Las mejores prácticas para una administración simple y segura de dispositivos

Productividad móvil para su negocio.
Libertad de elección para sus empleados.
Seguridad y control total para TI.

La elección de los empleados se ha convertido en la piedra angular de la estrategia de TI. Al permitir a la gente elegir los mejores dispositivos para sus necesidades, las organizaciones pueden mejorar la productividad y flexibilidad, así como la satisfacción en el trabajo. Con la estrategia adecuada, TI puede garantizar las políticas y tecnologías apropiadas para proteger la información empresarial al tiempo que reduce los costes y proporciona una gran experiencia de usuario.

Su estrategia debe permitir a su organización:

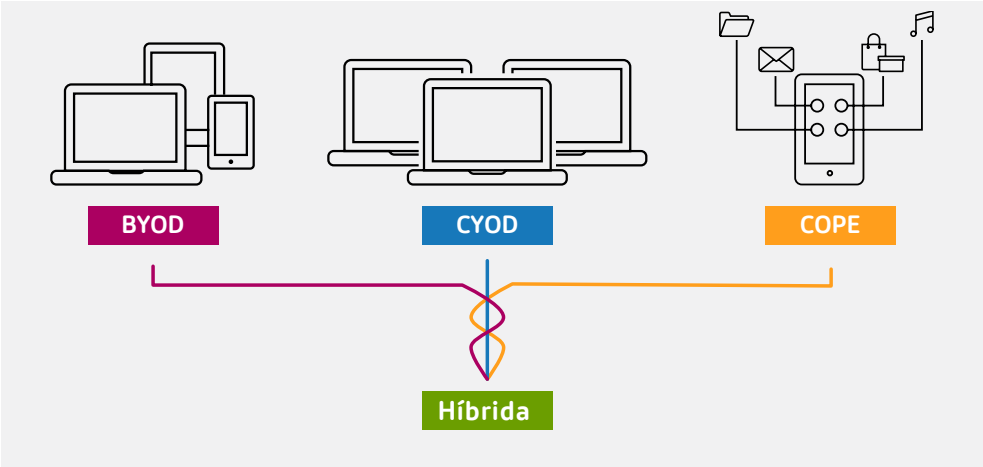
- **Facilitar que las personas** que elijan sus propios dispositivos para mejorar la productividad, la colaboración y la movilidad.
- **Proteger la información confidencial** de pérdidas y robos al mismo tiempo que aborda la privacidad, el cumplimiento normativo y los mandatos de gestión de riesgos.
- **Reducir costes y simplificar la gestión** mediante el aprovisionamiento en autoservicio, así como la supervisión y la administración automatizadas.
- **Simplificar las TI** con una única solución integral para gestionar y proteger los datos, las aplicaciones y los dispositivos.

A continuación se ofrecen 8 prácticas recomendadas para diseñar una estrategia que combine la simplicidad para los empleados con una seguridad, control y administración eficaces para TI:

1. Elegir una política

Debido a que la movilidad y consumerización continúan transformando las TI, hay varias políticas que combinan la libertad de elección con un mayor control para TI:

- Traiga su propio dispositivo (BYOD): Permite a los usuarios utilizar sus dispositivos personales para el trabajo.
- Elija su propio dispositivo (CYOD): Permite a los empleados elegir un dispositivo propiedad de la compañía de entre un pequeño grupo de dispositivos para utilizarlos con fines de trabajo.
- Propiedad de la compañía, habilitado para uso personal (COPE): Permite a los empleados elegir un dispositivo propiedad de la empresa de una lista aprobada y utilizar sus propias aplicaciones, así como aplicaciones corporativas en dicho dispositivo.
- Planteamiento híbrido: Se puede utilizar una combinación para reforzar la movilidad de la manera correcta para los diferentes usuarios y grupos. Por ejemplo, COPE podría usarse junto con CYOD o BYOD.



Si bien los matices de las políticas pueden variar, todos comparten los principios más fundamentales de la administración unificada de terminales (UEM), incluidas sus implicaciones de seguridad. Las principales diferencias se refieren al coste.

Los usuarios de BYOD pagarán sus propios dispositivos y servicios de datos, a veces con una ayuda parcial o completa proporcionada por la empresa. En los casos de COPE y CYOD, la empresa paga el dispositivo y el uso de datos. Una política de BYOD también puede necesitar abordar consideraciones más allá del alcance de COPE y CYOD como, por ejemplo, la cuestión de si a los empleados se les debe pagar horas extras por consultar el correo electrónico después de las horas de trabajo o los fines de semana.

