[logotipo da organização]

[nome da organização]

**PLANO DO PROJETO**  
**para implementação do Sistema de Gestão da Segurança da Informação**

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

**Histórico de alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Criado por** | **Descrição da alteração** |
|  | 0.1 | Advisera | Esboço básico do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc153224161)

[2. Documentos de referência 3](#_Toc153224162)

[3. Projeto de implementação do SGSI 3](#_Toc153224163)

[3.1. Objetivo do projeto 3](#_Toc153224164)

[3.2. Resultados do projeto 3](#_Toc153224165)

[3.3. Prazos 5](#_Toc153224166)

[3.4. Organização do projeto 5](#_Toc153224167)

[3.4.1. Patrocinador do projeto 5](#_Toc153224168)

[3.4.2. Gerente do projeto 5](#_Toc153224169)

[3.4.3. Equipe do projeto 6](#_Toc153224170)

[3.5. Principais riscos do projeto 6](#_Toc153224171)

[3.6. Ferramentas para a implementação do projeto e geração de relatórios 6](#_Toc153224172)

[4. Gestão de registros mantidos de acordo com este documento 7](#_Toc153224173)

[5. Validade e gestão de documentos 7](#_Toc153224174)

# Finalidade, escopo e usuários

A finalidade do Plano do projeto é definir claramente o objetivo do projeto de implementação do Sistema de Gestão da Segurança da Informação (SGSI), os documentos a serem elaborados, prazos e papéis e responsabilidades no projeto.

O Plano do projeto é aplicado a todas as atividades realizadas no projeto de implementação do SGSI.

Os usuários deste documento são membros da [alta direção] e da equipe do projeto.

# Documentos de referência

* Norma ISO/IEC 27001
* Norma ISO 22301
* [decisão ou qualquer documento similar que descreva o lançamento do projeto]
* [metodologia de gestão de projeto]

# Projeto de implementação do SGSI

## Objetivo do projeto

Implementar o Sistema de Gestão da Segurança da Informação de acordo com a norma ISO 27001 até [data].

## Resultados do projeto

Durante o projeto de implementação do SGSI, os seguintes documentos (alguns deles contêm anexos que não são mencionados aqui) serão elaborados:

* **Procedimento de controle de documentos e registros** – procedimento que descreve as regras básicas de elaboração, aprovação, distribuição e atualização de documentos e registros
* **Procedimento para identificação de requisitos** – procedimento para identificação de obrigações estatutárias, regulamentares, contratuais e outras
* **Documento sobre o escopo do SGSI** – um documento que define precisamente os ativos, os locais, a tecnologia, etc., que fazem parte do escopo
* **Política da segurança da informação** – este é um documento chave usado pela gestão para controlar a gestão da segurança da informação
* **Metodologia de avaliação e tratamento de riscos** – descreve a metodologia de gestão de riscos à informação
* **Tabela de avaliação de riscos** – a tabela é o resultado da avaliação dos valores, das ameaças e das vulnerabilidades dos ativos
* **Tabela de tratamento de riscos** – uma tabela em que os controles de segurança adequados são selecionados para cada risco inaceitável
* **Relatório de avaliação e tratamento de riscos** – um documento no qual constam todos os documentos chave elaborados no processo de avaliação e tratamento de riscos
* **Declaração de aplicabilidade** – um documento que determina os objetivos e a aplicabilidade de cada controle de acordo com o Anexo A da norma ISO 27001
* **Plano de tratamento de riscos** – um documento de implementação que especifica os controles a serem implementados, o responsável pela implementação, os prazos e os recursos
* **Procedimento de auditoria interna** – define como é feita a seleção de auditores, como os programas de auditoria são elaborados, como as auditorias são realizadas e como os resultados das auditorias são informados
* **Procedimento de ação corretiva** – descreve o processo de implementação de ações corretivas e preventivas
* **Relatório de medição** – resume os objetivos do SGSI, o método de medição, a frequência de medição e os resultados. É usado para concluir o quão eficaz é a segurança da informação em sua organização
* **Minuta da análise crítica pela direção** – usada para criar minutas da reunião de análise da adequação do SGSI

Os prazos para as políticas e procedimentos que descrevam detalhadamente as regras de segurança serão descritos no Plano de tratamento de riscos, pois, no momento da elaboração deste Plano de projeto, não se sabe quais destes documentos serão necessários.

