



Informe de divulgación

Finalización del soporte a Windows XP

Tipo de documento: *Informe*
Autor del documento: *AndalucíaCERT*
Código del Documento: *CERT-IF-5062-140121*
Edición: *0*
Categoría: *Público*
Fecha de elaboración: *21/01/2014*
Nº de Páginas: *1 de 17*

<i>Informe de divulgación Finalización del soporte a Windows XP</i>		Código	<i>CERT-IF-5062-140121</i>
		Edición	<i>0</i>
		Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 2 de 17	

1 TABLA DE CONTENIDOS

TABLA DE CONTENIDOS.....	2
OBJETO.....	3
ALCANCE.....	3
SITUACIÓN.....	3
IMPLICACIONES.....	4
ANÁLISIS DE RIESGOS.....	7
MEDIDAS TEMPORALES (MIENTRAS SE CAMBIA EL S.O.).....	8
RECOMENDACIONES.....	9
¿ACTUALIZAR O CAMBIAR?.....	10
CONCLUSIONES.....	16
REFERENCIAS.....	17

<i>Informe de divulgación Finalización del soporte a Windows XP</i>	Código	<i>CERT-IF-5062-140121</i>
	Edición	<i>0</i>
	Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 3 de 17

2 OBJETO

El Objetivo de este documento es informar de la finalización por parte de Microsoft del soporte para Windows XP, así como plantear las implicaciones que puedan derivarse del uso de un sistema operativo obsoleto y sin soporte.

Por último se plantea una serie de recomendaciones que deben tenerse en cuenta para la migración, y consejos que pueden ayudar a mitigar los riesgos mientras se planifica y finaliza la migración de los sistemas.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía y al público en general. En él se describe la problemática actual debida al fin de soporte de Windows XP, sus implicaciones y algunas recomendaciones temporales de seguridad.

4 SITUACIÓN

Como consecuencia del final del ciclo de vida tras 12 años desde que el sistema operativo saliera a la venta, a partir del próximo 8 de Abril del 2014 Microsoft dejará de prestar servicios de soporte para Windows XP.

A partir de ese momento, dicho sistema operativo dejará de recibir actualizaciones, incluyendo parches de seguridad, hotfixes no vinculados con la seguridad y soporte para incidencias o actualizaciones de contenidos técnicos online para todos los clientes.

Para quienes decidan quedarse con Windows XP a partir de esa fecha, Microsoft prevee la aparición de vulnerabilidades 0-days de forma continuada y que podrían afectar a millones de ordenadores. Se calcula que el 30% de ordenadores mundiales aun siguen utilizando este sistema operativo, siendo actualmente el segundo sistema operativo más utilizado por los usuarios.

Sin embargo, debido a esto, junto a que el proceso de migración en algunas organizaciones puede ser un proceso lento, y para evitar panorama dantesco lleno de malwares ejecutándose libremente por millones de PC antiguos (y no tan antiguos), Microsoft ha decidido seguir ofreciendo parches antimalware para WindowsXP hasta 2015. Estas herramientas que buscan y eliminan código malicioso de nuestro equipo y que habitualmente recibíamos dentro de las actualizaciones periódicas, se mantendrán hasta el 14 de Julio del 2015.

Evidentemente, los parches antimalware no pueden considerarse una extensión del soporte de XP. Se trata tan sólo de proporcionar actualizaciones a una de las herramientas que puede ayudar a que cada Windows XP instalado no se transforme en un grave riesgo de seguridad en la organización, mientras se realiza la migración a una nueva plataforma, algo que podría afectar negativamente a la imagen de Microsoft.

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 4 de 17

5 IMPLICACIONES

En general no es recomendable mantenernos en un entorno obsoleto. Esto tiene una serie de implicaciones importantes que es necesario conocer para poder tomar decisiones adecuadas, ser conscientes de la situación y poder actuar en consecuencia:

- **Riesgo de seguridad:** Al no haber más actualizaciones, los sistemas son susceptibles de ser atacados por troyanos, spyware, ciber-delincuentes, etc., que aprovechan a su favor esa falta de seguridad, tanto del sistema operativo como de los programas instalados en él. El software anti-malware tampoco podrá protegerlos completamente una vez que Windows XP deje de tener soporte.



