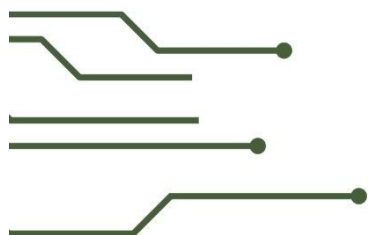


TRIBUNAL REGIONAL ELEITORAL  
DO ACRE

# PLANO DE GESTÃO DE RISCOS DE TI 2026



SECRETARIA DE  
TECNOLOGIA DA  
INFORMAÇÃO





## Histórico de alterações

| Documento              |                                                                                                                                                                                                                                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descrição              | Plano de Gestão de Riscos de TI                                                                                                                                                                                                       |
| Finalidade             | Descrever os conceitos, definições, objetivos, responsabilidades e o processo de gestão de riscos de TI do TRE-AC.                                                                                                                    |
| Unidade responsável    | Secretaria de Tecnologia de Informação – STI                                                                                                                                                                                          |
| Publicação na internet | <a href="https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic">https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic</a> |

| Versionamentos |            |                 |                                                                     |
|----------------|------------|-----------------|---------------------------------------------------------------------|
| Versão         | Data       | Responsável     | Descrição                                                           |
| 1.0            | 28/07/2023 | ASPGOVTI e GSTI | Criação do documento                                                |
| 1.1            | 04/08/2023 | CGTIC           | Validação da versão 1.0 e pequenas adaptações                       |
| 2.0            | 12/01/2026 | CGTIC           | Aprovado pelo CGTIC. Validação da versão 2.0 e pequenas adaptações. |



## Índice

|                                                                        |    |
|------------------------------------------------------------------------|----|
| 1. Introdução.....                                                     | 4  |
| 2. Objetivo .....                                                      | 4  |
| 3. Glossário.....                                                      | 5  |
| 4. Responsabilidades.....                                              | 6  |
| 4.1. Do Proprietário do risco de TI .....                              | 6  |
| 4.2. Do Comitê Gestor de Tecnologia da Informação - CGTIC .....        | 6  |
| 4.3. Da Assistência de Planejamento e Governança de TI - ASPGOVTI..... | 7  |
| 4.3. Da Coordenadoria de Controle Interno - COCIN .....                | 7  |
| 5. Processo de Gestão de Riscos de TI.....                             | 7  |
| 5.1. Fluxo.....                                                        | 8  |
| 5.2. Escopo.....                                                       | 8  |
| 5.2.2. Escala de Probabilidades .....                                  | 9  |
| 5.2.2. Escala de Impactos .....                                        | 9  |
| 5.2.3. Matriz Probabilidade X Impacto .....                            | 10 |
| 5.2.4. Escala para Avaliação de Controles.....                         | 10 |
| 5.3. Analisar e Avaliar os Riscos.....                                 | 11 |
| 5.3.2. Identificar os riscos.....                                      | 11 |
| 5.3.3. Analisar os riscos.....                                         | 12 |
| 6. Planilha contendo o Plano de Gestão de Riscos de TI .....           | 12 |



## 1. Introdução

A gestão de riscos de TI é um conjunto de processos que auxiliam na identificação e a implementação de ações protetivas para a eliminação ou atenuação das ameaças que podem trazer prejuízos à organização.

Gerenciar riscos é o processo de planejar, organizar, dirigir e controlar os recursos humanos e materiais de uma organização, no sentido de minimizar os efeitos dos riscos e aproveitar as oportunidades encontradas sobre os objetivos dessa organização. Dessa forma, a gestão de riscos de TI é considerada um importante artefato do planejamento estratégico de uma instituição.

## 2. Objetivo

O Plano de Gestão de Riscos em Tecnologia da Informação tem por objetivo o auxílio da tomada de decisão desde a detecção de ameaças externas aos ativos de informação, implantação e entrega de serviços de Tecnologia da Informação. Para que o objetivo seja alcançado é necessário que sejam definidos:

- a) As tarefas que compõem o processo de gestão de riscos;
- b) As técnicas e ferramentas que favoreçam a identificação, avaliação, monitoramento, tratamento e comunicação de riscos para a área de Tecnologia da Informação;
- c) Os papéis e suas respectivas responsabilidades quanto à gestão de risco.



