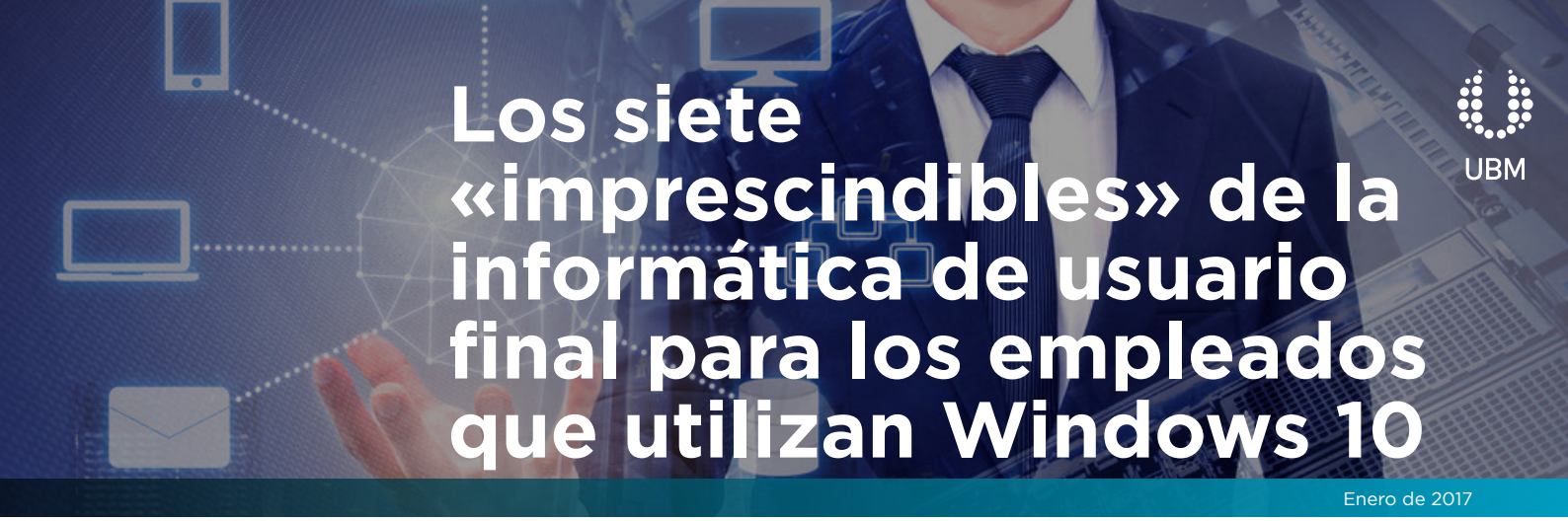

Los siete «imprescindibles» de la informática de usuario final para los empleados que utilizan Windows 10

UBM

Enero de 2017

El sistema operativo de Microsoft ofrece nuevas oportunidades para garantizar la productividad en cualquier lugar y la seguridad en todas partes. Aquí le explicamos cómo sacar el máximo provecho de estas oportunidades.

El lugar de trabajo ha cambiado radicalmente. Las personas cambian de manera fluida entre equipos de escritorio, portátiles, tabletas y teléfonos móviles —así como de una red o ubicación a otra—, intentando seguir el ritmo de las exigencias cada vez mayores del trabajo y de la vida. También utilizan un conjunto más amplio de recursos digitales en constante evolución, que incluyen tanto aplicaciones tradicionales como basadas en la cloud. Además, con la llegada del despliegue ágil y continuo, las aplicaciones y los sistemas operativos tienen que actualizarse con más frecuencia.

Los enfoques convencionales de la gestión de escritorios y de la gestión de dispositivos móviles (MDM) ya no son adecuados para este nuevo espacio de trabajo digital. El departamento de TI de las empresas debe modificar drásticamente y con rapidez la manera en que gestiona el acceso de los usuarios a los recursos digitales para brindar una experiencia coherente en todos los dispositivos, aunque los sistemas operativos y las plataformas evolucionen sin cesar.

Con Windows 10, el departamento de TI puede adoptar la gestión unificada de terminales, que se aplica de forma más eficaz al nuevo espacio de trabajo digital.

La incapacidad de adaptarse a las nuevas reglas del trabajo digital con un enfoque totalmente unificado de la gestión de terminales tendrá como resultado deficiencias de productividad, una seguridad más débil, fallos de conformidad, una menor implicación de los empleados y una reducción del retorno de las inversiones en tecnología.