- **Problemas de software:** Programas nuevos y actualizaciones de los actuales (Office, antivirus, ERP, ...) pueden dejar de funcionar en Windows XP ya que los fabricantes no desarrollarán actualizaciones para este sistema.
- **Problemas de hardware:** Los nuevos equipos, equipos ya existentes y/o nuevos componentes no estarán certificados para funcionar con Windows XP. Habrá problemas de drivers que harán imposible su instalación. Esto también implica una menor posibilidad a la hora de elegir modelos de PC, así como la imposibilidad de reponer componentes de los sistemas actuales.
- **Problemas de soporte:** Al no haber soporte por parte de Microsoft para los problemas que puedan surgir, aumenta la responsabilidad y el esfuerzo para mantener seguros los sistemas por parte de los departamentos técnicos, lo que se podría traducir en un aumento de los costes del personal.
- **Incumplimiento de políticas de seguridad e incumplimientos legales:** El Esquema Nacional de Seguridad (ENS) deja bien claro la necesidad de gestionar las vulnerabilidades existentes en los equipos, algo que con Windows XP ya no sería posible. Concretamente nos encontramos con los siguientes apartados:
 - **Artículo 20 del RD 3/2010 (Integridad y actualización del sistema):** Indica que *“Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos”*.
 - **Anexo II del RD 3/2010, apartado 4.3.4 Mantenimiento [op.exp.4]:** Indica que *“Para mantener el equipamiento físico y lógico que constituye el sistema,[...]”*
 - *a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.*

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 5 de 17	

- b) Se efectuará un seguimiento continuo de los anuncios de defectos.
 - c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización”.
- **Guía CCN-STIC-814 Seguridad en el correo electrónico (Apartado 3.1 Equipos de usuario):** Se indica que “Es necesario garantizar la seguridad de los equipos de usuario utilizados para procesar dicho correo. Para ello, se debe bastionar el equipo de usuario de forma adecuada, sea cual sea su sistema operativo, teniendo en cuenta, sin menoscabo de otros cualesquiera, los siguientes extremos:
- a) Actualización correcta del sistema operativo en cuanto a releases y parches de seguridad. Debemos garantizar que tenemos notificación de nuevas actualizaciones por parte del fabricante, y que éstas se incluyen en la política de Parches y Vulnerabilidades correspondiente, tal y como se ha indicado con anterioridad para los servidores de correo.”

Por otra parte, es necesario indicar que las tasas de infección por malware en ordenadores que ejecutan Windows XP SP3 son muy superiores a las de las versiones posteriores de Windows, cuyas arquitecturas son más seguras, debido a que han ido incorporando distintos mecanismos de protección. Todo esto hace que Windows XP sea un objetivo preferente a la hora de intentar lanzar cualquier tipo de ataque.

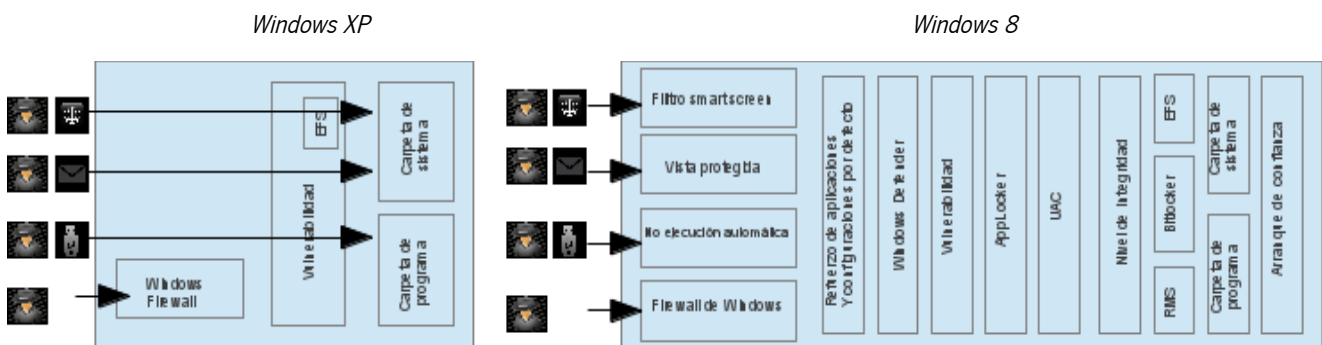


Ilustración 1: Vulnerabilidades WindowsXP vs Windows 8

En las siguientes imágenes se pueden observar comparativas entre las tasas de infección y las tasas de encuentro de malware (porcentaje de malware que se encuentra para una plataforma determinada) para las distintas versiones de Windows, así como el porcentaje de infección por sistema operativo. Estas tasas se incrementarán previsiblemente tras la finalización del soporte con la publicación de nuevas vulnerabilidades que no serán parcheadas.

