Microsoft

Windows XP – Fin de soporte el 08.04.2014

Los componentes de un Entorno Seguro – Cómo resistir frente a los ciberataques actuales

Windows XP – El soporte cesa el 8 de abril de 2014. Por qué le afecta.

Windows XP Service Pack 3 (SP3) y Office 2003 llegarán al final de su periodo de soporte extendido el próximo 8 de abril de 2014. A partir de esa fecha Microsoft no ofrecerá soporte público para estos productos, ni parches de seguridad, parches de programación, soporte de incidencias o actualizaciones de contenido técnico online.

Seguir utilizando Windows XP SP3 después de la fecha de final de soporte puede exponer a las organizaciones a riesgos de seguridad y cumplimiento, o a la ausencia de soporte por parte de fabricantes de hardware y desarrolladores de software. A fin de reducir los riesgos de ataque y proteger sus infraestructuras de TI, se recomienda encarecidamente a las grandes compañías y organizaciones del sector público que actualicen desde Windows XP a Windows 7 o Windows 8 y que adopten unas medidas adecuadas de actualización para asegurarse un buen nivel de protección.

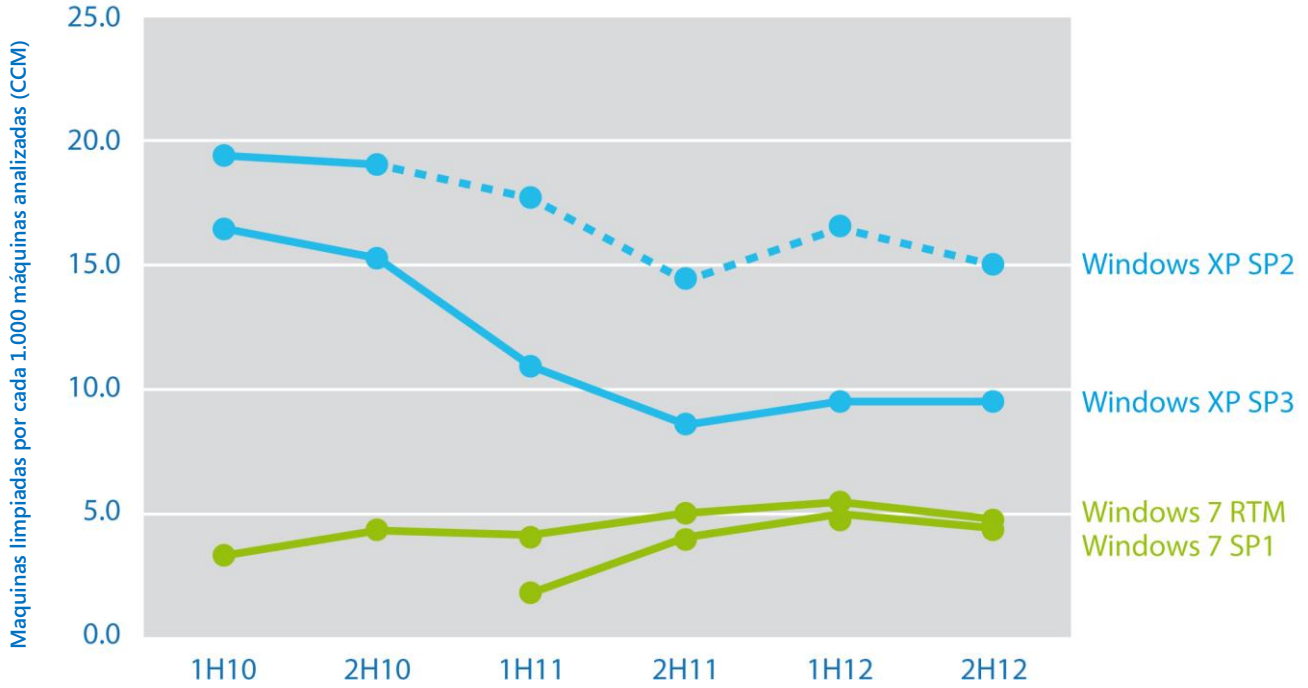
Windows XP era bueno en su momento, pero los tiempos han cambiado.

