# PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Data: 05/07/2021

Versão 1.0

## HISTÓRICO DE ALTERAÇÕES

|  |
| --- |
| **DOCUMENTO** |
| **Descrição** | Documentação dos planos de Segurança da Informação |
| **Objetivo** | Este documento descreve os processos do Plano de Gestão de Riscos de Segurança da Informação |
| **Responsável** | **Equipe** | **Criado em** |
| GESIN – DITI | 05/07/2021 |
| **Setor** | Gerência de Infraestrutura e Segurança da Informação - GESIN |

**SUMÁRIO**

[PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO 1](#_heading=h.gjdgxs)

[​ HISTÓRICO DE ALTERAÇÕES 2](#_heading=h.30j0zll)

[PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO 3](#_heading=h.1fob9te)

[PAPÉIS E RESPONSABILIDADES 4](#_heading=h.3znysh7)

[CONTROLE DE EXECUÇÃO 4](#_heading=h.2et92p0)

[FERRAMENTAS 4](#_heading=h.tyjcwt)

[DESCRIÇÃO DAS ATIVIDADES: 5](#_heading=h.3dy6vkm)

[DEFINIÇÃO DO CONTEXTO DO PLANO DE GESTÃO DE RISCO: 6](#_heading=h.1t3h5sf)

[DEFINIÇÃO DO PROCESSO DE AVALIAÇÃO DE RISCOS: 7](#_heading=h.4d34og8)

[TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO: 8](#_heading=h.2s8eyo1)

[ACEITAÇÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO: 9](#_heading=h.17dp8vu)

[COMUNICAÇÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO: 10](#_heading=h.3rdcrjn)

[DEFINIÇÃO DE MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: 11](#_heading=h.26in1rg)

[DESCRIÇÃO DOS DOCUMENTOS DE SAÍDA: 12](#_heading=h.lnxbz9)

[Anexo A – Solicitar o levantamento de Ativos do órgão ou instituição para preenchimento e classificação, tendo como orientações respostas para as seguintes questões: 12](#_heading=h.35nkun2)

[​ Anexo A 13](#_heading=h.1ksv4uv)

[Mapa de Risco – Solicitar o levantamento de Ativos do órgão ou instituição e atualizar com os formulários de riscos entregues no ato da confecção do plano e em futuras atualizações. 13](#_heading=h.44sinio)

[Anexo B 14](#_heading=h.9bq6thsu6l2s)

[Formulário de Registro dos Riscos – utilizar o formulário como levantamento inicial e padronizar para futuras atualizações 14](#_heading=h.z337ya)

# PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O plano de Gestão de Riscos de Segurança da Informação, é parte integrante do POSIN (Política de Segurança da Informação) da Secretaria de Estado da Administração do Governo do Estado de Santa Catarina. Composto por medidas, regras, diretrizes e normas a serem adotadas no que diz respeito a gestão de riscos de segurança da informação.

Seguindo a norma ABNT NBR ISO/IEC 27005:2019, vamos utilizar suas diretrizes para o processo de gestão de riscos de segurança da informação, atendendo particularmente aos requisitos de um SGSI, conforme a NBR ISO/IEC 27001.

As atividades do processo de gestão de riscos de segurança da informação são:

• definição do contexto;

• processo de avaliação de riscos;

• tratamento do risco de segurança da informação;

• aceitação do risco de segurança da informação;

• comunicação e consulta do risco de segurança da informação; e

• monitoramento e análise crítica de riscos de segurança da informação.



Os modelos anexos devem ser preenchidos conforme sugestão descrita e classificados para tornar visual o mapeamento de riscos de segurança da informação e balizar a conformidade segundo a LGPD.

# PAPÉIS E RESPONSABILIDADES

|  |  |
| --- | --- |
| **Papéis** | **Responsabilidades** |
| [Nome/Sigla]. | [breve descrição]. | [atribuições de competência]. |

# CONTROLE DE EXECUÇÃO

|  |  |  |
| --- | --- | --- |
| **Controle** | **Método de execução** | **Frequência** |
| [Nome/Sigla]. | [A ser feito]. | [Período Mensal/Anual etc]. |

# FERRAMENTAS

|  |  |
| --- | --- |
| **POSIN/SEA** | **Política de Segurança da Informação da SEA** |
|  | POSINPlanilha de Mapa de Risco |

# DESCRIÇÃO DAS ATIVIDADES:

Cada atividade terá uma descrição breve, seguindo os moldes abaixo para auxiliar o entendimento do órgão em questão e facilitar o preenchimento dos documentos de saída e assim tornar o mais conforme possível segundo a LGPD.

**Objetivo:**

Levantar informações macro até o nível mais detalhado de todo o ambiente do local em questão no contexto de segurança da informação. Isto permitirá ver o grau de conformidade com a LGPD e identificar todos os pontos a serem melhorados.

**Responsável:**

Pessoa que concatenará as informações levantadas e/ou responder por elas.