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 6 de 17	

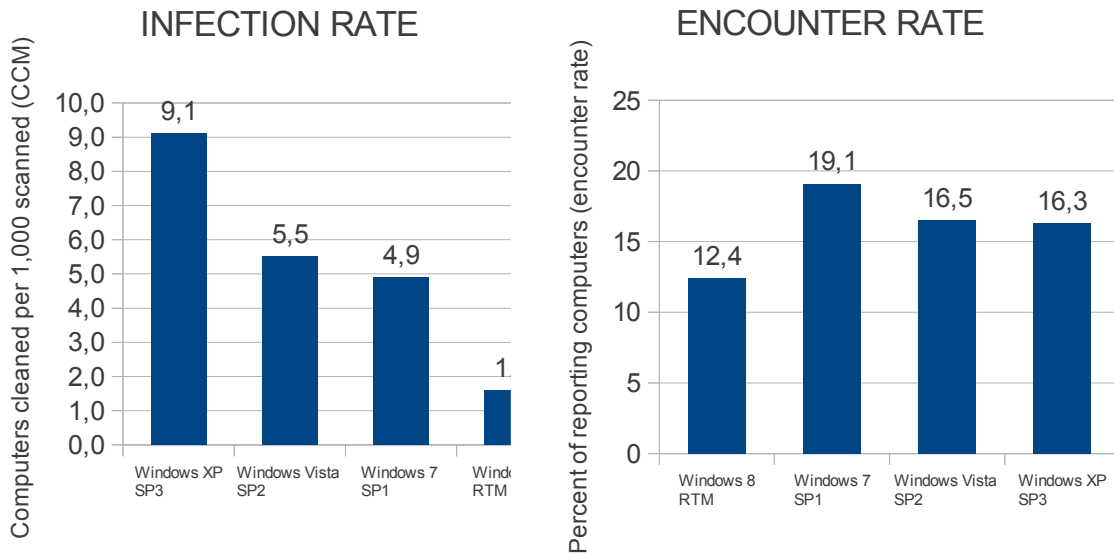


Ilustración 2: Tasas de infección vs. Tasas de encuentro de malware (fuente: Microsoft Informe SIR Vol. 15)

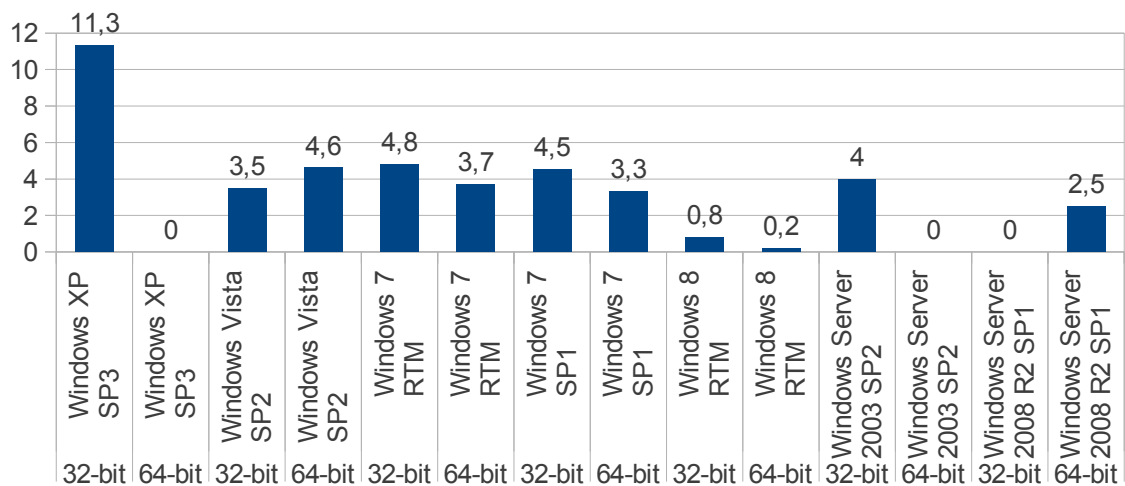


Ilustración 3: Tasa de infección (CCM) por sistema operativo y Service Pack

Es importante tener en cuenta que el despliegue de un nuevo S.O. exige tiempo para su planificación y ejecución. Por tanto, si se toma la decisión de cambiar el sistema operativo, es necesario abordar de la manera más inmediata posible su plan de migración desde Windows XP.

<i>Informe de divulgación Finalización del soporte a Windows XP</i>	Código	<i>CERT-IF-5062-140121</i>
	Edición	<i>0</i>
	Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 7 de 17

6 ANÁLISIS DE RIESGOS



Con todo lo expuesto, se hace necesario realizar un estudio de la exposición que nuestros activos tienen a las distintas amenazas que pueden surgir debido a la falta de soporte por parte de Microsoft. Para ello es necesario conocer aquellos activos que se van a ver afectados de manera directa o indirecta por este hecho.

A la hora de clasificar los riesgos para planificar la migración resulta necesario categorizar los distintos activos con el objetivo de tener una idea clara de a cuales hay que dar un tratamiento prioritario. Para ello es importante realizar las siguientes tareas:

- Identificar los activos más importantes.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos (los que están sujetos a un riesgo máximo).