2. Idoneidad e incorporación

Las organizaciones deben dejar claro quién puede utilizar dispositivos personales, ya sea sobre una base ad hoc para complementar un terminal corporativo, como un reemplazo permanente para un dispositivo de empresa o cualquier otra modalidad entre ambos. Esto puede ser visto como un privilegio a conseguir, una respuesta a las demandas de los empleados, una exigencia para determinados tipos de puestos, un riesgo excesivo para algunos casos de uso, o más probablemente, una combinación de todas estas cosas.

Una forma de determinar quién debería ser elegible, es aplicar criterios tales como el tipo de trabajador, la frecuencia de sus viajes, su rendimiento o si un individuo exige un acceso offline a datos confidenciales. Sin embargo, la elegibilidad se define en un amplio nivel, los jefes deben dar siempre la aprobación final sobre qué miembros del equipo son candidatos apropiados para recibir una ayuda económica. Los jefes también pueden aconsejar aplicar BYOD, COPE o CYOD dentro del contexto de otros incentivos departamentales, privilegios y medidas disciplinarias.

Los contratistas son generalmente los candidatos ideales para un BYOD. Muchas organizaciones ya esperan que los contratistas traigan sus propios dispositivos y, al hacerlo, ayudan al cumplimiento normativo del mismo.

3. Dispositivos permitidos

Para evitar tener en el entorno empresarial una diversidad inmanejable de dispositivos, puede limitar el tipo de dispositivos móviles al que su empresa dará soporte. La granularidad de esta política dependerá de sus requisitos de usuario, riesgos de seguridad y recursos de soporte. En general, cuanto más granular sea su política en términos de tipos de dispositivos, versiones del sistema operativo y números de modelo, más recursos necesitará para probar y dar soporte a los dispositivos especificados.

Para mantener claras las líneas de propiedad, los participantes de BYOD deben comprar sus dispositivos personales a través de los canales normales de consumo en lugar del departamento de compras de una organización. Quizá quiera dar descuentos a los empleados, si están cubiertos bajo sus acuerdos de proveedor corporativo.

Algunas personas también pueden querer equipos suplementarios, como monitores o teclados. Asegúrese de especificar quién comprará cada cosa y quién será el propietario de cada una de ellas.

4. Lanzamiento

La comunicación es vital para una implementación exitosa. Proporcione orientación para ayudar a las personas a decidir si desean participar y cómo elegir el dispositivo adecuado para sus necesidades. También deben comprender cómo se puede acceder a los datos, cómo se utilizan y almacenan, y la forma adecuada de configurar y utilizar las cuentas relacionadas con el trabajo para las aplicaciones y los servicios de consumo no gestionados.

Los datos de trabajo y empresariales deben mantenerse estrictamente segregados para soportar los requisitos de e-discovery y las políticas de retención de datos; asimismo, los correos electrónicos de trabajo nunca deberían enviarse desde cuentas personales. Las políticas de uso aceptables deben aplicarse del mismo modo tanto en dispositivos personales como corporativos.

También es importante proporcionar un programa de adopción de usuario para ayudar a los participantes a ponerse en marcha. Un correo de bienvenida con un enlace a un portal de autoservicio puede ayudar a la gente a ser productiva, más rápidamente.

5. Coste compartido

La reducción de costes es uno de los principales beneficios de BYOD, en el que las personas pagan algunos o todos los costes de varios dispositivos personales utilizados para el trabajo. Las empresas que ofrecen estipendios suelen hacerlo en el rango del 18 al 20 por ciento del coste del dispositivo. Los participantes también deben ser conscientes de que la aportación económica será tratada como ingreso a efectos fiscales. En regiones con mayores tasas de impuesto sobre la renta de las personas físicas, usted podría aumentar la aportación económica para mantener la misma ayuda neta para todos los participantes.

Si usted elige proporcionar una ayuda, deberá reflejar la participación plena de cada individuo. Las ayudas deben renovarse a intervalos regulares, para asegurar que los dispositivos personales no envejecen más que un dispositivo empresarial. Si un participante deja la compañía durante un ciclo BYOD, quizá desee reclamar la parte proporcional de la aportación correspondiente.

