

# Lista de verificación para la administración y seguridad de Mac para los equipos de TI en expansión

Una guía práctica con los pasos para ayudar a los equipos de TI a realizar con confianza la implementación, configuración y protección de equipos Mac.

## 1. Implementación y configuración

- ✓ Inscriba dispositivos automáticamente a través de Apple Business Manager
- ✓ Aplique los perfiles de configuración necesarios
- ✓ Utilice el aprovisionamiento sin intervención siempre que sea posible
- ✓ Proporcione instrucciones claras a los usuarios para su incorporación

## 2. Configuración y valores de referencia

- ✓ Propicie el uso del cifrado de FileVault
- ✓ Habilite el bloqueo de activación
- ✓ Aplique una configuración básica segura
- ✓ Configure permisos y restricciones del sistema
- ✓ Establezca versiones mínimas del sistema operativo

## 3. Actualizaciones de apps y sistemas operativos

- ✓ Implemente de forma automática las aplicaciones necesarias
- ✓ Mantenga actualizadas y parchadas las apps
- ✓ Programe las actualizaciones del sistema operativo para minimizar interrupciones
- ✓ Verifique la conformidad de las actualizaciones en todas las flotas

## 4. Identidad y acceso

- ✓ Integre los equipos Mac con su proveedor de identidad en la nube
- ✓ Exija una autenticación robusta a los usuarios
- ✓ Aplique controles de acceso sensibles al contexto
- ✓ Ajuste los niveles de acceso a las funciones de los usuarios

## 5. Seguridad de terminales

- ✓ Habilite la prevención de amenazas mediante IA y ML
- ✓ Utilice la detección y el bloqueo integrados en el dispositivo
- ✓ Monitoree las actividades de riesgo en las terminales
- ✓ Responda rápidamente a los incidentes
- ✓ Limite el acceso a los recursos confidenciales

## 6. Conformidad y monitoreo

- ✓ Compare los dispositivos contra su estándar de referencia
- ✓ Utilice flujos de trabajo automatizados para aplicar las políticas
- ✓ Revise periódicamente el estado de conformidad
- ✓ Reciba alertas en tiempo real cuando los dispositivos dejen de estar en conformidad

## 7. Sensibilización y capacitación del usuario

- ✓ Capacite a los usuarios para reconocer el phishing
- ✓ Promueva comportamientos e higiene seguros
- ✓ Fomente la notificación inmediata de actividades sospechosas
- ✓ Refuerce la capacitación durante la incorporación

La **administración** y la **seguridad** unificadas ayudan a los equipos de TI a reducir la complejidad y a proteger mejor su parque de Mac a medida que crece.

Descargar

Descargue la guía completa de administración y seguridad de Mac para empresas.

