# Administración unificada de dispositivos terminales: la manera moderna de proteger y administrar sus dispositivos

# Índice

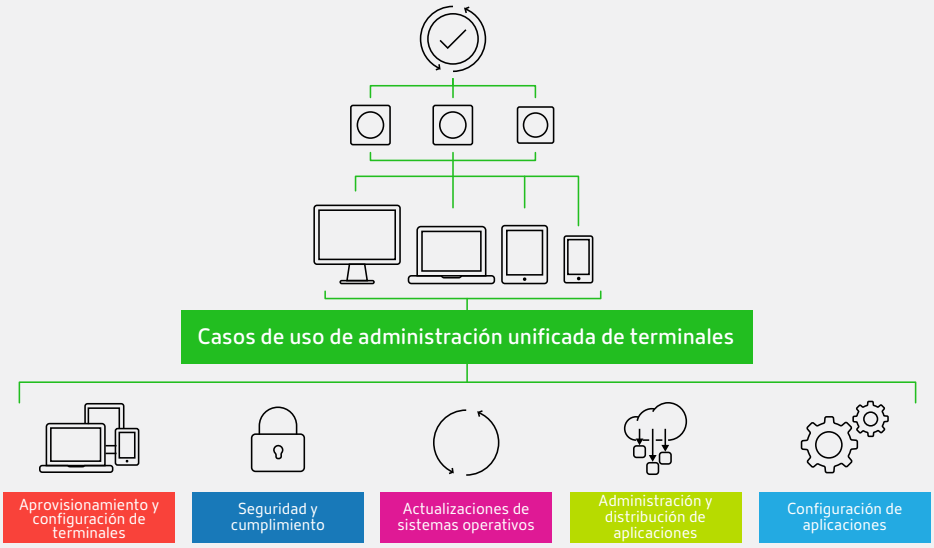

**¿Por qué elegir UEM?** 3

**Seguridad y productividad a través de la contenerización** 5

**Citrix Workspace, una solución de UEM para todas las necesidades** 6

En la actualidad, los empleados son móviles y, por ende, el lugar de trabajo se ve obligado a evolucionar. A medida que TI abandona los escritorios fijos y adopta computadoras portátiles, tabletas y teléfonos inteligentes, muchas organizaciones descubren que las herramientas en las que alguna vez confiaron ya no son suficientes.

En lugar de controlar y proteger distintos dispositivos en diversas plataformas, ahora hay una manera simple de administrarlos desde una única consola. Bienvenidos a la era de la administración unificada de dispositivos terminales (UEM), un moderno estilo de administración.




## ¿Por qué elegir UEM?

### Simplicidad

En el pasado, las organizaciones debían confiar en distintas herramientas de administración de clientes (CMT) y en la tecnología de administración de dispositivos terminales (EMM) para administrar su infraestructura de dispositivos terminales. Ahora, la administración unificada de dispositivos terminales (UEM) combina las capacidades de CMT y EMM en una sola solución, permitiendo que TI proteja y administre de manera segura las aplicaciones, los datos y los sistemas operativos de toda la empresa.

Dado que las herramientas de CMT y EMM tienen maneras completamente diferentes de trabajar, generalmente se requiere un grupo separado de personal y cierta capacitación para cada una. Por el contrario, la administración de todos los dispositivos desde una sola herramienta tiene más sentido para la empresa. No solo es más económico invertir en una herramienta de administración que en dos o tres, sino que también se incrementan considerablemente los ahorros operativos ya que se reduce la necesidad de contar con personal y capacitación especial. En consecuencia, se puede aprovechar el personal existente para objetivos más estratégicos.

## Uniformidad

En administración, la uniformidad, la seguridad y la capacidad de uso son fundamentales para la productividad del usuario y la protección de la información. Incluso las pequeñas diferencias no deseadas en las políticas de seguridad y administración pueden dejar brechas en la infraestructura que les permitirán a los hackers y al malware penetrar en la organización. Tener políticas uniformes facilita la identificación, la corrección y la supervisión de las brechas. La uniformidad en el acceso móvil a las aplicaciones y a la información también es importante para la productividad del usuario.

Estas son algunas de las maneras en las que la UEM ofrece uniformidad:

- Se unifican las aproximaciones a los sistemas, como los servicios de solución de problemas y líneas de soporte.
- Los sistemas operativos, como Windows 10 o macOS, tienen interfaces más uniformes en los distintos tipos de dispositivos.
- Los clientes pueden administrar fácilmente sus aplicaciones heredadas de Windows 32 con una solución de UEM entregada a través de Citrix Workspace durante todo el ciclo de vida de las aplicaciones (es decir, implementación de aplicaciones, configuración y desinstalación de aplicaciones, si fuera necesario).
- La generación de informes resulta más sencilla y más integral, lo que le brinda a TI un conocimiento más profundo para ayudar a mejorar la capacidad de uso y el rendimiento.