Ya han transcurrido doce años desde la aparición de Windows XP y el mundo ha cambiado mucho desde entonces. El uso de Internet ha crecido desde unos 360 millones de usuarios a más de 2.400 millones. Hemos asistido al surgimiento de la ciudadanía de Internet donde los miembros de la sociedad se conectan por correo electrónico, mensajería instantánea, videollamada, redes sociales y una amplia gama de aplicaciones basadas en web y para dispositivos. A medida que Internet se ha ido incorporando de manera más profunda en cada rincón de nuestra sociedad, se ha convertido cada vez más en el objetivo preferido de muchas formas de delincuencia (como se pone de relieve en el Informe de Inteligencia de la Seguridad, de Microsoft). Dada su rápida evolución, la seguridad del software ha tenido que evolucionar para seguir un paso por delante del delito informático. Para contribuir a la seguridad de los usuarios frente a cambios tan rápidos en el panorama de las amenazas en la red, Microsoft, normalmente proporciona soporte a las empresas y productos de desarrollo durante los 10 años siguientes a la aparición del producto, y para la mayoría de productos de consumidor, hardware y multimedia durante los cinco años siguientes a la fecha de aparición del producto.

De acuerdo con este ciclo de vida de soporte del producto definido hace ya bastante tiempo, a partir del 8 de abril de 2014, los usuarios de Windows XP SP3 dejarán de recibir actualizaciones de seguridad, actualizaciones y parches no relacionados con la seguridad, ni tampoco podrán disponer de opciones de soporte y asistencia técnica de parte de Microsoft, ni se actualizarán los contenidos técnicos en la web. Esto supone que las nuevas vulnerabilidades que pudieran descubrirse en Windows XP tras la finalización del servicio de soporte no podrán resolverse con nuevas actualizaciones de seguridad expedidas por Microsoft. Por tanto, en el futuro será muchísimo más sencillo para los atacantes poner en riesgo los sistemas basados en Windows XP utilizando medios para aprovechar vulnerabilidades no resueltas. En este escenario, el software de protección antimalware y otras medidas de seguridad se encontrarán en una seria desventaja y con el tiempo será cada vez más difícil proteger la plataforma Windows XP.

Podemos hacernos una idea de lo que ocurre con las tasas de infección por malware cuando una plataforma finaliza su periodo de soporte recordando como ejemplo el caso de Windows XP Service Pack 2 (SP2). El soporte para Windows XP SP2 terminó el 13 de julio de 2010. Aunque esta plataforma incluía numerosas mejoras en seguridad en el momento de su lanzamiento, a día de hoy tiene una tasa de infección por malware mucho más elevada que Windows XP SP3 o que cualquiera de los nuevos sistemas operativos Windows. Como puede verse en la gráfica de la página siguiente, los ordenadores con Windows XP sufren de manera habitual unas tasas de infección por malware notablemente más elevadas que otros ordenadores donde se ejecuta cualquier otra versión soportada de Windows. En gran medida esta mayor tasa de infección puede atribuirse al hecho de que algunas de las funcionalidades de seguridad integradas más importantes que se han incluido en las versiones más recientes de Windows no existen en Windows XP. Windows XP, diseñado en otra época, simplemente no puede hacer frente a las amenazas de una manera tan eficaz como los sistemas operativos más modernos, como Windows 7 y Windows 8.

El panorama de las amenazas en Internet ha cambiado en los últimos doce años, después de la aparición de Windows XP y en la misma medida ha evolucionado también el software de seguridad. Existen ahora muchas funciones de seguridad integradas en los sistemas operativos modernos que pueden proteger mejor a los usuarios frente a la actividad delictiva, como pueden ser:



Mejoras en el kernel:
Las versiones más recientes de Windows incluyen una serie de mejoras relacionadas con la seguridad del kernel de Windows que hacen más complicado el empleo de ciertas técnicas habituales de hacking, como la explotación de desbordamientos de buffer o la predicción de la ubicación del código en la memoria.

Protección antimalware en tiempo real:
In Windows 8, Windows Defender viene integrado en el sistema y proporciona por diseño protección en tiempo real frente al malware y software potencialmente no deseado.

BitLocker Drive Encryption:
Se introdujo por primera vez con Windows Vista y permite a usuarios y administradores cifrar discos duros completos y proteger los datos en los equipos frente a accesos no autorizados en caso de robo o pérdida. Con Windows 7 se presentó BitLocker To Go, que permite cifrar el contenido de dispositivos de almacenamiento removibles. En Windows 8 BitLocker se despliega y administra de manera aún más sencilla.

