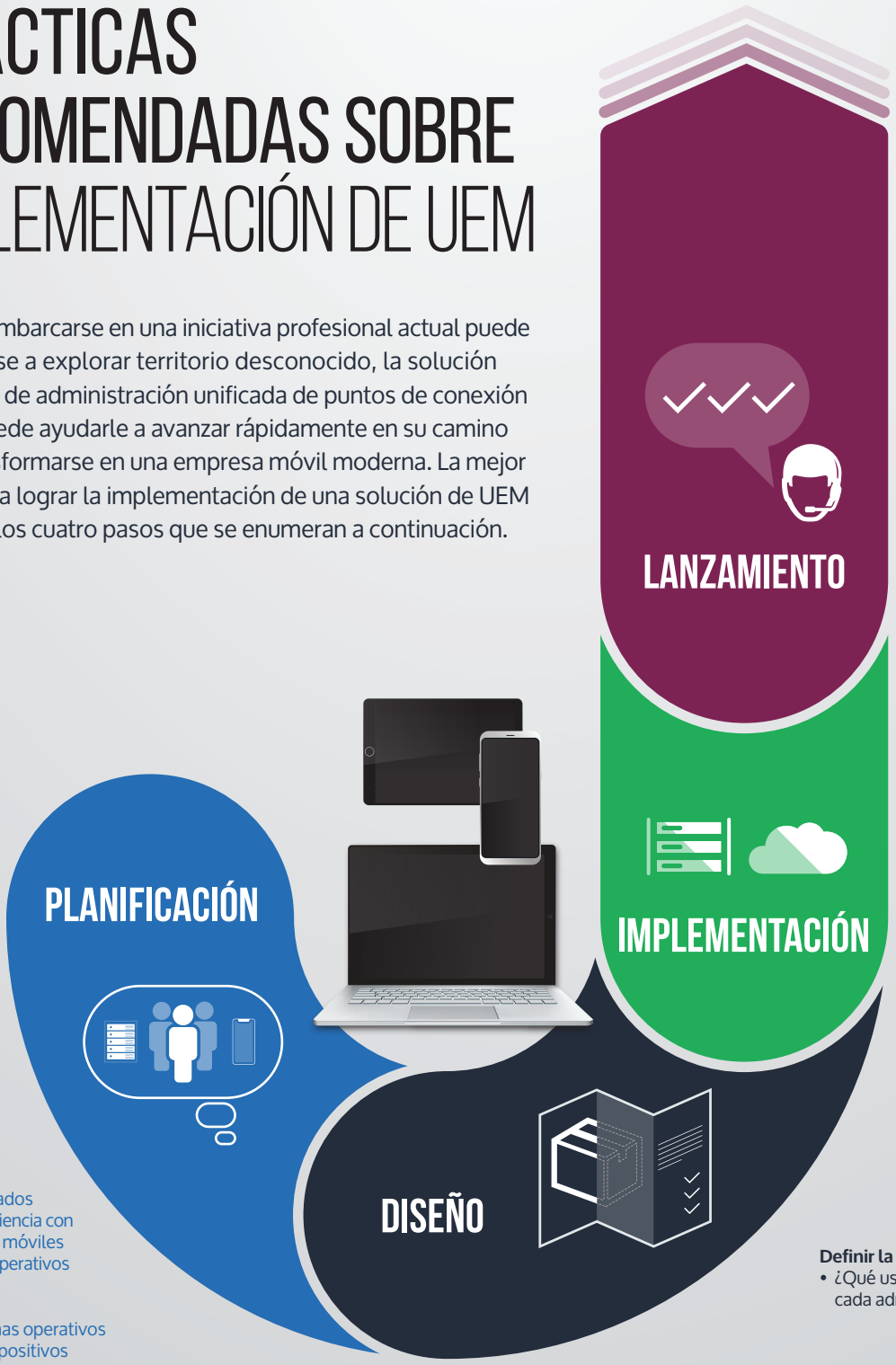
PRÁCTICAS RECOMENDADAS SOBRE IMPLEMENTACIÓN DE UEM

Aunque embarcarse en una iniciativa profesional actual puede asemejarse a explorar territorio desconocido, la solución adecuada de administración unificada de puntos de conexión (UEM) puede ayudarle a avanzar rápidamente en su camino para transformarse en una empresa móvil moderna. La mejor forma para lograr la implementación de una solución de UEM es seguir los cuatro pasos que se enumeran a continuación.



PLANIFICACIÓN

¿Sus empleados tienen experiencia con dispositivos móviles y sistemas operativos modernos?

¿Qué sistemas operativos móviles, dispositivos móviles y equipos de sobremesa modernos admitirá su organización?

¿Qué nivel de complejidad tiene su infraestructura de red?

¿Qué nivel de madurez tiene su marco de gobernanza, políticas y procesos informáticos?

DISEÑO

¿Su organización tecnológica puede desarrollar e implementar aplicaciones corporativas móviles?

¿Qué nivel de efectividad tienen los recursos de capacitación y formación de sus empleados?

¿Su equipo informático tiene experiencia con la autenticación de certificados?

¿Cuáles son los requisitos de seguridad de su empresa?

Definir los roles:
- ¿Cuántos administradores son necesarios para llevar a cabo esta iniciativa?
- ¿Cuáles son sus responsabilidades individuales?

