herramienta de gestión de derechos digitales diseñada para que las copias pirateadas de Windows no recibieran actualizaciones que no fueran críticas, para deshabilitar la personalización de funcionalidades en el sistema operativo, como la habilidad de elegir el wallpaper, y de mostrar mensajes que advirtieran al usuario que su sistema operativo podría no tener una licencia. Al lanzar WGA mediante los auspicios del servicio Windows Update, declarando que era una actualización de seguridad crítica, Microsoft generó hostilidad en muchos usuarios con copias pirateadas de Windows en sus sistemas ya que, de hecho, no solucionó ninguna vulnerabilidad en el sistema operativo y reunió información que podía ser usada para identificar los computadores que pudieran estar ejecutándolo de forma unívoca.

Mucha gente se mostró alienada por el inicial rechazo de Microsoft de brindar detalles acerca de lo que el programa hacía.

Independientemente de sus motivos para piratear Windows XP, muchos usuarios han respondido a la posición de Microsoft sobre la piratería de software deshabilitando Windows Update, por miedo a ver desactivadas sus copias o ser espiados por Microsoft. Estos computadores, que en general suelen estar faltos de años de parches, son ampliamente más vulnerables de ser explotados que sus homólogos, legales y actualizados.

Si cualquiera de los computadores que ejecutan Microsoft Windows XP y están bajo tu responsabilidad están en esta situación, este sería un buen momento para sacarlos de esa situación. Si no puedes instalar una nueva versión de Windows, entonces instala la versión licenciada legal de Windows XP que viene con el computador, utilizando los medios de recuperación adecuados para el computador combinados con la llave de ID de producto en la etiqueta de Certificado de Autenticación, al costado o debajo de la unidad.

Si el hardware que estás utilizando no vino con una licencia legal para Windows XP, tu mejor opción es utilizar una licencia comercial de la versión Professional de una copia cerrada de software que aún esté en su envoltura, que a veces puede hallarse en sitios online de ofertas y tiendas de segunda mano. Esto te permitirá ejecutar el sistema operativo en cualquier hardware seleccionado, virtual o físico, hasta que el SO pueda ser remplazado por una versión más moderna y segura.

27 Microsoft. "Description of the Windows Genuine Advantage Notifications application." Microsoft Corp. *https://windows.microsoft.com/en-US/windows/help/genuine/faq*.

ESTRATEGIAS DE BACKUP PARA WINDOWS XP

Más allá de los motivos para seguir usando Windows XP ya pasada su publicitada fecha de expiración[28, 29, 30], lo más importante que deben hacer los usuarios es asegurar que sus equipos seguirán trabajando adecuadamente sin importar la fecha límite, ya pasada (8 de abril de 2014). Si tu uso de Windows XP es de rutina, probablemente no haya nada adicional que debas hacer con tu instalación, más que descargar el último set de actualizaciones de Windows desde Microsoft. Por supuesto, otros programas que ejecutes bajo el sistema operativo podrían seguir recibiendo actualizaciones, y éstas deberían instalarse para mantener las aplicaciones confiables y seguras ante vulnerabilidades que pudieran llevarlas a ser explotadas. En particular, sería una buena idea comprobar las mejoras de Adobe Flash, Adobe Reader y Oracle Java, ya que estos programas suelen ser explotados por los atacantes[31]. *Más adelante* encontrarás otra información sobre las actualizaciones de Windows y tus aplicaciones.

Sin embargo, si pretendes utilizar Windows XP para ejecutar alguna aplicación crítica para el negocio, todo se vuelve más complejo. Por ejemplo, si el computador se usa para ejecutar software específico, necesitarás preservar los materiales de instalación para ese software propietario (sin acceso libre al código fuente) en caso de que el computador deba ser reemplazado. Si el software en cuestión utiliza algún tipo de mecanismo de protección de copia, deberías asegurarte de tener la habilidad para reactivar el software una vez reinstalado – un asunto que puede ser problemático si la compañía que fabricó el software ya no se sigue trabajando (o no tiene soporte para ello).

En este caso, utilizar un software de clonación de disco puede ser el mejor método para tener un "clon" del sistema operativo cerca. De todas formas, recuerda que clonar puede requerir de una copia de respaldo y recuperación completa de la unidad de disco duro (HDD) del computador, por lo que podrías acabar perdiendo información importante si tienes que restaurar una copia más antigua del sistema. Hablaremos más sobre el backup en breve.

Respaldando tu hardware: problemas con las interfaces

Si el computador que ejecuta Windows XP es usado para controlar equipamiento industrial o científico, se vuelve más importante mantener copias de backup no solo del software, sino también del hardware. Si la máquina usa hardware especializado, como una tarjeta controladora serial, paralela o digital para comunicarse con el equipamiento, deberías al menos tener una tarjeta controladora extra para instalar en la PC, junto con cualquier cableado, software y controladores de dispositivo necesarios para que funcione.

Esto puede volverse aún más difícil de gestionar si se requiere hardware más antiguo. A lo largo de los años, las placas base (motherboards) han utilizado una variedad de (en su mayoría, incompatibles) espacios de

28 Microsoft. "Support for Windows XP is ending." (business messaging). Microsoft Corp. https://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx.

29 Microsoft. "Support for Windows XP is ending." (consumer messaging). Microsoft Corp. https://windows.microsoft.com/en-us/windows/end-support-help.

30 Margel, Rob. "Download the Windows XP End Of Support Countdown Gadget." Microsoft Corp. https://blogs.msdn.microsoft.com/robmar/2011/04/20/download-the-windows-xp-end-of-support-countdown-gadget/.

31 Selinger, Markus. "Adobe & Java Make Windows Insecure." AV-Test. http://www.av-test.org/en/news/news-single-view/artikel/adobe-java-make-windows-insecure/.

expansión para tarjetas, desde ISA[32] (1981) a EISA[33] (1988) a VLB[34] (1992) a PCI[35, 36] (1993) a AGP[37] (1996) hasta PCIe[38,39] (2004). Hoy en día, es difícil hallar placas base fabricadas con espacios de expansión PCI, más aún las tecnologías de interfaz antigua. Si tu uso de Windows XP requiere de una de estas tarjetas, podrías acabar gastando un buen tiempo y mucho dinero intentando hallar partes de repuesto para mantener la ejecución de Windows XP en hardware ya desgastado.

Respaldando tu hardware: problemas con las unidades de disco

Las tarjetas de expansión y sus interfaces no son la única tecnología que cambian con el tiempo. Incluso componentes estándar como los discos duros lo hacen. A lo largo de los años, desde que se lanzó Windows XP, las unidades de disco duro han aumentado en capacidad de megabytes a gigabytes a terabytes. Si bien las placas base de computador se han ajustado con el tiempo para utilizar mayores capacidades de disco duro, las más antiguas solo podrían reconocer discos duros de hasta cierto tamaño, como 8GB o 137GB, dependiendo de cómo operen sus BIOS[40, 41]. Sigla para *Sistema Básico de Entrada/Salida* (en inglés), un BIOS es una pequeña pieza de software embebida en un chip en la placa base que controla cómo se enumera (reconoce y accede) al hardware cuando se inicia el computador.

En algunos casos, los fabricantes de computadores o placas pueden haber lanzado BIOS actualizadas para permitir que equipos más viejos usen discos duros de mayor capacidad, pero podría ser difícil localizar esas actualizaciones, especialmente si el fabricante no brinda soporte para modelos viejos, o ya no está en el negocio. Algunos fabricantes de unidades de disco incluyen un interruptor DIP que puede añadirse a un disco duro para que figure como de 8GB de tamaño para la BIOS del computador, eliminando conflictos como la falta de reconocimiento de la unidad de disco. Por supuesto, realizar esto significa dejar el espacio extra vacío y malgastado, ya que no será visible para el computador.

Unidades de disco duro PATA versus SATA

En 2001, era común utilizar un disco duro con interfaz de trasferencia de datos AT[42] (ATA, en inglés, también conocido como EIDE, por Enhanced Integrated Drive Electronics) en la PC, que se conectaría a la placa base utilizando una cinta de cable de 40 pines (u 80 más adelante). El motivo para el alto número de cables era que las señales se transferían en paralelo entre la PC y el disco duro. En 2003, la interfaz serial ATA[43] (SATA) para discos duros fue ratificada, completada con cableado diferente e incompatible que utilizaba menos cables, dando como resultado el uso de

32 Wikipedia. "Industry Standard Architecture." Wikimedia Foundation. https://en.wikipedia.org/wiki/Industry_Standard_Architecture.

33 Wikipedia. "Extended Industry Standard Architecture." Wikimedia Foundation. https://en.wikipedia.org/wiki/Extended_Industry_Standard_Architecture.

34 Wikipedia. "VESA Local Bus." Wikimedia Foundation. https://en.wikipedia.org/wiki/VESA_Local_Bus.

35 PCI-SIG. "Conventional PCI." http://www.pcisig.com/specifications/conventional/.

36 Wikipedia. "Conventional PCI." Wikimedia Foundation. https://en.wikipedia.org/wiki/Conventional_PCI.

37 Wikipedia. "Accelerated Graphics Port." Wikimedia Foundation. https://en.wikipedia.org/wiki/Accelerated_Graphics_Port.

38 PCI-SIG. "PCI Express®." PCI-SIG Administration. http://www.pcisig.com/specifications/pciexpress/.

39 Wikipedia. "PCI Express." Wikimedia Foundation. https://en.wikipedia.org/wiki/PCI_Express.

40 DEW Associates Corp. "Hard Drive Size Limitations and Barriers In Depth." http://www.dewassoc.com/kbase/hard_drives/hard_drive_size_barriers.htm

41 Torres, Gabriel. "Hard Disk Drives Capacity Limits." Hardware Secrets. http://www.hardwaresecrets.com/hard-disk-drives-capacity-limits/.

42 Wikipedia. "Parallel ATA." Wikimedia Foundation. https://en.wikipedia.org/wiki/Parallel_ATA.

43 Serial ATA International Organization. "Technical Overview." https://www.sata-io.org/technical-overview.

menos cableado. Si bien llevó otros cuatro años hasta que las interfaces SATA se volvieran algo común, su introducción causó un renombramiento inmediato del estándar original ATA al estándar Paralelo (PATA).

Ahora bien, hay un motive detrás de esta lección de historia de discos duros, y es esencial para Windows XP: Microsoft nunca lanzó oficialmente una versión de Windows XP con soporte nativo para interfaces de disco duro SATA incluidas en el CD de instalación. Microsoft refiere a este software de controlador de dispositivo[44] como "inbox" cuando están en los CDs (o DVDs) en la versión del producto en caja de Microsoft Windows que se vende en locales.

Por supuesto, Microsoft trabajó con varios fabricantes de discos duros, chips de control y computadores para asegurarse que SATA funcionara en Windows XP, pero para la mayoría de las personas, el medio para obtener una copia de Windows XP con soporte SATA integrado era adquirir un nuevo equipo con Windows XP cargado allí por el fabricante, que habría añadido los controladores de dispositivo de SATA como parte de las personalizaciones que hicieron en Windows XP para los computadores que vendieron. Es posible para los consumidores añadir los controladores de dispositivo SATA cuando instalan una versión en caja de Windows XP desde el comienzo, pero esto requería descargarlo de disquetes, o de tecnología incluso más antigua. Los departamentos de IT podrían también crear versiones semi personalizadas de Windows XP con controladores de dispositivo de SATA incluidas allí. Sin embargo, el proceso no es amigable para el usuario. No fue hasta 2007, con el lanzamiento de Windows Vista, que una persona pudo adquirir una copia empaquetada de Windows de un local y esperar una instalación exitosa en sus computadores equipados con SATA, al menos sin tener que realizar múltiples pasos.

44 A device driver is a specialized small program that allows a particular piece of hardware to communicate with the operating system.

Problemas con nuevos tamaños de sector de disco y Esquemas de partición de disco

Además de estos cambios en los conectores ajenos a las unidades de disco duro, también estaban ocurriendo cambios dentro de los discos: Desde comienzos de la década de 1980, los fabricantes de discos duros han estado creando discos que utilizaban sectores[45] de 512 bytes en extensión, siendo un sector el bloque de datos más pequeño que puede ser leído o escritos desde un disco. Por ejemplo, si crearas un archivo de 100 bytes de extensión, seguiría ocupando un sector de disco de 512 bytes. Si crearas un archivo de 513 bytes, ocuparía dos sectores, y así sucesivamente. Sin embargo, acceder a los sectores de forma individual introduce muchos gastos generales de Input/Output (entrada/salida) al buscar, leer y escribir datos, por lo que el sistema de almacenamiento agrupa sectores en grandes bloques llamados clústeres, que pueden alcanzar los 256 KB (o *512 sectores* de 512-bytes de extensión)[46].

Llevar un registro de cómo se almacenan los archivos en discos duros es trabajo para el sistema de almacenamiento, pero saber cómo se distribuye el espacio (o la forma en que se divide el disco/volumen) para los sistemas de almacenamiento en discos duros ha sido el trabajo del Master Boot Record (MBR)[47], un estándar que surgió en 1983 y, en su última implementación, tiene un límite de 232 sectores (o sea, 4.294.967.295 sectores, o 2.199 terbytes). Cuando se lanzó Windows en 2001, las unidades de disco duro estaban recién ingresando en el rango del gigabyte (GB), pero hoy, los consumidores ya pueden acceder a los discos duros de 8TB.

45 Wikipedia. "Disk Sector." Wikimedia Foundation. https://en.wikipedia.org/wiki/Disk_sector.

46 Microsoft. "Default cluster size for NTFS, FAT, and exFAT." Microsoft Corp. https://support.microsoft.com/en-us/help/140365/default-cluster-size-for-ntfs,-fat,-and-exfat.

47 Wikipedia. "Master Boot Record." Wikimedia Foundation. https://en.wikipedia.org/wiki/Master_boot_record.

Para que los computadores puedan hacer uso de las cada vez más amplias capacidades de disco duro, los proveedores de sistemas operativos y fabricantes de discos duros introdujeron varios cambios:

- *En 2010 se introdujo formalmente un nuevo estándar para dividir las unidades de disco duro, llamada Tabla de Particiones GUID (GPT)[48]. Teóricamente, esta soporta discos duros de hasta 9,4 zettabytes (9,4 miles de millones de terabytes). Windows XP no reconoce unidades de disco duro con estándar de partición GPT.*
- *Asimismo, un nuevo estándar se introdujo para el tamaño de sectores. En lugar de seguir utilizando el estándar de casi 30 años de antigüedad de 512 bytes por sector, los fabricantes de unidades de disco acordaron una transición, que comenzó en enero de 2011, a sectores de 4.096 bytes (4 kilobytes), un cambio al que se refirió como tecnología de Formato Avanzado (AF)[49, 50, 51]. Windows XP no soporta los discos duros con sectores de Formato Avanzado (4KB) de forma nativa, pero se hará más referencia a ello adelante.*

Estos abordajes son sensibles, dada la naturaleza de las capacidades de almacenamiento en constante crecimiento; sin embargo, introducen problemas adiciones para quien utilice o mantenga sistemas Windows XP. Incluso si los usuarios no necesitan usar una partición de disco mayor a los 2TB con sus instalaciones de Windows XP, podrían acabar usando discos duros de sectores de Formato Avanzado (4KB) dada la falta de disponibilidad de discos con sectores de 512-bytes nativos.

48 Wikipedia. "GUID Partition Table." Wikimedia Foundation. https://en.wikipedia.org/wiki/GUID_Partition_Table.

49 International Disk Drive Equipment and Materials Association. "Advanced Format (AF) Technology." http://www.idema.org/?page_id=98.

50 International Disk Drive Equipment and Materials Association. "The Advent of Advanced Format." http://www.idema.org/?page_id=2369.

51 Coughlin, Thomas M. "Aligning with the Future of Storage." Coughlin Associates, Inc. https://tomcoughlin.com/Coughlin/Techpapers/2011_06%20Alignment%20White%20Paper%20(Coughlin%20Assoc.)%20final.pdf.

A diferencia de la tecnología de partición de disco GPT, los discos duros de Formato Avanzado[52] que utilizan sectores de 4KB etiquetados como "Formato Avanzado 512e", o simplemente discos duros "512e" ***son*** retrocompatibles con sistemas operativos antiguos como Windows XP que usan sectores de 512-bytes de extensión. La conversión entre sectores de 512 bytes y 4.096 bytes la lleva adelante la unidad de disco por sí misma. Esto introduce una pequeña falla de desempeño por los gastos generados de la emulación de sectores de 512 bytes.

Pequeña referencia a las Unidades de Estado Sólido

Dado que varias instalaciones actuales de Windows XP tienen requerimientos de almacenamiento modestos, podría ser tentador remplazar las unidades de disco duro con unidades de estado sólido (SSDs).

Hoy, las más nuevas unidades de estado sólido pueden operar 45 veces más rápido que los discos duros, especialmente que aquellos disponibles al mismo tiempo de Windows XP. Los discos duros también sufren fallas en su desempeño por la *fragmentación* de archivo, causada al tener que leer y escribir archivos dispersos en diferentes sectores de sus placas internas (los verdaderos discos dentro de las unidades de disco duro). En contraste, las unidades de estado sólido no tienen partes movibles y se accede a todas sus partes con la misma velocidad, lo que significa que la fragmentación de archivo tiene poco (o ningún) efecto sobre ellos.

Si bien las unidades de estado sólido no sufren de la fragmentación de archivo, con el tiempo sí pueden verse afectadas por problemas de desempeño comparables, al tener que mantener un registro de qué sectores (en los SSD, llamados *bloques*) se utilizan dentro de qué clústeres (aquí llamados *páginas*). Esto se resuelve permitiendo que las unidades

52 Wikipedia. "Advanced Format." Wikimedia Foundation. https://en.wikipedia.org/wiki/Advanced_Format.

de estado sólido identifiquen de forma periódica las páginas que ya no están en uso y las marquen como espacio libre, una técnica comúnmente conocida entre los programadores como *recolección de basura*. Para las unidades de estado sólido, a esta recolección de basura se la llama *recorte*, y, sin sorpresas, es llevado adelante por el sistema operativo, que lanza una orden TRIM a las unidades de estado sólido[53], lo que significa que el desempeño de la unidad se enlentecerá con el tiempo, incluso a velocidades por debajo de las de los discos duros.

