

[logo de la organización]

[nombre de la organización]

POLÍTICA DE GESTIÓN DE CAMBIOS

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

Commented [AES2]: No hay necesidad de escribir un documento separado para la Política de gestión de cambios si las mismas reglas están establecidas en los Procedimientos de seguridad para el departamento de TI.

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

How to manage changes in an ISMS according to ISO 27001
<https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/>

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.....3
- 2. DOCUMENTOS DE REFERENCIA.....3
- 3. GESTIÓN DE CAMBIOS3
- 4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO3
- 5. VALIDEZ Y GESTIÓN DE DOCUMENTOS4

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir cómo se controlan los cambios en el sistema de información.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del SGSI.

Los usuarios de este documento son empleados de [unidades organizativas para tecnología de la información y de la comunicación].

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusula A.8.32
- Política de seguridad de la información

Commented [AES5]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Políticas_generales".

3. Gestión de cambios

Cualquier cambio sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

1. Los cambios pueden ser propuestos por [indicar los cargos].
2. Los cambios deben ser autorizados por el [cargo], que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
3. Los cambios deben ser implementados por [cargo].
4. El [cargo] es el responsable de verificar que los cambios se han implementado de acuerdo a los requerimientos.
5. El [cargo] es el responsable de probar y verificar la estabilidad del sistema, el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.
6. La implementación de los cambios debe ser registrada y los registros almacenados [indicar todos los logs necesarios].
7. El [cargo] es responsable de actualizar todos los documentos políticos, procedimientos, planes, etc. que se han sido afectados por el cambio.

Commented [AES6]: Se puede especificar qué es y qué no se debe hacer, como por ejemplo, no se debe hacer cambios de configuración de hardware, etc.

Commented [AES7]: Otra forma de formular los pasos, puede ser: 1. El [cargo] es responsable de evaluar la necesidad de los cambios, 2. El [cargo] es responsable de autorizar los cambios, 3. El [cargo] es responsable de implementar los cambios, 4. El [cargo] es responsable de verificar que los cambios se han implementado de acuerdo a los requerimientos.

Los registros sobre los cambios son llevados en [indicar el nombre del formulario o informar un método diferente para registrar los cambios].

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Formato	Responsable para la generación del registro	Fecha de creación
---------------------	----------------------	---------	---	-------------------

Política de gestión de cambios

ver [versión] del [fecha]

Página 3 de 4

[Nombre del registro de cambio - en formato electrónico]	[Nombre de carpeta de Intranet]	[Fecha]	[Descripción de los cambios realizados]	[Estado]

Commented [AES8]: Modifique este registro para que coincida con el formato de los registros de cambios.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es [cargos], que debe verificar, como mínimo, la validez de los documentos que lo conforman.

Commented [AES9]: Esto es sólo una recomendación; ajustar la validez de los documentos.

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

- Cantidad de cambios no realizados de acuerdo con este documento.
- Cantidad de cambios que no corresponden a los resultados deseados.

[cargos]

[nombre]

[firma]

Commented [AES10]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.