Kaspersky sigue protegiendo versiones obsoletas de Windows

¿Cómo proteger estaciones de trabajo con sistemas operativos obsoletos?

kaspersky bring on the future

kaspersky.es

Kaspersky sigue protegiendo versiones obsoletas de Windows

Microsoft dejó de admitir el sistema operativo Windows XP hace varios años, lo que significa que los usuarios de este SO ya no reciben actualizaciones ni parches de seguridad del fabricante. Además, se filtró toda la codificación del sistema Windows XP, por lo que cualquiera puede encontrar nuevas maneras de hackear sus dispositivos. Esto hace que el popular sistema operativo sea extremadamente vulnerable. El problema se agrava por el hecho de que la mayoría de las soluciones de seguridad de nivel empresarial ya no admiten Windows XP ni Windows 7.

Después del 14 de octubre de 2025, Microsoft tampoco admitirá Windows 10.

Microsoft finalizó el soporte para Windows XP el 8 de abril de 2014, después de 12 años. El soporte para Windows 7 finalizó en enero de 2023, incluidas las actualizaciones de seguridad extendidas de pago. El soporte para Windows 10 finalizó en octubre de 2025. Las actualizaciones de seguridad y el soporte técnico ya no están disponibles para estos sistemas operativos heredados, de modo que los usuarios deben actualizar a una versión más moderna.

Según Microsoft, la forma recomendada de actualizar es comprar un nuevo dispositivo con la versión más reciente instalada.

A noviembre de 2023, más de 1.600 millones de computadoras en todo el mundo ejecutan el sistema operativo Windows. Según StatCounter, Windows posee alrededor del 70 % del mercado global de computadoras de escritorio, y Windows XP todavía constituye alrededor del 0,38 % de esa proporción. Esto significa que aproximadamente 6 millones de computadoras en todo el mundo todavía ejecutan Windows XP.

¿Por qué Kaspersky Security for Business ya no admite Windows XP?

Hasta 2020, nuestra solución de seguridad de endpoints integral, Kaspersky Security for Business, admitía el sistema operativo Windows XP, incluso después de que la mayoría de los proveedores de seguridad habían dejado de hacerlo. Pero, con el paso del tiempo, se tornó imposible.

La realidad es que, a diferencia de las versiones anteriores de Windows, el panorama de amenazas sigue evolucionando. Nos esforzamos por ofrecerles a nuestros clientes tecnologías de protección innovadoras para enfrentar amenazas cada vez más diversas y complejas (por ejemplo, el Control Adaptativo de Anomalías), pero independientemente de qué tan avanzadas y efectivas sean estas tecnologías, simplemente no funcionarán adecuadamente en Windows XP.

¿Hay una opción?

Los días de sistemas que todavía ejecutan versiones no admitidas de Windows están contados. La calidad y las capacidades de las soluciones de seguridad alternativas que siguen funcionando con ellas son extremadamente limitadas. La mayoría están dirigidas a dispositivos hogareños, y ninguna ofrece el nivel de seguridad que se requiere para un SO que el proveedor ya no admite. Además, es posible que estas mismas soluciones dejen de ser admitidas, ya que el mercado de productos de seguridad que admiten sistemas operativos Windows heredados está mermando con rapidez.

Actualice su sistema operativo

Los indicios son claros: es momento de que su empresa invierta en hardware y software modernos en lugar de seguir luchando con los crecientes riesgos e ineficiencias de los sistemas desactualizados y no admitidos. Ahora es el momento de desarrollar un plan de actualización a largo plazo.

Mientras usted siga utilizando un sistema operativo obsoleto, su empresa estará expuesta a riesgos significativos. Por un lado, Microsoft ya no proporciona soporte ni actualizaciones; por el otro, no podrá utilizar las versiones más recientes de soluciones de seguridad como Kaspersky Security for Business o Kaspersky Symphony.

¿Cómo mantenerse protegido?

Migrar a un nuevo sistema operativo lleva tiempo, y ninguna empresa puede darse el lujo de mantenerse desprotegido durante esta transición.

Por suerte, tenemos otra solución de seguridad de endpoints que admite versiones heredadas de Windows y seguirá admitiéndolas en el futuro próximo.