Control de Cuenta de Usuario (UAC):
Esta funcionalidad se introdujo con Windows Vista y permite evitar cambios no autorizados en los equipos haciendo que los usuarios operen sin privilegios de administrador excepto en los momentos en que necesiten llevar a cabo tareas administrativas. En Windows 7 y posteriores, UAC se ha mejorado y ofrece una experiencia de usuario más optimizada y natural.

AppLocker:
Apareció con Windows 7, y lo utilizan los departamentos de TI para restringir el catálogo de programas que pueden utilizar los usuarios, mediante la declaración de unas reglas potentes y flexibles. En Windows 8 los administradores pueden restringir el acceso a apps de Windows Store además de controlar las aplicaciones tradicionales de Windows

Arranque seguro con UEFI:
Se presentó con Windows 8, y se trata de una funcionalidad basada en hardware obligatoria para todos los equipos certificados para Windows 8. Sirve para evitar que se ejecuten sistemas operativos o código de firmware no autorizados en tiempo de arranque mediante el uso de bases de datos de firmas reconocidas de software e imágenes de software, que previamente se han aprobado como las únicas piezas de software autorizado a ejecutarse en la máquina.

Arranque seguro (*trusted boot*):
La característica llamada trusted boot de Windows 8 comprueba la integridad de los archivos de arranque de Windows e incorpora una funcionalidad llamada ELAM (Early Launch AntiMalware) que hace posible que el software de detección antimalware empiece a ejecutarse antes que cualquier software de otras procedencias. Al ejecutarse el software de protección en un momento muy inicial del proceso de arranque de la máquina, se garantiza la operatividad y la integridad del propio software de protección. Dentro del proceso de arranque, Windows ejecuta además el Arranque Medido (*Measured Boot*), con el que software de otros fabricantes ejecutado en un servidor remoto puede comprobar el nivel de seguridad de cada uno de los componentes en tiempo de arranque de una manera que, para el malware, resulta muy difícil de burlar. Si se detecta algún intento de alterar el proceso original de arranque de Windows o del driver ELAM, Trusted Boot recupera el sistema reinstalando los archivos originales.

Pero por encima de todas las medidas y funciones de seguridad de que disponen hoy día los sistemas operativos modernos, las prácticas de desarrollo también han evolucionado mucho a lo largo de la década pasada pero hay que reconocer que también lo han hecho las propias amenazas. En la tabla de la página siguiente se muestran las principales amenazas detectadas en los momentos de aparición de Windows XP, Windows Vista, Windows y Windows 8

Principales amenazas

- Internet empezaba a crecer.
- El correo electrónico aún no era un medio utilizado de forma generalizada

1995

Windows 95

Principales amenazas

- Melissa (1999). Love Letter (2000).
- Muchas de esas amenazas aprovechan recursos de ingeniería social.

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Control de Accesos
- Perfiles de Usuario
- Directivas de seguridad
- EFS (Encrypting File System) basado en archivos
- Soporte para smartcards y PKI
- Windows Update

Principales amenazas

- Code Red y Nimda (2001) Blaster (2003), Slammer (2003)
- Los ataques del 11 de Septiembre.
- La mayoría explotan los desbordamientos de buffer
- Pequeños bloques de scripting.
- Tiempo medio desde la detección al parche: de varios días a semanas.

2004

Windows XP SP2

- ASLR (Address Space Layout Randomization)
- Data Execution Prevention (DEP)
- SDL (Ciclo de Vida de Desarrollo de Seguridad)
- Actualizaciones automáticas active por defecto
- Firewall active por defecto
- Centro de Seguridad de Windows

Soporte para protocolo de seguridad para conexión inalámbrica WPA

Principales amenazas

- Zotob (2005).
- Ataques de "alzamiento de pila".
- Rootkits.
- Explotación de vulnerabilidades de desbordamiento de buffer
- Pequeños bloques de scripting
- Expansión de los ataques de phishing.
- Usuarios ejecutando tareas con privilegios de Admin.

2007

Windows Vista

- BitLocker
- Patchguard
- Mejoras en ASLR y DEP
- SDL complete
- Control de Cuentas de Usuario
- Filtro SmartScreen en Internet Explorer
- DRM (Digital Rights Management)
- Mejoras en el firewall
- Exigencia de firma digital en drivers de dispositivos
- Soporte para TPM
- Niveles de Integridad de Windows
- Configuración segura "por defecto" (para funcionalidades de Windows e Internet Explorer

Principales amenazas

- Crimen organizado.
- Botnets.
- Robos de identidad.
- Conficker (2008).
- Tiempo desde la detección al parche: días.