Tenga en cuenta que el reparto de costes tiene implicaciones al introducir su programa BYOD en la organización. Un despliegue de todo-en-una-vez puede aumentar el coste ya que la gente se puede inscribir —y reclamar sus aportaciones económicas— en todos los puntos al final del ciclo de actualización. Ofrecer el programa a personas cuyos dispositivos están al final del ciclo de vida propagará el impacto. Por otro lado, las organizaciones que no ofrecen una aportación económica pueden favorecer la plena participación desde el primer día.

Además, cualquier política de BYOD, tanto si se comparten gastos como si no, debe dejar claro quién pagará por el acceso a la red fuera del firewall corporativo, ya sea vía red móvil, Wi-Fi público o de banda ancha en el hogar.

6. Seguridad y cumplimiento normativo

Un requisito crucial tanto para los dispositivos personales como para los empresariales es proteger los datos sin afectar la experiencia del usuario. Para programas que permiten aplicaciones y datos personales en los dispositivos utilizados para el trabajo, la gestión de aplicaciones móviles (MAM) posibilita mantener las aplicaciones personales y corporativas separadas del contenido corporativo.

La instalación de aplicaciones corporativas en dispositivos personales aumenta el riesgo. Sin embargo, una estrategia que combina la administración unificada de terminales, la virtualización de aplicaciones y escritorios y el uso compartido de archivos seguros hace que esto sea innecesario. La información del negocio permanece segura en su centro de datos o nube. En casos donde es necesario que los datos residan en el dispositivo móvil, puede proteger los datos empresariales mediante el mantenimiento en contenedores, cifrado y mecanismos de borrado remoto. También puede deshabilitar la impresión o el acceso al almacenamiento en el lado del cliente, en sitios tales como discos locales y almacenamiento USB.

Puede controlar y proteger el acceso a aplicaciones y datos con políticas basadas en la propiedad del dispositivo, el estatus o la ubicación. Inscribir y administrar cualquier dispositivo, establecer requisitos de palabra clave, detectar dispositivos liberados (jailbroken) y realizar un borrado completo o selectivo de un dispositivo no cumple con las normas, perdido, robado o que pertenezca a un empleado o contratista que ha dejado la organización. Garantice la seguridad de las aplicaciones a través del acceso seguro a aplicaciones a través de túneles de aplicaciones, listas negras, listas blancas y políticas dinámicas contextuales.

Para proteger su red, puede aplicar tecnología de control de acceso a la red (NAC) que autentica personas que se conectan a la red y comprueba si sus dispositivos tienen software antivirus actualizado y parches de seguridad.

Fuera del firewall, la virtualización y el cifrado pueden disipar la mayoría de las vulnerabilidades de seguridad del Wi-Fi, cifrado WEP, wireless abierto, 3G/4G y otros métodos de acceso de los consumidores. Las capacidades de seguridad de red proporcionan la visibilidad y la protección contra amenazas móviles internas y externas; bloqueo de dispositivos rogue, usuarios no autorizados y aplicaciones no normalizadas; y la integración con sistemas de gestión de eventos y de seguridad de la información (SIEM).

En caso de que un participante BYOD deje la organización, haya una brecha en la política o un dispositivo personal se ha perdido o robado, TI debe tener un mecanismo para cancelar el acceso inmediato a los datos y aplicaciones, incluyendo desaprovisionamiento automático de cuentas SaaS relacionadas con el trabajo y el borrado selectivo de los dispositivos perdidos. Esta funcionalidad también es esencial para dispositivos empresariales COPE o CYOD, haciendo posible reasignar un dispositivo de propiedad corporativa a un nuevo usuario sin la posibilidad de que los datos que se hayan dejado en el dispositivo caigan en las manos de un usuario que no está autorizado para acceder a ellos.

En lugar de permitir un BYOD abierto, en los que la gente puede traer cualquier dispositivo para acceder a aplicaciones y datos empresariales, algunas organizaciones eligen un enfoque administrado. En este escenario, TI gestiona directamente el dispositivo de propiedad personal, incluyendo registro, validación, autorización y recursos a los que accede el dispositivo.

7. Supervisión y gestión

La monitorización y la gestión en curso son esenciales para garantizar el cumplimiento de las políticas y determinar su retorno de la inversión.

Algunas soluciones UEM incrementan la productividad y la eficacia de TI mediante la automatización de diversos aspectos de supervisión y gestión, tales como especificar las acciones a realizar en respuesta a diversas infracciones. Estas pueden incluir el borrado total o selectivo del dispositivo, marcar el dispositivo que no cumple las normas, anular el dispositivo, o enviar una notificación al usuario para corregir un problema dentro de un límite de tiempo como, por ejemplo, eliminar una aplicación que se encuentre en la lista negra antes de tomar medidas más severas.