## Administración para todos los dispositivos

Las herramientas CMT fueron creadas en una época en que los escritorios, las computadoras portátiles y los dispositivos eran fijos, eran distribuidos por la empresa y generalmente estaban conectados a la red de área local (LAN) de la empresa. Dado que debían unirse a un dominio de la empresa con una política de grupo para realizar la configuración inicial y la posterior administración, el usuario no podía conectarse, configurar ni actualizar su propio dispositivo. El mantenimiento estaba a cargo del equipo de TI, que se desempeñaba como el superusuario principal.

Algunas organizaciones todavía usan soluciones de CMT y, en consecuencia, el equipo de TI dedica mucho tiempo a crear uno o varios conjuntos de imágenes personalizadas del sistema y a introducirlos a través de la LAN en pocos a cientos de escritorios y computadoras portátiles que están conectados a la red. Con esta metodología, la incorporación de nuevos dispositivos o el reemplazo de una computadora portátil extraviada o robada con todas las aplicaciones necesarias es un proceso que consume demasiado tiempo y demasiados recursos y obstaculiza la productividad del usuario.

Dado que los paquetes de aplicaciones de CMT se personalizan y generan paquetes de distribución complejos, requieren un nivel más alto de asistencia técnica. Por el contrario, las API y las herramientas de UEM fueron diseñadas para admitir usuarios móviles conectados en forma inalámbrica con sus dispositivos de elección. Además, ofrecen los siguientes beneficios:

- Los usuarios pueden adquirir un dispositivo con un sistema operativo configurado por el proveedor. Mediante el uso de una aplicación de configuración y de un portal de UEM de la empresa, los usuarios pueden registrarse y configurar sus propios dispositivos a través de una conexión Wi-Fi o celular, con poca o sin ayuda de TI.
- Los usuarios también pueden usar un portal de tienda de aplicaciones de la empresa e instalar aplicaciones con aprobación previa de TI.
- Cuando sea necesario, TI puede lanzar actualizaciones globales a los dispositivos móviles a través de la nube, SaaS y aplicaciones virtuales.

## Seguridad y productividad a través de la contenerización

La política “Traiga su propio dispositivo” (BYOD) se ha convertido en una importante tendencia porque ofrece grandes ahorros en costos para la organización. No obstante, mezclar los datos entre los dispositivos BYOD y los dispositivos de propiedad de la empresa habilitados para uso personal (COPE) pone en riesgo a las organizaciones. La contenerización es una de las maneras en que UEM admite los estilos de trabajo BYOD y COPE. Mediante el uso de encapsulamiento de las aplicaciones, cifrado y otros métodos similares, TI puede separar las aplicaciones y los datos corporativos y personales en cada dispositivo, restringiendo o desactivando interacciones entre ellos en función de las políticas de seguridad establecidas por la empresa.

La contenerización también logra la protección contra malware y la prevención contra la filtración de datos (DLP). Dado que los datos y aplicaciones empresariales y personales se encuentran aislados en el dispositivo, si se descarga malware con las aplicaciones personales o en la exploración, esto no afecta a las aplicaciones empresariales contenerizadas y no se puede transmitir a la red de la empresa cuando se conecta el dispositivo.

Otra forma en que la contenerización brinda protección contra la filtración de datos es a través de la configuración y la aplicación de políticas que regulan la capacidad del usuario para cortar y pegar datos desde aplicaciones empresariales a aplicaciones personales, pegar o adjuntar datos o archivos de la empresa en mensajes de correo electrónico personales e imprimir archivos que contienen datos confidenciales.

### En qué sentido Windows 10 es diferente

Con Windows 10, la contenerización se puede lograr mediante la administración de derechos digitales a través de la aplicación de cifrado Windows Information Protection (WIP) en todos los datos y aplicaciones de la empresa. Luego, TI puede aplicar las políticas para evitar que los usuarios corten y peguen contenido cifrado en las aplicaciones no administradas sin usar cifrado WIP, incluido el software cliente del correo electrónico personal.

