[logotipo da organização]

[nome da organização]

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

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Commented [AES2]: Para aprender como classificar informação, leia este artigo:

Classificação da Informação de acordo com a ISO 27001 https://advisera.com/27001academy/pt-br/blog/2014/05/14/classificacao-da-informacao-de-acordo-com-a-iso-27001/

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 garantir que essas informações sejam protegidas adequadamente.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), ou seja, a todos os tipos de informações, independentemente do formato (documentos em papel ou formato eletrônico, aplicativos e bancos de dados, conhecimentos de pessoas, etc).

Os usuários deste documento são todos os funcionários da [nome da organização].

Commented [AES4]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11 e A.8.12
- Política de segurança da informação
- Relatório de avaliação e tratamento de riscos
- Declaração de aplicabilidade
- Inventário de ativos
- Lista de obrigações legais, regulamentares, contratuais e outras
- Procedimento de gestão de incidentes
- [Procedimentos de segurança para o departamento de TI] / [Política de descarte e destruição]
- Política de segurança de TI

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

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação ISO 27001.

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "07_Aplicabilidade_de_controles" do Kit de documentação ISO 27001.

Commented [AES8]: Caso não tenha esta lista, então nestes itens liste todos os requisitos da legislação e contratuais relativos a classificação da informação.

Commented [AES9]: Selecione o documento que descreve a eliminação segura de dados.

3. Informação classificada

3.1. Passos e responsabilidades

Os passos e as responsabilidades de gestão da informação são:

Nome do passo	*Responsabilidade*
1. Inserir o ativo de informações no Inventário de ativos	[cargo]
2. Classificação de informações	Proprietário do ativo
[illegible]	[illegible]
[illegible]	[illegible]

Se informações classificadas forem recebidas de fora da organização, o [cargo] é responsável por sua classificação de acordo com as regras descritas nesta Política. [illegible]

3.2. Classificação de informações

3.2.1. *Critérios de classificação*

O nível de confidencialidade é determinado com base nos seguintes critérios:

- valor da informação – com base nos impactos analisados durante a avaliação de riscos
- sensibilidade e criticidade das informações – com base nos maiores riscos calculados para cada item de informação durante a avaliação de riscos
- [redacted]

Commented [AES10]: Isso também inclui regulamentos de privacidade.

3.2.2. *Nível de confidencialidade*

Todas as informações devem ser classificadas de acordo com os níveis de confidencialidade.

Nível de confidencialidade	*Rótulos*	*Critérios de classificação*	*Restrição de acesso*
Público	(sem rótulo)	Tornar a informação pública não pode prejudicar a organização de qualquer forma.	As informações estão disponíveis para o público.
Uso interno	USO INTERNO	O acesso não autorizado às informações pode causar danos pequenos e/ou inconveniências à organização.	As informações são disponibilizadas a todos os funcionários e a alguns terceiros.
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Commented [AES11]: Os níveis de confidencialidade e os [redacted]

A regra básica é usar o menor nível de confidencialidade, garantindo um nível adequado de proteção [redacted]

3.2.3. *Lista de pessoas autorizadas*

As informações classificadas como "Restritas" e "Confidenciais" devem ser acompanhadas por uma Lista de pessoas autorizadas em que o proprietário das informações especifica os nomes ou as funções das pessoas que têm direito de acesso às informações.

[illegible]

3.2.4. Reclassificação

Os proprietários de ativos devem analisar o nível de confidencialidade de seus ativos de informações a cada [dois anos] e avaliar se o nível de confidencialidade pode ser alterado. [illegible]

Commented [AES12]: Isso é apenas uma recomendação; [illegible]

3.3. Rótulos das informações

Os níveis de confidencialidade são rotulados da seguinte forma:

- **documentos em papel** – o nível de confidencialidade é indicado no canto superior direito de todas as páginas do documento; ele também é indicado na capa ou no envelope que contém o documento ou na pasta de armazenamento em que o documento é armazenado
- **documentos eletrônicos** – o nível de confidencialidade é indicado no canto superior direito de todas as páginas do documento
- [illegible]
- [illegible]
- **mídia de armazenamento eletrônico** (discos, cartões de memória, etc.) – o nível de confidencialidade deve ser indicado na superfície superior da mídia
- [illegible]

3.4. Gestão de informações classificadas

Commented [AES13]: Todas as regras definidas neste [illegible]

Todas as pessoas que acessam informações classificadas devem seguir as regras listadas na tabela a seguir. O [cargo] deve iniciar uma ação disciplinar sempre que as regras forem violadas ou se as informações forem transmitidas a pessoas não autorizadas. Todos os incidentes relacionados à gestão de informações classificadas devem ser informados de acordo com o Procedimento de gestão de incidentes.