Definir la visibilidad:
- ¿Qué usuarios y dispositivos ve y gestiona cada administrador?

Asignar acciones
- ¿De qué acciones se puede encargar cada administrador?

Administrar la distribución
- ¿Qué aplicaciones, políticas y configuraciones puede distribuir cada administrador a los usuarios/dispositivos?

IMPLEMENTACIÓN

¿Y la implementación local?

¿Y la implementación basada en la nube?

LANZAMIENTO

¿Su personal de soporte técnico comprende los problemas de administración de los diferentes sistemas operativos?

¿Su personal de soporte técnico colabora con expertos de dispositivos según sea necesario?

¿Su personal de soporte técnico tiene acceso a los recursos que necesitan para proporcionar el nivel de soporte esperado?

¿Su personal de soporte técnico tiene acceso a oportunidades educativas constantes, de forma que puedan mantenerse al día de las últimas tendencias?

MobileIron

La administración unificada de puntos de conexión (UEM) de MobileIron permite a sus empleados disfrutar de un acceso fluido a las aplicaciones y datos corporativos a través de dispositivos móviles, equipos de sobremesa y servicios en la nube segurizados, a la vez que mantienen un total control de su privacidad.

Paquetes de UEM de MobileIron	Silver	Gold	Platinum
Opciones de implementación de UEM local y basada en la nube	✓	✓	✓
Sentry es una puerta de enlace incluida que administra, registra y seguriza el tráfico entre el dispositivo móvil y los sistemas corporativos *back-end*.	✓	✓	✓
Apps@Work es un *storefront* o escaparate de aplicaciones corporativas que administra tanto las aplicaciones desarrolladas internamente como las aplicaciones corporativas de terceros que se pueden ofrecer a los usuarios.	✓	✓	✓
AppConnect es un contenedor segurizado para aplicaciones corporativas con VPN específicas para aplicaciones, habilitado para las aplicaciones permitidas por AppConnect.		✓	✓
Email+ es un paquete de aplicaciones móviles de productividad segurizado que incluye correo electrónico, contactos, calendario y tareas para dispositivos iOS y Android.		✓	✓
Docs@Work permite acceder, anotar, compartir y crear documentos en una gran variedad de sistemas de administración de contenido en correo electrónico, *in situ* y en la nube.		✓	✓
Web@Work es un navegador móvil corporativo segurizado que permite a los usuarios finales acceder a los recursos web internos de forma rápida y sencilla.		✓	✓
Administra equipos de sobremesa macOS durante todo el ciclo de vida: aprovisionamiento, configuración, seguridad y control, implementación de aplicaciones, supervisión y cumplimiento, así como el fin del ciclo de vida.		✓	✓
Help@Work permite a los usuarios compartir sus pantallas con un agente de soporte técnico, con el fin de solucionar problemas de forma más eficiente y rápida.			✓
Tunnel ofrece funciones de VPN por aplicación, con el fin de permitir autorizar que aplicaciones específicas puedan acceder a los recursos corporativos detrás del *firewall* sin ningún tipo de intervención por parte del usuario final.			✓
MobileIron Monitor es una solución integral basada en un panel que permite mantener en buen estado todos los componentes principales de la UEM de MobileIron.			✓
Las integraciones con ServiceConnect permiten simplificar los flujos de trabajo con la aplicación de MobileIron para Splunk Enterprise e integración con ServiceNow.			✓
MobileIron Bridge permite utilizar los scripts de Objetos de Directiva de Grupos (GPO) para habilitar la seguridad y administración pormenorizadas de los PC con Windows 10.	Add-on SKU requiere los paquetes de UEM de MobileIron		
MobileIron Access ofrece un control de acceso condicional segurizado para servicios en la nube como Microsoft Office 365, Salesforce, G Suite y Box, entre otros.	Add-on SKU requiere los paquetes de UEM de MobileIron		
MobileIron Threat Defense permite proteger sus datos corporativos detectando y corrigiendo las amenazas conocidas y del día cero en dispositivos móviles, sin necesidad de conexión a Internet y sin que los usuarios tengan que intervenir.	Add-on SKU requiere los paquetes de UEM de MobileIron		

MobileIron potencia su empresa móvil actual

MobileIron UEM

Saque partido al potencial de los dispositivos, las aplicaciones y los servicios en la nube modernos y seguros que hacen posible la innovación corporativa.
https://www.mobileiron.com/en/solutions/enterprise-mobile-management-emm

MobileIron ACCESS

Control de acceso condicional segurizado para servicios en la nube como Microsoft Office 365, Salesforce, G Suite y Box, entre otros.
www.mobileiron.com/en/access

MobileIron THREAT DEFENSE

Con una sola aplicación, las empresas pueden proteger los datos corporativos detectando y corrigiendo las amenazas conocidas y del día cero en el dispositivo móvil, sin necesidad de intervención por parte del usuario.
https://www.mobileiron.com/en/threat-defense

MobileIron BRIDGE

Haga uso de los Objetos de Directiva de Grupos (GPO) existentes, con el fin de habilitar la seguridad y administración pormenorizadas de los PC con Windows 10.
www.mobileiron.com/en/bridge

MobileIron

401 East Middlefield Road • Mountain View, CA 94043
www.mobileiron.com • globalsales@mobileiron.com

Tel.: +1.877.819.3451
Fax: +1.650.919.8006