[logotipo da organização]

[nome da organização]

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

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 the ISMS Policy According to ISO 27001"

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]: Este artigo ajudará você a entender o propósito da Política de segurança da informação:

Política de segurança da informação: o quão detalhada deve ser? https://advisera.com/27001academy/pt-br/blog/2010/12/18/politica-de-seguranca-da-informacao-o-quao-detalhada-deve-ser/

Commented [AES4]: Este artigo ajudará você a entender o conteúdo da Política de segurança da informação:

O que você deveria escrever em sua Política de Segurança da informação de acordo com a ISO 27001? https://advisera.com/27001academy/pt-br/blog/2016/05/31/o-que-voce-deveria-escrever-em-sua-politica-de-seguranca-da-informacao-de-acordo-com-a-iso-27001/

Commented [AES5]: Se você precise de um documento que fornecerá regras detalhadas para a segurança da informação, então favor usar a Política de segurança de TI.

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 [AES6]: 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

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de Gestão da Segurança da Informação (SGSI), como definido no documento de escopo do SGSI.

Os usuários deste documento são funcionários da [nome da organização], assim como as partes externas relevantes.

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

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 5.2, 5.3, 6.2, 7.4 e A.6.3
- Documento sobre o escopo do SGSI
- Metodologia de avaliação e tratamento de riscos
- Declaração de aplicabilidade
- Lista de obrigações legais, regulamentares, contratuais e outras
- [outros documentos internos]
- [Política de continuidade de negócios]
- [Procedimento de gestão de incidentes]

Commented [AES8]: Você pode encontrar um modelo para este documento na pasta "04_Escopo_do_SGSI" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES9]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES10]: Você pode encontrar um modelo para este documento na pasta "07_Aplicabilidade_de_controles" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES11]: Você pode encontrar um modelo para este documento na pasta "03_Identificacao_de_requisitos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES12]: Liste outros documentos internos da organização associados a esta Política - por exemplo, plano de desenvolvimento estratégico, plano de negócios, documento sobre gestão estratégica de riscos, etc.

Commented [AES13]: 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 [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.

3. Terminologia básica de segurança da informação

Confidencialidade – características das informações que estão disponíveis

Integridade – características das informações que somente são alteradas

Disponibilidade – características das informações que somente pode ser acessada por pessoas

Segurança da informação – preservação da confidencialidade,

Sistema de gestão da segurança da informação – a parte do sistema de gestão que cuida do planejamento,

4. Gerenciando a segurança da informação

4.1. Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são os seguintes: criar uma melhor imagem no mercado e reduzir os danos causados por possíveis incidentes, e se eles estão em linha com os objetivos de negócios da organização, estratégia e planos de negócios. O [cargo] é responsável por rever estes objetivos SGSI gerais e por definir novos objetivos.

Os objetivos dos controles de segurança ou grupos de controles, são definidos por [Lista de funções que executam autorização] e aprovados pelo [cargo] na Declaração de aplicabilidade.

Todos os objetivos devem ser revisados pelo menos uma vez por ano.

A [nome da organização] irá mensurar o atendimento de todos os objetivos. O [cargo] é responsável por definir o método para a medição da realização dos objetivos – a medição será executada ao menos uma vez por ano e o [cargo] irá analisar e avaliar os resultados da medição e reportá-los para a [alta direção] como material de entrada para a Análise crítica pela direção.

O [cargo] é responsável por registrar os detalhes sobre os métodos de medição, periodicidades e resultados no Relatório de medição.

4.2. Requisitos de segurança da informação

Esta Política e todo o SGSI deve estar em conformidade com os requisitos legais e regulamentares levantes à organização na área de segurança da informação, bem como com as obrigações contratuais.

Uma lista detalhada de todos os requisitos contratuais e legais, na Lista de obrigações legais, regulamentares, contratuais e outras.

4.3. Controles da segurança da informação

Os processos para selecionar os controles (salvaguardas) estão definidos na Metodologia de avaliação e tratamento de riscos.

Os controles selecionados e seu status de implementação estão listados na Declaração de aplicabilidade.

4.4. Continuidade de negócios

A gestão da continuidade de negócios é descrita na Política de continuidade de negócios.

4.5. Responsabilidades

As responsabilidades básicas para o SGSI são:

- o [cargo] é responsável por garantir que o SGSI seja implementado de acordo com esta Política e para garantir todos os recursos necessários
- o [cargo] é responsável pela coordenação operacional do SGSI, bem como reportar sobre o desempenho do SGSI
- a [alta direção] deve analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar minutas sobre a reunião. A finalidade da revisão da gestão é definir a adequabilidade e a eficácia do SGSI.

Commented [AES15]: Se necessário, altere e/ou adicione outros objetivos, como: conformidade com regulamentações/legislação, quantidade de incidentes, satisfação com o usuário, etc.

Você pode definir outros objetivos, como: conformidade com regulamentações/legislação, quantidade de incidentes, satisfação com o usuário, etc.

Commented [AES16]: Para saber mais sobre o alinhamento entre a ISO 27001 e o negócio, veja este artigo:

Alinhando a segurança da informação com a ISO 27001 e o negócio

Commented [AES17]: Para obter informações sobre a importância dos objetivos de controle, consulte este artigo:

ISO 27001 control objectives – Why are they important?

Commented [AES18]: Por exemplo, objetivos para controles

Commented [AES19]: Verifique se essa frequência é adequada.

Commented [AES20]: Inclua o nome da sua organização.

Commented [AES21]: Você pode encontrar um modelo para

Commented [AES22]: Liste também outras áreas que são

Commented [AES23]: Exclua este item se a continuidade de

Commented [AES24]: Para entender melhor as responsabilidades da alta direção, consulte este artigo:

Papéis e responsabilidades da alta direção na ISO 27001 e ISO 22301

Commented [AES25]: Membro da alta direção.

Commented [AES26]: Uma ou mais pessoas;

Commented [AES27]: Este deve ser o principal corpo de alta

Commented [AES28]: Estes são mandatórios de acordo com a

- [illegible]
- a proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário de cada ativo
- todos os incidentes e as fragilidades de segurança devem ser reportados ao [cargo]
- [illegible]
- [illegible]

Commented [AES29]: Ou refira-se ao Procedimento de gestão de incidentes.

Commented [AES30]: Diversos responsáveis podem ser [illegible]

Commented [AES31]: Este treinamento ajudará você a treinar [illegible]

Commented [AES32]: Estas são recomendadas; você pode [illegible]

4.6. Comunicação da Política

O [cargo] deve garantir que todos os funcionários da [nome da organização], [illegible]

Commented [AES33]: Inclua o nome da sua organização.

5. Suporte para a implementação do SGSI

Deste modo, o [cargo ou organismo da alta direção no escopo do SGSI] declara que a implementação [illegible]

Commented [AES34]: Para entender melhor a provisão de recursos, consulte este artigo:

[illegible]

6. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES35]: Isso é apenas uma recomendação; [illegible]

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

- quantidade de funcionários e terceiros que têm um papel no SGSI, mas não conhecem este documento
- não conformidade do SGSI com as leis e as regulamentações, as obrigações contratuais e outros documentos internos da organização
- [illegible]
- [illegible]

[cargo]
[nome]

Commented [AES36]: A Política de segurança da informação [illegible]

_____

[assinatura]

Commented [AES37]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.