[logo de la organización]

[nombre de la organización]

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

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Commented [AES2]: No es necesario que esta Política se presente como un documento independiente si las mismas reglas están establecidas en la Política de seguridad de TI.

Commented [AES3]: Para obtener más información sobre este tema, lea este artículo:

Clear desk and clear screen policy and what it means for ISO 27001 https://advisera.com/27001academy/blog/2016/03/14/clear-desk-and-clear-screen-policy-what-does-iso-27001-require/

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.

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

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 definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los puestos de trabajo, instalaciones y equipos ubicados dentro del 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.7.7 and A.8.1
- Política de seguridad de la información
- [Política de clasificación de la información]

Commented [AES6]: Puede encontrar una plantilla para este

Commented [AES7]: Puede encontrar una plantilla para este

3. Política de escritorio y pantalla limpios

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la [Política de clasificación de la información], es considerada sensible en esta Política de escritorio y pantalla limpios.

3.1. Protección del puesto de trabajo

3.1.1. Política de escritorio limpio

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también dispositivos móviles (terminales), y los medios de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos, dispositivos móviles y medios deben ser archivados de forma segura, de acuerdo a lo establecido en la [Política de clasificación de la información]. Cuando los documentos y los medios de almacenamiento ya no sean necesarios, deben eliminarse de acuerdo con la [Política de eliminación y destrucción].

Commented [AES8]: Cambie esta referencia a "Procedimientos

Commented [AES9]: Puede eliminar esto si los controles A.7.10

3.1.2. Política de pantalla limpia

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona no

Commented [AES10]: Adaptar al sistema que se utiliza en la organización.

[redacted]

Las pizarras de información (p. ej., las disponibles en las salas de reuniones) deben borrarse cuando ya no se necesiten.

3.2. Protección de instalaciones y equipos compartidos

Commented [AES11]: Eliminar todo este punto si el control [redacted]

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

Las instalaciones para envío y recepción de correo [indicar las instalaciones y su ubicación] están protegidas por [indicar la forma de protección cuando la persona autorizada está ausente].

Commented [AES12]: Por ejemplo, cerrando la instalación, etc.

[redacted]

Commented [AES13]: Por ejemplo, cerrando la instalación, etc.

[redacted]

Commented [AES14]: Por ejemplo, mediante el bloqueo de la [redacted]

[redacted]

Commented [AES15]: Por ejemplo, más de dos semanas.

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

4. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[redacted]

Commented [AES17]: Esto es sólo una recomendación; ajustar [redacted]

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

- [redacted]

[cargo]
[nombre]

[firma]

Commented [AES18]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.