**Entradas:**

* Levantamentos diversos;
* Identificação dos objetos ou situações mencionadas;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Definir cada atividade que embasará o preenchimento dos documentos necessários.

**Saídas:**

Documentos auxiliares e comprobatórios da situação atual do local que irá guiar as boas práticas. Se utilizar de metodologias gráficas de fácil visualização de fatores críticos da organização.

## DEFINIÇÃO DO CONTEXTO DO PLANO DE GESTÃO DE RISCO:

**Objetivo:**

Levantar informações macro até o nível mais detalhado de todo o ambiente do local em questão no contexto de segurança da informação que impactam direta ou indiretamente os dados institucionais. Todas essas informações servirão para mitigar, na medida do possível, os riscos a privacidade de dados armazenados. Este plano visa deixar de forma clara os pontos críticos a serem trabalhados melhor pelo órgão, respaldo técnico e/ou legal para outros determinados temas e anuência da alta gestão de todos os pontos.

**Responsável:**

Pessoa que concatenará as informações levantadas ou responsável legal.

**Entradas:**

* Levantamentos dos riscos inerentes ao órgão referente aos dados sensíveis;
* Identificação dos pontos fracos e ameaças;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Através de delegações, identificar responsáveis por dados, sistemas, arquivos físicos e toda a forma de interação com informações de terceiros ou sensíveis da organização que embasará o preenchimento dos documentos necessários.

**Saídas:**

* Anexo A
* Anexo B

## DEFINIÇÃO DO PROCESSO DE AVALIAÇÃO DE RISCOS:

**Objetivo:**

Classificar os riscos identificados e facilitar a visualização dos pontos a serem atacados pela organização.

**Responsável:**

Pessoa de cada setor capacitada a dar a informação juntamente com responsável por tomadas de decisões da organização.

**Entradas:**

* Classificação através Matriz de Risco;
* Mapeamento de ativos (Hardware e software);
* Anuência e/ou aceites da alta gestão;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Utilizar a matriz de risco para classificar os riscos levantados e deixar de forma clara e visual as informações para tomadas de decisão futuras.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|  | Baixo Risco |
|  | Médio Risco |
|  | Alto Risco |

 | Probabilidade | Muito Baixo (muito incomum) | Baixo(incomum) | Médio (possível) | Alto (comum) | Muito Alto (frequente) |
| Impacto | Muito Baixo | 0 | 1 | 2 | 3 | 4 |
| Baixo | 1 | 2 | 3 | 4 | 5 |
| Médio | 2 | 3 | 4 | 5 | 6 |
| Alto | 3 | 4 | 5 | 6 | 7 |
| Muito Alto | 4 | 5 | 6 | 7 | 8 |

**Saídas:**

* Anexo A
* Anexo B

## TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO:

**Objetivo:**

Tratar os riscos que foram levantados e classificados da melhor maneira possível, mitigando ao máximo e/ou declarando atribuindo responsabilidade a alta gestão.

**Responsável:**

Alta gestão junto a reuniões setoriais.

**Entradas:**

* Reuniões diversas;
* Soluções com programação de tempo detalhadas;
* Sugestões de eliminar/diminuir quando possíveis determinados riscos com seus respectivos prazos;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Plano de ação para cada caso em que serão criadas tarefas com prazo determinado e assinaturas dos responsáveis.

**Saídas:**

* Anexo A
* Anexo B

## ACEITAÇÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO:

**Objetivo:**

Declarar formalmente o aceite de determinado risco e sua justificativa. Essa informação deve ser sempre em conjunta com todas as partes envolvidas.

**Responsável:**

Pessoa que concatenará as informações levantadas e tomadora de decisões da instituição.

**Entradas:**

* Reuniões diversas;
* Declarações da alta gestão o não tratamento de determinado risco, com motivo justificado;
* Plano de tratamento do risco (para embasamento das decisões de aceitação tomadas);
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Através de reuniões setoriais com a alta gestão, serão decididos os riscos que são impossíveis, não necessários ou ainda não interessantes para a organização de mitigá-los.

**Saídas:**

* Anexo A
* Anexo B

## COMUNICAÇÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO:

**Objetivo:**

Criar meios de divulgação do plano de gestão de riscos a toda organização, com intuito de engajamento dos colaboradores.

**Responsável:**

Pessoa do setor responsável pela comunicação do órgão.

**Entradas:**

* Definição das formas de comunicação do Plano de Gestão;
* Definição das formas de comunicação do Plano de Segurança da informação;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Através dos meios de comunicação divulgar todo plano de segurança da informação bem como seus produtos.

**Saídas:**

* Anexo A
* Anexo B

## DEFINIÇÃO DE MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS DE SEGURANÇA DA INFORMAÇÃO:

**Objetivo:**

Através de todas as atividades levantadas e trabalhadas, deve-se não só arquivar o plano, mas mantê-lo vivo com políticas de monitoramento constante, verificação das validades das informações, dos ciclos que devem ser retomados de tempos em tempos.

