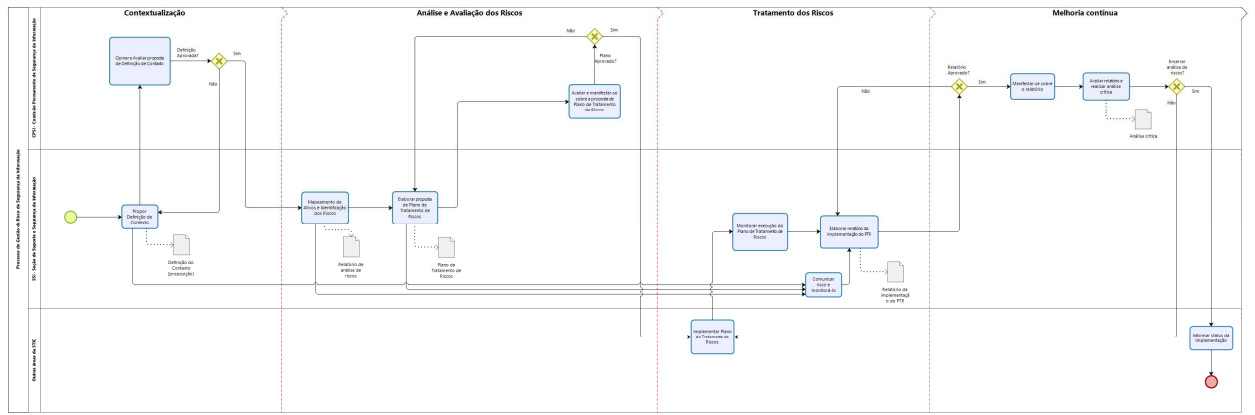


## ANEXO I - PORTARIA N° 183/2020 - GP



ANEXO II - PORTARIA Nº 183/2020 - GP



**TRIBUNAL REGIONAL ELEITORAL RIO GRANDE DO NORTE**

## **Manual do Processo de Gestão de Riscos da Segurança da Informação**

---

**Versão 1.0**

Natal/RN  
Agosto/2020

## CONTROLE DE VERSÕES

<b>VERSÃO</b>	<b>Validado CPSI</b>	<b>RESPONSÁVEL</b>
1.0	31.08.2020	Marcos Flávio Nascimento Maia

## **APRESENTAÇÃO**

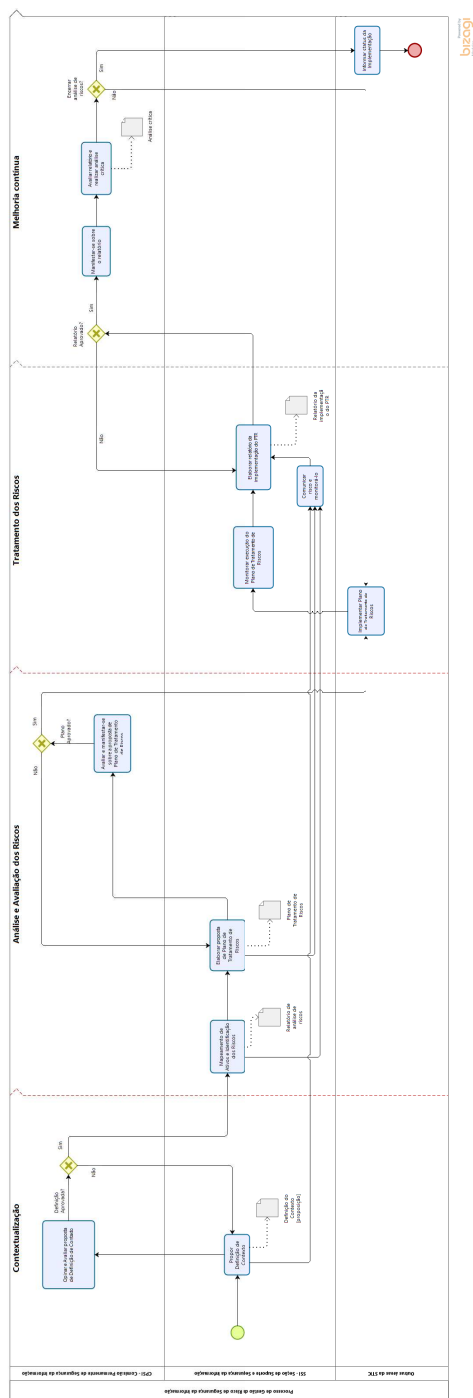
O objetivo deste manual é estabelecer responsabilidades e descrever as atividades para a Gestão de Riscos da Segurança da Informação no Tribunal Regional Eleitoral do Rio Grande do Norte, com o intuito de minimizar a ocorrência de ameaças que podem interferir (negativamente) no recurso de informação utilizado pela organização para atingir os seus objetivos corporativos e possibilitar realizar ações respaldadas teoricamente.

