[logo de la organización]

[nombre de la organización]

POLÍTICA SOBRE DISPOSITIVOS MÓVILES, TELE-TRABAJO Y TRABAJO DESDE CASA

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:

How to Use ISO 27001 To Secure Data When Working Remotely https://advisera.com/27001academy/blog/2021/10/27/how-to-use-iso-27001-to-secure-data-when-working-remotely/

Commented [AES3]: No es necesario redactar un documento separado para la Política de dispositivos móviles, tele-trabajo y trabajo desde casa si las mismas reglas están establecidas en la Política de seguridad de TI.

Commented [AES4]: 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 del presente documento es evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la organización.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todas las personas, datos y equipos incluidos en el alcance del SGSI.

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

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

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.6.7, A.7.9, y A.8.1
- Política de seguridad de la información
- [Política de clasificación de la información]
- [Política de seguridad de TI]

Commented [AES6]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES7]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "09_Anexo_A_de_ISO_27001_Controles_de_seguridad".

Commented [AES8]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "09_Anexo_A_de_ISO_27001_Controles_de_seguridad".

3. Computación móvil

3.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos sin importar dónde se utilice dicho equipo.

[redacted]

Commented [AES9]: Eliminar este párrafo si el control A.7.10 [redacted]

3.2. Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

[redacted]

- [redacted]
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

Commented [AES10]: Eliminar si el control A.7.9 está marcado [redacted]

- Las actualizaciones de parches y demás configuraciones del sistema son realizadas [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina el proceso].
- La protección contra códigos maliciosos se instala y actualiza [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina este proceso].
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- La persona que utilice equipos informáticos móviles fuera de las instalaciones debe observar las instrucciones del fabricante con respecto a la protección del equipo (por ejemplo, de las condiciones climáticas, exposición a interferencias electromagnéticas, vibraciones físicas, etc.).
- [illegible]

[illegible]

4. Tele-trabajo y trabajo desde casa

4.1. Introducción

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización, incluido el trabajo desde casa. La tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

[illegible]

4.2. Normas adicionales para el tele-trabajo

Todas las personas que realicen tele-trabajo deben seguir las reglas de computación móvil definidas en la sección 3 de este documento, y las reglas definidas a continuación:

- El lugar físico donde se realiza el tele-trabajo debe estar protegido por [especificar cómo se implementa técnicamente, o hacer referencia a un documento que defina el proceso]
- [illegible]
- [illegible]

Commented [AES11]: Por ejemplo, acceso semanal al servidor

Commented [AES12]: Por ejemplo, obligando a instalar la

Commented [AES13]: Por ejemplo, accediendo a la red de la

Commented [AES14]: Por ejemplo, al establecer un canal de

Commented [AES15]: Especifique el tipo de información

Commented [AES16]: Por ejemplo, mediante encriptado de

Commented [AES17]: Si su organización no cuenta con una

Commented [AES18]: Si su organización no tiene una Política

Commented [AES19]: Se eliminará en caso de que no se

Commented [AES20]: Puede utilizar la siguiente formación de

Commented [AES21]: Ejemplos de elementos a utilizar son:

Commented [AES22]: Por ejemplo, fuente de alimentación

Commented [AES23]: En caso de que la Política de escritorio y

- La protección de los derechos de propiedad intelectual de la organización, ya sea para software u otros materiales que puedan estar protegidos por derechos de propiedad intelectual, debe implementarse de acuerdo con la [Política de clasificación de la información]
- La devolución de datos y equipos en caso de terminación del empleo debe implementarse de acuerdo con la [Política de seguridad de TI]
- [redacted]
- [redacted]

Commented [AES24]: Si su organización no cuenta con una [redacted]

Commented [AES25]: Puede eliminar este texto si no hay [redacted]

Commented [AES26]: Por ejemplo, participar en reuniones con [redacted]

Commented [AES27]: Puede eliminar este texto si no hay [redacted]

Commented [AES28]: Por ejemplo, cambiar configuraciones en [redacted]

5. Gestión de registros guardados en base a este documento

Nombre del registro	***Ubicación de archivo***	[redacted]	[redacted]	[redacted]
[Autorización para tele-trabajo]	[indicar, teniendo en cuenta la forma de conceder autorización]	[redacted]	[redacted]	[redacted]

Commented [AES29]: Modifique estos registros para que [redacted]

Commented [AES30]: Modificar según sea necesario.

Solamente el [cargo] puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

6. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[redacted]

Commented [AES31]: Esto es sólo una recomendación; ajustar [redacted]

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

- Cantidad de incidentes relacionados con llevar equipamiento de computación móvil fuera de las instalaciones de la organización sin autorización.
- [redacted]

[cargo]
[nombre]

[firma]

Commented [AES32]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.