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security proporciona protección y soporte completos hasta que esté listo para migrar a los sistemas operativos Windows más recientes que no entren en conflicto con las últimas tecnologías de seguridad en Kaspersky Security for Business.

Kaspersky Embedded Systems Security es un sistema de seguridad multicapa sólido basado en un motor antimalware probado, y ofrece todos los beneficios de la administración centralizada a través de la consola familiar de Kaspersky Security Center. La solución ligera está diseñada específicamente para los sistemas operativos Windows a partir de Windows XP SP2.

Ofrece una protección simple estable para empresas que necesitan tiempo para actualizar versiones heredadas de Windows o que no pueden migrar a otro sistema operativo. El producto es adecuado para sitios de fabricación susceptibles a tiempo de inactividad, sistemas automatizados, operaciones de mecanizado de baja potencia, pero críticas, y cualquier entorno que requiera una protección multicapa confiable, independientemente de las limitaciones del sistema operativo.

Comparación de funciones

En la siguiente tabla se enumeran las características incluidas en Kaspersky Embedded Systems Security y Kaspersky Endpoint Security para Windows. Esta información lo ayudará a comprender lo que obtendrá de la actualización a Kaspersky Embedded Systems Security y qué cambiará. Kaspersky Embedded Systems Security incluye las principales características de seguridad con las que está familiarizado en Kaspersky Security for Business, todo administrado desde una única consola.

Función	Kaspersky Embedded Systems Security para Windows 4.0	Kaspersky Endpoint Security para Windows 12.x (para estaciones de trabajo)	Lo que obtiene
Compatibilidad y soporte			
Soporte para sistemas operativos más antiguos, a partir de Windows XP	+	-	Uso seguro de estaciones de trabajo con sistemas obsoletos que son difíciles o imposibles de actualizar.
Soporte para hardware heredado/características deficientes del sistema	+	-	Seguridad incluso para sistemas de baja potencia.
Protección contra amenazas			
Protección contra amenazas de archivo	+	+	Protección contra amenazas basadas en archivos como malware o herramientas de doble propósito legítimas mal utilizadas.
Protección contra amenazas de correo electrónico	-	+	Protección contra ataques por correo electrónico.
Protección contra amenazas web	-	+	Protección contra amenazas web.
Protección contra amenazas de red	+	+	Protección contra ataques de red.
Detección precisa de amenazas que utilizan métodos basados en firmas (prevención de la ejecución)	+	+	Detección precisa de malware sin falsos positivos (la función principal de cualquier plataforma de seguridad de endpoints).
Análisis heurístico y modelos de aprendizaje automático en el lado del cliente (antes y durante la ejecución de malware)	+	+	Detección de amenazas nuevas y desconocidas a través del análisis integral de indicadores estadísticos indirectos.