As principais motivações para o estabelecimento do presente processo são o alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria, a necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente, o correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Riscos da Segurança da Informação com maior qualidade, e a formalização de um processo sistemático para gerenciamento dos riscos de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

## Índice

1.1 PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO.....	6
1.1.1 Elementos do processo.....	6
1.1.1.1 <input type="checkbox"/> Propor Definição do Contexto .....	6
1.1.1.2 <input type="checkbox"/> Opinar e Avaliar proposta de definição de Contexto .....	6
1.1.1.3 <input type="checkbox"/> Mapeamento de Ativos e Identificação dos Risco.....	6
1.1.1.4 <input type="checkbox"/> Elaborar proposta de Plano de Tratamento de Riscos.....	6
1.1.1.5 <input type="checkbox"/> Avaliar e manifestar-se sobre a proposta de Plano de Tratamento de Riscos.....	7
1.1.1.6 <input type="checkbox"/> Implementar Plano de Tratamento de Riscos.....	7
1.1.1.7 <input type="checkbox"/> Comunicar risco e monitorá-lo .....	7
1.1.1.8 <input type="checkbox"/> Monitorar execução do Plano de Tratamento de Riscos.....	7
1.1.1.9 <input type="checkbox"/> Elaborar relatório da implementação do PTR .....	8
1.1.1.10 <input type="checkbox"/> Manifestar-se sobre o relatório.....	8
1.1.1.11 <input type="checkbox"/> Avaliar relatório e realizar análise crítica .....	8
1.1.1.12 <input type="checkbox"/> Informar status da Implementação .....	8
2 RESOURCES.....	9
2.1 CPSI - COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO (FUNÇÃO) .....	9
2.2 SSI - SEÇÃO DE SUPORTE E SEGURANÇA DA INFORMAÇÃO (FUNÇÃO) .....	9
2.3 OUTRAS ÁREAS DA STIE (FUNÇÃO) .....	9

## Processo de Gestão de Riscos da Segurança da Informação



## 1.1 Processo de Gestão de Riscos de Segurança da Informação

---

### 1.1.1 Elementos do processo

#### 1.1.1.1 ☐ *Propor Definição do Contexto*

##### **Descrição**

Compreende a proposição dos objetivos, escopo e limites da avaliação de riscos a ser realizada, com a identificação das partes interessadas e observados os critérios definidos na Política de Segurança da Informação.

##### **Executante SSI**

#### 1.1.1.2 ☐ *Opinar e Avaliar proposta de definição de Contexto*

##### **Descrição**

A Comissão Permanente de Segurança da Informação avalia as definições e pode tecer observações para auxiliar e/ou subsidiar a Presidência na avaliação do documento. Ela também é responsável por avaliar o contexto proposto para a análise de riscos a ser executada, podendo aprová-lo ou não. Em caso de não-aprovação, encaminha para as correções necessárias.