**Responsável:**

Todo grupo de trabalhado da LGPD do órgão.

**Entradas:**

* Documentos preenchidos após a aplicação do plano de gestão de riscos;
* Arquivamento e manutenção da base de dados com os alertas devidos para revisitar;
* Outras ocorrências importantes para o órgão.

**Descrição das Atividades:**

Criar uma metodologia cíclica de alimentar os planos de gestão de risco, os documentos e manter sempre atualizados.

**Saídas:**

* Anexo A
* Anexo B

# DESCRIÇÃO DOS DOCUMENTOS DE SAÍDA:

#### Anexo A – Solicitar o levantamento de Ativos do órgão ou instituição para preenchimento e classificação, tendo como orientações respostas para as seguintes questões:

a. Qual o escopo da gestão de riscos a ser adotado?

b. Quais os ativos relevantes que serão considerados, e que formarão o escopo?

c. Quais ativos são pouco relevantes?

d. Como você delimita os elementos do escopo? Por meio de limites físicos? Limites legais? Limites tecnológicos? Limites contratuais? Limites organizacionais?

e. Em que ambiente a organização opera? Qual a relevância do ambiente para a gestão de riscos? A sua organização opera em um ambiente controlado? Em um ambiente hostil? Com muitas ameaças?

Levar em conta para a delimitação do escopo os itens abaixo que podem influenciar a gestão de riscos:

a. Objetivos estratégico, estratégias e políticas de negócios e serviços da organização;

b. Processos de negócios;

c. Funções e estruturas organizacionais;

d. Requisitos legais, regulatórios e contratuais aplicáveis;

e. Política de segurança da informação da organização;

f. Abordagem geral de gestão de riscos da organização;

g. Ativos de informação;

h. Quantidade de sítios físicos da organização e suas características geográficas;

i. Restrições afetando a organização;

j. Expectativas dos intervenientes e outras partes interessadas;

k. Ambiente sociocultural;

l. Interfaces (ex: de troca de informação com o meio ambiente).

Devem ser providas justificativas para quaisquer exclusões de ativos do escopo indicado.

O resultado da atividade é uma declaração preliminar de escopo de gestão de riscos, um documento formal.

Se utilizar de matriz gráfica para tornar visual e de fácil identificação dos principais problemas a serem solucionados.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|   | Baixo Risco |
|   | Médio Risco |
|   | Alto Risco |

 | Probabilidade | Muito Baixo (muito incomum) | Baixo(incomum) | Médio (possível) | Alto (comum) | Muito Alto (frequente) |
| Impacto | Muito Baixo | 0 | 1 | 2 | 3 | 4 |
| Baixo | 1 | 2 | 3 | 4 | 5 |
| Médio | 2 | 3 | 4 | 5 | 6 |
| Alto | 3 | 4 | 5 | 6 | 7 |
| Muito Alto | 4 | 5 | 6 | 7 | 8 |

# Anexo A

#### Mapa de Risco – Solicitar o levantamento de Ativos do órgão ou instituição e atualizar com os formulários de riscos entregues no ato da confecção do plano e em futuras atualizações.

|  |
| --- |
| **MAPA DE RISCO** |
| **Análise do Risco** | Nível do Risco | Resposta ao Risco | Tratamento do Risco | Responsável | Prazo /Periodicidade |
| Item | Eventos de Risco | Causas | Consequência | Probabilidade de Ocorrência | Impacto |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|  | Baixo Risco |
|  | Médio Risco |
|  | Alto Risco |

 | Probabilidade | Muito Baixo (muito incomum) | Baixo(incomum) | Médio (possível) | Alto (comum) | Muito Alto (frequente) |
| Impacto | Muito Baixo | 0 | 1 | 2 | 3 | 4 |
| Baixo | 1 | 2 | 3 | 4 | 5 |
| Médio | 2 | 3 | 4 | 5 | 6 |
| Alto | 3 | 4 | 5 | 6 | 7 |
| Muito Alto | 4 | 5 | 6 | 7 | 8 |

**Órgão ou entidade Pública:**

**CNPJ:**

**Endereço:**

**Telefone/fax:**

...............................(local), ........................(data)

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

 Assinatura do Responsável

#

# Anexo B

#### Formulário de Registro dos Riscos – utilizar o formulário como levantamento inicial e padronizar para futuras atualizações

|  |
| --- |
| **Formulário de Registro dos Riscos, Ações e Responsabilidades** |
| Risco: |  |
| Probabilidade |  | Resposta: |  |
| Impacto |  | Dano potencial:  |  |
| Id | Ação Preventiva | Responsável / Prazo | Procedimento |
| a |  |  |  |
| b |  |  |  |
| Id | Ação de Contingência | Responsável / Prazo | Procedimento |
| 1 |  |  |  |
| 2 |  |  |  |

**Órgão ou entidade Pública:**

**CNPJ:**

**Endereço:**

**Telefone/fax:**

...............................(local), ........................(data)

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

 Assinatura do Responsável