La identificación o modelado de amenazas sirve para estudiar los posibles ataques a los que se encuentran expuestos los diferentes activos identificados. Para este caso, las amenazas más comunes en los sistemas operativos Windows XP una vez finalizado el soporte oficial serían las siguientes:

- **Ataques externos:** Aprovechando vulnerabilidades conocidas actualmente o en el futuro para intentar acceder a los sistemas objetivos de manera directa, indirecta (con interacción del usuario) o provocar ataques de denegación de servicio.
- **Malware:** Aunque se haya ampliado hasta 2015 la actualización de los parches antimalware, hay que recordar que ningún antivirus es 100% fiable, y que es posible que Windows XP se vea bombardeado, de manera constante, con ataques 0-day que puedan ser aprovechados por los distintos tipos de malware (trojanos, gusanos, botnets, ...), antes incluso de que se pueda sacar una actualización que los detecte.
- **Robo/pérdida/fuga de información confidencial:** Consecuencia de un ataque o por una infección, puede quedar expuesta información confidencial de la organización a terceros, pudiendo ser usada para extorsión, chantaje, espionaje, etc.
- **Problemas de Hardware:** Como es obvio, los fabricantes de hardware también dejarán de sacar controladores y actualizaciones de los mismos para Windows XP. Esto tiene una doble consecuencia:

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 8 de 17

- Sólo el hardware antiguo podrá ser usado en los sistemas WindowsXP, por lo que será más difícil encontrar ciertos componentes. Esto puede llevar a una degradación del uso del sistema, y/o incluso a no poder ser usado hasta que se consiga un componente compatible.
- Los nuevos componentes no funcionarán en WindowsXP.
- **Ataques Internos:** En ocasiones, son los propios miembros de la organización los que llevan a cabo los ataques, basándose en la confianza de otros usuarios o en el conocimiento que se tiene de las infraestructuras de la organización.

Una vez conocidas las amenazas será necesario establecer el impacto que pueda llegar a tener en el caso de materializarse, así como la probabilidad de que esto ocurra. Esto variará dependiendo de muchos factores como la situación de la máquina en la red, medidas que se tomen, uso del sistema afectado, etc.

Existen varias metodologías que nos pueden ayudar a realizar un análisis de riesgo como Magerit, OCTAVE o CRAMM.

Una vez que tengamos una idea clara qué activos son los que mayor riesgo poseen, podremos priorizar el proceso de migración correctamente, procediendo a actuar sobre los sistemas que más riesgo posean.



7 MEDIDAS TEMPORALES (MIENTRAS SE CAMBIA EL S.O.)

Como ya se ha comentado, aunque lo ideal sería tener los sistemas migrados antes de la fecha de fin de soporte, por diversos motivos, en algunos casos esto no va a ser posible. Con el fin de mitigar los riesgos de las distintas amenazas en el periodo de transición, se recomienda las siguientes medidas temporales para los sistemas con Windows XP:

- **Instala un antivirus y un firewall con soporte** para Windows XP.
- **Desactiva los plugins** si es posible, ya que son una puerta de entrada para mucho malware: Los virus más peligrosos de los últimos años han infectado millones de PCs gracias a vulnerabilidades de Java y otros plugins. Los complementos son un punto débil, incluso para los más seguros de los navegadores. Toma el ejemplo de Firefox, que ha bloqueado Java por defecto, y desactiva o desinstala los plugins más críticos. Java es uno, pero también puedes hacer otro tanto con Flash y Adobe Reader.
- **Mantén actualizadas tus aplicaciones** (mientras puedas): Windows deja de actualizarse, pero tú todavía puedes actualizar los demás programas. Un detector de vulnerabilidades de software comprueba la versión de las aplicaciones instaladas y las actualiza por ti. Sin embargo, es necesario indicar que las actualizaciones para los programas en Windows serán cada vez menos frecuentes.

<i>Informe de divulgación Finalización del soporte a Windows XP</i>		Código	<i>CERT-IF-5062-140121</i>
		Edición	<i>0</i>
		Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 9 de 17	

- **Usar navegadores con soporte para Windows XP:** La última versión de Internet Explorer disponible para Windows XP es Internet Explorer 8. Amén de anticuada, se volverá cada vez más vulnerable, ya que su parcheo depende enteramente de Microsoft. Por suerte, Firefox y Opera anunciaron que seguirán dando soporte a Windows XP por más tiempo, y Google hará otro tanto con Chrome hasta abril de 2015, lo que debería darle un respiro a muchos usuarios. Si no lo has hecho ya, cámbiate a Chrome o Firefox.
- **Monitorización de red y de host:** Es necesario prestar una especial atención a los sistemas con Windows XP, ya que se van a volver un punto crítico en la seguridad de la organización. Es por ello que será necesaria una monitorización constante, que nos notifique de cualquier suceso extraño que ocurra en los sistemas. Para ello es recomendable la instalación de sistemas de detección de intruso de red (ej: Snort) o de host (OSSEC) que nos avisen de eventos anómalos.
- **Usar siempre una cuenta de usuario estándar** en lugar de la de administración.
- **Segregación de los sistemas Windows XP en una red aparte** (si es posible, sin acceso a Internet).

