[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

POLÍTICA DE GESTÃO DE MUDANÇAS

Commented [AES2]: Esta Política não precisa constar em um documento separado se as mesmas regras forem descritas pelos Procedimentos de segurança para o departamento de TI.

Commented [AES3]: Para saber mais sobre o assunto, leia este artigo:

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]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é definir como as mudanças feitas nos sistemas de informação são controladas.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a toda a tecnologia de informação e comunicação do escopo.

Os usuários deste documento são funcionários da [unidades organizacionais da tecnologia de informação e comunicação].

2. Documentos de referência

- Norma ISO/IEC 27001, cláusula A.8.32
- Política de segurança da informação

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

3. Gestão de mudanças

Todas as mudanças feitas nos sistemas operacionais ou de produção devem ser feitas da seguinte forma:

Commented [AES6]: É possível especificar quais mudanças são

Commented [AES7]: Outra forma de elaborar as etapas pode

1. as mudanças podem ser propostas por [especifique os cargos]
2. as mudanças devem ser autorizadas pelo [cargo], que deve avaliar a sua justificativa de negócio e potenciais impactos negativos de segurança
3. as mudanças podem ser implementadas pelo [cargo]
4. o [cargo] é responsável por verificar se todas as mudanças foram implementadas de acordo com a solicitação
5. o [cargo] é responsável por testar e verificar a estabilidade do sistema – o sistema não deve ser colocado em produção antes que testes completos sejam realizados
6. a implementação das mudanças deve ser informada para: [relacione os cargos que devem ser informados]
7. o [cargo] é responsável por atualizar todos os documentos (políticas, procedimentos, planos, etc.) que forem afetados pela mudança

Os registros de mudanças são mantidos [forneça o nome do formato ou descreve outro método para registro das mudanças].

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]

[Nome do registro de mudança] – em formato eletrônico	[nome da pasta na intranet]	[cargo]	[redacted]	[redacted]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[redacted]

Commented [AES8]: Isso é apenas uma recomendação; ajuste

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de mudanças que não foram feitas de acordo com este documento
- [redacted]

[cargo]
[nome]

_____
[assinatura]

Commented [AES9]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.