Una UEM diseñada para funcionar con Windows 10 ayuda a impulsar otras características fundamentales de la administración y puede:

- Imponer y aplicar una gran cantidad de políticas y configuraciones
- Aplicar contraseñas y cifrado a cualquier información descargada desde servicios como SharePoint o una red compartida
- Habilitar el registro automático de nuevos dispositivos a través de Azure Active Directory
- Administrar aplicaciones aprovisionadas por la empresa en forma separada de las aplicaciones instaladas por el usuario y distribuir las aplicaciones de Windows 32 a través de paquetes .msi
- Aplicar e implementar actualizaciones
- Evitar el acceso a sitios web peligrosos

Todo esto se logra sin la necesidad de tocar el dispositivo conectándolo a la LAN de la empresa. Además, cualquier aplicación de Windows 32 bits que no se pueda aprovechar de esta manera se puede implementar en los dispositivos móviles a través de las soluciones de virtualización de escritorios.

### En qué sentido Apple macOS es diferente

Con el sistema operativo High Sierra, Apple también comenzó a incorporar en el sistema operativo de escritorio la mayoría de estas API de administración de registro automático y basadas en políticas que tiene iOS y se vendrán más novedades con macOS.

## Citrix Workspace, una solución de UEM para todas las necesidades

Citrix ofrece una solución de UEM completa e integrada para administrar varias plataformas, entre ellas, dispositivos iOS, Android, Windows 10 y macOS, incluidos escritorios, equipos portátiles y Chromebooks, y soporte para herramientas y dispositivos de IoT, como Citrix Workspace Hub y Alexa for Business. Como parte de Citrix Workspace, Citrix Endpoint Management, anteriormente XenMobile, combina UEM con virtualización de aplicaciones y escritorios, sincronización y uso compartido de archivos, servicios seguros de puerta de enlace de red y mejoras en la seguridad y productividad para Office 365.

Una VPN móvil ayuda a evitar que aplicaciones infectadas con malware accedan a los recursos detrás del firewall. También proporciona identificadores únicos de dispositivos móviles asignados en el nivel de la aplicación, no solo en el nivel del dispositivo, para controlar, filtrar y bloquear conexiones o dispositivos individuales. Esta integración brinda acceso a las aplicaciones de productividad de Office junto con todas las demás aplicaciones que necesitan los usuarios, incluidas las aplicaciones heredadas de Windows, SaaS, web y aplicaciones móviles, y todo está disponible desde una tienda unificada de aplicaciones.

### Compatibilidad y seguridad

Citrix Endpoint Management que se entrega a través de Citrix Workspace proporciona compatibilidad para todas las API de administración empresarial de sistemas operativos a medida que se van presentando. También agrega sus propias y exclusivas capacidades que brindan uniformidad de administración en todos los sistemas operativos de los dispositivos. Estas incluyen características de cifrado y contenerización, además de las ofrecidas por las API del sistema operativo y su propio kit de herramientas y SDK para el encapsulamiento de las aplicaciones individuales con el fin de proteger la información confidencial asociada. Esto garantiza una perfecta experiencia productiva para el usuario además de protecciones uniformes necesarias para la empresa.

### Citrix Secure Mail

Citrix Secure Mail, un cliente de correo electrónico empresarial y un administrador de información personal con una interfaz sencilla, se parece mucho a las soluciones cliente de correo electrónico nativas de los dispositivos, con muchas características adicionales que mejoran la seguridad y la capacidad de uso en un entorno empresarial. Con Citrix Secure Mail, todos los mensajes de correo electrónico, contactos y elementos de calendario de la empresa se almacenan en forma separada de las aplicaciones personales del dispositivo. Además, Secure Mail:

- Puede abrirse a través de registro único una vez que el usuario inicia sesión en Secure Hub
- Ofrece autenticación de factores múltiples, borrado remoto y cifrado de datos en tránsito e inactivos
- Tiene restricciones de aplicación sobre archivos adjuntos de correo electrónico y para imprimir y cortar y pegar información desde otras aplicaciones a los correos electrónicos
- Se integra con las herramientas existentes de prevención contra la filtración de datos (DLP) de las organizaciones, que controlan y restringen contenido enviado en los correos electrónicos de la empresa

Además, Citrix Secure Mail se integra perfectamente con la aplicación móvil Citrix Secure Web para que los enlaces web de los correos electrónicos se abran en un entorno seguro y aislado con el fin de minimizar las amenazas. También se integra con nuestro servicio de colaboración en contenido, lo que facilita la incrustación de enlaces en el correo electrónico en lugar de adjuntar archivos, para un mayor control del uso compartido de contenido.

Citrix Secure Mail también ofrece características cómodas y excepcionales que mejoran la experiencia del usuario, por ejemplo, la visualización de la disponibilidad de los invitados a la reunión, y un simple toque para participar de las reuniones en línea.