CONSEJO	La ausencia de una orden TRIM solo obstaculiza a Windows XP al instalarlo directo de una unidad de estado sólido. Puedes ejecutar Windows XP como "invitado" (en una máquina virtual) en hardware moderno que soporte TRIM, de Windows 7 en adelante, que permiten al sistema operativo "anfitrión" administrar las operaciones TRIM.

Respaldando tu hardware

Es importante recordar que el índice de fallas de cualquier parte de un computador es 100%... eventualmente. Incluso si tu equipo no usa ninguna tarjeta de expansión "especial" u otro hardware, sigue siendo una buena idea mantener repuestos disponibles, como discos duros y ventiladores, que contienen partes mecánicas que se gastan con el tiempo. Las partes de estado sólido sin componentes movibles como la memoria, placas base y algunas fuentes de energía pueden sufrir fallas a medida que se vuelven más antiguas y atraviesan ciclos de expansión y contracción térmica durante su uso normal.

Incluso partes como las unidades de disco duro, de las que uno podría pensar que se mantienen relativamente sin cambios con el tiempo, deben tener un suministro especial pensadas para ellas, dados los cambios tecnológicos como las interfaces SATA y la sectorización de Formato Avanzado.
En casos como este, la mejor opción puede ser mantener no solo un inventario de partes reemplazables, sino un computador entero (o dos) que haya sido construido y configurado para ejecutar esa aplicación crítica para el negocio. De esta manera, si ese viejo computador con Windows XP falla, puedes removerlo, instalar el nuevo, y seguir funcionando en minutos tras cargar tu copia de backup o archivos de datos en el nuevo computador. Podrías incluso reemplazar el equipo "en uso" con el "extra" dos o tres veces al año, permitiéndote realizar un mantenimiento preventivo, de limpieza y recambio de partes mecánicas antes de que ocurra una falla. Por cuestiones de confianza y durabilidad, las partes y computadores de repuesto deberían guardarse en ambientes climatológicamente controlados. Algunos componentes, como las placas base y controladores de almacenamiento tienen baterías incorporadas. Estas deberían ser desconectadas y removidas antes de almacenarse por largos períodos para evitar daños. Un depósito en tu oficina debería cumplir con los requisitos para el propósito. Un espacio sin calefacción ni aire acondicionado no es lo ideal, ya que la exposición excesiva al calor, al frío, a la humedad y a la sequedad puede reducir la vida útil de los materiales electrónicos, incluso cuando no están encendidos.

Respaldando tu software

Ahora que tienes una idea de los pasos a tomar para mantener el hardware para que ejecute Windows XP, veamos los requerimientos para respaldar lo que hace al software. La discusión será más acotada que la sección de hardware, arriba, no porque sea más simple – no lo es – sino porque es muy compleja. En lo que hace a backups, ESET tiene un White Paper dedicado exclusivamente a la materia (en inglés), *Options for Backing Up Your Computer*[54]. En consecuencia, solo veremos algunos aspectos esenciales de los presentes en este documento para respaldar tu máquina.

53 Wikipedia. "Trim (computing)." Wikimedia Foundation. https://en.wikipedia.org/wiki/Trim_(computing)

54 Goretsky, Aryeh. "Options for backing up your computer." ESET. http://www.eset.com/fileadmin/Images/US/Docs/Home/Staying_Secure/2205_19_0_EsetWP-OptionsBackingUpComputer.pdf.

Si buscas respaldar un computador que ejecuta Microsoft Windows XP, hay dos formas básicas de backup que pueden llevarse adelante:

- *La primera es un backup de archivos, que significa básicamente realizar copias de los archivos del computador en otro sitio. Por ejemplo, del disco duro del computador a un recurso compartido de red, una unidad de disco duro externa enchufada al puerto USB, etc. La ventaja de este abordaje es que los archivos son fácilmente accesibles y están disponibles mediante la simple conexión de una unidad externa de disco duro en un nuevo computador, conectándose al recurso compartido que contiene los archivos, etc.*
- *El segundo mecanismo es un backup "blob" (objeto binario). Con este mecanismo, los archivos (o incluso el disco duro completo) se respaldan en bloques monolíticos. Estos bloques pueden variar en tamaño de megabytes a gigabytes, para facilitar su almacenamiento en medios ópticos, como CDs y DVDs, o para grabar. La implementación más común en la copia de discos, donde se copian los contenidos del disco duro, en uso o no, a otra unidad de disco, unidad de grabado u otro medio de almacenamiento con la misma capacidad del disco duro original, o mayor.*

Nuevamente, para acceder a información más detallada, incluyendo las ventajas y desventajas de cada mecanismo, cómo programar respaldos, y, lo más importante, cómo probarlos, recomendamos acceder al White paper de ESET sobre backups (en inglés).

CONFIGURANDO XP PARA EL USO A LARGO PLAZO

Si planeas seguir utilizando Microsoft Windows XP durante un período extendido, pasada la fecha límite, 8 de abril de 2014, tenemos una variedad de recomendaciones para ti.

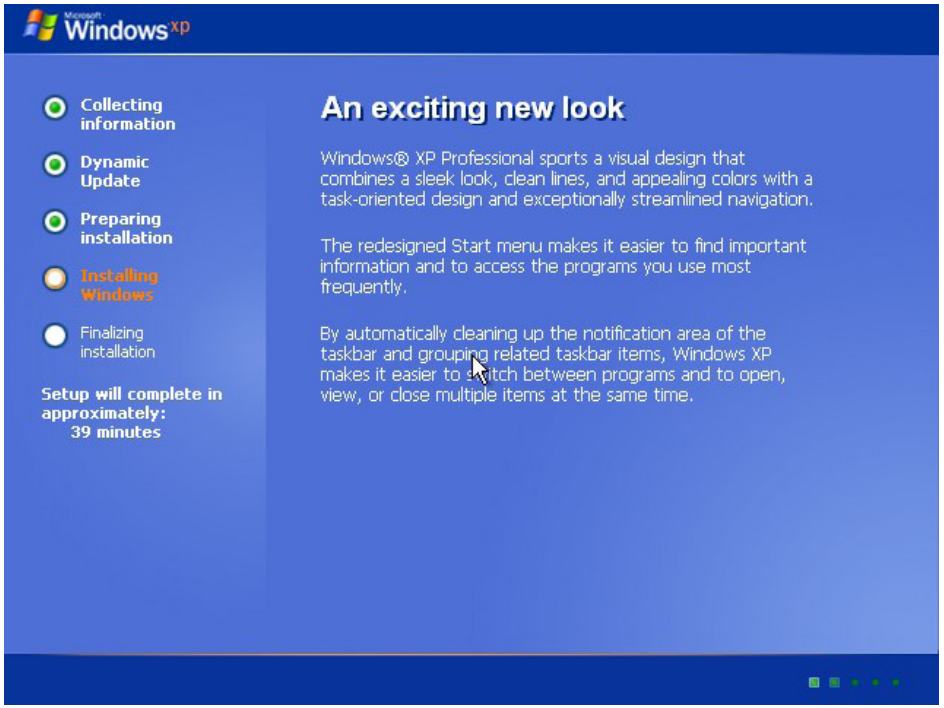


Figura 3: pantalla de instalación de Windows XP

Primero, comienza por preparar tu PC para un uso extendido mediante una instalación limpia de Windows XP. Si la actual instalación tiene varios años de antigüedad, hay posibilidad de que esté plagado de restos y escombros que resultan de cualquier instalación vieja de Windows, como controladores de dispositivo faltantes o desactualizados, programas completamente desinstalados, programas obsoletos o que ya no estén en uso, pero sigan presentes, atajos rotos, asociaciones de archivos mal hechas, y más. Ya que tener una mezcla de errores de software y sistema operativo puede afectar la confiabilidad, estabilidad y desempeño del equipo en el largo término, comenzar de cero con una instalación nueva de este sistema operativo antiguo es un paso importante para prepararlo para ser usado ahora que ya no tiene el soporte de Microsoft.

Como recordatorio, no utilices el computador para acceder a Internet mientras instalas todos los Service Pack, parches, revisiones y otras actualizaciones de Windows XP. XP es vulnerable a los ataques y el computador debería contar con un firewall que prevenga la explotación de sus vulnerabilidades todavía sin solucionar. Es preferible descargar las actualizaciones de Windows XP en un equipo con sistema operativo moderno y seguro, y transferirlas luego al que ejecuta Windows XP. Esto aplica también al software de seguridad.

Instalar XP nuevamente

De ser posible, comienza con una unidad de disco duro vacía y sin formatear – o al menos una que puedas eliminar previo a la instalación. Usar una unidad vacía ayuda a asegurar la ausencia de problemas de software o archivos de sistema para comenzar, que pueden existir si se usa una versión ya instalada de Windows XP. Hemos mencionado los pasos necesarios para asegurar la compatibilidad entre la unidad de disco duro y Windows XP. Si el disco duro usa una interfaz SATA, asegúrate que tu medio de instalación para Windows tenga ya añadidos los controladores de dispositivo, o que tú cuentas con ellos para instalarlos mediante un disquete, ya que el instalador de Windows XP no reconoce conexiones de red o USB. El soporte para unidades ópticas adicionales puede ser limitado, lo que vuelve a los disquetes la mejor manera de instalar controladores de dispositivo si éstos no están presentes en el medio de instalación. Una vez que la instalación de Windows XP haya finalizado, podrás acceder a estos otros tipos de dispositivos.

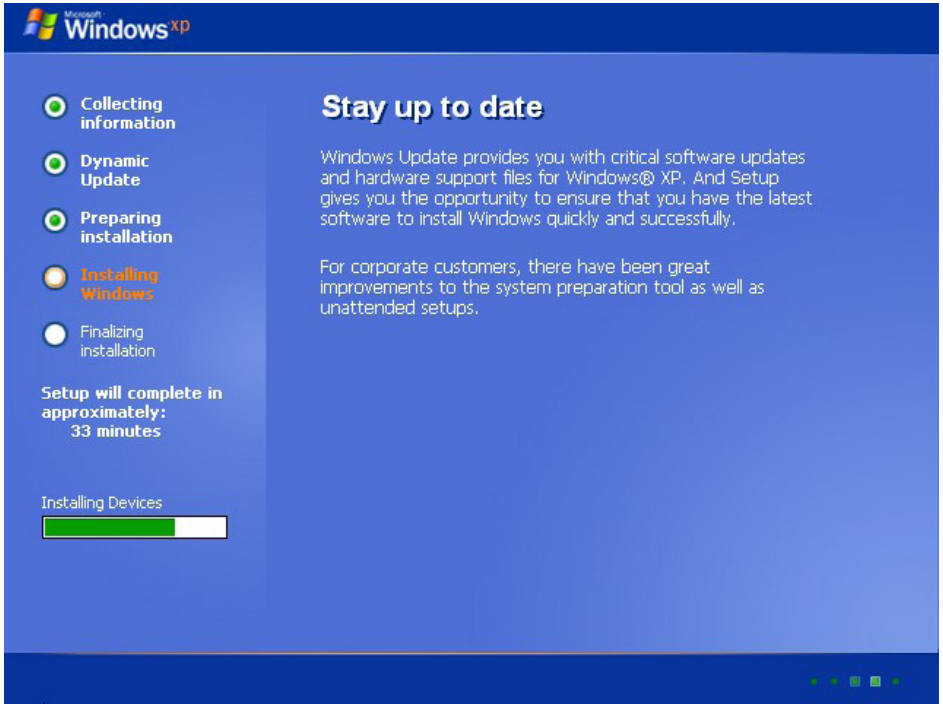


Figure 4: Otra pantalla de instalación de Windows XP

Para conectarte a cualquier red, incluyendo Internet, podrías necesitar instalar controladores de dispositivo para la tarjeta de interfaz de red (también conocida como adaptador de red) del computador. Estos podrían haber estado incluidos en la versión de Windows XP del fabricante del computador que estás instalando. En caso de no estarlo, podrían figurar en un CD o DVD que vino con el computador. Si tampoco sucede, podrías tener que descargarlos desde el sitio web de soporte del fabricante en otro computador, copiarlos al CD, DVD o USB, y transportarlos para ser instalados en el "nuevo" computador que ejecuta Windows XP.

Instalar los Service Pack de Windows XP

Probablemente haya varios años de actualizaciones para aplicar, incluyendo uno o varios de los Service Pack de Microsoft para Windows XP. Un Service Pack reúne no solo cientos de actualizaciones existentes en un único paquete, sino también cambios en las configuraciones por defecto de cuando se lanzó Windows XP. Los Service Pack contienen además versiones nuevas de viejas actualizaciones existentes, y permite aplicarlas al sistema operativo en conjunto y no individualmente.

Para conocer qué Service Pack, si hay alguno, se instaló con tu versión de Microsoft Windows XP, haz clic en el botón de inicio, escribe "`winver.exe`" y presiona Enter. La versión de Windows se desplegará junto con el nivel de Service Pack. Si no se despliega ninguna información del Service Pack, entonces la versión RTM (de distribución a fabricantes, por sus siglas en inglés) original de Windows XP es la instalada.

Si tienes suerte, tu medio de instalación para Windows XP incluye el Service Pack 3 – el último lanzado para XP – y tu descarga se limitará a cualquier actualización requerida pos-SP3. Eso sigue siendo equivalente a varios cientos de megabytes de actualizaciones, pero no es una cantidad insuperable, especialmente con una conexión a Internet veloz.

Cabe destacar que el Service Pack 3 es para versiones de Windows XP de 32-bits únicamente; la última edición de Service Pack de 64-bits para Windows XP es el 2.

La siguiente tabla da un panorama de los mayores cambios que cada Service Pack trajo a Microsoft Windows XP, junto con los enlaces a las páginas del sitio de Microsoft de donde puede descargarse cada Service Pack:

Service Pack	Fecha de lanzamiento	Características destacadas y mejoras / Enlaces de descarga
1	Septiembre, 2002	Más de 300 correcciones de fallos menores. Soporte de USB 2.0; Soporte de Microsoft Java y .NET Framework. Configuración del Applet de Acceso a Programa y Panel de Control por defecto. **Descarga:** `http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/xpsp1a_8441053935adbfc760b966e5e413d3415a753213.exe`
2	Agosto, 2004	Más de 820 correcciones de fallos; mejoras al Wi-Fi y Bluetooth; soporte de Acceso Protegido al Wi-Fi nativo, bloqueador de pop ups en Internet Explorer 6; Prevención de Ejecución de Datos; eliminación de raw sockets; Centro de Seguridad de Windows; mejoras de Firewall de Windows. **Descarga:** `http://www.microsoft.com/en-us/download/details.aspx?id=28`
3	Mayo, 2008	Más de 1,700 correcciones de fallos; mejoras al BITS, Prevención de Ejecución de datos, Políticas de grupo, IPSec, MMC, RDP, Windows Imaging, Windows Installer, Gestión de Windows Script y certificado X.509 ; Soporte de Wi-Fi Protected Access 2; cliente de Network Access Protection para empresas. **Descarga:** `https://www.microsoft.com/en-us/download/details.aspx?id=55245`

**En febrero 2003, Microsoft Java Support fue removido del SP1 por una demanda con Sun Microsystems y el Service Pack lanzado nuevamente como SP1a.*

Estamos proveyendo enlaces a los sitios de descarga de cada Service Pack de Windows XP en caso de que desees descargarlos e instalarlos de forma independiente antes de comenzar el proceso de Windows Update. Estos sitios de descarga pueden cambiar en el futuro, por lo que es recomendable guardar actualizaciones importantes del sistema operativo como éstas en una locación fácil de recordar, para que puedan ser instaladas a futuro sin tener que descargarlas nuevamente.

CONSEJO	Para acelerar el proceso de actualizar Microsoft Windows XP, descarga todos los Service Pack(s) que necesites e instálalos de forma independiente ***antes*** de ejecutar Windows Update. Esto reduce la cantidad de tiempo que se ocupa descargando actualizaciones para Windows XP, ya que se mostrarán solo las actualizaciones posteriores al Service Pack 3.

Las actualizaciones del Service Pack de Windows XP son, en teoría, *acumulativas*. Esto significa que el Service Pack 2 contiene todas las actualizaciones del Service Pack 1, y que el Service Pack 2 contiene todas las actualizaciones del Service Pack 2 y Service Pack 1. En la práctica, Microsoft no recomienda la instalación del Service Pack 3 en equipos que ejecuten el RTM original o las versiones SP1 de Windows XP, por lo cual conviene que instales el Service Pack 2 antes, para actualizar el sistema operativo de RTM a SP1, reiniciar, e instalar el Service Pack 3.

Actualizaciones de Windows

Incluso si estás realizando una instalación nueva de Microsoft Windows XP con el Service Pack más actualizado, tendrás aún varios años de actualizaciones posteriores al Service Pack 3 para instalar tras hacer los cambios necesarios para obtener acceso a la red, como instalar los controladores de dispositivo para un adaptador de red.

