[logotipo da organização]

[nome da organização]

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

POLÍTICA PARA O USO DE CRIPTOGRAFIA

Commented [AES2]: Para saber mais sobre esse problema, leia este artigo:

How to use the cryptography according to ISO 27001 https://advisera.com/27001academy/blog/2015/12/14/how-to-use-the-cryptography-according-to-iso-27001-control-a-10/

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

Commented [AES3]: 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 definir as regras para o uso de controles criptográficos, bem como as regras para uso de chaves criptográficas, a fim de proteger a confidencialidade, a integridade, a autenticidade e o não repúdio das informações.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os sistemas e as informações do escopo do SGSI.

Os usuários dos documentos são [liste os cargos das pessoas que precisam estar em conformidade com esta Política].

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.31 e A.8.24
- Política de segurança da informação
- [Política de classificação da informação]
- [Lista de requisitos legais, regulamentares, contratuais e outros]

Commented [AES4]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

Commented [AES5]: Caso não tenha esta listam então liste todos os requisitos da legislação e contratuais para o uso da criptografia.

3. Uso da criptografia

3.1. Controles criptográficos

De acordo com a Política de classificação da informação, bem como as obrigações legais e contratuais, a organização deve proteger os sistemas ou as informações dos seguintes controles criptográficos:

Nome do sistema / tipo de informação	***Ferramenta criptográfica***	[illegible]	[illegible]
Sistema de pagamento eletrônico	*Token de segurança*	[illegible]	[illegible]
Comunicação entre servidores na sala de dados e os dispositivos móveis	*Software de criptografia XXXX*	[illegible]	[illegible]

Commented [AES6]: Isso também inclui os canais de [illegible]

Commented [AES7]: Liste todos os itens regulamentados pela [illegible]

O [cargo] é responsável pela elaboração de instruções detalhadas sobre o uso das ferramentas criptográficas mencionadas. [illegible]

3.2. Chaves criptográficas

Commented [AES8]: Na maioria dos casos, a organização não [illegible]

O [cargo] é responsável por descrever as seguintes regras relacionadas ao gestão de chaves:

Commented [AES9]: Dependendo das necessidades, as responsabilidades podem ser ampliadas.

- geração de chaves criptográficas privadas e públicas

- ativação e distribuição de chaves criptográficas
- definição do tempo-limite para uso de chaves e sua atualização periódica (de acordo com a avaliação de riscos)
- armazenar chaves, identificando quem tem autorização para acessá-las
- [illegible]

As chaves são gerenciadas por seus proprietários de acordo com as regras mencionadas acima.

[illegible]

Commented [AES10]: Ex.: armazenando-os em local de acesso restrito

Commented [AES11]: Ex.: por meio de cópia de segurança

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	***Local de armazenamento***	[illegible]	[illegible]	[illegible]
[Registros de gestão de chaves]	Computador de [cargo]	[illegible]	[illegible]	[illegible]
[Instrução detalhada no uso de ferramentas criptográficas]	[intranet da organização]	[illegible]	[illegible]	[illegible]
[Regras para a gestão de chaves]	[intranet da organização]	[illegible]	[illegible]	[illegible]

Commented [AES12]: Altere esses registros para combinar [illegible]

Commented [AES13]: Ajuste conforme adequado.

Somente o [cargo] pode conceder aos demais funcionários o acesso a qualquer um dos registros mencionados acima.

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES14]: Isso é apenas uma recomendação; [illegible]

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

- quantidade de incidentes relacionados a perdas, ao comprometimento e à destruição das chaves criptográficas
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES15]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.