[logo de la organización]

[nombre de la organización]

POLÍTICA TRAE TU PROPIO DISPOSITIVO (BYOD)

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [AES1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

Commented [AES2]: Para obtener más información sobre este tema, lea este artículo:

What is a BYOD policy, and how can you easily write one using ISO 27001 controls?
https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/

Commented [AES3]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Advisera	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir cómo [nombre de la organización] retendrá el control sobre su información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización.

Este documento se aplica a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información sensible dentro el alcance del Sistema de Gestión de Seguridad de la Información (SGSI). Entre estos dispositivos se incluye a los ordenadores personales, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, etc. En esta Política se identificará a estos dispositivos como BYOD.

Los usuarios de este documento son todos los empleados de [nombre de la organización].

Commented [AES4]: Incluya el nombre de su organización.

Commented [AES5]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.14, A.6.7, y A.8.1

3. Reglas de seguridad para el uso de BYOD

Las reglas de la presente Política aplican para todos los BYOD, ya sea de uso personal o que se utilicen para trabajar, dentro o fuera de las instalaciones de la organización.

3.1. Política de la empresa

[Nombre de la organización] adhiere al uso generalizado de BYOD para actividades laborales; por ejemplo, para realizar trabajos para la organización.

Commented [AES6]: Incluya el nombre de su organización.

Commented [AES7]: También puede escribir algo como esto:

[redacted]

[redacted]

3.2. Quiénes pueden utilizar BYOD y para qué

El [cargo] creará una Lista de cargos y/o personas a quienes se les permite utilizar BYOD junto con las aplicaciones y bases de datos a las cuales pueden acceder con sus propios dispositivos.

[redacted]

3.3. Qué dispositivos están permitidos

El [cargo] creará una Lista de dispositivos aceptados que pueden ser utilizados como BYOD, junto con configuraciones obligatorias para cada dispositivo.

Commented [AES8]: Por ejemplo, cortafuegos, copias de [redacted]

3.4. Uso aceptable

Lo siguiente es obligatorio para todos los BYOD:

- [describir cómo se debe realizar la creación de copias de seguridad para información de la organización]
- [detallar qué software de seguridad debe ser instalado; por ej., software antivirus, prevención de intrusiones, software para administración de dispositivos móviles, etc.]
- [describir el método de encriptación que se utilizará y para qué]
- [describir el método de autenticación que se utilizará]
- [describir el método seguro de conexión a la red de la organización]
- Cuando se utilicen BYOD fuera de las instalaciones de la organización, no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados bajo llave.
- Cuando se utilice BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Se deben instalar periódicamente parches y actualizaciones.
- La información clasificada debe contar con protección adicional de acuerdo con la [Política de clasificación de la información].
- Notificar al [cargo] antes de eliminar, vender o entregar un BYOD a terceros para su reparación.

Commented [AES9]: Por ejemplo, claves, contraseñas, lectores biométricos, etc.

Commented [AES10]: Por ejemplo, VPN

Commented [AES11]: Eliminar si no existe esta Política.

No se permite hacer lo siguiente con los BYOD:

- Permitir el acceso a cualquiera que no sea el empleado propietario del dispositivo.
- Instalar aplicaciones que están enumeradas en la Lista de aplicaciones prohibidas para BYOD.
- Almacenar material ilegal en el dispositivo.
- Instalar software sin licencia.
- Conectarse por Bluetooth con cualquier tipo de dispositivo.
- Conectarse a redes Wi-Fi desconocidas.
- Almacenar claves localmente, excepto cuando se utilicen las siguientes aplicaciones: [detallar las aplicaciones permitidas en las que se puede almacenar claves].
- Almacenar localmente la siguiente información: [detallar información sensible].
- Transferir datos de la organización a otros dispositivos no permitidos.

3.5. Derechos especiales

[Nombre de la organización] tiene el derecho de ver, editar y borrar todos los datos de la organización que se encuentran almacenados, transferidos o procesados en BYOD.

Commented [AES12]: Incluya el nombre de su organización.

[Cargo] está autorizado a configurar cualquier BYOD en conformidad con la presente Política y a controlar su uso a través de [especificar el nombre del software para gestión de dispositivos móviles].

Commented [AES13]: Elimínelo si no utiliza ningún software de

[Nombre de la organización] tiene el derecho de realizar el borrado completo de todos los datos del BYOD si considera que es necesario para la protección de los datos de la organización, sin el consentimiento del propietario del dispositivo.

Commented [AES14]: Incluya el nombre de su organización.

Commented [AES15]: Si es técnicamente posible, aquí puede

3.6. Reembolso

[Nombre de la organización] no abonará a los empleados (los propietarios de BYOD) ningún costo por el uso del dispositivo con fines laborales.

[illegible]

- [illegible]
- [illegible]

3.7. Violaciones de seguridad

Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente al [cargo]. [illegible]

3.8. Formación y concienciación

El [cargo] está a cargo de la formación de los empleados nuevos y existentes sobre el uso adecuado de los BYOD, como también de concientizar sobre las amenazas más comunes.

4. Gestión de registros guardados en base a este documento

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Lista de usuarios permitidos para BYOD y a qué pueden acceder]	[intranet de la organización]	[cargo]	Solamente el [cargo] puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por 3 años.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES16]: Incluya el nombre de su organización.

Commented [AES17]: O, al contrario, puede definir un monto a [illegible]

Commented [AES18]: Incluya el nombre de su organización.

Commented [AES19]: Ajústelos de acuerdo con las prácticas de [illegible]

Commented [AES20]: Generalmente, es el gerente de [illegible]

Commented [AES21]: Esta formación le ayudará a aumentar la [illegible]

Commented [AES22]: Modifique estos registros para que [illegible]

Commented [AES23]: Modificar según sea necesario.

Commented [AES24]: Modificar según sea necesario.

Commented [AES25]: Modificar según sea necesario.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año. El [cargo] revisará la Lista de usuarios habilitados, la Lista de dispositivos aceptados y la Lista aplicaciones prohibidas cada 3 meses.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el uso de BYOD.
- Cantidad de empleados que utilizan BYOD sin autorización.

[cargo]
[nombre]

[firma]

Commented [AES26]: Esto es sólo una recomendación; ajustar el intervalo según sea necesario.

Commented [AES27]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.