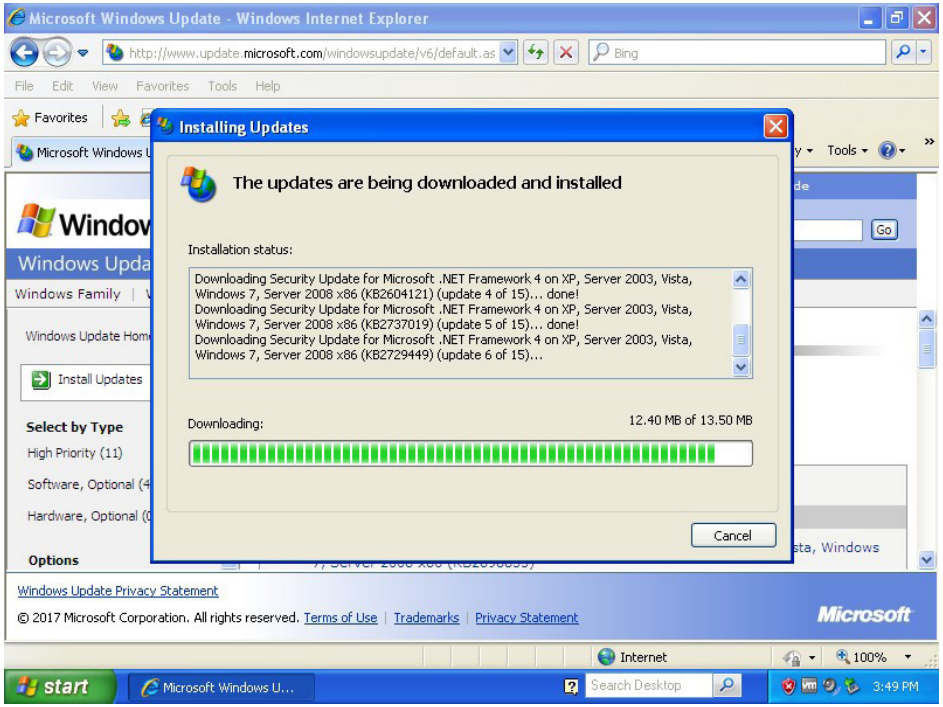


Figure 5: Windows Update ejecutado desde el buscador web en Windows XP

Una vez que Windows XP obtenga acceso a la red, el siguiente paso será permitir la ejecución de las Actualizaciones Automáticas de Windows XP, para que el sistema operativo descargue e instale todos los parches, hotfixes y Service Packs que han sido lanzados desde que se creó el medio de instalación de Windows XP.

Dependiendo del tiempo que tenga tu instalación de Windows XP, el sistema operativo puede ser tan antiguo que requiere una renovación del mecanismo Windows Update en sí antes de poder descargar cualquier actualización futura. Esto puede hacerse abriendo el **Panel de Control**, ingresando al **Centro de Seguridad** haciendo clic sobre él, seleccionando la opción de *Actualizaciones Automáticas* debajo en la

ventana, y asegurándote que las Actualizaciones Automáticas estén configuradas como *automáticas* (*recomendado*).

Figura 6: Habilitando actualizaciones automáticas desde el Centro de Seguridad de Windows

Esto permitirá que Windows XP descargue mejoras críticas para el mecanismo de actualización del sistema operativo, tras la cual será necesario un reinicio del equipo. Una vez hecho, permite que las *Actualizaciones Automáticas* procedan a instalar cualquier actualización crítica necesaria. Tras instalarse estas últimas, puedes instalar las actualizaciones de seguridad y soluciones de errores iniciando **Windows Update** desde el Menú de Inicio. Si el atajo de Windows Update no está disponible, abre Internet Explorer y dirígete a http://update.microsoft.com/ para comenzar el proceso de descarga e instalación de actualizaciones. A diferencia de las versiones más recientes de Windows, que tienen una aplicación dedicada a instalar Windows Updates, Windows XP las instala desde el buscador de Internet Explorer.

ADVERTENCIA	Según cuándo tus discos de instalación de Windows XP se hayan creado, podrían ser cinco, diez o incluso más años de desactualizaciones. Como resultado, Windows XP será **muy inseguro**, no solo hasta estar completamente emparchado (un proceso que puede tomar algunas horas dependiendo de la velocidad de tu conexión a internet y los varios reinicios requeridos) sino también hasta que finalices asegurándolo aún más contra los ataques. Para ayudar a proteger Windows XP mientras está siendo instalado, es importante seguir estas dos instrucciones: 1. Si es posible, **no** conectes el computador directamente a Internet utilizando un modem, ya que una conexión directa significa que los atacantes tendrán fácil acceso al equipo desprotegido. En cambio, asegúrate que tu computador está conectado a un router, que, como su nombre implica, rompa la conexión directa que el computador tiene a Internet, y viceversa, haciéndolo un objetivo más difícil para los atacantes. La mayoría de las conexiones a Internet utilizan un router hoy en día, pero las conexiones directas siguen estando disponibles en muchos sitios del mundo. Contacta tu proveedor de servicio de Internet si no estás seguro de qué clase de conexión a Internet proveen. 2. No visites ningún sitio web, descargues programas o ejecutes software que se conecte a Internet hasta que Windows XP haya finalizado con sus actualizaciones por completo y tú hayas tomado medidas extra para protegerlo. Utilizar Windows XP vuelve a un computador un objetivo claro, y no deberías utilizarlo en Internet hasta haber minimizado esa amenaza lo máximo posible. Así como con Windows Updates y controladores de dispositivos, descarga software de seguridad para Windows XP en un computador ya asegurado, y trasládalo al equipo para la instalación. Si existe la opción de un "instalador web" y un "instalador offline", elige el instalador offline para que el programa completo pueda instalarse. Seguirá necesitando descargar algunas actualizaciones una vez finalizada la instalación, pero el programa completo será instalado y podrá ofrecer cierta protección.

En la pestaña de actualizaciones *opcionales* de Windows Update, puedes encontrar una opción para instalar Microsoft Security Essentials (MSE), el programa antimalware gratuito de Microsoft (más conocido como anti-virus) para uso hogareño y pequeños negocios con menos de 55 PCs[55, 56]. If you are planning on using anti-malware software from a different vendor (including ESET) you should not install MSE onto the computer. We will discuss anti-malware software in greater depth, below.

Windows Updates versus Microsoft Updates

Durante la instalación de actualizaciones de Windows desde el browser de Internet Explorer, podrías ver también una solicitud de instalación de ***Microsoft Update***.

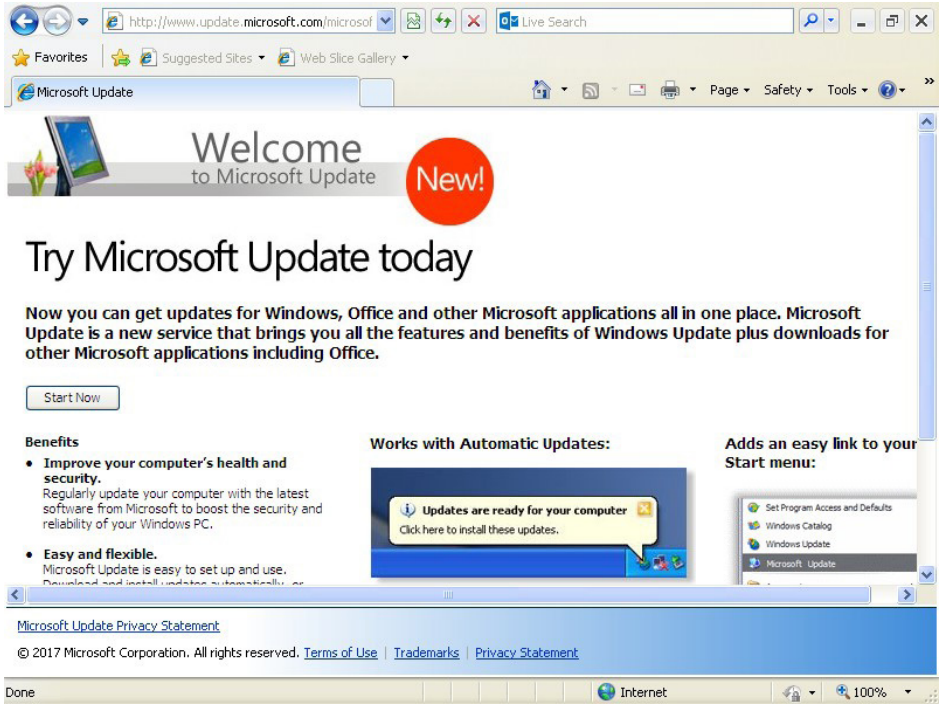


Figura 7: Windows Update solicita Microsoft Update

Mientras Windows Update provee actualizaciones para los archivos centrales del sistema operativo, no brinda ninguna actualización para aplicaciones, como Microsoft Live Essentials, Office, Skype y Silverlight.

55 Microsoft. "Microsoft Security Essentials – Protect Your PC." *http://windows.microsoft.com/en-US/windows/security-essentials-download*.

56 Microsoft "Microsoft Safety & Security Center: Get free virus protection with Microsoft Security Essentials." *http://www.microsoft.com/security/pc-security/microsoft-security-essentials.aspx*.

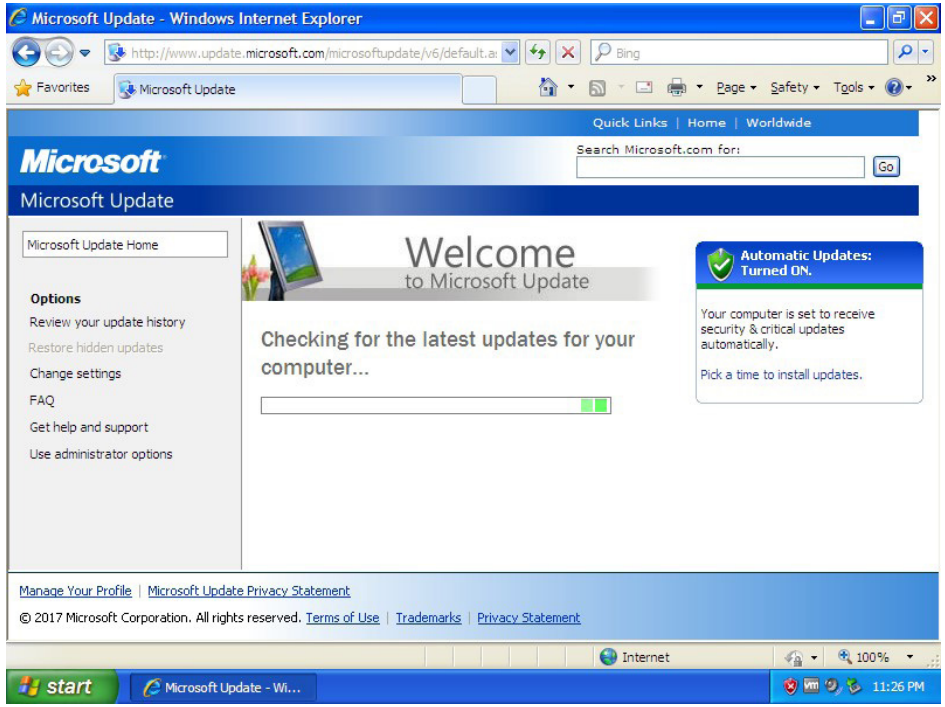


Figura 8: Microsoft Update buscando actualizaciones

Recomendamos que habilites Microsoft Update para obtener actualizaciones para estos programas.

Para actualizar Microsoft Windows XP por completo, podrías necesitar ejecutar Windows Update o Microsoft Update varias veces, ya que algunas de las mejoras iniciales que se descargan podrían requerir más actualizaciones por sí solas. Sigue ejecutando estos actualizadores de forma manual hasta que todas las mejoras estén instaladas y no se ofrezcan nuevas.

CONSEJO	Windows Update y Microsoft Update muestran cada actualización disponible como una línea única con una casilla de verificación por delante en Internet Explorer. Cuando seleccionas una actualización, se expande hacia abajo para mostrar varias líneas de texto descriptivo. Para minimizar la cantidad de scrolling que debe hacerse para ver la lista, comienza desde abajo y ve subiendo desde allí hasta el comienzo.

Instalación de Controladores de dispositivo

Durante el proceso de Windows Update, probablemente se te pida instalar software de controlador de dispositivo faltante o actualizado para permitir que Microsoft Windows XP funcione mejor con el hardware del computador. En el pasado, Windows Update ha tenido algunos problemas con la identificación y provisión de controladores de dispositivo correctos, provocando que algunos equipos tengan un desempeño pobre, o que incluso no reaccionen. Esto ha llevado a ciertas personas a recomendar dirigirse al sitio de soporte del fabricante de hardware para descargarlos, o a intentar identificar el verdadero chip del fabricante, ir a su sitio de soporte y descargar los controladores desde allí.

Microsoft ha hecho un gran esfuerzo para mejorar la correcta detección de hardware y la descarga de los controladores de dispositivo correctos desde Windows Update en los últimos años, y ha aliviado estos asuntos en gran medida. Sin embargo, eso no siempre significa que Windows Update vaya a proveer los *últimos* controladores de dispositivo para el hardware de un computador, solo aquellos que han sido lanzados por el fabricante del computador o de los chips dentro de él. Algunos fabricantes ofrecen un programa que automáticamente identifica controladores faltantes o

desactualizados y los instala automáticamente[57, 58, 59]. Si tu equipo lo hace, considera usarlo para descargar controladores de dispositivo si tienes preocupaciones sobre Windows Update.

Para asegurar que tienes los controladores de dispositivo de Microsoft Windows XP más recientes para tu equipo, te recomendamos que visites el sitio de soporte del fabricante, desde un computador con un sistema operativo al día que sea soportado y tenga un software de seguridad instalado actualizado, los descargues y luego los transfieras mediante CD, DVD o USB para la instalación en un computador ejecutando Windows XP.

Los fabricantes de computadores no suelen soportar Microsoft Windows XP de forma indefinida con actualizaciones de controladores de dispositivo, y algunos pueden incluso quedar fuera de uso y, en consecuencia, discontinuarse su soporte. Por este motivo, recomendamos que, luego de descargar cualquier controlador de dispositivo necesario, los guardes en una locación fácil de recordar, así como una copia separada en una carpeta de archivo segura.

Aquí hay una pequeña (y, por necesidad, incompleta) lista de controladores de dispositivo que podrías querer utilizar al identificar los controladores que son necesarios para instalar Windows XP en tu computador:

¿Requerido? / ¿Descargado?	Descripción	Proovedores Frecuentes
☐/☐	Controladores de audio para tarjeta de sonido Versión: _____	Analog Devices, AMD (antes ATI), C-Media, Creative Labs, IDT, M-Audio, Realtek, SigmaTel, Turtle Beach, VIA
☐/☐	Controladores de conjunto de chips para placa madre Version: _____	AMD (antes ATI), Intel, nVidia, SIS, ULI (antes ALI), VIA, Winbond
☐/☐	Específicos para computador *(para mouse y teclado, administración de energía, funcionalidades específicas para placa madre, tarjetas de expansión, y más).* Version: _____	Acer (antes Gateway), AMD (antes ATI), ASRock, Asus, Clevo, Dell, ECS, EVGA, Foxconn, Fujitsu, Gigabyte, Hewlett-Packard (antes Compaq), Intel, Lenovo (antes IBM), MSI, Packard Bell, PNY, Samsung, Shuttle, SONY, Supermicro, Toshiba, Tyan, VIA, XFX, ZOTAC
☐/☐	Controladores de red para conexiones de red por cable *(Ethernet, Fibra, Anillo Token)* Version: _____	ASIX, Atheros, Broadcom, Cisco, Hewlett-Packard (antes 3Com), Intel, Marvell, nVidia, Ralink, Realtek, SIS, SMC, US Robotics, VIA, Winbond
☐/☐	Controladores de red para conexiones inalámbricas *(Bluetooth, Wi-Fi)* Version: _____	Agere, Atheros, Broadcom, CSR, Intel, Ralink, Realtek, TDK, Toshiba, VIA
☐/☐	Controladores SATA, PATA o SCSI para controladores de unidad de disco Version: _____	3ware, ALI, Adaptec, AMD (antes ATI), Areca, Avago, High Point, Intel, ITE, JMicron, LSI, Marvell, nVidia, Promise, Silicon Image, SIS, VIA
☐/☐	Controladores de impresora para impresora Version: _____	Brother, Canon, Citizen, Dell, EPSON, Hewlett-Packard, Lexmark, Kodak, Konica, Kyocera, OKI, Panasonic, Ricoh, Xerox
☐/☐	Controladores de video para tarjetas de video Version: _____	AMD (antes ATI), Hauppauge, Intel, Matrox, nVidia, S3, SIS, VIA

57 Dell. "Dell Driver Download Manager FAQs." *http://support.dell.com/support/topics/global.aspx/support/downloads/en/downloads_faq*.

58 "HP Customer Support – Software and Driver Downloads." *https://support.hp.com/us-en/drivers*.

59 Lenovo. "ThinkVantage System Update." *http://support.lenovo.com/en_US/detail.page?LegacyDocID=TVSU-UPDATE*.

Es recomendable descargar siempre los controladores de dispositivo ***directamente*** desde el chip de silicio (circuito integrado) o el sitio web del fabricante, como deberías hacerlo con cualquier otro software. Evita visitar sitios de terceros, ya que no hay garantía de su seguridad o la confiabilidad de sus archivos. En algunos casos, esto puede ser inevitable; sin embargo, asegúrate de comprobar los archivos cuidadosamente con tu software de seguridad antes de usarlos.

Además de los controladores de dispositivo para mantener un registro el hardware del computador, podría haber actualizaciones disponibles para el hardware por sí solo en la forma de nuevo firmware de BIOS (software que se almacena en un chip y ejecuta cuando el computador se inicia). Las placas madre, y algunas tarjetas de expansión, suelen tener un chip programable que contiene instrucciones sobre cómo comunicarte con los varios dispositivos que se conecten a él. Los fabricantes los actualizan periódicamente para añadir compatibilidad con nuevos dispositivos, mejorar el desempeño y, sí, incluso solucionar errores (después de todo, es software). Averigua con el fabricante del dispositivo para determinar si hay una actualización del firmware de BIOS disponible – y necesaria – para tu hardware.

Tras instalar los últimos controladores de dispositivo para el hardware del computador, deberías tener no solo una versión completamente actualizada de Microsoft Windows XP, sino una instalación que también cuenta con los últimos controladores de dispositivo para soporte de hardware. Si bien aún no se han instalado aplicaciones de terceros o software utilitario, este puede ser un buen momento para crear un backup (o más de uno) del disco duro de tu computador. Un backup de imagen aquí brinda una ventaja al hacer más rápida la recuperación si el sistema operativo no funciona. Esto puede ahorrar el tiempo y el esfuerzo requerido para reconstruir Windows XP de cero, si surgiera un problema y el único backup se ve dañado o no está.

Este respaldo del disco provee una copia básica que rápidamente puede volver a cargarse en caso de haber un problema al instalar el software especializado que solo se ejecuta con Microsoft Windows XP.