Función	Kaspersky Embedded Systems Security para Windows 4.0	Kaspersky Endpoint Security para Windows 12.x (para estaciones de trabajo)	Lo que obtiene
Espacios locales aislados a través de la emulación	+	+	Detección de malware cifrado/ amenazas invisibles sofisticadas al emular la ejecución en un entorno simulado seguro.
Análisis de comportamiento	+	+	Detección de amenazas avanzadas desconocidas mediante el análisis de comportamientos.
Protección contra exploits	+	+	Prevención del aprovechamiento de vulnerabilidades en aplicaciones críticas.
Firewall	+	+	Limita las conexiones innecesarias, no verificadas y peligrosas entre el sistema y nodos externos.
Integración con Advanced Detection and Response (Kaspersky EDR, Kaspersky MDR)	MDR	EDR, MDR	Capacidades adicionales para detectar amenazas complejas y amplias capacidades de respuesta automatizadas en la infraestructura.
Integración en KSN/KPSN	+	+	Datos actualizados de amenazas directamente de la infraestructura en la nube de Kaspersky.
Análisis de firmware	+	+	Análisis de firmware dirigido diseñados para detectar malware específico oculto, por ejemplo, en una unidad flash UEFI.
Protección de cifrado para carpetas de la red	+	+	Protección contra ransomware.
Fortalecimiento del sistema (reducción de la superficie de ataque)			
Configuración compacta de seguridad basada en la denegación predeterminada	+	-	Configuración compacta que utiliza pocos recursos del sistema: la política de denegación predeterminada se utiliza como la base y se deshabilitan los niveles de protección que utilizan más recursos.
Autodefensa	+	+	Protección contra niveles de seguridad reducidos como resultado de una interrupción de los componentes de la solución.
Protección contra cambios de configuración no autorizados	+	+	Protección contra la degradación de la seguridad debido a cambios no autorizados en la configuración de la solución.
Control de programas	+	+	Protección contra el uso de dispositivos externos que no son de confianza, lo que reduce el riesgo de infecciones y filtraciones de datos.
Control de dispositivos	+	+	La habilidad de controlar el uso de recursos web individuales y sus categorías, lo que reduce la probabilidad de infección, omisión de ataques de phishing y, en consecuencia, la pérdida de información y credenciales.
Control web	-	+	Análisis de escenarios de uso de programas y detección de actividades sospechosas para detectar amenazas avanzadas.
Control adaptable para anomalías	-	+	Controla las ejecuciones de programas y bloquea ejecuciones no autorizadas, incluido malware basado en archivos.
Sistema de prevención de intrusiones	-	+	Protección contra ataques en función de una cantidad específica de acciones permitidas para aplicaciones en las que no se confía lo suficiente.

Función	Kaspersky Embedded Systems Security para Windows 4.0	Kaspersky Endpoint Security para Windows 12.x (para estaciones de trabajo)	Lo que obtiene
Administración de vulnerabilidades y parches	+ (Compliance Edition)	+ (a partir de Kaspersky Next EDR Optimum)	Monitoreo de vulnerabilidades en sistemas instalados en estaciones de trabajo y reparación de los mismos a través de actualizaciones automáticas oportunas.
Control de integridad del sistema			
Monitoreo de la integridad de los archivos	+ (Compliance Edition)	+ (Solo en Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Detección de cambios no autorizados en el sistema (incluidos aquellos realizados cuando está apagado), lo que implica la detección de cualquier interferencia.
Análisis de registros	+ (Compliance Edition)	+ (Solo en Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Detección de actividades prohibidas en el sistema mediante el monitoreo de cambios en los registros del sistema.
Monitoreo del acceso al registro	+ (Compliance Edition)	+ (Solo en Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Monitoreo y bloqueo de intentos de realizar cambios no autorizados en el registro del sistema.
Supervisión y administración			
Administración local centralizada mediante Kaspersky Security Center	+	+	Un ecosistema de seguridad unificado que permite la administración centralizada de productos Kaspersky.
Administración de los ajustes de la aplicación a través de la consola local del dispositivo	+	+	La capacidad de configurar la solución ante la ausencia de comunicación con el servidor de control.
Kaspersky Security Center Cloud Console	+	+	Implementación sencilla y ahorro de recursos: sin necesidad de instalar y mantener un servidor de administración independiente.
Control de línea de comandos	+	+	Facilidad de administración y flujos de trabajo simples que no requieren una interfaz gráfica.
Integración con sistemas SIEM	+	+	La solución complementa el panorama de seguridad con los datos del evento en el nivel de la estación de trabajo.

Uso industrial

Si su sistema de control industrial o sistema SCADA ejecuta Windows XP, recomendamos Kaspersky Industrial CyberSecurity para nodos, una solución especializada para proteger ICS. Proporciona soporte continuo para sistemas operativos heredados a largo plazo, al tiempo que mantiene la compatibilidad con sus sistemas industriales.

No se demore

Actualice su sistema operativo lo antes posible. Si su empresa desea seguir funcionando de forma efectiva y segura desde una perspectiva TI, necesita comenzar a planificar su transición ahora mismo. Mientras toma e implementa decisiones, Kaspersky Embedded Systems Security protege sus estaciones de trabajo heredadas.

Descubra cómo proteger su infraestructura existente que ejecuta sistemas operativos Windows heredados con Kaspersky Embedded Systems Security. Para ello, abra este vínculo.

latam.kaspersky.com