### Citrix Secure Web

Citrix Secure Web, un explorador web que TI puede usar para aplicar políticas y restricciones en la exploración web, es especialmente beneficioso al conectarse a la red e intranet corporativa. Las organizaciones pueden aplicar políticas que controlen a qué sitios web pueden y no pueden acceder los usuarios y qué proxy de firewall de la empresa se usa para acceder a ellos y pueden analizar y filtrar direcciones URL para garantizar que sean seguras. Esto ayuda a proteger a las organizaciones de las amenazas basadas en la web, especialmente cuando los usuarios se encuentran en redes Wi-Fi públicas.

### Citrix Content Collaboration

Citrix Content Collaboration es una aplicación de sincronización y uso compartido de archivos móviles segura y de clase empresarial, que proporciona características, seguridad y administración de tipo empresarial y es más cómoda que las herramientas Box y DropBox diseñadas para consumidores. En lugar de obligar a los usuarios a almacenar toda la información en la nube, las organizaciones pueden aprovechar las zonas de almacenamiento para almacenar archivos compartidos, ya sea a nivel local detrás del firewall, en el servicio en nube de Citrix Content Collaboration o en otro servicio de almacenamiento de nube pública de su elección. Además, Citrix Content Collaboration:

- Proporciona conectores para redes compartidas de Windows y Microsoft SharePoint de manera que los archivos no tengan que migrarse a otro servicio para su uso compartido
- Ofrece una solución fácil de usar que los novatos pueden usar para crear, completar y almacenar aplicaciones móviles basadas en formularios que se ejecutan en distintos dispositivos
- Ayuda a las organizaciones a digitalizar y automatizar rápidamente flujos de trabajo y procesos manuales, mejorando la productividad y eliminando el doble ingreso de datos y el papeleo en el campo
- Se integra perfectamente con otras aplicaciones de productividad de Citrix y que no pertenecen a Citrix
- Aprovecha las sólidas características de seguridad y administración de Citrix Endpoint Management para proteger y asegurar los datos de la empresa

### Aplicación Citrix Workspace

Esta aplicación universal les ofrece a sus equipos acceso centralizado a todos los escritorios, archivos y aplicaciones web, móviles, SaaS, Windows y Linux, a través de una interfaz completa y fácil de usar.

### Mejorar IoT con Citrix Workspace

Citrix Workspace también extiende la administración de la movilidad a la tecnología en constante evolución. Los lugares de trabajo habilitados por IoT pueden sintetizar datos de distintas fuentes para responder a las necesidades del usuario, incrementando así la eficiencia y la productividad del lugar de trabajo. Por ejemplo, el software de propiedad exclusiva de Citrix puede automatizar las funciones del espacio de trabajo, como el inicio de un escritorio personalizado cuando el usuario aborda una estación de trabajo; el ajuste de la temperatura y la iluminación de la sala, el inicio de una reunión virtual cuando el personal ingresa a la sala de conferencias o el uso de balizas para conectar a los usuarios automáticamente a las impresoras cercanas. Esta tecnología emergente garantiza que la organización esté preparada para adaptarse rápidamente al futuro del trabajo.

### Lograr el avance de la empresa con Citrix Workspace

Citrix Workspace permite simplificar, proteger, administrar y controlar todos los tipos de dispositivos terminales, aplicaciones y software desde un solo panel. Todo el espacio de trabajo, exclusivo de Citrix, tiene seguridad contextual con analítica de extremo a extremo en la infraestructura, las aplicaciones, las redes y los dispositivos para ofrecer una supervisión inigualable. Para sus usuarios finales, Citrix Workspace proporciona un solo punto de entrada a las aplicaciones y a los datos que necesitan para ser productivos y colaborar con cualquier dispositivo terminal.

Nuestra solución completa de UEM no solo integra la administración, la seguridad, la virtualización de aplicaciones y escritorios y la movilidad en una infraestructura centralizada sino que también proporciona un marco y capacitación en IoT a nivel empresarial para que la empresa esté preparada para la tecnología futura. Además, nuestras tecnologías de nube le proporcionan la flexibilidad de incrementar o reducir su infraestructura según las necesidades cambiantes de su empresa. La entrega de UEM a través de Citrix Workspace como servicio es la manera más rápida, simple y flexible de incorporar de manera segura las tecnologías del espacio de trabajo digital a su organización.

## Descubra cómo podemos ayudarlo a simplificar la administración de su espacio de trabajo en Citrix.com/UEM


**Ventas empresariales**
América del Norte | 800-424-8749
Resto del mundo | +1 408-790-8000

**Ubicaciones**
Oficina principal | 851 Cypress Creek Road Fort Lauderdale, FL 33309, Estados Unidos
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, Estados Unidos