

\_\_\_\_\_

**Commented [AES1]:** Para aprender como preencher este documento, e ver exemplos reais do que você precisa escrever, veja este vídeo tutorial 'How to Write ISO 27001/ISO 22301 Document Control Procedure'

Para acessar o tutorial: Em sua caixa de entrada, encontre o e-mail que você recebeu no momento da compra. Lá, você verá um link e uma senha que lhe permitirá acessar o vídeo tutorial.

[logotipo da organização]

[nome da organização]

**Commented [AES2]:** Todos os campos desse documento que aparecem entre colchetes devem ser preenchidos.

## PROCEDIMENTO DE CONTROLE DE DOCUMENTOS E REGISTROS

**Commented [AES3]:** Para aprender como gerenciar documentos, leia estes artigos:

- How to manage documents according to ISO 27001 and ISO 22301  
<https://advisera.com/27001academy/blog/2021/06/27/how-to-manage-documents-according-to-iso-27001-and-iso-22301/>
- Gestão de registros na ISO 27001 e ISO 22301  
<https://advisera.com/27001academy/pt-br/blog/2014/11/25/gestao-de-registros-na-iso-27001-e-iso-22301/>
- Quão detalhada deveria ser a documentação da ISO 27001?  
<https://advisera.com/27001academy/pt-br/blog/2014/09/23/quao-detalhada-deveria-ser-documentacao-da-iso-27001/>

Além disso, dê uma olhada neste livro: Managing ISO Documentation: A Plain English Guide  
<https://advisera.com/books/managing-iso-documentation-plain-english-guide/>

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

**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 .....	3
2. DOCUMENTOS DE REFERÊNCIA .....	3
3. CONTROLE DE DOCUMENTOS INTERNOS .....	3
3.1. FORMATAÇÃO DE DOCUMENTOS.....	3
3.2. APROVAÇÃO DO DOCUMENTO .....	3
3.3. PUBLICAÇÃO E DISTRIBUIÇÃO DE DOCUMENTOS; RETIRADA DE USO .....	4
3.3.1. <i>Documentos com o menor nível de confidencialidade</i> .....	4
3.3.2. <i>Documentos com nível de confidencialidade mais alto</i> .....	4
3.4. ATUALIZAÇÕES DE DOCUMENTOS.....	4
3.5. CONTROLE DE REGISTROS .....	4
4. DOCUMENTOS DE ORIGEM EXTERNA .....	5
5. GESTÃO DE REGISTROS MANTIDOS DE ACORDO COM ESTE DOCUMENTO.....	5
6. VALIDADE E GESTÃO DE DOCUMENTOS.....	6

### 1. Finalidade, escopo e usuários

A finalidade deste Procedimento é garantir o controle sobre a criação, a aprovação, a distribuição, o uso e as atualizações dos documentos e registros (também chamados de informações documentadas) usados no Sistema de Gestão da Segurança da Informação (SGSI) [Sistema de Gestão da Continuidade de Negócios (SGCN)].

**Commented [AES5]:** Este trecho deve ser inserido no lugar do SGSI caso o procedimento refira-se exclusivamente à gestão da continuidade de negócios.

Este Procedimento aplica-se a todos os documentos e registros listados ao SGSI [SGCN], independentemente de terem sido criados dentro da [nome da organização] ou terem origem externa à organização. Este procedimento compreende todos os documentos e registros armazenados em qualquer forma possível – papel, áudio, vídeo, etc.

**Commented [AES6]:** Inclua o nome da sua organização.

Os usuários deste documento são funcionários da [nome da organização] que trabalham no escopo do SGSI [SGCN].

**Commented [AES7]:** Inclua o nome da sua organização.

### 2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 7.5 e A.5.33
- Norma ISO 22301, cláusula 7.5
- Política da segurança da informação
- Política de continuidade de negócios
- Política de classificação da informação
- [outros documentos e regulamentações que especificam o controle de documentos]

**Commented [AES8]:** Exclua este item se o procedimento referir-se somente à gestão da continuidade de negócios.

**Commented [AES9]:** Exclua isto se você não está implementando continuidade de negócios.

**Commented [AES10]:** Exclua este item se o procedimento referir-se somente à gestão da continuidade de negócios.

**Commented [AES11]:** Exclua isto se você não está implementando continuidade de negócios.

**Commented [AES12]:** Exclua este item se tal documento não existir.

**Commented [AES13]:** Ex.: contratos com clientes.

### 3. Controle de documentos internos

Os documentos internos são todos os documentos criados na organização.

