Implementar políticas de "Trae tu propio dispositivo" (BYOD, por sus siglas en inglés) en un departamento de TI requiere establecer directrices claras para garantizar la seguridad de la información (tanto a nivel departamental como de los usuarios/contribuyentes) y la productividad del personal.

Políticas de Uso de BYOD:

1. Objetivo

Establecer directrices para el uso seguro y eficiente de dispositivos personales en el lugar de trabajo, garantizando la protección de los datos corporativos y la privacidad de los contribuyentes.

2. Alcance

Estas políticas se aplican a todos los empleados, contratistas, consultores y otras personas que utilicen dispositivos personales para acceder a los recursos de la empresa (poner ejemplos de que recursos son).

3. Dispositivos Permitidos

- Teléfonos inteligentes (iOS, Android)
- Tablets (iOS, Android)
- Computadoras portátiles (Windows, macOS)
- Otros dispositivos aprobados por el departamento de TI (aqui ya es poner que otros dispositivos son aprobados)

4. Requisitos de Seguridad

- Autenticación: Los dispositivos deben estar protegidos por contraseñas fuertes (recomendando que tales contraseñas sean de 8 caracteres mínimo y a la par tengan símbolos especiales) y deben habilitar la autenticación multifactor (MFA) donde sea posible.
- Encriptación: Los datos sensibles almacenados en los dispositivos deben estar encriptados. (ver que más poner en esto)
- Software de Seguridad: Los dispositivos deben tener instalado y actualizado un software de seguridad (antivirus, anti-malware). Se recomienda usar: (poner recomendaciones).

- Actualizaciones: Los sistemas operativos y las aplicaciones deben mantenerse actualizados con los últimos parches de seguridad. (aqui falta algo)

5. Acceso y Uso de Datos Corporativos
   - VPN: Los empleados deben utilizar una red privada virtual (VPN) para acceder a la red corporativa desde dispositivos personales.
   - Aplicaciones Autorizadas: Solo se deben utilizar aplicaciones autorizadas por la empresa para acceder a los datos corporativos. Esta lista se verá en la última página de estás políticas.
   - Separación de Datos: Se deben utilizar aplicaciones que permitan la separación de datos personales y corporativos (se podría hablar de una máquina virtual en especifico para esto).

6. Privacidad y Monitoreo
   - Privacidad del Usuario: La empresa no accederá ni verá los datos personales de los contribuyentes en sus dispositivos.
   - Monitoreo Corporativo: La empresa se reserva el derecho de monitorear el acceso y uso de los datos corporativos en los dispositivos personales.

Todo esto con base a las políticas de privacidad que se establecen en la constitución política de los Estados Unidos Mexicanos (art. 6o, base A y Art. 16 segundo párrafo), asi como en la LGPDPPSO (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados)

7. Responsabilidades del Usuario
   - Informe de Pérdida/Robo: Los empleados deben informar de inmediato cualquier pérdida o robo de sus dispositivos personales al departamento de TI.
   - Uso Adecuado: Los dispositivos personales no deben ser utilizados para actividades ilegales o inapropiadas durante el acceso a los recursos corporativos.
   - Conformidad con Políticas: Los empleados deben cumplir con todas las políticas de seguridad y uso aceptable de la empresa.

8. Políticas de Finalización

- Revocación de Acceso: Al finalizar la relación laboral, la empresa revocará el acceso del dispositivo a los recursos corporativos.
- Eliminación de Datos: La empresa se reserva el derecho de eliminar de forma remota los datos corporativos de los dispositivos personales al finalizar la relación laboral. Esto de acuerdo a las políticas de privacidad que se establecen el la constitución política de los Estados Unidos Mexicanos (art. 6o, base A y Art. 16 segundo párrafo), asi como en la LGPDPPSO (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados)

9. Capacitación y Concienciación
- Programas de Capacitación: La empresa proporcionará capacitación regular sobre las políticas de BYOD y las mejores prácticas de seguridad.
- Concientización: Los empleados serán informados periódicamente sobre las amenazas de seguridad y las medidas preventivas.

10. Cumplimiento y Sanciones (a salud del mtro.)
- Cumplimiento: El cumplimiento de estas políticas es obligatorio.
- Sanciones: El incumplimiento de estas políticas puede resultar en sanciones disciplinarias, incluyendo la terminación del empleo.

11. Revisión de Políticas
- Actualización Regular: Estas políticas serán revisadas y actualizadas regularmente para adaptarse a las nuevas amenazas y tecnologías. A la par de las actualizaciones en el marco jurídico.
- Comentarios y Sugerencias: Los empleados pueden enviar comentarios y sugerencias sobre estas políticas al departamento de TI para su consideración.

Es importante comunicarlas claramente a todos los empleados y asegurarse de que entiendan y acepten los términos antes de utilizar sus dispositivos personales para el trabajo.

Tabla de Aplicaciones descargables y no descargables.

Aplicaciones descargables	Aplicaciones NO descargables