CONSEJO	Las copias de backup deberían guardarse siempre en lugares seguros y fáciles de recordar. De esa manera, podrás accede a ellos fácilmente en caso de necesitar una restauración. De hecho, este es un buen momento para verificar que el backup esté funcionando correctamente, llevando a cabo una restauración a un disco en blanco extra de tu inventario de partes. Esto te permitirá verificar que el backup esté funcionando antes de que surja una situación de emergencia en la que realmente lo necesites, pero halles que no está funcionando. Recuerda: el mejor momento para solucionar problemas es **antes** de que se vuelvan una emergencia que provoque pérdidas de productividad e ingresos en tu negocio.

Preparación para el uso

Ahora que ya cuentas con tu instalación base de Microsoft Windows XP, actualizada con los últimos Service Pack y *hot fixes*, y con todos los controladores de dispositivo necesarios para operar, es hora de comenzar a cargar ese software que solo pueda ejecutarse bajo Windows XP.

Es importante tener en cuenta no deberías instalar todo el software que sueles usar en un computador; el objetivo de esta actividad es, después de todo, crear un sistema que ejecute Microsoft Windows XP que pueda ser utilizado tanto como se lo necesite antes de reemplazarlo con una versión más moderna y segura de Windows. Cualquier programa adicional que se sume al computador significará otra pieza de software con sus propias vulnerabilidades para explotar por un atacante. Mantener al mínimo la cantidad de software instalado reduce el "tamaño" de la "superficie de ataque" del computador, es decir, el tamaño del riesgo.

Dependencias del framework

Si el software que estás instalando depende de un framework en particular, como .NET de Microsoft, Microsoft Silverlight, Adobe Flash, Adobe Reader u Oracle Java, instala la última versión compatible con Windows XP. Si el desarrollador sigue actualizándolo en el futuro, descarga e instala también estas actualizaciones, ya que las vulnerabilidades en el software o framework pueden ser explotadas por un atacante. Si el software requiere una versión más antigua e insegura de un framework, o el framework ya no soporta Windows XP, instala la versión más reciente y confirma con su desarrollador para ver tiene recomendaciones adicionales sobre cómo asegurarlo.

Buscadores Web

Si bien el buscador de Microsoft, Internet Explorer 8.0[60] , ya no es un objetivo, sigue habiendo amenazas que pueden explotarlo, y dado que ya no se lo actualiza para Windows XP, es recomendable usar un nuevo buscador web que reciba actualizaciones de seguridad.

Google Chrome y Mozilla Firefox son dos buscadores muy utilizados; sin embargo, Google Chrome dejó de soportar Windows XP y Windows Vista en abril de 2016 en el lanzamiento de su versión 49[61]. Si bien esto lo convierte en una mejor opción para la búsqueda de sitios web modernos que Internet Explorer, sigue siendo poco recomendado para la seguridad y la privacidad. La Fundación Mozilla anunció que Firefox sería soportado en Windows XP[62] y Vista hasta junio de 2018, luego de esta fecha la fundación analizaría si continuar dando soporte (en septiembre de 2018 se puso fin a esto).

Dado que Google Chrome está basado en Chromium, un proyecto de código abierto, y Mozilla Firefox fue también lanzado como un proyecto de código abierto, es posible que haya varias de estas bases de código en buscadores web que continúen el soporte de Windows XP. Si puedes optar por usar dicho buscador, asegúrate de probarlo a fondo para ver si es compatible.

PDF Readers

Como se mencionó anteriormente, para evitar que se expanda la superficie de ataque del sistema, deberías evitar la instalación de cualquier software adicional ajeno a lo que es absolutamente necesario con Windows XP. El software que lee o imprime archivos PDF puede, sin embargo, ser un requerimiento. El lector de PDF más popular es Adobe Acrobat Reader, y Adobe Acrobat Reader XI (alias v11.0) es soportado en Windows XP con Service Pack 3 para 32 bits o Service Pack 2 para 64 bits[63].

La especificación del documento PDF permite que JavaScript sea utilizado para automatizar procesos de trabajo y formularios, y estos suelen ser usados como vectores de ataque debido a que pueden contener código malicioso. Es importante mantener al día la versión de Adobe Acrobat Reader para protegerte de las vulnerabilidades. Si tienes que usar Adobe Acrobat Reader, verifica que el Modo Protegido, la Vista Protegida y la Seguridad Mejorada de Adobe Reader estén habilitadas, y deshabilita

60 Wikipedia. "Internet Explorer 8." Wikimedia Foundation. *http://en.wikipedia.org/wiki/Internet_Explorer_8*.

61 Pawliger, Marc. "Update to Chrome platform support." Google, Inc. *https://chrome.googleblog.com/2015/11/updates-to-chrome-platform-support.html*.

62 Mozilla. "Update on Firefox Support for Windows XP and Vista." Mozilla Blog. *https://blog.mozilla.org/futurereleases/2017/10/04/firefox-support-for-windows-xp-and-vista/*.

63 Wikipedia. "Adobe Acrobat version history." Wikimedia Foundation. *https://en.wikipedia.org/wiki/Adobe_Acrobat_version_history#Adobe_Acrobat_and_Reader*.

JavaScript[64, 65]. Si no puedes deshabilitar JavaScript, bloquéalo lo más posible siguiendo las instrucciones de Adobe[66, 67].

Si tu uso de archivos PDF no requiere la automatización de formularios o procesos, considera utilizar otro lector de PDF que soporte Windows XP pero no contenga soporte para JavaScript, como Evince o Sumatra PDF, para un lector de PDF predeterminado[68, 69].

Recordatorio: has backup

AA esta altura, el computador está configurado para su uso, pero es en esencia inseguro. En la siguiente sección explicaremos cómo reforzar la seguridad de Microsoft Windows XP mediante el uso de herramientas y prácticas de Microsoft, así como a través de software de terceros que puedes instalar.

Aparte de ser menos seguro que las versiones más recientes de Microsoft Windows, Windows XP tiene menos capacidad para recuperarse de problemas causados por software incompatible. Siendo este el caso, existe la mínima posibilidad de que algunas recomendaciones de seguridad aquí detalladas no funcionen con tu instalación de Windows XP, o el software que se ejecuta sobre él. Por este motivo, recomendamos hacer otra copia de respaldo del computador ahora, antes de comenzar a asegurarlo. Así, de ocurrir un problema por alguno de los pasos destacados, serás capaz de restablecer el computador rápidamente a un estado anterior de trabajo.

Para más información sobre las copias de backup, revisa la sección previa, ***Respaldando tu software***.

64 Arkin, Brad. "Introducing Adobe Reader Protected Mode." Adobe Systems, Inc. *http://blogs.adobe.com/security/2010/07/introducing-adobe-reader-protected-mode.html*.

65 Adobe. "Application Security Overview." Adobe Systems, Inc. *http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html*.

66 Adobe. "JavaScripts in PDFS as a security risk." Adobe Systems, Inc. *https://helpx.adobe.com/acrobat/using/javascripts-pdfs-security-risk.html*.

67 Adobe. "JavaScript Controls" Adobe Systems, Inc. *https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/javascript.html*.

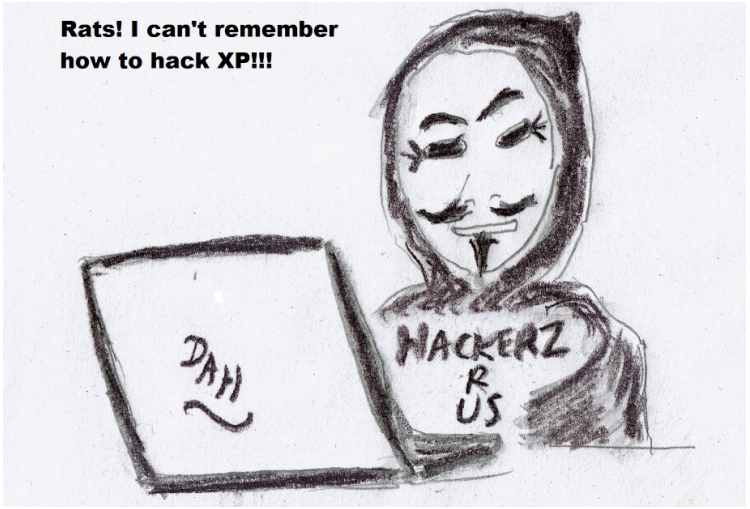
68 Evince. "Evince." The GNOME Project. *https://wiki.gnome.org/Apps/Evince*.

69 Kowalczyk, Krzyystof. "Sumatra PDF." *https://www.sumatrapdfreader.org/*.

ASEGURANDO WINDOWS XP PARA UN USO PROLONGADO

Ahora que el computador que ejecuta Microsoft Windows XP está actualizada y configurada con aquel software que no pueda ser ejecutado desde una versión más nueva de Microsoft Windows, es tiempo de comenzar a hacerlo más seguro.

Durante los años transcurridos, Microsoft ha hecho numerosas inversiones en la seguridad de Microsoft Windows XP, y la versión actualizada y emparchada de Windows XP, que existe desde el 8 de abril de 2014, es



ampliamente más segura que la versión de Windows XP disponible el 25 de octubre de 2001, pero la necesidad de retrocompatibilidad con una variedad de hardware y software, además de algunas limitaciones prácticas sobre cuánto puede cambiar un sistema operativo a lo largo de su ciclo de vida, significa que algunas opciones predeterminadas de Windows XP lo vuelven inseguro para ser usado hoy en día.

En las secciones siguientes veremos qué pasos pueden seguirse para hacer que Windows XP sea más seguro utilizando herramientas propias de Microsoft, algunas de las cuales están incluidas en Microsoft Windows XP, y otras que podrías tener que descargar. Luego, veremos qué clase de protección adicional puede sumarse con herramientas externas. Pero, antes de comenzar con esos dos pasos, me gustaría hacer referencia a un "paso cero", que no suele mencionarse en el contexto de la seguridad de un sistema operativo: la seguridad física.

NOTA:

Las siguientes instrucciones han sido escritas específicamente para usuarios hogareños y pequeñas empresas que pueden no tener acceso a un equipo de IT para gestionar sus computadores.

Muchas de las instrucciones a lo largo del paper explican cómo asegurar un computador único que ejecuta Microsoft Windows XP que no está conectado a un dominio de Active Directory (herramienta de gestión centralizada de permisos de acceso).

Los computadores conectados a un dominio de Active Directory son administrados por un equipo de IT que debería determinar el nivel apropiado de seguridad para ellos.

Seguridad Física

Si el equipo que ejecuta Microsoft Windows XP va a estar ubicado en un sitio de público acceso (o semi accesible), vale la pena considerar cómo asegurarlo de atacantes potenciales. Esto incluye no solo el robo físico del computador, sino también el acceso no autorizado.

Si el software que ejecuta el computador no los usa, puede ser una buena idea desconectar el teclado y el mouse – limitando así el acceso a sus dispositivos de entrada – para reducir el riesgo de que el computador se utilice de forma errónea. Ten en cuenta que los conectores circulares PS/2 usados por teclados y ratones viejos **no** son de conexión en caliente (la capacidad de enchufarse o desenchufarse, sin apagar el equipo, y funcionar correctamente). El computador debe estar apagado antes de conectarlos o desconectarlos. Los teclados y mouse con conexión USB sí lo son, y pueden ser conectados y removidos mientras el equipo está en funcionamiento.

Existe una variedad de soluciones contra el robo físico disponibles para asegurar un computador para que no resulte fácil de robar, abrir o modificar. Los mecanismos exactos variarán en base al tamaño, tipo y locación del equipo (además de tu presupuesto), pero puede ser desde algo tan simple como un cable para prevenir que pueda trasladarse hasta tornillos contra robos para que el chasís no pueda abrirse fácilmente, hasta cercamientos metálicos que bloqueen el acceso a los puertos del computador.

Si bien el robo de un equipo es bastante evidente, es probable que se generen daños mayores si el atacante logra acceder al computador para instalar software, alterar su información, copiar archivos del mismo, y demás. Por este motivo, es importante limitar el acceso únicamente a aquellos dispositivos de entrada y salida del computador que son necesarios para el negocio. Esto incluye no solo puertos de expansión como USB, sino

también acceso al interruptor de alimentación, teclado y mouse, unidad de disquete, unidades de CD y DVD, u otras partes del computador.

En ciertos casos, un cercamiento físico podría no restringir el acceso a estos dispositivos externos, pero aun así resultaría posible instalar cubiertas físicas en los dispositivos para bloquear el acceso a puertos no utilizados. Si esto no resulta posible, podrías aun ser capaz de deshabilitarlos en la configuración del BIOS del computador y luego proteger el acceso al BIOS mediante una contraseña. Como último recurso, puede resultar necesario abrir el computador y desconectar su cableado.

Controlar los accesos físicos a los puertos del computador puede ser de menor importancia si el equipo se encuentra en un área inaccesible al público y disponible solo para uso de personal confiable; sin embargo, sigue siendo recomendable pensar en cómo protegerlo no solo del robo, sino también contra posibles pérdidas por incendios, inundaciones u otras vías de daño.

Asegurando Microsoft XP con las herramientas integradas de Microsoft

Como hemos mencionado, el Microsoft Windows XP de 2014 es muy distinto a la versión que se lanzó en 2001. Si bien en 2007 se hicieron varios cambios a la seguridad en Windows XP con el lanzamiento del Service Pack 2, seguía habiendo límites respecto a cuánto podía modificarse sin romper la compatibilidad con las aplicaciones que existían en aquel entonces[70]. Afortunadamente, ya que tú estás a cargo de la instalación final de Windows XP, tienes la oportunidad de reforzar la configuración de seguridad por fuera de lo que Microsoft puede hacer por su cuenta.

70 Microsoft. "Release notes for Windows XP Service Pack 2." Microsoft Corp. http://support.microsoft.com/kb/835935.

Configurando las cuentas como Usuario para mayor seguridad

Si recientemente has creado una nueva instalación de Microsoft Windows XP para utilizar a largo plazo, entonces es probable que tu cuenta tenga privilegios de Administrador. Estas cuentas tienen la posibilidad de hacer cambios que afectan a todos los usuarios del dispositivo, así como al sistema operativo. Si bien esto puede no parecer peligroso, es uno de los principales problemas de seguridad – si no *el* principal – que ha enfrentado Windows XP desde su aparición.

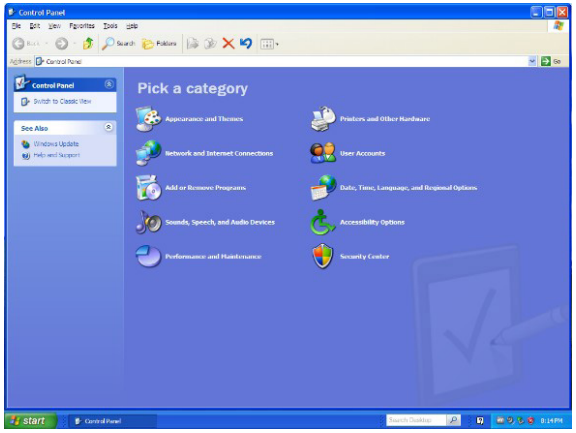
A pesar de que la creación de nuevos usuarios con privilegios de Administrador facilitó a los usuarios la instalación de nuevo hardware y software y la configuración de sus sistemas, y puede haber parecido una buena idea cuando se introdujo Windows en 2001, también significó que, si un usuario ejecutaba un virus, troyano, gusano u otro tipo de programa malicioso accidentalmente, ese malware tendría acceso completo al computador sin necesidad de engañar al usuario para que le dé acceso mediante ingeniería social y técnicas sofisticadas para escalar sus privilegios. De allí en adelante, el malware – no el usuario – tenía un control absoluto del dispositivo.

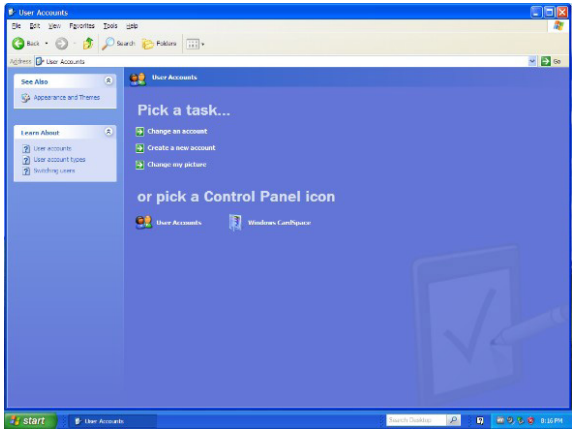
Con esto en mente, uno de los pasos más importantes a tomar para asegurar un computador es eliminar los privilegios de Administrador de las cuentas que regularmente tendrán acceso a él y modificarlos para que tengan solo privilegios de Usuario.

ADVERTENCIA	Es probable que tu computador tenga una cuenta llamada Administrador, con privilegios de Administrador. No modifiques los privilegios en esta cuenta. Debe haber al menos una cuenta en el equipo con privilegios de Administrador para permitirte instalar (o actualizar) software, conectarse a una red, llevar a cabo backups y demás funciones administrativos. Sin embargo, deberías evitar utilizar esta cuenta con privilegios de administrador para un uso rutinario del computador.

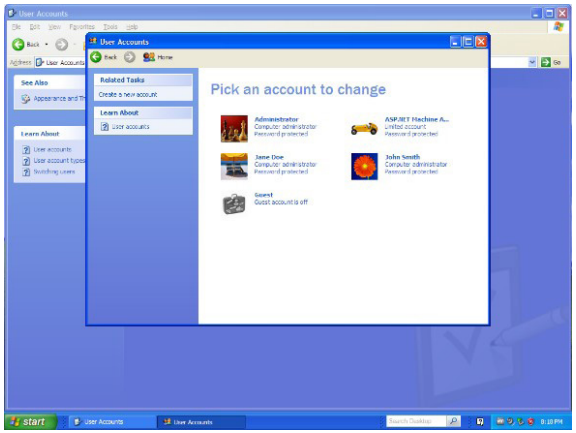
A continuación, repasaremos cómo cambiar de privilegios de Administrador a privilegios de Usuario, paso a paso:

1. Abre el **Panel de Control** desde el Menú de Inicio, y selecciona la categoría *Cuentas de Usuario*. El componente de *Panel de Control de Cuentas de Usuarios* (nombre de archivo: `LUSRMGR.CPL`) comenzará.