2009

Windows 7

- Mejoras en ASLR y DEP
- SDL completo
- Mejoras en la pila IPSec
- Cuentas de servicio gestionadas
- Mejoras en Control de Cuentas de Usuario
- Mejoras en la auditoría
- Filtro SmartScreen en Internet Explorer
- AppLocker
- BitLocker To Go
- Servicio Biométrico de Windows
- Centro de Actividades de Windows
- Windows Defender

Principales amenazas

- Crimen organizado, actores potenciales desconocidos.
- Ataques dirigidos muy sofisticados.
- Operación Aurora (2009)
- Stuxnet (2010).

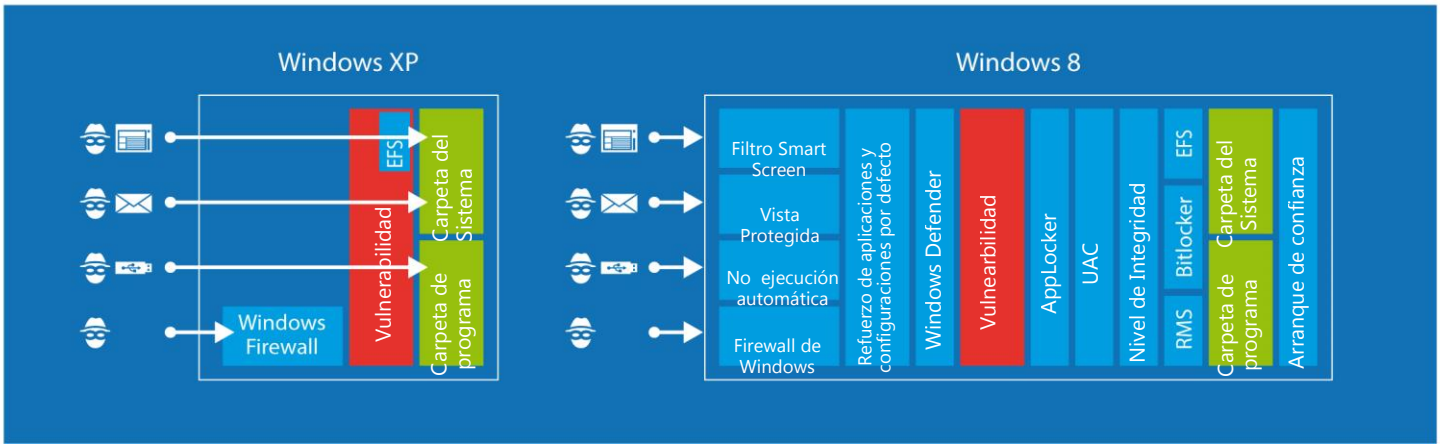
2012

Windows 8

- UEFI (Arranque seguro)
- TPM basado en firmware
- Arranque Seguro (con ELAM)
- Arranque controlado y soporte para Atestado Remoto
- Mejoras sustanciales en ASLR y DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (sin plugins y con Modos Protegidos mejorados)
- Reputación de Aplicaciones pasa al núcleo del S.O.
- BitLocker: Encriptado de disco duro y soporte para cifrado del espacio utilizado del disco
- Smartcard virtual
- Contraseña gráfica, PIN
- Control de Acceso dinámico
- Antivirus integrado

El riesgo que supone no tener soporte para Windows XP nunca más

Los delincuentes informáticos están muy al tanto del cese del soporte para XP y de que no habrá más actualizaciones de seguridad, así que podemos suponer que en seguida aparecerán nuevos ataques que aprovechen esta circunstancia. Además, el nuevo sistema operativo ofrece nuevas oportunidades para el teletrabajo, para compartir documentos e información, para el uso de soluciones de movilidad y conexión a servicios en la nube sin afectar a su seguridad. El efecto resultante de todo esto es que las amenazas actuales se contienen mucho mejor con Windows 8 que con Windows XP.