Durante o projeto de implementação da gestão de continuidade dos negócios, os seguintes documentos (alguns deles contêm anexos que não são mencionados aqui) serão elaborados:

* **Política de gestão de continuidade de negócios** – estabelece uma estrutura básica para a SGCN e determina o escopo e as responsabilidades
* **Questionários de análise de impacto nos negócios** – análise de impactos qualitativos e quantitativos sobre os negócios, de recursos necessários, etc.
* **Estratégia de continuidade de negócios** – define as atividades críticas, as interdependências, os objetivos do tempo de recuperação, a estratégia de gerenciamento e garantida da continuidade de negócios, a estratégia de recuperação de recursos e a estratégia para atividades críticas individuais
* **Plano de continuidade de negócios** – uma descrição detalhada de como responder a desastres ou outras interrupções nos negócios e de como recuperar-se de todas as atividades críticas
* **Plano de treinamento e conscientização** – uma visão geral detalhada sobre como os funcionários serão treinados para realizar as tarefas planejadas e como eles são conscientizados sobre a importância da continuidade de negócios
* **Plano de exercícios e testes** – descreve como os planos serão exercitados e testados com o objetivo de identificar as ações corretivas necessárias e aprimorar o plano
* **Plano de revisão e manutenção do SGCN** – uma visão geral detalhada sobre como os planos e outros documentos do SGCN devem ser mantidos para garantir seu funcionamento em caso de interrupção nos negócios
* **Formulário de revisão de pós-incidentes** – um formulário usado para analisar a eficácia dos planos após um incidente
* **\***

## Prazos

Os prazos para a aceitação de documentos individuais durante a implementação do SGSI são:

|  |  |
| --- | --- |
| ***Documento*** | ***Prazos para aceitação do documento*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Os prazos para a aceitação de documentos individuais durante a implementação do SGCN são:

|  |  |
| --- | --- |
| ***Documento*** | ***Prazos para aceitação do documento*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

A apresentação final dos resultados do projeto está planejada para [data].

## Organização do projeto

### Patrocinador do projeto

Cada projeto possui um "patrocinador" que não participa ativamente do projeto. O patrocinador deve receber periodicamente informações do gerente do projeto sobre o status do projeto e intervir se o projeto for interrompido.

[Nome, cargo] foi nomeado como patrocinador do projeto.

### Gerente do projeto

O papel do gerente é garantir os recursos necessários para a implementação do projeto, coordenar o projeto, informar o patrocinador sobre o progresso e realizar as tarefas administrativas relacionadas ao projeto. O gerente do projeto deve ter autoridade suficiente para garantir a implementação ininterrupta do projeto de acordo com os prazos estabelecidos.

[Nome, cargo] foi nomeado como gerente do projeto.

### Equipe do projeto

O papel da equipe do projeto é auxiliar nos diversos aspectos da implementação do projeto, realizar tarefas conforme especificado no projeto e tomar decisões sobre as diversas questões que requerem uma abordagem multidisciplinar. A equipe do projeto reúne-se antes da versão final de um documento da seção 2 do Plano do projeto ser concluída e sempre que o gerente do projeto considerar necessário.

*Tabela de participantes do projeto*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Nome* | *Unidade organizacional* | *Cargo* | *Telefone* | *E-mail* |
| John Doe | Departmento de TI | Administrador de Sistemas | 00 1111-1234 | john.doe@yourcompany.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Principais riscos do projeto

Os principais riscos na implementação do projeto são:

1. Extensão de prazos na fase de avaliação de riscos
2. Extensão de prazos durante o desenvolvimento dos planos de continuidade de negócios
3. Atividades que gerem custos desnecessários e perda de tempo
4. Seleção de muitos controles e/ou controles custosos

As medidas para reduzir os riscos mencionados acima são:

* O gerente do projeto monitora se todas as atividades do projeto são realizadas nos prazos definidos e busca a intervenção do patrocinador em tempo hábil
* A contratação de um consultor para garantir que tempo ou recursos não sejam desperdiçados em atividades que não são importantes para o projeto e que as atividades individuais não se desviem da direção correta
* A contratação de um consultor para propor os controles com melhor custo-benefício

## Ferramentas para a implementação do projeto e geração de relatórios

Uma pasta compartilhada que contenha todos os documentos elaborados durante o projeto será criada na rede local. Todos os membros da equipe do projeto terão acesso a esses documentos. Somente o gerente do projeto [e os membros da equipe do projeto] têm autorização para alterar e excluir arquivos.

O gerente do projeto elaborará um relatório de implementação do projeto mensalmente e o encaminhará ao patrocinador do projeto.

# Gestão de registros mantidos de acordo com este documento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Nome do registro*** | ***Local de armazenamento*** | ***Responsável pelo armazenamento*** | ***Controles para proteção do registro*** | ***Tempo de retenção*** |
| Relatório de implementação do projeto (em formato eletrônico) | Pasta compartilhada para atividades relacionadas ao projeto | Gerente do projeto | Somente o gerente do projeto tem autorização para editar dados. | O relatório é armazenado por três anos. |

# Validade e gestão de documentos

Este documento é válido a partir de [data].

O proprietário do documento é o [cargo].

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

* se todos os funcionários envolvidos no projeto realizam suas atividades de acordo com este documento
* se todos os prazos do projeto são cumpridos

[cargo]

[nome]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[assinatura]