Afortunadamente, con la llegada de Windows 10, el departamento de TI puede reconsiderar la manera en que adapta la gestión de terminales a los nuevos estilos de trabajo digital de los usuarios. En concreto, el departamento de TI puede adoptar la gestión unificada de terminales (UEM), que lleva las prácticas convencionales de política de grupo a un nivel superior gracias a las nuevas prestaciones «push» y al conocimiento del contexto, que se adaptan de manera más eficaz al nuevo espacio de trabajo digital.

Los siete imprescindibles para los empleados que utilizan Windows 10

Los siete «imprescindibles» pueden ayudar al departamento de TI a aprovechar al máximo el sistema operativo más reciente de Microsoft para prestar mejor servicio a la empresa.

1. Unificar los silos de gestión de escritorios y dispositivos móviles

Uno de los aspectos principales del concepto de UEM es la eliminación de los silos de gestión de escritorios y dispositivos móviles. En cuanto a lógica y funcionalidad, un terminal sigue siendo un terminal, independientemente de su formato o del tipo de conexión de red que utilice. Los usuarios tienen que hacer el mismo trabajo, tanto si están en la oficina como en otro lugar. Por lo tanto, tiene sentido adoptar un enfoque unificado que les proporcione acceso a las aplicaciones y a los recursos que necesitan en los distintos dispositivos.

Varios avances recientes facilitan este enfoque unificado. Uno es la introducción de las API de MDM como nuevo estándar para la gestión del sistema operativo. Estas API permiten al departamento de TI realizar la transición de la gestión tradicional basada en objetos de política de grupo (GPO), que era adecuada principalmente para dispositivos en un dominio con conexiones de red fijas, a un modelo móvil o de cloud que se puede aplicar más universalmente en todas las plataformas y sin dependencias de red y de dominio. Otro avance es la introducción de un conjunto unificado de API (como parte de las «aplicaciones universales» de Windows 10), que permite ejecutar una única base de código, e implementarla y gestionarla fácilmente en cualquier dispositivo Windows.

Si el departamento de TI comprende y aprovecha estas nuevas funciones administrativas de Windows 10, puede iniciar la transición hacia la UEM. A medida que las organizaciones cambian a este nuevo modelo, al menos durante algún tiempo, el departamento de TI necesitará también la capacidad de complementar estas eficiencias modernas de la UEM con las funciones tradicionales de gestión de PC (por ejemplo, soporte para los GPO, uso de scripts y secuencias de tareas o empaquetado e implementación de aplicaciones Win32) desde la cloud, según sea necesario. Con esta solución salen ganando tanto la empresa como el equipo de operaciones de terminales.

2. Redefinir la incorporación de dispositivos

Tradicionalmente, el departamento de TI incorporaba los dispositivos nuevos mediante un proceso de creación de imágenes preparadas previamente que consumía recursos de TI y retrasaba la entrega al usuario final. Pero ya no se aceptan los retrasos en la incorporación. Las empresas necesitan que los empleados nuevos sean productivos inmediatamente. Los jóvenes esperan que el departamento de TI les ofrezca para los PC el mismo modelo de servicio inmediato que utilizan en sus teléfonos móviles. El departamento de TI tiene muchas otras cosas que hacer, aparte de cargar imágenes en dispositivos.

Un repositorio automatizado de recuperación de áreas de trabajo permite al departamento de TI actualizar los nuevos «productos» de área de trabajo con más frecuencia y rapidez, así como con más precisión.

Al proporcionar un sistema operativo en el que se puede confiar para conectarse a la red de forma segura e inmediata —y que después permite a los dispositivos obtener los archivos binarios, la configuración y los permisos de forma inalámbrica—, Windows 10 ofrece un entorno muy propicio para este tipo de incorporación optimizada.

Para aprovechar este modelo de incorporación más eficiente, el departamento de TI debe rediseñar su metodología y sustituir la creación de imágenes de dispositivos por el aprovisionamiento de áreas de trabajo. Normalmente, esto implica crear un conjunto de plantillas de área de trabajo digital que los usuarios pueden recuperar automáticamente en función de sus identidades, funciones, plataforma y versión del sistema operativo y otros criterios diversos. Un repositorio automatizado de recuperación de áreas de trabajo también permite al departamento de TI actualizar los nuevos «productos» de área de trabajo con más frecuencia y rapidez, así como con más precisión de la que tenía en el pasado. De este modo, puede seguir mejor el ritmo de la rápida evolución de los requisitos empresariales y técnicos.