Vulnerabilidad de Windows XP comparada con Windows 8

Se trata de riesgos efectivos y que no solo afectan a la seguridad. Entre los riesgos adicionales podemos hablar de:

- **Aplicaciones de negocio no soportadas**. Al cesar el soporte para Windows XP el 08.04.2013, los fabricantes independientes de software ya han dejado de probar las nuevas versiones de su software en Windows XP y las nuevas versiones de los paquetes críticos para las empresas seguramente exigirán como mínimo Windows 7
- **Hardware no soportado**. Los fabricantes de hardware y OEMs también han dejado de probar los nuevos dispositivos en Windows XP. Muchas máquinas que se venden actualmente no soportan XP y no disponen de drivers para este sistema.
- **A partir del 8 de abril de 2014 se dejará de dar soporte con Software Assurance**, de manera que los clientes que necesiten soporte para XP deberán firmar un Contrato de Soporte Personalizado (CSA) para XP. Entre los gastos extra que ello supone están las cuotas de inscripción y una tarifa por dispositivo.

Otras ventajas adicionales de la migración

Las organizaciones que han migrado a Windows 7 o Windows 8 ya disfrutan de las ventajas que suponen una experiencia muy mejorada de usuario y gestión. Una de las grandes ventajas de la migración es que ofrece la posibilidad de transformar procesos manuales obsoletos. La consecuencia directa de las capacidades de Windows 8 son ahorros reales y tangibles.

- **Conexión desde cualquier lugar**
  Los usuarios disponen de acceso seguro y sin complicaciones a sus datos, aplicaciones y compañeros de trabajo. Necesitan seguir manteniendo su productividad en cualquier lugar, en cualquier momento y sobre una gran variedad de dispositivos.
- **Experiencias personalizadas**
  La productividad individual mejora al ofrecer a los usuarios experiencias personales que anticipan sus preferencias y se adaptan a sus estilos de trabajo peculiares.
- **Infraestructura inteligente**
  Soluciones de nivel empresarial pensadas para ayudarle a mantener el máximo nivel de seguridad, para optimizar la gestión y para reducir los costes.
- **DDPS (Desktop Deployment Planning Serices)**
  Puede preparar ejecutar con éxito un despliegue de Microsoft Office, con la ayuda de estos servicios de planificación completos que ofrecen partners cualificados de Microsoft.
- **MAAP (Microsoft App Accelerate Program)**
  Para probar las capacidades de los productos y servicios en entorno de laboratorio, definir los requisitos de los nuevos despliegues, llevar a cabo un piloto y desplegar finalmente una solución de Estilo de trabajo Flexible.
- **Windows To-Go**

A medida que cobran importancia en entre las organizaciones los escenarios de uso de equipos personales (BYOD, "*bring-your-own-device*") y de movilidad, las empresas necesitan disponer de alternativas para que los usuarios puedan seguir manteniendo su productividad en cualquier lugar donde se encuentren. Windows To Go es una nueva funcionalidad para usuarios de Windows 8 en grandes organizaciones que les permite arrancar una versión completa de Windows desde memorias USB externas conectadas a PCs. Las unidades con Windows To Go pueden utilizar las mismas imágenes del sistema que se emplean en las organizaciones para sus equipos portátiles y de escritorio, y se administran igual, por lo que son una nueva y eficaz opción para la movilidad.

- **Coste reducido**

  Un informe de IDC demuestra que mantener instalaciones antiguas de Windows XP supone para las organizaciones unos costes mucho más elevados que migrar a una solución basada en Windows 7. El coste anual por PC en el caso de Windows XP asciende a 870 USD frente a los costes equivalentes por instalación de Windows 7, que suponen 168 USD al año por equipo. En este diferencial de 701 USD por equipo y año se incluyen costes de TI y costes laborales de usuario final. (*Fuente: informe "Mitigating Risk: Why Sticking with Windows XP is a Bad Idea. ". IDC, mayo 2012*).

  Nosotros somos plenamente conscientes de que cualquier migración hacia sistemas nuevos supone toda una serie de retos y por ello hemos desarrollado una familia de herramientas que facilitan las labores de migración hacia plataformas modernas.

Cómo puede ayudar Microsoft

Podemos ayudar a nuestros clientes del Sector Público y de la empresa privada a proteger su información y sus propias infraestructuras de TI mejorando la salud de su ecosistema de TI. Microsoft puede contribuir a crear un ecosistema de TI más seguro y saludable por medio de una estrategia de dos etapas que se basa en los conocimientos exclusivos de Microsoft y en nuestra amplia experiencia previa:

1) **Llevar a cabo una Evaluación de Riesgos de Seguridad de Microsoft, con la que los clientes pueden obtener una panorámica general de su situación actual de riesgo.**

   Ayudar a las organizaciones a conocer su entorno actual respecto de las amenazas y la seguridad es un buen punto de partida para empezar a hablar de migrar los sistemas Windows XP. Una de las auditorías a considerar es la MSRA (Microsoft Services Security Risk Assessment). Esta oferta está orientada a definir y delimitar los riesgos de seguridad en una aplicación y la infraestructura sobre la que se ejecuta. Aplica una metodología formal y ayuda a las organizaciones a conocer su nivel de exposición a riesgos derivados de posibles agujeros de seguridad en aplicaciones críticas y a evaluar sus controles y procesos de seguridad contrastándolos contra prácticas estándar de la industria. Con todo esto se puede delimitar una línea de base de seguridad que servirá para medir los progresos posteriores.