8 RECOMENDACIONES

Con el fin de soporte para Windows XP se debe asumir la necesidad, más tarde o más temprano, de una migración de sistema operativo. A continuación se citan una serie de buenas practicas que les pueden resultar de utilidad a la hora de afrontar una migración de sistema operativo en su organización:

- **Creación, mantenimiento y actualización de un inventario completo de activos (hardware, software y usuarios):** A menudo las organizaciones no mantienen inventarios actualizados del hardware y software, así como tener conocimiento de quién los usa. Esto lleva a grandes pérdidas de tiempo a la hora de aplicar una actualización, localización de incompatibilidades documentadas entre periféricos, y potenciales fallos de seguridad en aplicaciones no usadas y/o desactualizadas.
- **Reducir el contenido de la migración a lo útil y necesario:** La eliminación de aplicaciones inservibles, obsoletas o redundantes reduce el tiempo de migración y el esfuerzo necesario para realizarla. Cada aplicación eliminada redonda en tiempo ganado que se requiere en probar, reparar y reinstalar.
- **Pruebas de aplicación, recuperación y adaptación al nuevo entorno:** Es necesario determinar la compatibilidad de aplicaciones con el nuevo sistema operativo. En los proyectos de migración, la realización de pruebas de compatibilidad de aplicaciones, recuperación y adaptación al nuevo entorno suponen una de las fases mas largas, complicadas y propensa a errores. Es por ello que es conveniente intentar automatizar, en la medida de lo posible, las pruebas de aplicaciones y la aplicación de posibles soluciones con el objetivo de reducir el tiempo de migración y el coste del mismo, así como minimizar el riesgo de fallos posteriores.

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 10 de 17	

- **Implementación de sistemas automáticos y migración en el contenido de los usuarios:** La migración del usuario final puede causar pérdidas de productividad. Los despliegues dinámicos permiten ir más allá de las migraciones manuales, y realizar la implementación y configuración del nuevo sistema operativo, aplicaciones, paquetes de servicio y parches de manera automática.
- **Administración y feedback del usuario:** El soporte al nuevo entorno comienza tan pronto como se migra al primer usuario. Es importante contar con una serie de herramientas automáticas que realicen el seguimiento, monitorización y la administración de los sistemas. Así mismo es conveniente contar con herramientas que permitan al usuario notificar de manera fácil y rápida cualquier incidente que ocurra, tanto durante la migración como después de la misma. Esto nos ayudará a detectar de manera eficaz cualquier problema en el despliegue y actuar lo antes posible si se trata de un fallo generalizado.
- **Formación y capacitación de los usuarios al nuevo entorno.** Contar con un plan de formación orientado a los usuarios es fundamental. Los usuarios deben estar preparados para desenvolverse en el nuevo entorno y ser motivados para que el cambio no se convierta en un trauma. Como apoyo a la formación es recomendable contar con equipo preparado para resolver las dudas que les vayan surgiendo a los usuarios (servicios helpdesk).

9 ¿ACTUALIZAR O CAMBIAR?

A la hora de proyectar este tipo de migración se plantea una disyuntiva sobre si merece la pena actualizar a una versión de Windows superior, o si por el contrario sería conveniente desarrollar un cambio a otro sistema operativo. Para ello podríamos tener en cuenta los siguientes factores:

- Coste: Quizás uno de los factores más importantes. Aquí se tendrá que tener en cuenta todo el gasto que supone la migración, el coste inicial y el coste recurrente: licencias, soporte, formación, inversión en hardware, tiempo necesario para realizar la migración, etc.
- Impacto del cambio.
- Formación de los usuarios actuales.
- Necesidades específicas de aplicaciones y usuarios.
- Hardware instalado en los dispositivos. ¿Es un sistema antiguo? ¿Qué especificaciones tiene? ¿Es compatible con versiones actuales de Windows?



Vamos a estudiar las dos opciones generales: La actualización a Windows 7 u 8 y el cambio a otro sistema operativo, en este caso Linux.

Informe de divulgación Finalización del soporte a Windows XP	Código	<i>CERT-IF-5062-140121</i>
	Edición	<i>0</i>
	Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 11 de 17

9.1 ACTUALIZAR VERSIÓN MÁS NUEVA

Desde Microsoft se recomienda la actualización a Windows 8 aunque, dependiendo del hardware de nuestro equipo y de otros factores de compatibilidad, sería interesante considerar la opción de actualizar a Windows 7.