#### 3.1. Formatação de documentos

O texto do documento é escrito em fonte Calibri, tamanho 11. Os títulos dos capítulos são escritos em tamanho 14, negrito. Os subtítulos de nível 2 são escritos em tamanho 12, negrito. Os subtítulos de nível 3 são escritos em tamanho 11, negrito e itálico.

**Commented [AES14]:** Adapte à prática-padrão da organização.

*[Conteúdo borrado]*

**Commented [AES15]:** Exclua se, de acordo com a ISO 27001, a

Todos os documentos também devem definir seus usuários.

#### 3.2. Aprovação do documento

Todos os documentos, independentemente de serem novos ou novas versões de documentos existentes, devem ser aprovados pelo [cargo].

**Commented [AES16]:** Ex.: gerente de segurança da informação, gerente de continuidade de negócio, CEO, etc.

*[Conteúdo borrado]*

O procedimento podem também precisar que algumas pessoas da organização analisem o documento antes que eles seja enviado para aprovação do responsável.

Os documentos de propriedade da organização devem ser armazenados em um sistema de gerenciamento de documentos (SGD).

Commented [AES17]: Ex.: gerente de segurança da

Commented [AES18]: Alternativamente, você pode definir que

### 3.3. Publicação e distribuição de documentos; retirada de uso

#### 3.3.1. Documentos com o menor nível de confidencialidade

No caso de documentos aos quais o acesso é permitido para todos os funcionários que fazem parte do escopo do SGSI [SGCN], o [cargo] deve publicá-los na intranet, na pasta [nome da pasta] com direitos de leitura somente. Quando um novo documento ou uma nova versão do documento for publicada, o [cargo] deve informar a todos os funcionários listados como usuários do documento por e-mail. Se for necessário que alguns funcionários recebam uma versão impressa do documento, isso é de responsabilidade do [cargo].

Commented [AES19]: Ex.: gerente de continuidade de

Commented [AES20]: Altere se os documentos forem

Commented [AES21]: Inclua o nome da pasta na qual você

Commented [AES22]: Ex.: gerente de continuidade de

Os documentos com um nível de confidencialidade mais elevado, conforme especificado na Política de classificação da informação, e cuja distribuição é limitada, são publicados pelo proprietário do documento na intranet, com direitos de leitura somente, em uma pasta à qual somente pessoas especificadas na lista de distribuição do documento têm acesso. O proprietário do documento deve enviar uma notificação por e-mail sobre o documento a todas as pessoas que constam na lista de distribuição.

Commented [AES23]: Ou se um sistema de gestão de

Commented [AES24]: Ex.: gerente de continuidade de

Commented [AES25]: Ex.: gerente de continuidade de

Commented [AES26]: Modifique se houver um sistema de

#### 3.3.2. Documentos com nível de confidencialidade mais alto

Os documentos com um nível de confidencialidade mais elevado, conforme especificado na Política de classificação da informação, e cuja distribuição é limitada, são publicados pelo proprietário do documento na intranet, com direitos de leitura somente, em uma pasta à qual somente pessoas especificadas na lista de distribuição do documento têm acesso. O proprietário do documento deve enviar uma notificação por e-mail sobre o documento a todas as pessoas que constam na lista de distribuição.

Commented [AES27]: Ex.: gerente de continuidade de

Commented [AES28]: Para mais informações sobre classificação de informações, consulte:

Commented [AES29]: Exclua se, de acordo com a ISO 27001, a

Commented [AES30]: Exclua se esse tipo de política não existir.

Commented [AES31]: Altere se os documentos forem

Todo documento deve ter uma tabela "Histórico de alterações" que deve ser usada para registrar as alterações feitas no documento.