2) **Ayuda para el despliegue de Windows 7 u 8 y garantizar que las nuevas funcionalidades se utilizan de manera eficiente.**

   La Guía de Migración de Windows XP a Windows 7 (http://technet.microsoft.com/en-us/ee150430.aspx) incluye diversas herramientas que se pueden descargar de Internet.
   El Modo Windows XP para Windows 7 y Windows 8 permite a los usuarios instalar y ejecutar aplicaciones diseñadas para Windows XP directamente desde un PC con Windows 7. El Modo XP es un entorno integrado con una serie de funciones de productividad como son la integración de carpetas para permitir el acceso transparente a los discos del sistema Windows que hace la función de host desde las aplicaciones ejecutadas en Modo XP, el acceso directo a aplicaciones en Modo XP desde el menú Todos los Programas en la máquina host, soporte para dispositivos USB en Modo XP, portapapeles compartido entre el sistema host con Windows y las aplicaciones en Modo XP y también la redirección de impresoras para dichas aplicaciones.

¡Prepare y ejecute su migración de Windows XP de forma que, como muy tarde, a comienzos de 2014 ya esté terminada!

Windows XP fue en su día un sistema operativo muy bueno y ha aportado valor real a una gran cantidad de personas y organizaciones en todo el mundo durante más de una década. Pero todas las cosas buenas se terminan alguna vez. Esperamos que esta información le haga reflexionar sobre la importancia de migrar a un sistema operativo moderno, que cuente con mejores medidas de protección y que suponga también una llamada de atención urgente para las organizaciones que llevan con retraso sus planes de migración.

En definitiva, el tiempo pasa rápidamente. El soporte y el mantenimiento para Windows XP finalizarán el próximo día 8 de abril de 2014. Para entonces será fundamental que tanto empresas como consumidores hayan migrado ya a sistemas Windows 7 o Windows 8: nuestros sistemas operativos modernos se han creado para el futuro, ya sea en términos de nuevos modelos de uso -como son la computación en movilidad o el empleo de interfaz táctil- como –y esto es lo más importante, en lo que significa un mayor nivel de seguridad

Los componentes de un Entorno Seguro – Cómo resistir frente a los ciberataques actuales

Este informe forma parte de una serie de documentos que explican cómo mejorar la capacidad de resistencia frente a los ciberataques actuales. Sigue el modelo basado en "Protección-Contención-Detección-Respuesta-Recuperación". Dicho brevemente, este esquema se basa en la constatación de que contra los actuales atacantes no basta con aplicar medidas de protección, sino que tenemos que estar preparados para contener posibles intrusiones, detectarlas a tiempo, responder a la incidencia y tener capacidad de recuperación. La información sobre amenazas es la base de todas las actividades y orienta los pasos a seguir en cada fase.

- **Protección** de los sistemas frente a ataques por medio de una combinación de formación, implementación y evaluaciones. Los esfuerzos se centran en:
- **Contener** los movimientos laterales del atacante y evitar el acceso a privilegios elevados impidiendo o limitando la capacidad de abusar de las credenciales.
- **Detectar** ataques activos o sistemas atacados antes de que se conviertan en un problema más agudo dentro del cliente.
- **Responder** a las intrusiones en cuanto se detectan.
- **Recuperarse** de una intrusión ejecutando los planes de restauración previstos.
- **La información sobre amenazas** orienta sobre la situación actual y los pasos a seguir.

Más información disponible en:

Portal de Microsoft Security:
http://www.microsoft.com/security

Blog de Informática de Confianza:
http://blogs.technet.com/b/security/archive/2013/04/09/the-countdown-begins-support-for-windows-xp-ends-on-april-8-2014.aspx

Informe de Inteligencia de Seguridad V14:
http://www.microsoft.com/security/sir/default.aspx