La actualización de Windows XP a Windows 7 u 8 no está soportada. No es un capricho de Microsoft, las diferencias de arquitecturas entre Windows XP y Windows 7 u 8 son demasiado pronunciadas. Es posible, sin embargo, plantear la migración del perfil del usuario. Esta operación que se puede llevar a cabo entre distintas versiones del conocido sistema operativo, consiste en mover la siguiente información del perfil:

- Usuario y contraseña de inicio de sesión.
- Datos y carpetas.
- Configuración de los componentes de Windows.
- Configuración de las aplicaciones compatibles: Exclusivamente las configuraciones, no las aplicaciones en sí.

Si optamos por Windows 7 deberíamos revisar si nuestro equipo cumple los requisitos mínimos que indica Microsoft; es decir, 1 GB de RAM para instalar la versión de 32 bits (2 GB de RAM en la de 64 bits) y un procesador con una frecuencia de como mínimo 1 GHz. Aunque siempre se recomienda contar con un hardware algo superior para una mejor experiencia del usuario.

En el caso de plantearnos un salto a Windows 8, los requisitos mínimos de hardware que plantea Microsoft son similares a los de Windows 7; es decir, 1GB de RAM y un procesador de 1 GHz. Sin embargo, la realidad es que si quieres poder trabajar de una manera más o menos fluida, tu equipo debería contar con 2GB de memoria RAM y un procesador de 2 GHz.

En general, antes de comenzar la migración a una nueva versión de Windows es conveniente:

- Comprobar los requerimientos de los equipos en los que se vaya a realizar la migración.
- Comprobar la compatibilidad de aplicaciones que funcionan en Windows XP: Existe la posibilidad de que las aplicaciones actuales ya no se desarrollen.
- Comprobar la compatibilidad de hardware instalado, así como comprobar que existen los controladores para la versión correspondiente de Windows.
- Determinar versión a instalar: de 32 o 64 bits, dependiendo del sistema.
- Asegurarse de tener copia de seguridad de todos los datos, así como de las configuraciones de los programas.
- En caso de una migración de gran tamaño y de contar con plataformas similares (modelos de equipos uniformes) se recomienda tener una imagen con la versión del sistema operativo elegida, para realizar el platado volcando directamente al disco (sistema operativo, drivers, aplicaciones, etc...) en lugar de instalar los sistemas de manera individual.

Informe de divulgación Finalización del soporte a Windows XP		Código	<i>CERT-IF-5062-140121</i>
		Edición	<i>0</i>
		Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 12 de 17	

Para la realización del proceso de migración, se cuenta con dos alternativas distintas dependiendo si se va a realizar a nivel de usuario o a nivel de administración de sistemas (más automatizable y pensado para la migración de múltiples equipos):

- **A nivel de usuario individual:** [Windows Easy Transfer](#). Ayuda a transferir los archivos del usuario, correos electrónico, imágenes y configuración.
- **A nivel de una organización con multitud de máquinas a migrar:** [User State Migration Tools](#) (USMT). Para migrar los fichero de usuarios y configuraciones en grandes despliegues de Windows XP y Vista.

Vamos a centrarnos en esta última, ya que es la que más nos interesa para el presente documento.

9.1.1 COMPROBANDO LA COMPATIBILIDAD DE APLICACIONES



Para ayudarnos a la hora de determinar qué aplicaciones corporativas, controladores de hardware e incluso aplicaciones web están preparadas para dar el salto a una nueva versión de Windows que vayamos a instalar, Microsoft pone a nuestra disposición el conjunto de herramientas [Aplicación Compability Toolkit](#) (ACT), que nos permitirán analizar nuestros sistemas y recolectar de forma centralizada gran cantidad de información de nuestros equipos, de forma que podamos hacer una análisis muy aproximado del impacto de la actualización al nuevo sistema.

Para poner en funcionamiento un sistema centralizado de recolección de información necesitamos los siguientes elementos:

- Una base de datos SQL Server Express o superior. ACT 5.6 funciona con SQL Server 2005 ó 2008, mientras que ACT 6.0 funciona con SQL Server 2008 en adelante.
- Una carpeta compartida en el sistema de archivos. Será donde los equipos cliente nos dejen sus logs.
- Una cuenta del servicio para el agente recolector de datos. El agente recolector de datos se ejecuta en equipos de cliente, y para acceder a la carpeta de datos necesita permisos en la misma.
- Un Windows cliente ACT puede gestionar de forma centralizada toda la información desde un Windows cliente.

El funcionamiento de esta herramienta se divide en tres pasos:

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 13 de 17

1. **Recopilación de información:** En esta fase se realiza un inventario de las aplicaciones y se recogen los datos de compatibilidad de aplicación a través de los evaluadores de compatibilidad.
2. **Analizar los resultados:** Se categorizan y priorizan las aplicaciones según los resultados obtenidos, mostrando un informe.