Commented [AES32]: Altere se os documentos forem

Commented [AES33]: Para saber mais sobre o assunto, leia este artigo:

### 3.4. Atualizações de documentos

A pessoa listada como proprietária do documento é responsável pela sua atualização. As atualizações são realizadas de acordo com a frequência definida para cada documento e pelo menos uma vez por ano.

Todo documento deve ter uma tabela "Histórico de alterações" que deve ser usada para registrar as alterações feitas no documento.

Commented [AES34]: Altere se os documentos forem

Commented [AES35]: Altere se os documentos forem

### 3.5. Controle de registros

Todo documento interno no SGSI [SGCN] deve definir como os registros resultantes do uso de um documento devem ser gerenciados, ou seja, ele deve especificar: (1) o título do registro, (2) o local de armazenamento, (3) a pessoa responsável pelo armazenamento, (4) os controles de proteção do registro e (5) tempo de retenção.

Os controles de proteção de acesso aos registros armazenados devem de ser permitidos de acordo com o nível de acesso dos registros, de acordo com a classificação de confidencialidade dos registros, para a proteção de acesso aos registros, com base em informações de documentos armazenados, no registro que descreva o controle de acesso.

O direito de acesso e recuperação dos registros é determinado pelo proprietário desses registros. O [cargo] é responsável pela destruição dos registros cujo tempo de retenção foi ultrapassado.

#### 4. Documentos de origem externa

Todos os documentos externos que servem para o planejamento e operação do SGSI [SGCN] devem ser registrados no Registro de correspondência externa. O Registro de correspondência externa deve conter as seguintes informações: (1) número do documento, (2) remetente, (3) nome do documento, (4) data de recebimento e (5) nome da pessoa para quem o documento foi enviado.

Os registros de origem externa devem ser armazenados no SGSI, com base no Registro de correspondência externa, e devem ser armazenados em um registro de correspondência externa. O SGSI deve conter informações de documentos armazenados, no registro que descreva o controle de acesso.

#### 5. Gestão de registros mantidos de acordo com este documento

Nome do registro	Local de armazenamento	Responsável	Controles de proteção de registros	Tempo de retenção
Registro de correspondência externa (formato eletrônico – planilha do Excel)	[nome da pasta na intranet]	[nome do responsável]	[controles de proteção de registros]	[tempo de retenção]

Somente o [cargo] pode conceder aos demais funcionários o acesso ao Registro de correspondência externa.

**Commented [AES34]:** Ex.: gerente de continuidade de

**Commented [AES35]:** Deve-se fornecer mais detalhes se os

**Commented [AES36]:** Adapte o nome do documento para o sistema de manutenção de registros existente na organização.

**Commented [AES37]:** Adicione mais informações se

**Commented [AES38]:** Ex.: gerente de continuidade de

**Commented [AES39]:** Ex.: gerente de continuidade de

**Commented [AES40]:** Ex.: gerente de continuidade de

**Commented [AES41]:** Exclua se esse tipo de política não existir.

**Commented [AES44]:** Ex.: gerente de continuidade de

**Commented [AES42]:** Altere este registro para combinar com

**Commented [AES43]:** Adapte à prática-padrão da organização.

**Commented [AES45]:** Ex.: gerente de continuidade de

## 6. Validade e gestão de documentos

Este documento é válido a partir de [data].

Compreensão de documentos (AES46), que deve incluir a, se necessário, análise e discussão com o pessoal [AES46/47].

**Commented [AES46]:** Ex.: gerente de continuidade de negócios, segurança e conformidade.

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

**Commented [AES47]:** Isso é apenas uma recomendação; não é uma exigência.

- quantidade de documentos obsoletos ou desatualizados
- quantidade de documentos que não foram distribuídos aos funcionários conforme planejado
- quantidade de documentos que não foram atualizados regularmente ou que não foram armazenados corretamente

[cargo]

[nome e sobrenome]

[assinatura]

**Commented [AES48]:** Somente necessário se a cláusula 3.2. indicar que os documentos em papel devem ser assinados.