8. Soporte y mantenimiento del dispositivo

Un programa BYOD a menudo reduce el mantenimiento de TI requerido para cada dispositivo porque el usuario es también el dueño. Dicho esto, una política debe indicar explícitamente cómo se gestionarán y se pagarán diversas tareas de soporte y mantenimiento para evitar el incremento de la complejidad y la carga de trabajo para TI. En la mayoría de los programas CYOD o COPE, TI es totalmente responsable del mantenimiento y soporte de los dispositivos.

Cómo Citrix Workspace permite la administración segura de dispositivos

Cualquier programa de administración de dispositivos debe incluir tecnologías que proporcionen acceso seguro a aplicaciones y archivos corporativos en dispositivos personales. Citrix Workspace incluye todas las capacidades clave necesarias para hacer BYOD, CYOD y COPE simple, seguro y eficaz para cualquier organización. Combina la administración unificada de terminales, la virtualización de escritorios de Windows y de las aplicaciones, el intercambio seguro de archivos y la entrega de aplicaciones, por lo que puede hacer que las aplicaciones y los datos empresariales estén disponibles en cualquier dispositivo que las personas utilicen para hacer su trabajo al tiempo que se mantiene la seguridad y el control.

Gestión unificada de terminales

Obtenga un aprovisionamiento basado en la identidad así como el control de aplicaciones, datos y dispositivos, desaprovisionamiento automático de cuentas para los usuarios que dejan de tener activo el servicio y borrado selectivo de los dispositivos perdidos. Citrix Workspace no solo le permite administrar dispositivos, incluido IoT, sino que también permite seguridad y control a nivel de aplicación para que pueda proteger los datos corporativos sin afectar al uso de contenidos personales en dispositivos BYOD, CYOD o Cope. La gestión de terminales de Citrix Workspace le permite elegir qué estrategia MAM es la mejor para usted, ya sea una plataforma MAM como Samsung Knox o AppConfig, Citrix MDX (que proporciona un nivel adicional de cifrado de aplicaciones sin inscripción de dispositivos) o Intune MAM.

Virtualización de aplicaciones y puestos de trabajo de Windows

En lugar de instalar y administrar aplicaciones y escritorios de Windows en cada dispositivo individual, puede entregarlos como servicios on-demand disponibles en cualquier dispositivo. Puesto que las aplicaciones y datos se gestionan en el centro de datos o la nube, TI mantiene centralizada la protección de los datos, el cumplimiento normativo, el control de acceso y la administración de usuarios de una forma igual de sencilla tanto en dispositivos personales como corporativos, dentro del mismo entorno unificado.

Tienda unificada de aplicaciones

Dé acceso a la gente con un solo clic a aplicaciones móviles, Web, SaaS, empresariales y Windows desde una tienda de aplicaciones unificada. Independientemente de qué dispositivo elijan las personas, ya sean equipos Windows o Mac, iOS, Android o productos móviles basados en Windows o Google Chromebooks, la experiencia del usuario es la misma en todos los dispositivos, ubicaciones y redes.

Acceso seguro

Un marco de administración unificado permite que TI proteja, controle y optimice el acceso a las aplicaciones, los escritorios y los servicios en cualquier dispositivo además de auditar e informar para dar soporte al cumplimiento normativo y la protección de datos. Solo Citrix proporciona una micro-VPN única para proteger aún más los datos de las aplicaciones entre el dispositivo móvil y los recursos corporativos detrás del firewall.

Intercambio seguro de archivos

Todos pueden compartir archivos de forma segura y colaborar con cualquier persona dentro o fuera de la organización y sincronizar archivos en todos los dispositivos. El control de acceso basado en políticas, la auditoría, los informes y el borrado remoto del dispositivo ayudan a mantener el contenido del negocio seguro.

Con las políticas y la tecnología adecuadas, puede encontrar el equilibrio entre la libertad de elección de los empleados y la seguridad y el control. Obtenga más información acerca de cómo Citrix Workspace puede ayudarle a hacer que la administración de dispositivos sea simple y segura en www.citrix.es/workspace

Ventas empresariales
Norteamérica
| 800-424-8749 Todo el mundo | +1 408-790-8000

Ubicaciones
Sede central | 851 Cypress Creek Road Fort Lauderdale, FL 33309 EE. UU.
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 EE. UU.