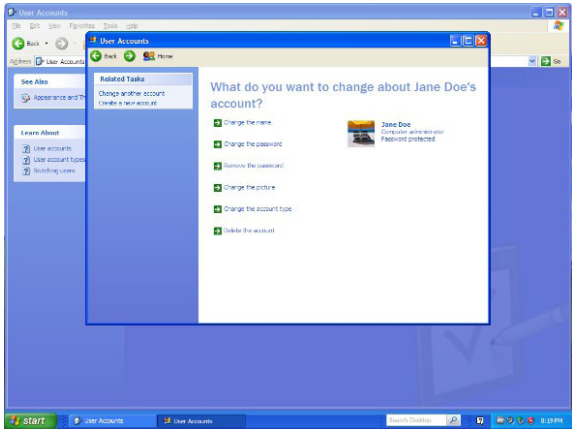




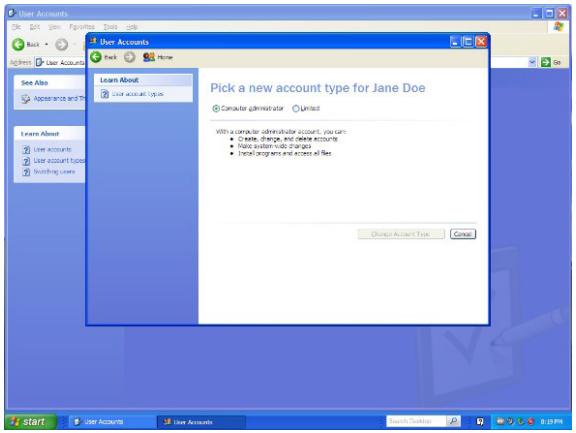
2. En el componente de **Cuentas de Usuario**, selecciona *Modificar una cuenta*. La ventana de *Selecciona una cuenta para modificar aparecerá.*



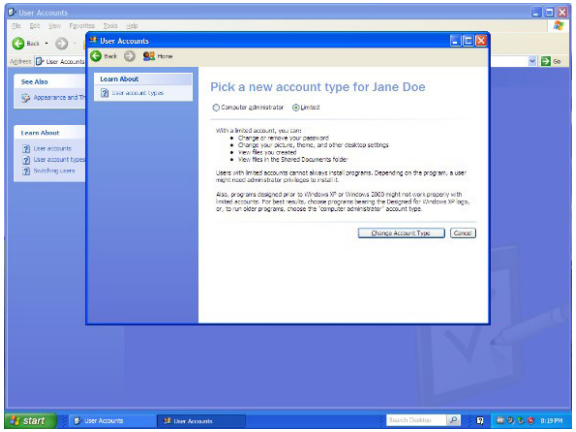
3. En la ventana de *Selecciona una cuenta para modificar*, elige la cuenta a cambiar. La ventana *Qué quieres modificar de la cuenta de (nombre de usuario)* aparecerá.



4. En la ventana de *Qué quieres modificar de la cuenta de (nombre de usuario)*, elige la opción *Modificar el tipo de cuenta*. La ventana de *Selecciona un nuevo tipo de cuenta para Usuario* aparecerá.



5. En la ventana *Selecciona un nuevo tipo de cuenta para Usuario*, elige "Limitado" y haz clic en el botón ***Modificar Tipo de Cuenta*** para realizar los cambios.



En este ejemplo, la cuenta ha sido ahora modificada de una cuenta de "Administrador" a una de "Usuario".

CONSEJO	Si estás ejecutando una versión Professional o Tablet PC de Microsoft Windows XP, puedes utilizar el **Usuario Local y el complemento de Directiva de Grupos** (MMC) (nombre de archivo: `LUSRMGR.MSC`) para llevar adelante estos pasos. Esto probablemente agilice el proceso, especialmente si hay múltiples cuentas que requieren la modificación de sus privilegios.

Normalmente, las aplicaciones que están correctamente creadas para Microsoft Windows XP no deberían requerir que la cuenta que las ejecute tenga privilegios de Administrador. Es posible que una aplicación necesite llevar adelante una acción que requiera de privilegios Administrativos, o puede suceder que la aplicación no esté correctamente escrita. Sin importar cuál sea el caso, si necesitas de estos privilegios para ejecutar cualquier sistema heredado (aplicación) para la que necesites Windows XP, considera las siguientes dos opciones:

1. *Crea una cuenta con privilegios de Administrador para ingresar cuando la aplicación debe ejecutarse. Esto funciona mejor si la aplicación solo requiere ser ejecutada de forma periódica, como al final del día laboral o la semana de trabajo, debido a los asuntos de seguridad citados en relación a ingresar con privilegios de Administración.*

   Si bien renombrar la cuenta de Administrador es una mejor práctica, la aplicación puede requerir que la cuenta tenga este nombre y no ejecutarse si ésta es renombrada o si se intenta ejecutar utilizando una cuenta de privilegios de Administrador con otro nombre. Si este es el caso, permite que el programa use la cuenta, pero crea otra con privilegios de Administrador para llevar adelante todas las otras actividades que requieran privilegios de Administrador.

2. *Considera utilizar el comando **RunAs** para iniciar la aplicación con privilegios de Administrador*[71, 72, 73]*. Al usuario se le solicitarán credenciales con privilegios de Administrador para ejecutarla.*

ADVERTENCIA	Si bien las credenciales de privilegio de Administrador pueden guardarse con **RunAs** en Microsoft Windows XP para saltear el pedido de credenciales, no es recomendable ya que, una vez habilitado, permite que ***otros programas*** sean ejecutados con privilegios de Administrador – un gran problema de seguridad.

Deshabilitando AutoRun

Como mencionamos en la sección *Una breve historia de la seguridad de Windows XP*, la funcionalidad de AutoRun en XP se encontró con la Ley de las Consecuencias Imprevistas cuando fue adoptada, no solo por software educacional y desarrolladores de juegos sino también por autores de malware. Si bien durante bastante tiempo antes del lanzamiento de Microsoft Windows XP los gusanos informáticos han estado atacando Windows de varias maneras (programas maliciosos ejecutándose en el sistema operativo, macros para Microsoft Office e incluso como instrucciones auto-replicantes para los servidores de base de datos), dependían de las conexiones de red para propagarse.

Los cambios hechos al AutoRun en Windows XP dieron a los autores de malware un mecanismo adicional para propagar sus creaciones, creando gusanos que podían pasar de un computador a otro utilizando unidades de USB como vector de infección[74, 75]. Mientras las conexiones de red siguieron siendo utilizadas para propagar gusanos, la funcionalidad de AutoRub provee a éstos de un mecanismo adicional para expandir – y en general volver a infectar – grupos de computadores, independientemente de si están directamente conectados uno a otro.

¿Cómo funciona AutoRun?

Para entender por qué esto era tan problemático, es importante comprender cómo funcionaba AutoRun originalmente bajo Microsoft Windows XP:

Cuando un medio extraíble, como CDs, DVD o unidades USB, se insertaban en un computador que ejecutaba Windows XP, el sistema operativo buscaba si había un archivo llamado `AUTORUN.INF` en el directorio raíz de la unidad extraíble[76, 77].

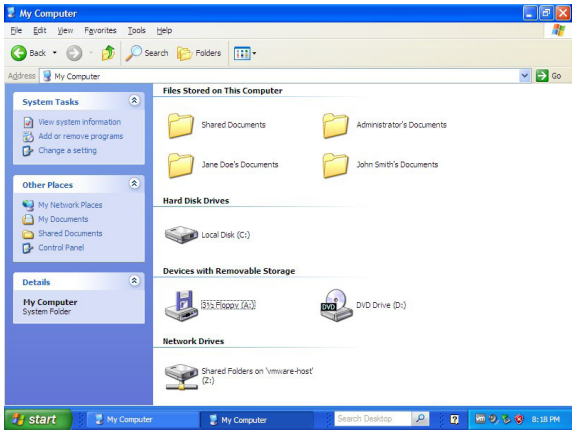


Figura 9: Ejemplo de un CD insertado en una PC sin el archivo `AUTORUN.INF`.

71 Microsoft. "Runas." Microsoft TechNet. http://technet.microsoft.com/en-us/library/cc771525.aspx.

72 Microsoft. "Runas." Windows XP Command Line Reference A-Z. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb490994(v=technet.10)

73 Wikipedia. "Runas." http://en.wikipedia.org/wiki/Runas.

74 Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. https://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/

75 Cobb, Stephen. "My Little Pronny: Autorun worms continue to turn." WeLiveSecurity. *http://www.welivesecurity.com/2012/12/07/autorun-worm-continues-to-turn/*.

76 Microsoft. "Autorun.inf Entries." Windows Dev Center. *http://msdn.microsoft.com/en-us/library/windows/desktop/cc144200%28v=vs.85%29.aspx*.

77 Wikipedia. "Autorun.inf." Wikimedia Foundation. *https://en.wikipedia.org/wiki/Autorun.inf*.

Los archivos AUTORUN.INF son solo archivos de texto plano ASCII que pueden ser creados en una aplicación como Notepad, pero que contienen instrucciones que el sistema operativo sigue automáticamente.

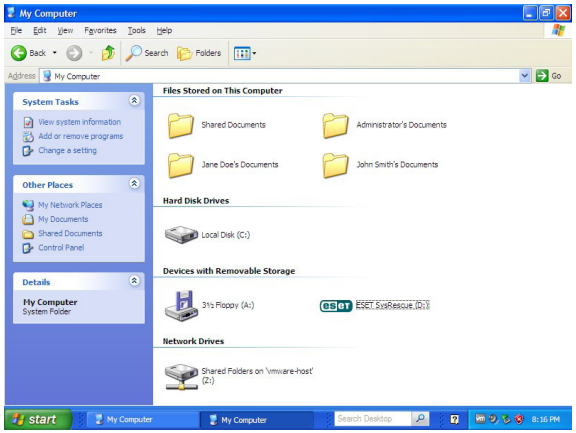


Figura 10: Ejemplo de un CD insertado en una PC con archivo AUTORUN.INF

Las acciones controladas mediante el archivo AUTORUN.INF pueden ir desde mostrar un ícono customizado para el medio extraíble hasta ayudar a instalar software de controlador de dispositivo, pero el comando preferido para los autores de malware era el de ejecutar un programa automáticamente[78].

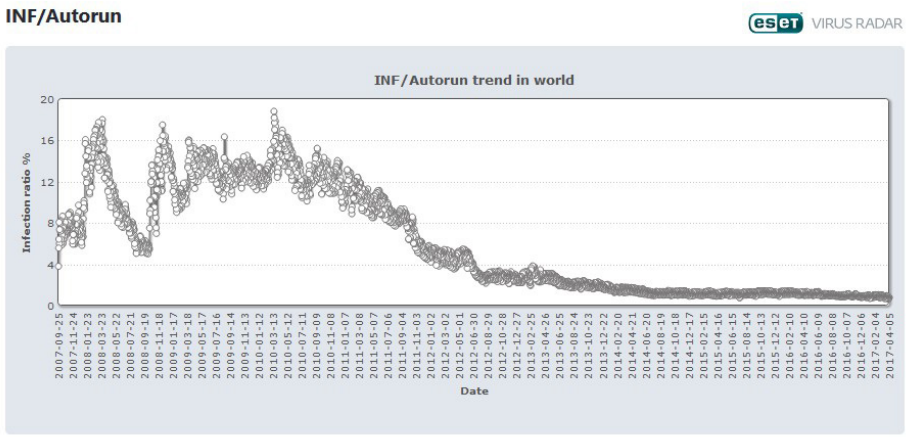


Figura 11: 10 años de detecciones de malware AutoRun

Esta simple acción daba a los autores de malware lo que necesitaban para propagar sus creaciones, y lo aprovecharon. ESET identifica el malware que utiliza archivos AUTORUN.INF como ***INF/Autorun***[79]. Al ver detecciones de la década pasada a través del VirusRadar® de ESET, vemos que se convirtió en la infección más reportada de 2007, y registró picos en 2008, ya que la técnica de infección fue utilizada por Conficker y otros gusanos[80]. No fue hasta 2010 que comenzó a decrecer, no solo debido a la rápida adopción de Microsoft Windows 7, sino también al lanzamiento de parches por la

78 Windows Dev Center. "Autorun.inf Entries." Microsoft Corp. *https://msdn.microsoft.com/en-us/library/windows/desktop/cc144200.aspx*.

79 VirusRadar Threat Encyclopaedia. "INF/Autorun." ESET, spol. s r.o. *http://virusradar.com/en/INF_Autorun/detail*.

80 Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. *https://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/*.

empresa que, por defecto, deshabilitaban AutoRun para medios extraíbles en Windows Vista y Windows XP[81, 82, 83].

Para deshabilitar la funcionalidad AutoRun en Microsoft Windows XP, descarga e instala la *Actualización para la funcionalidad AutoPlay* en Windows update, lanzada por Microsoft desde:

https://support.microsoft.com/?kbid=971029

Este sitio web contiene parches, no solo para todas las ediciones de Windows XP, sino también para todas las versiones de Windows Vista, Windows Server 2003 y Windows Server 2008. Como con muchos otros parches, puede requerirse un reinicio para que los cambios hechos en el sistema operativo tengan efecto.

Habilitar la Prevención de Ejecución de Datos

En 2004, con el lanzamiento del Service Pack 2 para Windows XP, Microsoft introdujo una funcionalidad llamada Prevención de Ejecución de Datos (DEP, por sus siglas en inglés)[84, 85, 86]. Esta permite al computador marcar si en un bloque de memoria o en un llamado a una *página*, se aloja un código de programa, o información no ejecutable, y solo permite que el código se ejecute desde páginas de memoria marcadas como ejecutable. Previo a la introducción de DEP, los atacantes podían cargar código en una página de memoria destinada a información y luego lanzar su ejecución. Implementar DEP en el hardware y software del computador puede prevenir que este tipo de ataques sean exitosos[87].

Hay varios componentes en la Prevención de Ejecución de Datos para Windows:

- *Debe estar instalado un procesador compatible que soporte el uso de un bit "No eXecute" (NX)[88]. El bit NX se utiliza para marcar si la página de memoria contiene código o información. Originalmente desarrollado por el fabricante de chips AMD para su línea de procesadores Athlon 64 en 2003, la tecnología fue licenciada a otros fabricantes de CPU incluido Intel, que lo añadió en 2004 a su línea Pentium 4. Los fabricantes de chip refieren al bit NX de diversas maneras: Intel lo llama bit XD (eXecute Disable), mientras que AMD lo llama "Enhanced Virus Protecion" (EVP) bit. Si estás tratando de definir si un procesador específico soporta el bit NX pero no lo menciona por ese nombre, fíjate si en su lugar se mencionan XD o EVP.*
- *Un sistema operativo que soporta el bit NX debe ser instalado. En el caso de Microsoft Windows XP, esto significa instalar el Service Pack 2 o el Service Pack 3. A partir de Windows Vista, el soporte de DEP es una funcionalidad estándar en el sistema operativo.*

Por defecto, Microsoft habilitó la Prevención de Ejecución de Datos solo para partes claves de Windows XP, y utilizó un modelo opcional para el resto de

81 Abrams, Randy. "Auto-Infect." WeLiveSecurity. https://www.welivesecurity.com/2007/12/18/auto-infect/.

82 Microsoft. "Update to the AutoPlay functionality in Windows." Microsoft Corp. https://support.microsoft.com/en-us/help/971029/update-to-the-autoplay-functionality-in-windows.

83 Harley, David. "Autorun and Conficker note dead yet: Threat Trends Report." WeLiveSecurity. https://www.welivesecurity.com/2012/01/10/autorun-and-conficker-not-dead-yet-threat-trends-report/.

84 Windows Dev Center. "Data Execution Prevention." Microsoft Corp. https://msdn.microsoft.com/en-us/library/windows/desktop/aa366553

85 Wikipedia. "Executable space protection." WikiMedia Foundation. https://en.wikipedia.org/wiki/Executable_space_protection

86 Microsoft. "A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003." Microsoft Corp. https://support.microsoft.com/en-us/help/875352/a-detailed-description-of-the-data-execution-prevention-dep-feature-in-windows-xp-service-pack-2-windows-xp-tablet-pc-edition-2005-and-windows-server-2003.

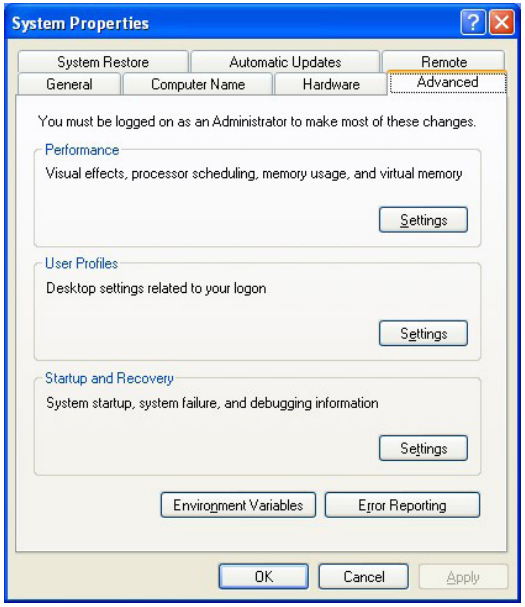
87 Hensing, Robert. "Understanding DEP as a mitigation technology part 1." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2009/06/12/understanding-dep-as-a-mitigation-technology-part-1/.

88 Wikipedia. "NX bit." Wikimedia Foundation. https://en.wikipedia.org/wiki/NX_bit.

los programas informáticos. Esto se hizo debido a una preocupación por problemas de compatibilidad con programas, servicios y unidades de disco de terceros. Sin embargo, siendo DEP una funcionalidad estándar en Windows XP desde 2004, es recomendable habilitarla para **todos** los programas, y excluir luego las aplicaciones que sean incompatibles, de haberlas[89, 90].