3. Definir políticas de forma inteligente para su extensión inmediata y automatizada por todas partes

La mayoría de las organizaciones de TI no han podido adoptar un enfoque completamente basado en políticas para la gestión de terminales. Esto se debe en parte a la necesidad de implementar de manera muy fragmentada cada uno de los atributos de políticas: un permiso de acceso a una instancia de SharePoint aquí, una restricción de geovallas allá, etc. El hecho de que se tarde tanto tiempo en desplegar las políticas en grandes cantidades de dispositivos dentro y fuera de la red empresarial, que además se deben de reiniciar para que las políticas nuevas o modificadas surtan efecto, ha socavado el uso de dichas políticas.

Para superar estos obstáculos, el departamento de TI necesita implementar una gestión de terminales verdaderamente basada en políticas que proporcione un punto unificado de control en todas partes para todos los atributos de políticas, ya sea a través de la MDM moderna, los GPO tradicionales o ambos. De esta forma, el departamento de TI puede definir políticas completas de acceso, autenticación, cifrado, inclusión en listas blancas, controles de sesión basados en el contexto, etc. para todos los dispositivos de Windows y los que ejecutan otras plataformas de sistema operativo (por ejemplo, iOS, Android, macOS y otros), dentro y fuera del perímetro de la empresa. Además, puede hacerlo con la confianza de que esas configuraciones de políticas surtirán efecto inmediatamente.

4. Habilitar el autoservicio contextual

Al disponer de una gestión de políticas eficaz, el departamento de TI puede avanzar con un paso más decidido hacia un modelo de autoservicio que permita a los usuarios añadir las aplicaciones y los recursos

permitidos a sus áreas de trabajo digitales. Esto se debe a que las políticas garantizan que los usuarios no puedan concederse a sí mismos acceso a las aplicaciones o los recursos a los que no deben acceder.

El departamento de TI debe facilitar el autoservicio simplificando la creación de portales de almacén de aplicaciones que dejen a los usuarios acceder a las aplicaciones permitidas disponibles —por ejemplo, aplicaciones tradicionales de Win32 y nuevas de la Tienda Windows, software comercial de terceros, aplicaciones desarrolladas internamente, software como servicio y aplicaciones remotas publicadas— según su identidad, funciones y responsabilidades, ubicación, etc. El departamento de TI también puede crear para estos almacenes políticas que salvaguarden el cumplimiento de las condiciones de las licencias y que, al mismo tiempo, optimicen el uso simultáneo mediante mecanismos de reciclaje y recuperación de licencias.

El resultado es una experiencia de usuario más similar a la del consumidor, que optimiza la productividad de los empleados mientras reduce las cargas de trabajo administrativas del departamento de TI.

Una solución de UEM compatible con las actualizaciones detalladas del sistema operativo de todos los dispositivos y redes mantiene la uniformidad de los terminales sin reducir la productividad de los usuarios.

5. Mantener las actualizaciones del sistema operativo sin la presión de aplicar parches con regularidad

Por motivos de seguridad y de soporte, es importante mantener actualizadas las versiones de los sistemas operativos de los terminales. Pero el modelo tradicional de aplicar parches masivos con regularidad causa interrupciones y es ineficiente. Además, limita la frecuencia con la que el departamento de TI lleva a cabo las actualizaciones, por lo que se crean grandes lagunas de vulnerabilidad y se retrasa la implementación de nuevas características del sistema operativo.

Cuando la empresa migra a Windows 10, el departamento de TI puede asumir el control de sus cadencias de actualización al definir las políticas de ejecución de actualizaciones de forma más flexible. Las actualizaciones de características pueden implementarse inmediatamente junto con las actualizaciones de seguridad esenciales («rama actual»), con un ligero retardo para permitir las pruebas anteriores al despliegue («rama actual para empresas») o en un momento elegido por el departamento de TI («rama de mantenimiento a largo plazo») para los despliegues especialmente sensibles, como los de sistemas médicos y financieros.

Aunque con Windows 10 es más sencillo superar el problema de los parches masivos, ya que permite las actualizaciones inalámbricas continuas, el departamento de TI sigue necesitando una solución de UEM compatible con las actualizaciones detalladas del sistema operativo en todos los dispositivos, en cualquier parte y en cualquier red, en cuanto estén disponibles. Esto mantiene la uniformidad de los terminales sin mermar la productividad de los usuarios. También minimiza las vulnerabilidades de seguridad al eliminar los retrasos en las correcciones esenciales.

6. Utilizar los informes y la automatización de políticas para simplificar la conformidad

La conformidad es una carga cada vez mayor para el departamento de TI a medida que aumenta la complejidad del entorno empresarial. Esta carga consta de procesos manuales no autodocumentados y de herramientas de gestión de terminales que producen informes fragmentados.

