[logotipo da organização]

[nome da organização]

PROCEDIMENTO DE AÇÃO CORRETIVA

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

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 Procedure for Corrective and Preventive Action".

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.

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

Commented [AES3]: Para aprender mais sobre este tópico, leia este artigo:

Uso prático das ações corretivas para a ISO 27001 e ISO 22301
https://advisera.com/27001academy/pt-br/blog/2013/12/11/uso-pratico-das-acoes-corretivas-para-a-iso-27001-e-iso-22301/

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 desde Procedimento é descrever todas as atividades relacionadas à iniciação, implementação e manutenção dos registros de correções e ações corretivas.

Este Procedimento aplica-se a todas as atividades implementadas no Sistema de Gestão da Segurança da Informação (SGSI) [Sistema de Gestão da Continuidade de Negócios (SGCN)].

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

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

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

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 10.1 e A.5.27
- Norma ISO 22301, cláusula 10.1
- Política da segurança da informação
- Política de continuidade de negócios
- Procedimento de auditoria interna
- Procedimento de gestão de incidentes

Commented [AES7]: Exclua se o procedimento referir-se somente à gestão da continuidade de negócios.

Commented [AES8]: Exclua se o procedimento referir-se somente à gestão da segurança da informação.

Commented [AES9]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação Premium da ISO 27001 e ISO 22301.

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

Commented [AES11]: Você pode encontrar um modelo para este documento na pasta "10_Documentos_principais_de_continuidade_de_negocios_da_ISO_22301" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES12]: Exclua se não for implementar a continuidade de negócios.

Commented [AES13]: Você pode encontrar um modelo para este documento na pasta "12_Auditoria_interna" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES14]: Você pode encontrar um modelo para este documento na pasta "09_Controles_de_seguranca_do_Anexo_A_da_ISO_27001" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES15]: Se a documentação se destinar somente à continuidade de negócios, substitua pelo Plano de resposta a incidentes.

Commented [AES16]: Ou SGCN.

3. Correções e ações corretivas

3.1. Não conformidades e correções

Uma não conformidade é qualquer falha em atender os requisitos dos padrões, documentações internas, regulamentações, contratos e outras obrigações dentro do SGSI. Não conformidades podem ser identificadas durante uma auditoria interna ou externa, com base na revisão de gestão, após incidentes, durante operações de negócio normais ou em qualquer outra ocasião.

[illegible]

3.2. Ações corretivas

A pessoa responsável deve avaliar a necessidade de eliminar a causa da não conformidade e impedir sua recorrência tomando ações corretivas. As principais diferenças é que as ações corretivas eliminam a causa de uma não conformidade, enquanto a correção foca somente no controle da não conformidade e trata das consequências diretas.

[illegible]

Commented [AES17]: Ou SGCN.

3.3. Implementação de ações corretivas

A ação corretiva é implementada da seguinte forma:

Passo	*Responsável pela implementação*
1. Revisando a não conformidade	Qualquer pessoa com um papel no SGSI
2. Determinação da causa da não conformidade	Responsável pela área em que a não conformidade foi identificada
[illegible]	[illegible]
[illegible]	[illegible]
5. Determinação das ações necessárias para eliminar as causas da não conformidade e garantir que as não conformidades não ocorram novamente	Responsável pela área em que a não conformidade foi identificada
6. Implementação das ações planejadas	Encarregado pela implementação, indicado pelo responsável
[illegible]	[illegible]
[illegible]	[illegible]
9. Fazer mudanças no SGSI se necessário	Pessoa que está a cargo da coordenação do SGSI

Cada uma das etapas acima deve ser registrada no [illegible]

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
Formulário de ação corretiva	[nome da pasta de armazenamento, em qual armário] [nome da pasta na intranet]	[illegible]	[illegible]	[illegible]

5. Validade e gestão de documentos

Commented [AES18]: Ou SGCN.

Commented [AES19]: Uma pessoa pode ser indicada para todas as ações corretivas (por exemplo, gerente/diretor de segurança [de continuidade de negócio]) ou o responsável pode ser autorizado a indicar uma pessoa sempre que uma nova ação corretiva for iniciada.

[illegible]

Commented [AES21]: Por exemplo, gerente de segurança ou [illegible]

Commented [AES20]: Ou SGCN.

Commented [AES22]: Ou SGCN.

Commented [AES23]: Você pode usar também, por exemplo, [illegible]

Commented [AES27]: A pessoa designada para lidar com a [illegible]

Commented [AES24]: Se os registros forem mantidos em papel.

Commented [AES25]: Se você usa uma aplicação, então [illegible]

Commented [AES26]: Se os registros forem mantidos em [illegible]

Este documento é válido a partir de [data].

[redacted]

Commented [AES28]: Por exemplo, gerente de continuidade [redacted]

Commented [AES29]: Isso é apenas uma recomendação; [redacted]

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

- quantidade de ações corretivas iniciadas
- [redacted]
- [redacted]

6. Anexos

Commented [AES30]: Exclua esta seção se estiver usando um aplicativo.

- Anexo 1 – Formulário de ação corretiva

[cargo]
[nome]

_____
[assinatura]

Commented [AES31]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.