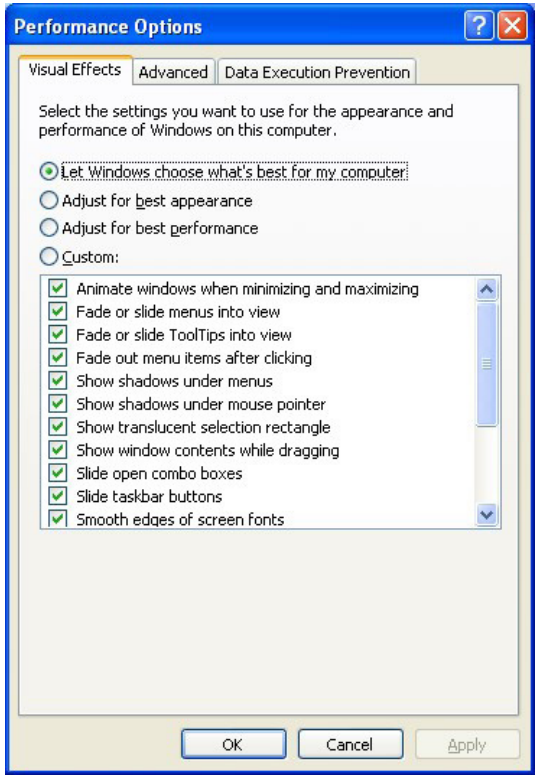
Aquí presentamos instrucciones paso a paso para habilitar la Prevención de Ejecución de Datos para todos los programas en Windows XP:

1. Abre las **Propiedades de Sistema** (nombre de archivo: `SYSDM.CPL`) en el Panel de Control. Aparecerá la ventana de *Propiedades del Sistema*.



2. Haz clic en la pestaña ***Avanzado*** para ver las configuraciones avanzadas para el sistema.

3. En la sección de *Rendimiento*, arriba en la pestaña ***Avanzado***, haz clic en el botón de *Configuración*. Aparecerá la ventana de Opciones de *Rendimiento*.

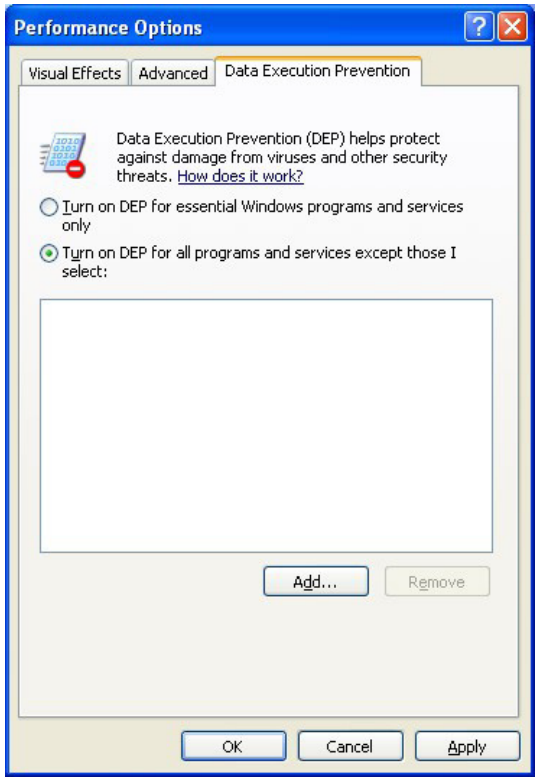


4. En la ventana de *Opciones de Rendimiento*, haz clic en la pestaña ***Prevención de Ejecución de Datos*** para ver las configuraciones de DEP.

89 Microsoft. "You receive a "Data Execution Prevention" error message in Windows XP Service Pack 2 or in Windows XP Tablet PC Edition 2005." Microsoft Corp. *https://support.microsoft.com/en-us/help/875351/you-receive-a-data-execution-prevention-error-message-in-windows-xp-se*

90 Hameed, C.C. "To DEP or not to DEP." Microsoft Ask the Performance Team Blog. *https://blogs.technet.microsoft.com/askperf/2008/06/17/to-dep-or-not-to-dep/*

5. Selecciona *Activar DEP para todos los programas y servicios excepto los que seleccione:*. Si tienes programas incompatibles con DEP, haz clic en el botón ***Agregar*** y añádelos a la lista de excluidos. Haz clic en el botón ***Aceptar*** una vez que hayas terminado de realizar los cambios al sistema.



Se solicitará un reinicio para aplicar los cambios en Windows XP.

Antes de avanzar, debemos aclarar que la Prevención de Ejecución de Datos no es infalible. Se han descubierto diversas vulnerabilidades que permitieron esquivar DEP, obligando a Microsoft a lanzar parches para solucionar las vulnerabilidades[91, 92, 93, 94]. Esto no significa que deba ser deshabilitado, sin embargo, por no ser 100% efectivo. Habilitar la Prevención de Ejecución de Datos provee una capa adicional de seguridad, y cuando se hace uso de un sistema operativo no soportado, como Windows XP, es importante tomar tantas medidas de seguridad como sea posible y práctico.

Configurar el Explorador de Archivos de Windows para mostrar extensiones de archivo

Microsoft ha implementado muchos cambios en Windows a lo largo de los años, desde el lanzamiento del primer Windows 1.0 en 1985 hasta Windows 10 en 2015. Algunos de los mayores cambios ocurrieron en la interfaz de usuario al mutar de Windows para Grupo de Trabajo en Windows 95, que introdujo a los usuarios al Menú de Inicio y la metáfora del Escritorio de Windows, que fueron apenas modificadas de versión a versión, pero se mantuvieron prácticamente iguales hasta el lanzamiento de Windows 8 en 2012.

En algunos casos, se tomaron decisiones para que Windows fuera más amigable a expensas de reducir su seguridad. Siempre existe un intercambio al aumentar la facilidad de uso por sobre la seguridad, y

91 Ness, Jonathan. "Additional information about DEP and the Internet Explorer 0day vulnerability." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/01/18/additional-information-about-dep-and-the-internet-explorer-0day-vulnerability/.

92 Roths, Andrew; et al. "DEP, EMET protect against attacks on the latest Internet Explorer vulnerability." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/11/03/dep-emet-protect-against-attacks-on-the-latest-internet-explorer-vulnerability/.

93 Miller, Matt. "On the effectiveness of DEP and ASLR." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/12/08/on-the-effectiveness-of-dep-and-aslr/.

94 Miller, Matt; Peteroy, William. "Mitigating the LdrHotPatchRoutine DEP/ASLR bypass with MS13-063." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2013/08/12/mitigating-the-ldrhotpatchroutine-depaslr-bypass-with-ms13-063/.

dichas decisiones probablemente se vieran impulsadas en parte porque los vectores de ataque no eran ampliamente comprendidos cuando las decisiones se tomaron. Un ejemplo de esto es la funcionalidad AutoRun en Windows XP, que se discutió arriba. Otro, es la configuración por defecto de **Windows Explorer** (nombre de archivo: `EXPLORER.EXE`) para visualizar archivos.

En Windows 3.x, el **Administrador de Archivos** (nombre de archivos: `WINFILE.EXE`) se utilizaba para ver directorios y lanzar programas[95]. Mostraba los archivos en un directorio, incluyendo sus nombres, extensiones de archivo y pequeños íconos dando una indicación del ejecutor del tipo de archivo, por ejemplo, el programa utilizado para abrirlo.

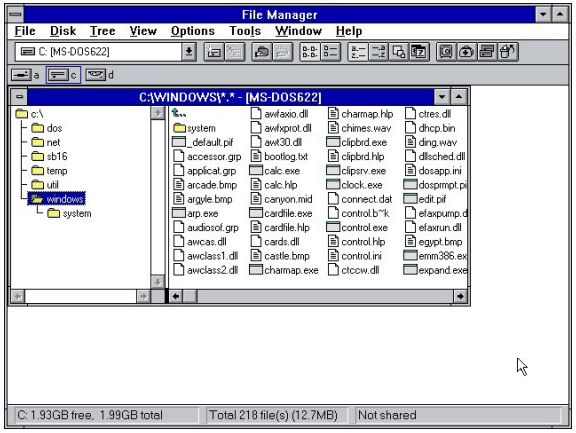


Figure 12: Windows for Workgroups 3.11 File Manager

Si bien esto tenía sentido en el mundo de Windows 3.x orientado al negocio, era visto como una manera menos amigable de visualizar archivos que aquella usada por la Macintosh de Apple, que hacía uso de la información almacenada dentro de archivos para determinar qué íconos se mostraban y qué aplicaciones los abrían[96, 97, 98, 99]. En el intento de hacer a Windows 95 atractivo para los consumidores al verse más amigable y de copiar la simplicidad de Macintosh, Microsoft tomó la decisión de no mostrar las extensiones de archivo por defecto al verse en Windows Explorer, el sucesor del Administrador de Archivos de Windows 3.x. Sin embargo, Explorer sigue mostrando un ícono basado en, ya sea la extensión de archivo, o embebido en como un recurso dentro del archivo. Mostrar los archivos de esta forma ha sido el comportamiento por defecto para Windows y ha permanecido sin cambios por más de 20 años, desde el lanzamiento de Windows 95 en 1995.

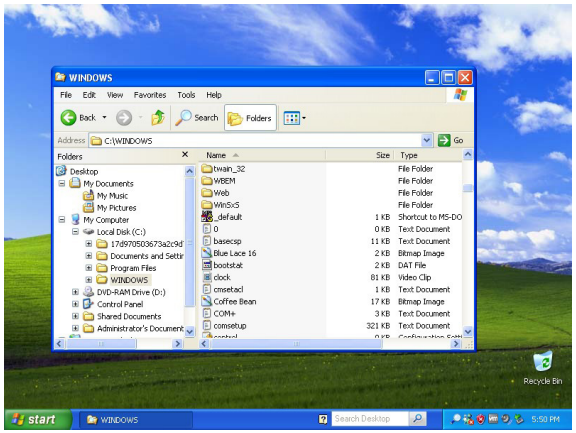


Figura 13: Explorador de Microsoft Windows XP

95 Wikipedia. "File Manager (Windows)." Wikimedia Foundation. https://en.wikipedia.org/wiki/File_Manager_(Windows).

96 Sanford, Glen D. "apple-history." Apple History. http://www.apple-history.com/.

97 Mac 512, The. "System Showcase." The Mac 512. http://www.mac512.com/macwebpages/system.htm

98 Wikipedia. "Macintosh." Wikimedia Foundation. https://en.wikipedia.org/wiki/Macintosh.

99 Wikipedia. "Classic Mac OS." Wikimedia Foundation. https://en.wikipedia.org/wiki/Classic_Mac_OS.

¿Por qué ocultar extensiones de archivo es un verdadero problema de seguridad? La razón es que es fácil crear archivos con una extensión duplicada – una extensión "falsa" seguida por la verdadera extensión – y como resultado de esta configuración por defecto, Explorer muestra solo la extensión de archivo falsa.

A modo de ejemplo, crear un archivo con el nombre "`My Notes.txt`" significa que contiene texto, y es abierto por el editor de texto por defecto de Windows, **Notepad** (nombre de archivo: `NOTEPAD.EXE`). Con la vista predeterminada de Explorer configurada para no mostrar extensiones, el archivo solo aparecería como "`My Notes`" en el computador. Crear un archivo con doble extensión, como "`MyNotes.txt.exe`" significa que la porción **`.txt`** se mostrará en Explorer, mientras que la porción **`.exe`** permanecerá oculta.

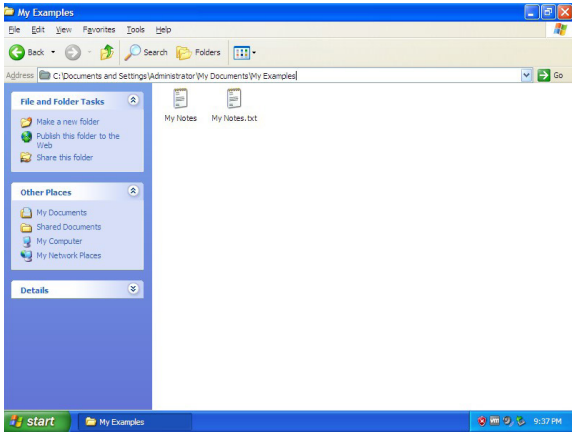


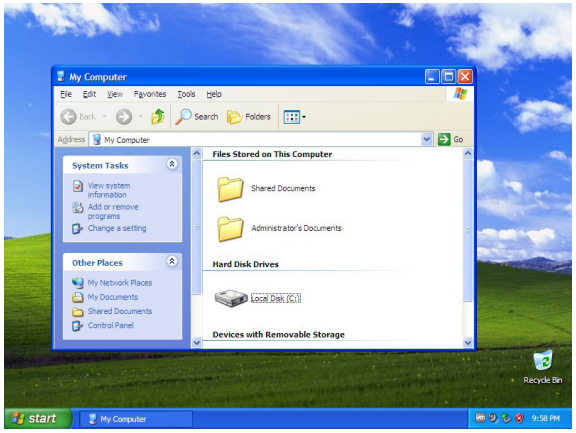
Figura 14: Mostrando archivos aparentemente iguales en Explorer

A lo largo de los años, esta configuración predeterminada, originalmente pensada para hacer a Microsoft Windows XP más amigable, ha llevado a cientos de millones de personas a ejecutar programas maliciosos accidentalmente, infectando sus computadores, y causando pérdidas económicas tan altas que eran casi incalculables.

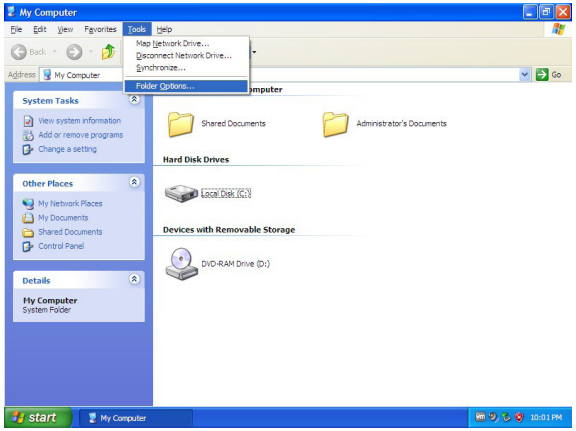
Hay una solución simple para esta vulnerabilidad de seguridad, y es activar el despliegue de extensiones de archivo en el Explorador de Windows. A continuación, verán las instrucciones, paso a paso, para hacerlo:

1. Haz clic en el botón de **Inicio** y elige ***Mi Equipo*** para abrir el Explorador de Windows

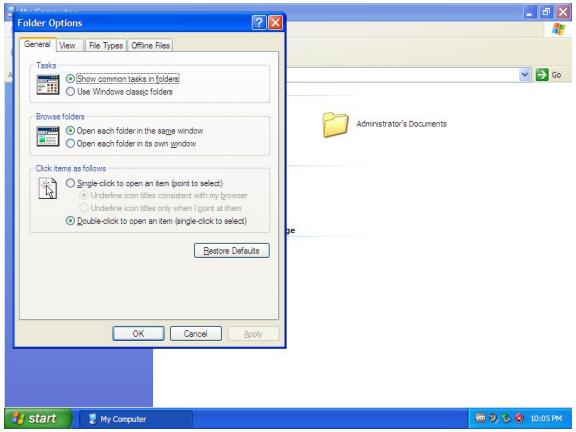
El Explorador de Windows aparecerá:



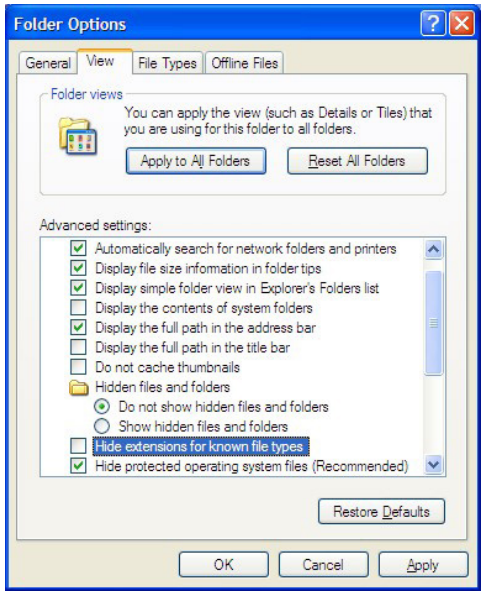
2. Selecciona *Accesorios → Opciones de Carpeta* del menú principal desplegado.



El ***panel de propiedades*** de las Opciones de Carpeta aparecerá.



3. En el ***panel de propiedades*** de Opciones de Carpeta, desmarca la opción *Ocultar las extensiones de archivo para tipos de archivo conocido*.

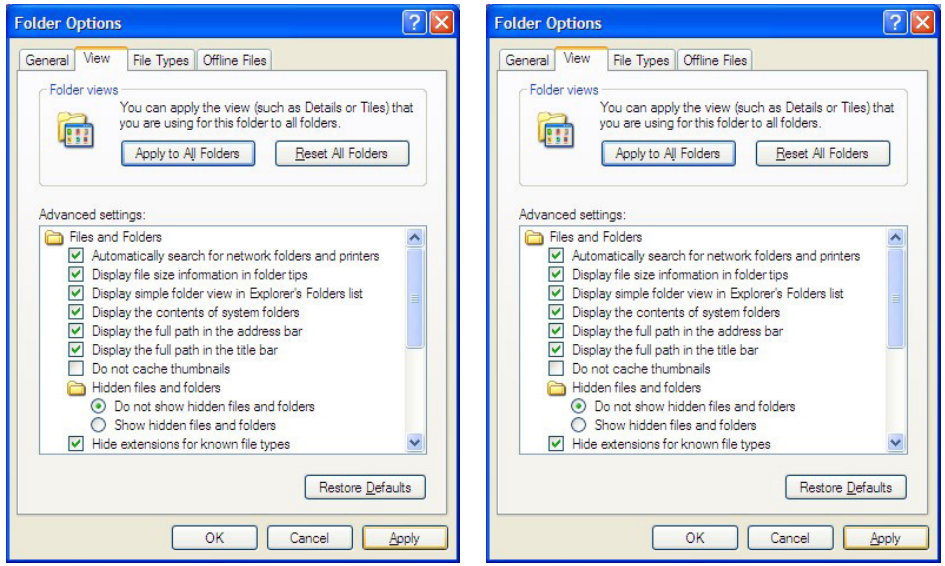


Recomendamos también modificar las siguientes configuraciones predeterminadas:

- *Marcar la opción Mostrar el contenido de las carpetas de sistema*
- *Marcar la opción Mostrar la ruta completa en la barra de título*
- *Marcar la opción Mostrar todos los archivos y carpetas ocultos (debajo de Archivos y carpetas ocultas)*
- *Desmarcar la opción Ocultar archivos protegidos del sistema operativo (recomendado)*

NOTA: Quizá sea conveniente aplicar otros cambios por conveniencia y para mejorar la productividad.