[illegible]

Commented [AES14]: Exclua este parágrafo se o controle [illegible]

[illegible]

Commented [AES15]: Selecione o documento que descreve a [illegible]

	Uso interno	*Restrito**	*Confidencial**
Documentos em papel	• se enviado para fora a organização, o documento deve ser	• o documento deve ser armazenado em um armário trancado com chave	• o documento deve ser armazenado em um cofre

	enviado como carta registrada • [redacted]	• os documentos só podem ser transferidos dentro e fora da organização dentro de um envelope fechado • se o documento for enviado para fora da organização, um serviço de confirmação de recebimento deve ser contratado • [redacted]	• o documento só pode ser transferido dentro e fora da organização por uma pessoa confiável em um envelope fechado e lacrado • o envio do documento por fax não é permitido • [redacted]
Documentos eletrônicos	• o acesso ao sistema de informações em que o documento estar armazenado deve ser protegido por uma senha forte • [redacted]	• o acesso ao sistema de informação onde o documento está armazenado deve ser protegido por uma autenticação de 2 fatores • [redacted]	• o documento deve ser armazenado em um formato criptografado • [redacted]

		[illegible]	• o documento só pode ser armazenado em servidores controlados pela organização • [illegible]
Sistemas de informações	• o acesso ao sistema de informações deve ser protegido por uma senha forte • [illegible]	• o acesso ao sistema de informação deve ser controlado por meio de uma autenticação de 2 fatores • os usuários devem desconectar-se do sistema de informações se saírem temporária ou permanentemente do local de trabalho • [illegible]	• o acesso ao sistema de informações deve ser controlado por meio de de autenticação de 2 fatores que use cartões inteligentes ou leitores biométricos • [illegible]

E-mails	• o remetente deve verificar atentamente o destinatário • todas as regras em "Sistemas de informações" são aplicáveis	• o e-mail deve ser criptografado se for enviado para fora da organização • o remetente deve verificar cuidadosamente o destinatário • todas as regras estabelecidas em "Sistemas de informações" se aplicam	• todos os e-mails devem ser criptografados • o remetente deve verificar cuidadosamente o destinatário • todas as regras estabelecidas em "Sistemas de informações" se aplicam
Mídia de armazenamento eletrônico	• as mídias ou os arquivos devem ser protegidos por senha • se enviado para fora a organização, a mídia deve ser enviada como carta registrada • a mídia só pode ser armazenada em área com acesso físico controlado	• as mídias e os arquivos devem ser criptografados • o mídia deve ser armazenada em um armário trancado com chave • se a mídia for enviada para fora da organização, um serviço de confirmação de recebimento deve ser contratado • somente o proprietário da mídia pode apagar ou destruir a mídia	• mídias e arquivos devem ser criptografados • a mídia deve ser armazenada em um cofre • a mídia só pode ser transferida dentro e fora da organização por uma pessoa confiável em um envelope fechado e lacrado • somente o proprietário da mídia pode apagar ou destruir a mídia
Informações transmitidas oralmente	• pessoas não autorizadas não devem estar presentes na sala quando as informações forem transmitidas	• a sala deve ser à prova de ruídos • a conversa não deve ser gravada	• a Sala deve ser à prova de som • a conversa conduzida por um canal de comunicação (ex.: chamada online) deve ser criptografada • a conversa não deve ser gravada

			• nenhum registro de transcrição deve ser mantido

*Os controles são implementados de modo cumulativo, o que significa que os controles de qualquer [illegible]

3.5. Mascaramento de dados

Commented [AES16]: Exclua este seção se o controle A.8.11 [illegible]

Se o proprietário do ativo decidir que a exposição de dados é uma preocupação (por exemplo, informações de identificação pessoal, segredos comerciais, etc.), a classificação da informação deve ser pelo menos “RESTRITA” e as seguintes regras adicionais devem ser aplicadas para evitar que os dados sejam exibido:

- Informações em mídia de papel: os dados não necessários ao usuário devem ser mascarados por meio de exclusão ou ocultação de dados (por exemplo, cobrindo o texto com uma faixa preta).
- [illegible]

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
[Lista de pessoas autorizadas a acessar os documentos]	Juntamente com as informações em que o nível de confidencialidade é indicado	[illegible]	[illegible]	[illegible]

Commented [AES17]: Altere este registro para combinar com [illegible]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES18]: 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 ao acesso não autorizado às informações
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES19]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.