La UEM reduce drásticamente esta carga de varias maneras. En primer lugar, proporciona un mecanismo automatizado y centralizado para definir y aplicar las políticas relacionadas con la conformidad en cualquier parte. En segundo lugar, proporciona una visibilidad unificada de todos los terminales, de modo que el departamento de TI pueda detectar fácilmente y remediar automáticamente las anomalías relacionadas con la conformidad en estos dispositivos.

En tercer lugar —y con frecuencia lo más importante cuando se realiza una auditoría de conformidad—, la UEM permite al departamento de TI consolidar los informes relacionados con la conformidad. Con estos informes unificados, resulta mucho más fácil proporcionar rápidamente a los auditores la documentación

que necesitan para dar su aprobación al departamento de TI. Los informes unificados también tienden a ser mucho más creíbles para los auditores porque eliminan los múltiples pasos de consolidación de datos que pueden introducir errores e inexactitudes en la documentación de conformidad.

7. Establecer funciones de privacidad que permiten el uso personal y empresarial de los dispositivos

El departamento de TI debe consensuar el uso mixto personal y empresarial de los dispositivos móviles. Para ello, puede adoptar un programa formal de uso de dispositivos personales, establecer directrices para el uso personal de los dispositivos que son propiedad de la empresa o utilizar una combinación de ambos. Pero cualquier enfoque del uso mixto requiere la abstracción segura del área de trabajo digital del empleado respecto al hardware subyacente.

Windows 10 facilita esta abstracción mediante la contenedorización de la conectividad, el contenido y las aplicaciones que tienen relación con el trabajo. El sistema operativo identifica el contenido corporativo basándose en atributos como el servidor de archivos de origen, el servidor de correo, la dirección IP y la dirección DNS. Ese contenido se puede colocar automáticamente en su propio contenedor y cifrarse sin que afecte a la experiencia de usuario. Esto permite que las políticas y las acciones administrativas (como los borrados remotos) se dirijan a los contenedores empresariales sin que el contenido personal se vea afectado.

Estas prestaciones técnicas son extremadamente valiosas, ya que los límites entre la vida laboral y personal son cada vez más difusos. La importancia de las protecciones de privacidad también aumenta constantemente debido a que la alta rotación y el mayor uso de trabajadores externos afectan al control de los datos, al igual que el impacto probable de los requisitos normativos como el Reglamento general de protección de datos de la Unión Europea sobre las obligaciones de las empresas y los empleados. Para abordar eficazmente estos problemas, el departamento de TI debe definir y automatizar correctamente todos los parámetros de políticas pertinentes.

El valor de la UEM

La inversión en UEM y en automatización de políticas merece la pena. El trabajo se está transformando radicalmente con la tecnología digital, que a su vez se está transformando radicalmente con la movilidad ubicua. Al adoptar las siete prácticas descritas anteriormente, las organizaciones de TI empresariales pueden obtener varias ventajas importantes, entre las que se incluyen:

- **Reducción importante de la administración de terminales.** Con un número de empleados y un presupuesto limitados, el departamento de TI no puede afrontar unos costes de propiedad de terminales que siguen aumentando sin control. La combinación de la UEM con Windows 10 elimina el tiempo y los gastos operativos de la ecuación de los terminales y permite dedicar unos recursos limitados a otras áreas.
- **Mejor experiencia de usuario final.** Cuanto más rápidamente pueda ofrecer el departamento de TI a los empleados lo que necesitan, más productivos serán. Y esa productividad se traduce directamente en clientes más felices, mayor innovación y mejor rendimiento empresarial.
- **Una empresa más segura.** Los terminales controlados indebidamente son una amenaza enorme. Los controles de terminales unificados y bien automatizados reducen significativamente los riesgos de seguridad e incumplimiento asociados, sin reducir la productividad.
- **Mejora de la agilidad empresarial.** Las empresas no pueden ser ágiles si la distribución de prestaciones digitales a los usuarios finales es lenta. Al quitar varios puntos de fricción de la distribución de prestaciones digitales, la UEM y Windows 10 posibilitan esta agilidad esencial.

Wayne Gretzky hizo famoso el consejo de su padre de «patinar hacia el sitio donde va a estar el disco, no al sitio donde ha estado». Esto es cierto también para la gestión de terminales. El departamento de TI debe adelantarse a la transformación de los terminales o afrontar las consecuencias, que incluyen mayores costes, vulneraciones más frecuentes de la ciberseguridad y frustración de los trabajadores jóvenes. Si se implementan y se gestionan correctamente a lo largo del tiempo, la UEM y Windows 10 ofrecen una alternativa extremadamente atractiva.