4. Una vez hechos los cambios, haz clic en ***Aplicar*** para hacer los cambios a la vista de la carpeta **actual**, luego sobre ***Aplicar a todas las Carpetas*** para modificar la forma en que se verán **todas** las carpetas. Presiona la opción ***OK*** una vez finalizado.



Si ahora visualizas una carpeta en el Explorador de Windows, los archivos se mostrarán con sus extensiones. Aquí está la misma carpeta vista en la Figura 14 una vez aplicados los cambios listados arriba:

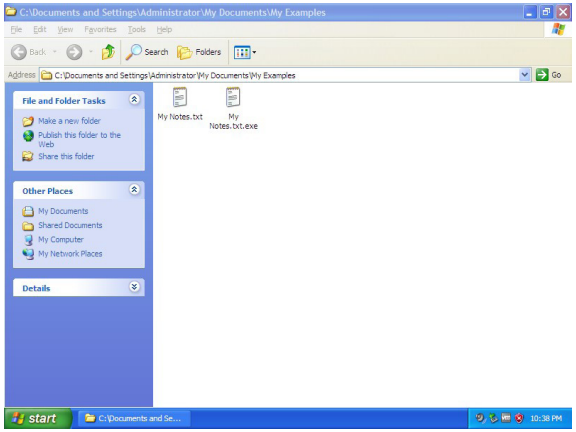


Figura 15: Mostrar las extensiones de archivo ayuda a identificar archivos

Como suele suceder con los cambios en el sistema operativo en Windows XP, puede requerirse un reinicio para que los mismos se apliquen.

CONSEJO	Los usuarios avanzados con experiencia en editar el registro de sistema de Windows pueden aplicar este cambio usando **REG.EXE** para ingresar la siguiente línea única desde el Símbolo del Sistema: `REG.EXE ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v "HideFileExt" /t REG_DWORD /d "0" /f` Usa "/d" para configurar el valor DWORD de `HideFileExt` a **1** para ocultar extensions de archivos, o a **0** para mostrarlas.

Firewall de Windows

En Windows XP, el Firewall de Windows (también conocido como Internet Connection Firewall antes de ser renombrado en el Service Pack 2) brinda protección básica, permitiendo que las conexiones de red entrantes sean bloqueadas. Esto difiere de versiones más nuevas de Microsoft Windows, en las que el Firewall es *bidireccional* y puede bloquear tanto las conexiones de red entrantes **como** salientes. Puede accederse al Firewall de Windows abriendo el **Panel de Control**, haciendo clic en el **Centro de Seguridad**, yendo a la sección *Administrar la Configuración de Seguridad* para: y seleccionando *Firewall de Windows*. Se iniciará luego el componente del Panel de Control del Firewall de Windows (nombre de archivo: `FIREWALL.CPL`).

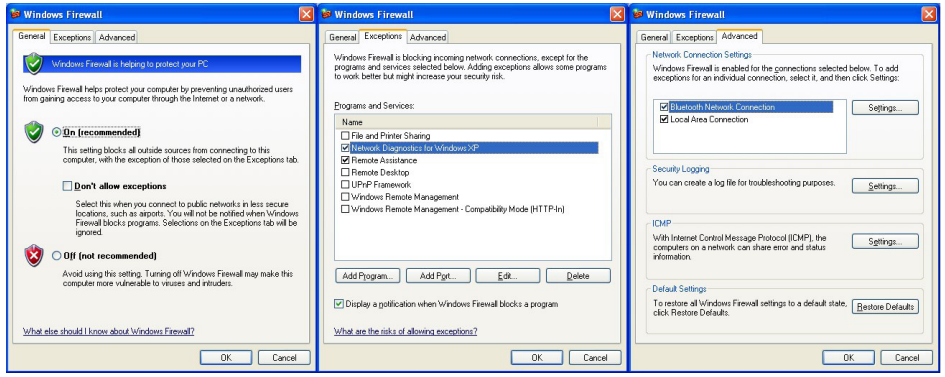


Figura 16: Pestañas General, Excepciones y Avanzado del Firewall de Windows

Si bien ningún computador que ejecute Microsoft Windows XP debería tener acceso directo a Internet por su propia seguridad, podría aún requerirse el acceso a una red local para compartir datos. El Firewall de Windows debería estar habilitado para restringir comunicaciones de red accidentales. En la pestaña ***General***, seleccionar *No permitir excepciones* bloqueará todas las conexiones de red entrantes, excepto aquellas iniciadas por el computador.

NOTA: El Firewall de Windows en Windows XP es un software básico y solo es capaz de bloquear conexiones de red entrantes, no salientes.

A diferencia de las secciones previas, en las que se proveyó una guía detallada, no es posible hacerlo con el Firewall de Windows. La configuración del firewall dependerá del tipo de acceso a la red que el computador necesite para desarrollar su función específica (o funciones). Revisa toda la información para esa sección, para determinar qué programas requieren acceso a Internet, y a qué servidores y en qué puertos. Esta información puede hallarse comúnmente en documentación y artículos de la base de conocimiento.

Si se requiere un firewall bidireccional, o si no estás seguro a qué servidores se necesita acceder (y en qué puertos), usa otro firewall en su lugar. Muchos firewall de terceros pueden ejecutarse en un modo interactivo que busca conexiones para que puedas armar el conjunto de reglas del firewall para permitir y denegar acceso a Internet. Una vez que hayas configurado las reglas de acceso necesarias, deshabilita la interactividad y pon al firewall en un modo estricto en el que solo las conexiones para las que hayas aplicado políticas o reglas se permitan, y todas las demás sean denegadas.

NOTA: Los firewall de software para computadores y los firewall de hardware para redes desempeñan distintas funciones. No se reemplazan entre sí, sino que se complementan.

Herramientas Adicionales de Microsoft para Asegurar Windows XP

Para cualquier sistema operativo tan popular como lo fue Microsoft Windows XP, era inevitable que se creara un amplio número de herramientas para protegerlo. Algunas de estas fueron exclusivas para Enterprise y requerían de entrenamiento especializado y mantenimiento constante para administrarlas; algunas eran específicas para usuarios hogareños con un único computador conectado directamente a Internet. Y algunas de las herramientas caían en medio de ambos segmentos.

Si bien no podemos abarcar cada herramienta de seguridad desarrollada por Windows XP durante sus trece años de vigencia, sí podemos analizar algunas de las que más útiles resultaran para remediar y defender una PC en el ecosistema hogareño o pequeña oficina.

Kit de Herramientas de Experiencia de Mitigación Mejorada

En 2009, Microsoft lanzó el Kit de Herramientas de Experiencia de Mitigación Mejorada (EMET, por sus siglas en inglés), una herramienta para proveer una capa extra de prevención contra el malware[100]. EMET no es un programa anti-malware en sí; funciona aplicando mitigaciones a programas para vulnerabilidades que, de otra forma, les requeriría ser recompiladas y distribuidas nuevamente[101]. Esto es particularmente útil para programas que tienen vulnerabilidades mitigadas por EMET pero para las que no existen nuevas versiones. Por estas razones, recomendamos su uso.

100 Serna, Fermin J.; Roths, Andrew. "Announcing the release of the Enhanced Mitigation Tookit." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2009/10/27/announcing-the-release-of-the-enhanced-mitigation-evaluation-toolkit/.

101 Microsoft. "Enhanced Mitigation Experience Toolkit." Microsoft TechNet. https://technet.microsoft.com/en-us/security/jj653751.

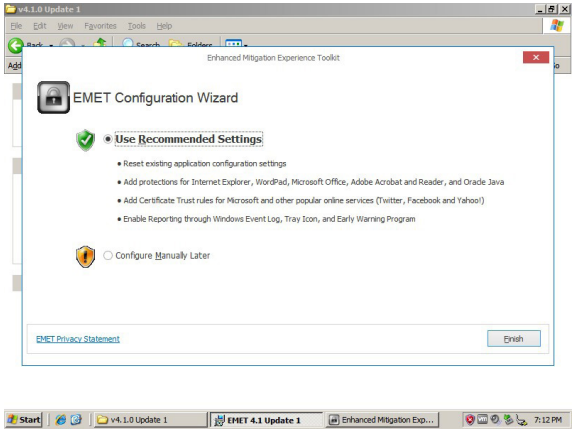


Figura 17: Instalando la actualización 1 de EMET 4.1.0 en Windows XP

El lanzamiento original de EMET soportaba cuatro mitigaciones para Windows XP. Cada una de estas respondía a una técnica de explotación, pero explicar estas técnicas en detalle se aleja del enfoque de este paper. Aquí hay una lista de esos exploits, junto con los enlaces a Microsoft que explican cómo operan (en inglés):

Nombre	Más Información
SEHOP	*Preventing the Exploitation of Structured Exception Handler (SEH) Overwrites with SEHOP*
Dynamic DEP	*Understanding DEP as a mitigation technology part 1*, *Understanding DEP as a mitigation technology part 2*
NULL page allocation	*Null page mitigation*
Heap spray allocation	*Nozzle: Counteracting Memory Exploits*

En abril de 2014 Microsoft lanzó la última versión de EMET oficialmente compatible con Windows XP, Update 1 de la versión 4.1.0. En el lanzamiento, Microsoft ha aumentado el número de mitigaciones para Windows XP a 10[102, 103].

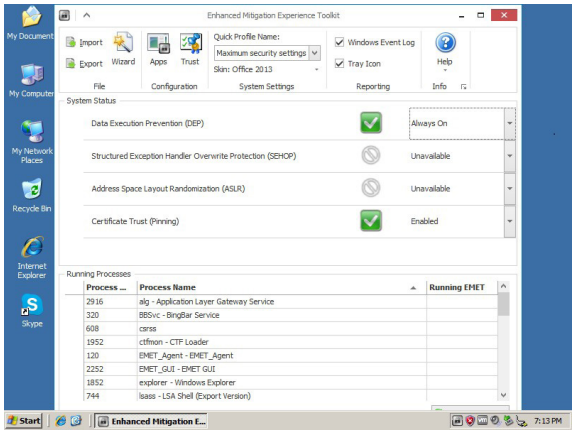


Figura 18: habilitando funcionalidades en EMET

Si bien es un número menor de mitigaciones disponibles para Windows Vista y sistemas operativos más nuevos, sigue proveyendo una capa adicional de seguridad para reforzar Windows XP contra ataques.

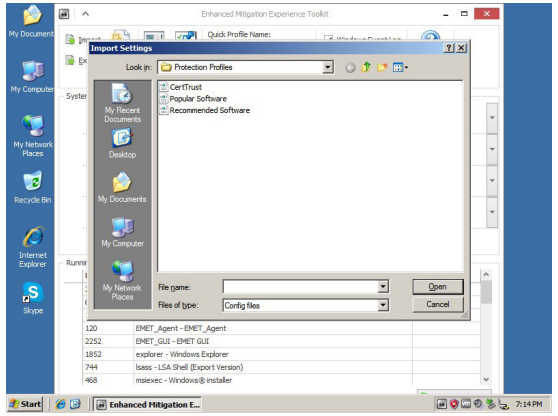


Figura 19: Importando Perfiles de Protección en EMET

Al instalar EMET, recomendamos utilizar las configuraciones por defecto de Microsoft, para habilitar todas las funcionalidades disponibles como la Prevención de Ejecución de Datos (DEP) y el Certificate Pinning, e importar todos los perfiles de protección provistos por Microsoft. Esto asegurará que EMET esté configurado al mayor nivel de seguridad posible en Microsoft Windows XP.

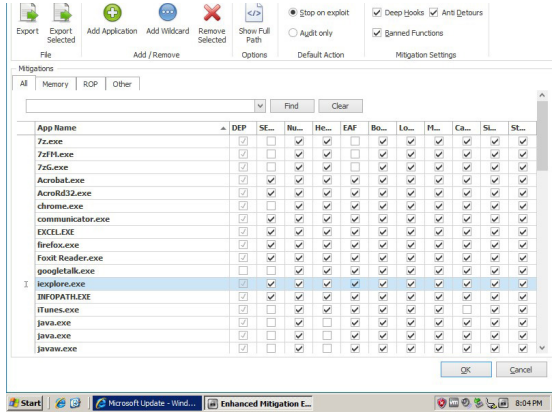


Figura 20: el botón Aplicaciones abre el gestor de Apps en EMET

102 Microsoft. "Introducing Enhanced Mitigation Experience Toolkit (EMET) 4.1." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2013/11/12/introducing-enhanced-mitigation-experience-toolkit-emet-4-1/

103 Microsoft. "An update is available for the Enhanced Mitigation Experience Toolkit 4.1: April 2014." Microsoft Corp. https://support.microsoft.com/en-us/help/2964759/an-update-is-available-for-the-enhanced-mitigation-experience-toolkit-4.1-april-2014.

Es posible que una o más aplicaciones sean incompatibles con las mitigaciones provistas por EMET. Si esto ocurre, EMET mostrará una notificación con el nombre del programa y la mitigación. Para solucionar esta incompatibilidad, abre EMET, ve a la sección ***Aplicaciones*** presionando `Ctrl+Shift+A`, y desmarca la mitigación para la aplicación en cuestión.

Al igual que con la Prevención de Ejecución de Datos, el Kit de Herramientas de Experiencia de Mitigación Mejorada no es una panacea ni un sustituto para ejecutar una versión más nueva y segura de Windows. Ha habido varios lanzamientos tras la actualización 1 de la versión 4.1.0 de EMET que solucionó vulnerabilidades y añadió nuevas mitigaciones; éstas, sin embargo, no están disponibles en Microsoft Windows XP. EMET no puede hacer a tu sistema invulnerable; lo que puede es volverlo más seguro.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) es una herramienta desarrollada por Microsoft para hallar configuraciones de seguridad débiles e identificar cualquier actualización de seguridad faltante para el sistema operativo, como también para Microsoft Office, y el servidor web IIS (Internet Information Services) y el sistema de gestión de base de datos SQL[104, 105, 106, 107]. MBSA está disponible para versiones de escritorio de Microsoft Windows, desde Windows 2000 a Windows 8.1 y sus versiones de servidor homólogas.

104 Microsoft. "Microsoft Security Baseline Analyzer." Microsoft TechNet. https://technet.microsoft.com/en-us/security/cc184924.aspx.

105 Microsoft. "Microsoft Security Baseline Analyzer 2.3 (for IT Professionals)." Microsoft Corp. https://www.microsoft.com/en-us/download/details.aspx?id=7558.

106 Microsoft. " How To: Use the Microsoft Baseline Security Analyzer." Microsoft Developer Network. https://msdn.microsoft.com/en-us/library/ff647642.aspx.

107 Wikipedia. "Microsoft Security Baseline Analyzer." Wikimedia Foundation. https://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer.

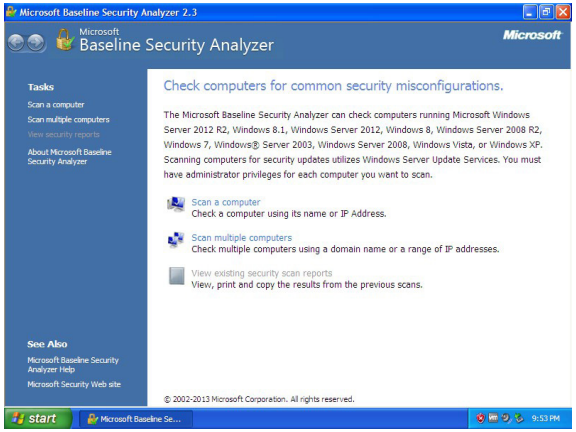


Figura 21: version 2.3 de Microsoft Baseline Security Analyzer en Windows XP.

Cuando se selecciona la opción *Scan a Computer*, MBSA preguntará qué equipo quieres analizar en búsqueda de problemas de seguridad, siendo la opción predeterminada el computador en el que se ejecuta.

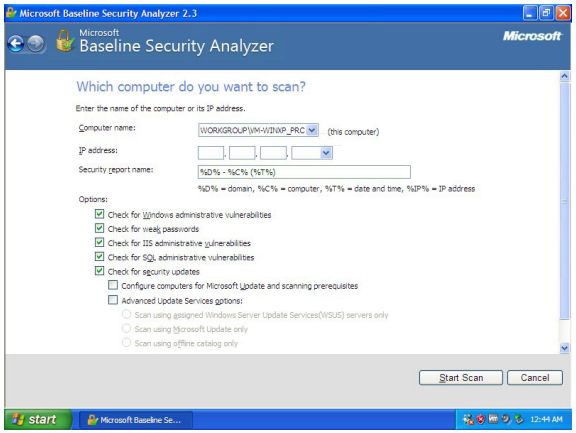


Figura 22: Microsoft Baseline Security Analyzer preguntando qué equipo analizar.

Al seleccionar *Start Scan*, el análisis comenzará, y el proceso puede llevar desde varios minutos a varias horas, dependiendo la antigüedad y velocidad del computador y su conexión de red.

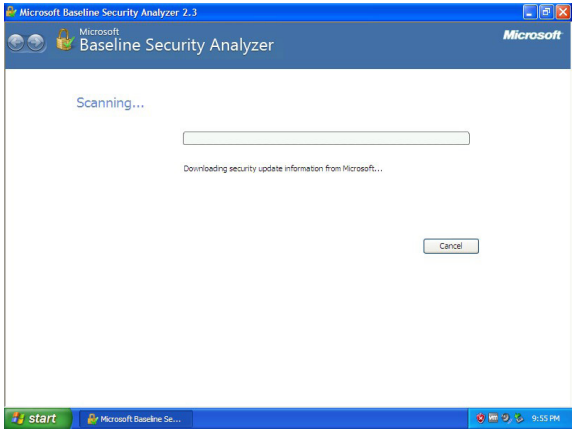


Figura 23: Microsoft Baseline Security Analyzer contacta a Microsoft para la última información

Luego de actualizar la información de seguridad, MSBA se ejecutará y presentará al usuario un reporte de sus hallazgos, que podría comprender varias pantallas de información.

