[logotipo da organização]

[nome da organização]

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

POLÍTICA DE CÓPIAS DE SEGURANÇA

Commented [AES2]: Para mais informações sobre este tema, leia este artigo:

Backup policy – How to determine backup frequency
https://advisera.com/27001academy/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

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

Commented [AES3]: 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 [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.

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 garantir que as cópias de segurança sejam criadas a intervalos estabelecidos e sejam testadas periodicamente.

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.8.13
- Política da segurança da informação
- [Estratégia de continuidade de negócios]

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

3. Cópias de segurança

3.1. Procedimento para cópias de segurança

As cópias de segurança devem ser criadas por todos os sistemas identificados na [Estratégia de continuidade de negócios] e com a frequência especificada no mesmo documento.

Commented [AES6]: Caso este documento não exista, todos os

[illegible]

Commented [AES7]: As cópias de segurança devem ser

Os registros do processo de criação de cópias de segurança são criados automaticamente nos sistemas em que as cópias de segurança são feitas.

3.2. Teste das cópias de segurança

As cópias de segurança e o processo de restauração dessas cópias devem ser testados pelo menos [uma vez a cada três meses] com a implementação do processo de restauração de dados no [identifique o servidor em que a restauração dos dados é realizada] e a verificação de que todos os dados tenham sido recuperados.

Commented [AES8]: Ajuste a frequência de acordo com os

[illegible]

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
[Registros do processo de criação de cópias de segurança] – formato eletrônico	Sistema que executa o processo de criação de cópias de segurança	[illegible]	[illegible]	[illegible]
[Registros de teste das cópias de segurança] – formato em papel	[nome da pasta/do armário de armazenamento]	[illegible]	[illegible]	[illegible]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES9]: Isso é apenas uma recomendação; ajuste a frequência conforme necessário.

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

- quantidade de testes de cópias de segurança malsucedidos

[cargo]
[nome]

_____
[assinatura]

Commented [AES10]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.