Open Reports	Application Name	Version	Company	My Assessment	Send and	Vendor Assess	Community Assessment	Active Issu	Computers
	7-Zip 9.20	9.20			✓		32 (81) 64	0	1
	Developer 2000 Demos for NT				✓		32 (0) 64	0	1
Quick Reports	Hyper-V Integration Services (...)	3.9200.1...	Microsoft...		✓		32 (0) 64	0	1
Windows 7 Reports	Microsoft Application Compati...	5.6.7324.0	Microsoft...		✓	32 ✓ 64	32 (208) 64	0	1
Applications	Microsoft Security Essentials	4.2.223.0	Microsoft...		✓	32 ✓ 64	32 (1) 64	0	1
Application Installation Pack...	MSN				✓		32 (77) 64	0	1
Computers	Windows Genuine Advantage...	1.9.0040.0	Microsoft...		✓		32 (120) 64	0	1
Devices	Windows Messenger				✓		32 (108) 64	0	1
Windows Vista SP1/SP2 Reports									
Applications									
Application Installation Pack...									

3. **Pruebas y mitigación:** Si existen problemas con alguna aplicación en particular, se consulta si es posible arreglarlo mediante alguna actualización o workaround disponible para que la aplicación pueda ser compatible.

9.1.2 ACTUALIZACIÓN A WINDOWS 7/8 DESDE WINDOWS XP MEDIANTE USMT

Las User State Migration Tools (USMT) es un conjunto de herramientas de línea de comandos que ofrecen a los profesionales de TI la capacidad de personalizar en gran medida la migración de perfiles de usuario, permitiendo un alto grado de automatización a la hora de realizar migraciones masivas de perfiles. Se pueden obtener gratuitamente como parte del Windows Automated Installation Kit (WAIK) en Windows 7 y como parte del Windows Automated Deployment Kit (ADK) para Windows 8 .

USMT se encuentra diseñado para administradores, requiriendo un sistema cliente conectado a un controlador de dominio de Windows Server, existen varios escenarios en los que el uso de USMT 4.0 no es aconsejable:

- Migraciones que requieren la interacción del usuario final.
- Migraciones que requieren personalizar los equipos uno a uno.

Las ventajas del uso de USTM para la realización de migraciones de manera masiva con los siguientes:

- Migra cuentas de usuario, configuraciones de sistema operativo y configuraciones de aplicación sin riesgo alguno.
- Reduce el costo derivado de la implementación de Window debido a que conserva el estado del usuario.

<i>Informe de divulgación Finalización del soporte a Windows XP</i>		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 14 de 17	

- Reduce el tiempo de inactividad del usuario final necesario para personalizar los escritorios y encontrar los archivos que faltan.
- Reduce el número de llamadas al departamento de soporte técnico.
- Reduce el tiempo necesario para que el usuario se familiarice con el nuevo sistema operativo.
- Aumenta la satisfacción de los empleados con la experiencia de migración.

La herramienta de migración de Microsoft USMT (User State Migration Tools) está compuesta por los siguientes componentes diferenciados que nos ayudarán en cada una de las fases de la migración:

- **scanstate.exe.** Programa que se encarga de recopilar toda la información de perfiles y almacenarla donde estimemos conveniente.
- **loadstate.exe.** Programa que se encarga de leer la información de perfiles almacenada y restaurarla en nuestro sistema actual.
- **Conjunto de archivos XML** que permiten realizar lo siguiente:
 - Seleccionar el contenido que se debe copiar y el que no.
 - Arbitrar en los conflictos entre el equipo de origen y el equipo de destino.
 - Modificar la ubicación del equipo de destino a la que se migran los datos.
 - Emular las configuraciones que falten.
 - Eliminar la configuración del equipo de destino.

Para llevar a cabo la migración con esta herramienta van a ser necesarios los siguientes componentes:

- Disco DVD del producto Windows a instalar: Para instalaciones automatizadas se recomienda la creación de imágenes de Windows que permitan realizar instalaciones desatendidas, para más información sobre la creación y personalización de instalaciones puede consultar los enlaces [Guía paso a paso de implementación básica de Windows](#) y [Desarrollo de Windows con Windows ADK](#).
- Disco DVD del Kit de instalación automatizada de Windows (WAIK o ADK).
- Equipo Origen de los datos a migrar.
- Conectividad de red.
- Equipo del técnico: El equipo del técnico puede ser cualquier equipo en el que se instale el AIK de Windows. Dicho equipo debe ejecutar Windows Server 2003, Windows Vista o Windows 7.
- Un equipo de destino (opcional): Puede ser el mismo equipo de origen o uno diferente. Dependiendo de si se trata de una actualización o un reemplazo.

Informe de divulgación Finalización del soporte a Windows XP		Código	CERT-IF-5062-140121
		Edición	0
		Fecha	21/01/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 15 de 17	

9.2 CAMBIAR DE SISTEMA OPERATIVO

Por otro lado, teniendo en cuenta que el principal impedimento para la migración para muchas empresas es el económico, el no tener costes de licencias por un sistema operativo, sin duda es una buena elección. Además es necesario tener en cuenta que en muchos casos, sobre todo en las organizaciones con sistemas más antiguos, será necesaria una actualización del hardware, ya que muchos de los controladores de los componentes no se encontraran soportados en las nuevas versiones de Windows, siendo un coste total inasumible para algunas organizaciones.