##### **Executante CPSI**

#### 1.1.1.3 ☐ *Mapeamento de Ativos e Identificação dos Risco*

##### **Descrição**

Atividade que consiste em elencar os ativos que compõem o escopo, suas características, seus relacionamentos com sistemas, processos de negócio, responsáveis, tecnologias envolvidas, etc. Com os ativos mapeados, são identificadas as ameaças e vulnerabilidades dos controles de TIC já implementados.

##### **Executante SSI**

#### 1.1.1.4 ☐ *Elaborar proposta de Plano de Tratamento de Riscos*

##### **Descrição**

Atividade que compreende a elaboração de plano visando à definição das formas de tratamento dos riscos e de implantação de controles, dos responsáveis por sua implementação e prazos estabelecidos.

**Executante SSI**

- 1.1.1.5 ☐ *Avaliar e manifestar-se sobre a proposta de Plano de Tratamento de Riscos*

**Descrição**

Esta atividade compreende a ciência sobre os resultados da análise e avaliação de riscos e a apreciação da proposta do Plano de Tratamento de Riscos. Nessa etapa, a Comissão Permanente de Segurança da Informação avalia o PTR e pode tecer observações para subsidiar a avaliação do documento.

**Executante CPSI**

- 1.1.1.6 ☐ *Implementar Plano de Tratamento de Riscos*

**Descrição**

Nessa atividade, as áreas da STIE implementam os controles para mitigar os riscos elencados, dentro de um prazo definido no PTR.

**Executante Outras áreas da STIE**

- 1.1.1.7 ☐ *Comunicar risco e monitorá-lo*

**Descrição**

Nesta atividade, a SSI comunica o risco às partes interessadas e também efetua o monitoramento dos riscos já avaliados, a fim de evitar que eles se concretizem.

**Executante SSI**

- 1.1.1.8 ☐ *Monitorar execução do Plano de Tratamento de Riscos*

**Descrição**

Esta fase tem por objetivo monitorar a execução do Plano, com a finalidade de assegurar sua implementação dentro dos prazos definidos.

**Executante SSI**



#### 1.1.1.9 ☐ *Elaborar relatório da implementação do PTR*

##### **Descrição**

Atividade que compreende a elaboração de relatório com as informações e resultados da execução do Plano de Tratamento de Riscos, bem como propostas de melhorias para o próximo ciclo. O relatório é apresentado a Comissão Permanente de Segurança da Informação. Se aprovado, é então encaminhado para avaliação e manifestação. Caso contrário, é encaminhado para readequação.

**Executante** SSI

#### 1.1.1.10 ☐ *Manifestar-se sobre o relatório*

##### **Descrição**

A Comissão Permanente de Segurança da Informação manifesta-se sobre o relatório apresentado.

**Executante** CPSI

#### 1.1.1.11 ☐ *Avaliar relatório e realizar análise crítica*

##### **Descrição**

Atividade que compreende a ciência e avaliação dos resultados do PTR e das propostas apresentadas para melhoria da Gestão de Riscos, bem como a realização da Análise Crítica sobre a análise de riscos como um todo.

**Executante** CPSI

#### 1.1.1.12 ☐ *Informar status da Implementação*

##### **Descrição**

Nesta etapa, a área que implementou o PTR reporta o fim da implantação do plano.

**Executante** Outras áreas da STIE

## 2 *RESOURCES*

### 2.1 CPSI - Comissão Permanente de Segurança da Informação (Função)

#### **Descrição**

Responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco, subsidiando a tomada de decisão pela Administração.

Responsável pela aprovação ou rejeição final de documentos e proposições referentes ao Tratamento de Riscos e às propostas de melhoria do processo.

### 2.2 SSI - Seção de Suporte e Segurança da Informação (Função)

#### **Descrição**

Responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TIC.

### 2.3 Outras áreas da STIE (Função)

#### **Descrição**

Compreende as áreas que gerenciam os sistemas, serviços e infraestrutura de TIC, responsáveis pela implementação dos controles definidos no tratamento dos riscos.