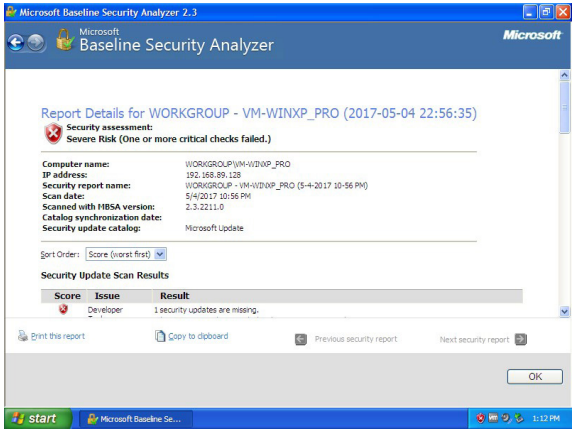


Figura 24: El inicio de un reporte finalizado de Microsoft Baseline Security Analyzer

Dependiendo de la extensión, puede ser más o menos sencillo imprimir el reporte, o copiarlo y pegarlo en otra aplicación, como un procesador de texto, para analizarlo en detalle.

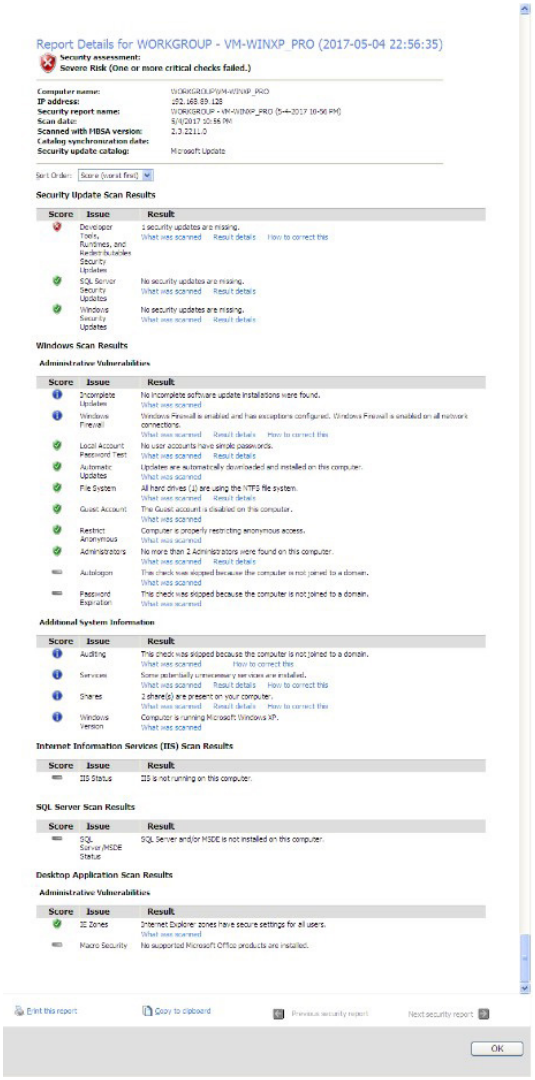


Figura 25: Un reporte de Microsoft Baseline Security Analyzer puede ser extenso.

Hacer clic en *Result Details* de cualquier entrada del reporte brindará mayor información sobre la naturaleza del problema que fue hallado, como una actualización de seguridad faltante, junto con enlaces a boletines de seguridad y links de descarga, según aplique.

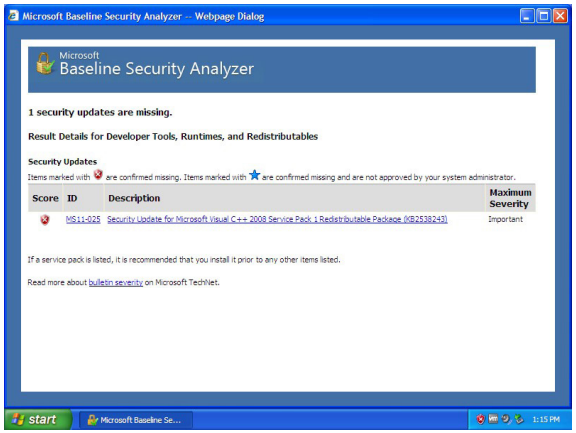


Figura 26: Microsoft Baseline Security Analyzer halló una actualización de seguridad faltante

Recomendamos atender cualquier problema de seguridad hallado por Microsoft Baseline Security Analyzer. Sin embargo, también es importante realizar un backup del sistema, por si alguna de las actualizaciones no es compatible con el hardware o software de tu dispositivo. Pueden acceder a más información sobre backups en la sección ***Respaldando tu Software***.

Microsoft Security Essentials

Microsoft Security Essentials fue el programa antimalware gratuito lanzado por Microsoft en septiembre de 2009, para Windows XP, Vista y Windows 7[108, 109]. Microsoft dejó de brindar la posibilidad de descargar Microsoft Security Essentials en abril de 2014, pero mantuvo ofreciendo actualizaciones para las copias ya instaladas hasta julio de 2015[110, 111, 112].

Debido a la velocidad con que aparecen nuevas amenazas, usar un programa antimalware que tiene varios años de desactualización no ofrece protección efectiva. Si el computador que ejecuta Windows XP tiene Microsoft Security Essentials instalado, debería ser removido y reemplazado con un software anti-malware que soporte Microsoft Windows XP de una compañía de seguridad con reputación.

Herramientas de terceros para asegurar Windows XP

Además de programas tales como EMET y MBSA, hay herramientas similares disponibles de terceros que pueden ayudar a reforzar la seguridad de Windows XP. Belarc y Flexera (antes Secunia) están entre las compañías que ofrecen herramientas que no solo buscan actualizaciones faltantes de Windows, sino también para programas tales como Adobe Flash y Oracle Java, que suelen ser objetivo de ataques. Podrían incluso hallar actualizaciones para el propio software de Microsoft que Microsoft Security Baseline Analyzer pasó por alto.

Belarc Advisor

Belarc, Inc. es una compañía que hace software de administración de sistemas para negocios[113]. Ofrece además un programa gratuito para consumidores finales llamado Belarc Advisor, que establece inventarios del software y el hardware, identifica actualizaciones de Microsoft faltantes, y provee un asesoramiento de seguridad del computador en el que se ejecuta[114]. Esto se muestra en forma de reporte desplegado en el buscador web.

108 Microsoft. "Get free virus protection with Microsoft Security Essentials." Microsoft Corp. *https://www.microsoft.com/en-us/safety/pc-security/microsoft-security-essentials.aspx*.

109 Mediati, Nick. "Microsoft Security Essentials Launches Tuesday." PCWorld. *https://www.pcworld.com/article/172762/microsoft_security_essentials_launches_tuesday.html*.

110 Microsoft. "Microsoft antimalware support for Windows XP." Microsoft Windows Security blog. *https://blogs.technet.microsoft.com/mmpc/2014/01/13/microsoft-antimalware-support-for-windows-xp/*.

111 Seltzer, Larry. "Microsoft to extend Windows XP anti-malware updates one year." ZDNet. *http://www.zdnet.com/article/microsoft-to-extend-windows-xp-anti-malware-updates-one-year/*

112 Ringer, Brian H. "End of Updates for (MSE) Microsoft Security Essentials and MSRT (Malicious Software Removal Tool) for Windows XP-July 14, 2015." Microsoft Answers. *https://answers.microsoft.com/en-us/protect/forum/all/end-of-updates-for-mse-microsoft-security/91800f6f-262e-48d0-8be7-7a8f9d768cbf?auth=1*.

113 Belarc. "About Belarc." Belarc, Inc. *http://www.belarc.com/en/about_us*.

114 Belarc. "Belarc Advisor." Belarc, Inc. *http://www.belarc.com/en/products_belarc_advisor*.

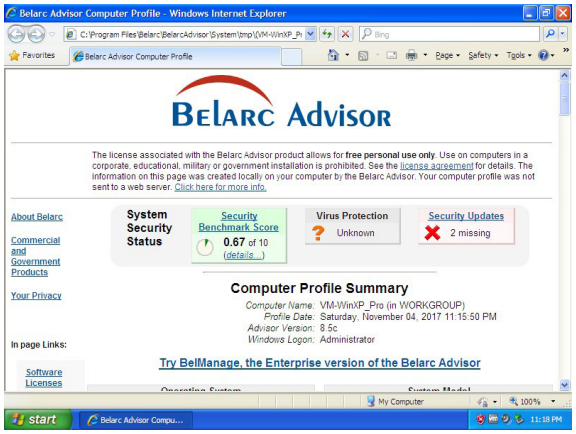


Figura 27: archivo .log de Belarc Advisor

La captura de pantalla de arriba muestra a Belarc Advisor tras ejecutarlo en un computador que fue analizado previamente y actualizado utilizando Microsoft Security Baseline Analyzer (MSBA).

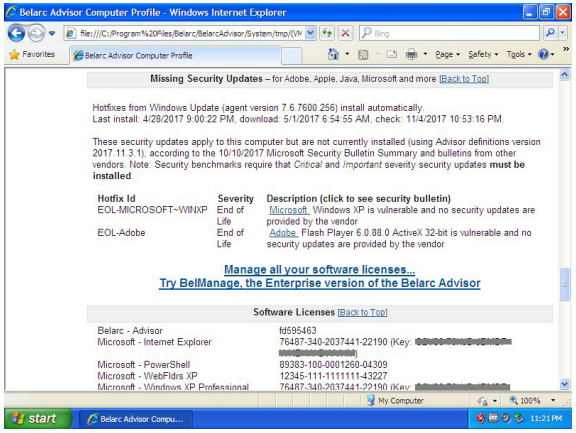


Figura 28: Belarc Advisor identificando a Windows XP y Adobe Flash como software cuyo ciclo de vida

Aquí, Belarc Advisor identificó dos actualizaciones no aplicadas para Microsoft Windows XP en este dispositivo, y otorgó un puntaje de 0,67 al nivel de seguridad del equipo en una escala de 0 a 10.

Figura 29: Belarc Advisor identifica debilidades en la gestión de contraseñas

Si bien este puntaje puede deberse parcialmente al hecho de que el sistema operativo ha alcanzado el fin de su ciclo de vida y no recibe ya actualizaciones de seguridad, indica que hay pasos adicionales que deben tomarse para mejorar la seguridad de Windows XP.

Secunia PSA

Secunia fue una compañía que creó el software de análisis de vulnerabilidades. En 2015, Secunia fue adquirida por Flexera, una empresa con ofertas complementarias[115, 116]. Flexer sigue distribuyendo Secunia PSI (Personal Software Inspector), un programa gratuito para consumidores que busca actualizaciones de seguridad para Microsoft Windows XP y otros paquetes de software[117].

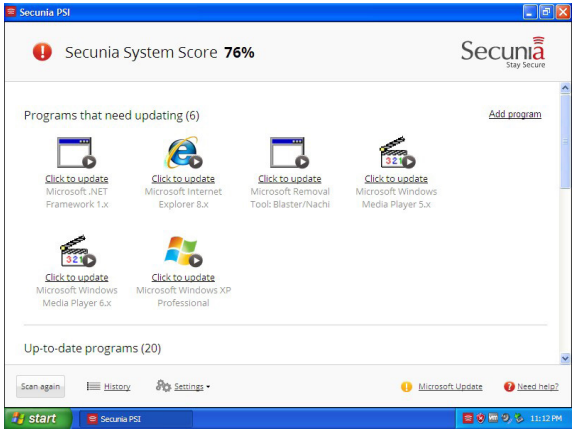


Figura 30: Secunia PSI identifica actualizaciones faltantes

Al ejecutarse en un computador particular que fue previamente analizado y actualizado utilizando Microsoft Security Baseline Analyzer (MSBA), Secunia PSI identificó seis programas que requerían actualización, y calculó que el equipo estaba un "76% seguro".

115 Flexera. "Software Buyers Optimize and Secure Your Business." Flexera Software. *https://www.flexera.com/enterprise/*.

116 Flexera. "Flexera Software Acquires Secunia, Adding Software Vulnerability Management Solutions That Reduce Cybersecurity Risks." Flexera Software. *https://www.flexera.com/producer/company/news-center/press-releases/Flexera-Software-Acquires-Secunia-Software-Vulnerability-Management.html*.

117 Flexera. "Free Instant Download: Personal Software Inspector." Flexera Software. *http://learn.flexerasoftware.com/SVM-EVAL-Personal-Software-Inspector*.

Software de seguridad de terceros

Como se dijo ***anteriormente***, Microsoft ya no brinda un software antimalware para Windows XP. Esto significa que es importante utilizar un software confiable, de una empresa de seguridad establecida que proteja a Microsoft Windows XP del malware. Hay varias compañías que siguen ofreciendo software de seguridad para Windows XP, incluyendo ESET.

Algunas compañías ofrecen una versión gratuita (con funcionalidades limitadas, soporte, y recordatorios para actualizar) mientras que otras ofrecen versiones pagas. Independientemente de cómo promocione una empresa su producto antimalware, si goza de buena reputación ofrecerá una versión de prueba capaz de detectar, remover y prevenir el malware – y posiblemente otras amenazas – de tu computador. Recomendamos ser cautelosos con las compañías que ofrecen productos que aseguran hallar amenazas, pero no las removerán hasta que el dispositivo sea adquirido. Una compañía reconocida y confiable te permitirá evaluar la habilidad del software para detectar **y** remover amenazas del sistema.

Averigua por cuanto tiempo seguirá la compañía brindado soporte para Windows XP. Por ejemplo, si esperas usar Windows XP otros tres años, no sería beneficioso utilizar el software de seguridad de una compañía que discontinuara su soporte para Windows antes de ese período.

Además de evaluar el software de seguridad, deberías contactarte con el departamento de soporte técnico de la compañía en busca de asistencia con la instalación y configuración. Incluso – especialmente – si conoces la respuesta, esto te permitirá determinar qué tan rápido y con qué profundidad responden a los requerimientos de soporte. Deberías también leer el resultado de pruebas independientes para determinar qué tan capaz es un software de seguridad de proteger el equipo.

Las compañías de seguridad con buena reputación y los evaluadores adhieren a los estándares y estatutos establecidos por la Organización para Estándares de Evaluación Antimalware (AMTSO, por sus siglas en inglés), una organización sin fines de lucro que funciona como cámara de compensación. Para obtener más información, visita el sitio web de AMTSO ***https://www.amtso.org/***.

Para la información más actualizada sobre el soporte de ESET para Windows XP, mira el artículo #3507 de la base de datos de ESET, ***Acerca del fin del soporte para Microsoft Windows XP y los productos ESET***.

EL FUTURO

En algún punto, llegará el momento de desmantelar los computadores que siguen ejecutando Microsoft Windows XP en tu ecosistema. Si bien es posible que sean reemplazados por un equipo que ejecute Windows Vista, Windows 7 y Windows 8.1 o quizás incluso macOS o Linux, es más probable que sea reemplazada con un computador ejecutando Windows 10, la más reciente, y tal vez la última versión de escritorio de Microsoft Windows en el futuro cercano.

Si bien Microsoft Windows 10 se ve y se comporta distinto a Windows XP, algunos de los principales cambios que presenta están en la seguridad. ESET ha llevado a cabo una profunda investigación sobre la seguridad de Windows 10, y aquí hay algunos de los recursos que te ayudarán a unir ese espacio de una década y media de cambios en Windows (en español y en inglés):

- Es hora de decirle adiós a Windows XP y Vista (otra vez). *(7/04/2017)*
- Windows 10 Anniversary Update: ¿la esperanza del cambio? *(17/01/2017)*
- Resumen de vulnerabilidades explotadas en Windows durante 2016 *(5/06/2017)*
- Tendencias 2017: la seguridad como rehén *[PDF] (12/2016)*
- Seguridad y privacidad en Windows 10: un análisis en profundidad *(23/06/2016)*
- Tendencias 2016: (In)security everywhere *[PDF] (02/2016)*
- Explotación de vulnerabilidades en 2015 y un repaso a nuevas propiedades de seguridad *(26/01/2016)*
- Explotación de vulnerabilidades en Windows durante 2015 *(20/01/2016)*
- Tendencias 2016 de ESET: la seguridad se vuelve parte de nuestras vidas *(12/01/2016)*
- Versiones antiguas de Internet Explorer quedarán sin soporte de Microsoft *(12/01/2016)*
- Should I stay or should I go ... to Windows 10? *(07/01/2016)*
- ESET predictions and trends for cybercrime in 2016 *(23/12/2015)*
- Una ambigua actualización de Windows 10 simplemente "mejora la funcionalidad" *(21/08/2015)*
- 20,000 NHS Wales PCs still running Windows XP from beyond the grave *(07/08/2015)*
- Windows 10, ¿Privacidad 0? *(06/08/2015)*
- ¿Serán las empresas vulnerables a 0-day debido a Windows 10? *(19/05/2015)*
- Finaliza el soporte técnico principal para Windows 7, ¿cómo te afecta a ti? *(13/03/2015)*
- Explotación de vulnerabilidades en Windows durante 2014 *(14/01/2015)*
- Six months with Windows 8 (white paper)
- A white paper: Windows 8's Security Features (white paper) *(9/10/2012)*

Reconocimientos:

El autor quiere agradecer a sus colegas Artem Baranov, Jean-Ian Boutin, Bruce P. Burrell, Graham Cluley, Stephen Cobb, Gerald Ellison, Nick FitzGerald, Greg Gallagher, Ondrej Kubovič, Andrew Lee, Fer O'Neil, Sabrina Pagnotta, Emilio Plumey, Ben Reed, Javier Segura y Darren Stordahl, así como Roger Fraumann de la Fundación Securing our eCity, por su ayuda en el armado de este White Paper. Además, un especial agradecimiento a VMware por la tecnología de virtualización usada durante la escritura de este White Paper.

www.eset.com/latam

ENJOY SAFER TECHNOLOGY™

esetla @esetla @esetla ESET Latinoamérica