Es por ello que quizás convenga plantearse el cambio en alguno (o en todos) los equipos a otro sistema operativo, como Linux.

Existe una gran cantidad de distribuciones diferentes, en los últimos años se está realizando un considerable esfuerzo en acercar Linux a los usuarios de escritorios, con el objetivo de facilitar la transición a los usuarios acostumbrados a sistemas Windows. Es por ello que han aparecido muchas distribuciones amigables como Ubuntu, GuadaLinux (distribución de la Junta de Andalucía basada en Ubuntu) o Linux Mint, que ofrecen un entorno de trabajo intuitivo y fácil de manejar.

Aun así se plantea una serie de ventajas e inconvenientes que es necesario plantear siempre:

Ventajas:

- Ahorro en el pago de licencias, tanto en el sistema operativo, como en los muchos programas libres, como por ejemplo LibreOffice.
- Mayor compatibilidad de Hardware (especialmente en equipos antiguos).
- Menor tasa de infección por malware.
- Gran apoyo de comunidades de usuarios.
- Software Libre, que es posible modificar y adaptar a las necesidades que se requieran.

Inconvenientes:

- Menos soporte técnico del proveedor, aunque si es posible encontrarlo en distribuciones como RedHat (de pago) o contratarlo con un tercero. Sin embargo, por regla general cualquier distribución se encuentra respaldada con una gran comunidad de usuarios en la que se puede contar con ayuda para resolver cualquier problema.
- Mayor curva de aprendizaje (cursos, formación, etc...): Sin embargo es necesario apuntar que esto podría ocurrir de la misma manera en la actualización a Windows 8, debido a los numerosos cambios que ha sufrido la nueva versión de este sistema operativo.

Informe de divulgación Finalización del soporte a Windows XP		Código	<i>CERT-IF-5062-140121</i>
		Edición	<i>0</i>
		Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 16 de 17	

- Problemas para hacer uso del software especialmente diseñado para Windows o que no tengan equivalente en Linux.
- Incompatibilidad de algunos formatos propietarios.
- Problemas de adaptación de aplicaciones corporativas.

Sería interesante poder plantear una migración combinada, estudiando las necesidades de cada usuario o grupo de usuarios, y actualizar o cambiar el sistema operativo según las necesidades, la complejidad, el presupuesto y el impacto. Por ejemplo, en un equipo de un usuario que necesite un procesador de texto básico y programas habituales como navegador, correo, etc ... se puede plantear cambiar a cualquier sistema Linux, mientras que un usuario que necesite programas muy específicos como Autocad u otros, podría plantearse la actualización a Windows 7 o Windows 8.

10 CONCLUSIONES

Es importante entender los riesgos que implican el permanecer con un sistema operativo obsoleto. Cada organización debería plantearse, si no se ha hecho ya, la migración a una versión superior de Windows, o el cambio a otro sistema operativo a corto plazo, ya que la máxima de la seguridad "ten tus sistemas actualizados" no va a poder ser cumplida, con todo lo que ello implica.

Es necesario comprender que las medidas temporales incluidas en este comunicado no deberían ser implementadas, en ningún caso, como una solución final, siendo sólo directrices que ayudan a mitigar el problema mientras se planifica y ejecuta la migración.

Se prevé que durante los siguientes meses tras el fin del soporte de Windows XP el número y la sofisticación de amenazas se incremente de manera significativa, de hecho, es muy posible que los cibercriminales estén haciendo acopio de 0-days, y los estén guardando para hacer uso de ellos cuando Microsoft no vaya a ofrecer una solución.

En cualquier caso, el fin del ciclo de vida de Windows XP supone un riesgo que debe de ser tomado en cuenta. Gestionado de forma adecuada debería de suponer una cierta molestia, pero si se trata de forma correcta el riesgo podrá ser controlado de forma adecuada.

<i>Informe de divulgación Finalización del soporte a Windows XP</i>		Código	<i>CERT-IF-5062-140121</i>
		Edición	<i>0</i>
		Fecha	<i>21/01/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 17 de 17	

11 REFERENCIAS

- [Fin de soporte Windows XP](#)
- [Upgrading from Windows XP to Windows7](#)
- [User State Migration in Windows XP](#)
- [Application Compatibility Toolkit \(ACT\) Technical Reference](#)
- [Guía de usuario de la Herramienta de migración de estado de usuario 4.0](#)
- [Microsoft Deployment Toolkit](#)
- [Guía paso a paso de implementación básica de Windows](#)
- [Desarrollo de Windows con Windows ADK](#)