### 3. Glossário

| Termos                                                                | Definição/Significado                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ameaça</b>                                                         | Se refere ao evento que possa explorar uma vulnerabilidade; Causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades                                                                                                                                                                                                                         |
| <b>Análise do Risco</b>                                               | Trata-se do uso sistemático de informações para identificar fontes e estimar o risco;                                                                                                                                                                                                                                                                                                                                  |
| <b>Ativo</b>                                                          | Qualquer elemento de valor para organização, seja tangível ou intangível, que esteja relacionado à Tecnologia da Informação.                                                                                                                                                                                                                                                                                           |
| <b>Avaliação de Riscos</b>                                            | Processo de comparar o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;                                                                                                                                                                                                                                                                                                     |
| <b>Comitê Gestor de Tecnologia da Informação e Comunicação (CGTI)</b> | Órgão colegiado de natureza consultiva e de caráter permanente em conformidade com as orientações emanadas pelo Conselho Nacional de Justiça (CNJ), Secretaria de Tecnologia da Informação (STI) e com Planejamento Estratégico do Tribunal Regional Eleitoral do Acre. O CGTI é responsável pelo alinhamento dos objetivos estratégico do TRE-AC e o apoio e priorização dos projetos a serem desenvolvidos pela STI; |
| <b>Evento</b>                                                         | é a ocorrência gerada com base em fontes internas ou externas que pode causar impacto negativo, positivo ou ambos;                                                                                                                                                                                                                                                                                                     |
| <b>Gerenciamento de Riscos</b>                                        | é o processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos, processos de trabalho e projetos da organização, positiva ou negativamente, nos níveis estratégico, tático e operacional;                                                                                            |
| <b>Impacto</b>                                                        | é a mudança adversa no nível obtido dos objetivos. Consequência avaliada dos resultados com a ocorrência de um evento em particular, em que determinada vulnerabilidade foi explorada, uma ameaça ocorreu e o risco se concretizou;                                                                                                                                                                                    |



Plano de Gestão de Riscos de TI

|                                      |                                                                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Probabilidade</b>                 | Chance do risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis.                                                                                                         |
| <b>Risco</b>                         | Evento incerto que produz uma consequência que pode ser negativa ou positiva.                                                                                                                                   |
| <b>Tecnologia da Informação (TI)</b> | Ativo estratégico que suporta processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações. |
| <b>Tratamento dos Riscos</b>         | Processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco; e                                                                               |
| <b>Vulnerabilidade</b>               | Qualquer fraqueza que possa ser explorada para comprometer a segurança da informação;                                                                                                                           |

## 4. Responsabilidades

### 4.1. Do Proprietário do risco de TI

- Gerir os riscos de TI sob sua responsabilidade;
- Submeter ao CGTIC os riscos de TI que extrapolarem sua competência e capacidade de gerenciamento;
- Encaminhar à ASPGOVTI o Plano de Gestão dos Riscos de TI sob sua responsabilidade.

### 4.2. Do Comitê Gestor de Tecnologia da Informação - CGTIC

- Revisar esta Política de Gestão de Riscos de Tecnologia da Informação e apresentar proposta de alteração ao COSET;
- Operacionalizar, no âmbito das unidades da STI, a aplicação dos recursos disponibilizados para a gestão de riscos;
- Dirimir eventuais dúvidas dos proprietários de risco, na execução do processo de Gestão de Riscos de Tecnologia da Informação;
- Deliberar sobre os riscos considerados médios e altos que, eventualmente, lhe forem apresentados pelos proprietários de risco;
- Submeter ao COSET, acompanhados de manifestação, os riscos de Tecnologia da Informação considerados extremos e os riscos residuais considerados altos;



#### Plano de Gestão de Riscos de TI

- Subsidiar o COSET com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;
- Revisar continuamente o modelo do processo de Gestão de Riscos de TI e submetê-lo à aprovação do COSET;
- Conscientizar os gestores sobre a importância da gestão de riscos de TI e a responsabilidade inerente a cada proprietário dos riscos.

#### **4.3. Da Assistência de Planejamento e Governança de TI - ASPGOVTI**

- Proceder à integração dos planos de gestão de riscos de TI a ela encaminhados, monitorando os riscos e reportando-os ao CGTIC, periodicamente;
- Divulgar e auxiliar à implementação e à operacionalização do processo de gerenciamento de riscos de TI nas unidades, equipes e comissões relacionadas à STI;
- Propor ao CGTIC melhorias para o processo e para esta Política de Gestão de Riscos de TI e para o processo correspondente.

#### **4.3. Da Coordenadoria de Controle Interno - COCIN**

- Incluir, nos planos de auditoria, ações de avaliação do gerenciamento de riscos de TI;
- Utilizar as ferramentas e técnicas de auditoria interna para analisar riscos e controles administrativos na área de TI;
- Avaliar os controles internos utilizados pela STI na gestão de seus riscos;
- Realizar auditorias periódicas com vistas a aferir o atendimento das diretrizes formuladas para a Gestão de Riscos de TI e a efetividade da Política de Gestão de Riscos de Tecnologia da Informação.

### **5. Processo de Gestão de Riscos de TI**

O processo de gestão de riscos consiste no conjunto de etapas e atividades relacionadas e necessárias para realizar o gerenciamento de riscos, contemplando a identificação de riscos, classificação, planejamento de respostas aos riscos, monitoramento e revisão e por fim a comunicação e aprendizado. Este processo se refere a uma gama de atividades abrangendo todos os níveis hierárquicos, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos e é suportado pela cultura e pela estrutura de gestão de riscos da entidade.

## 5.1. Fluxo

A figura a seguir apresenta o Processo de Gestão de Riscos de TI desenvolvido pelo TRE-AC.

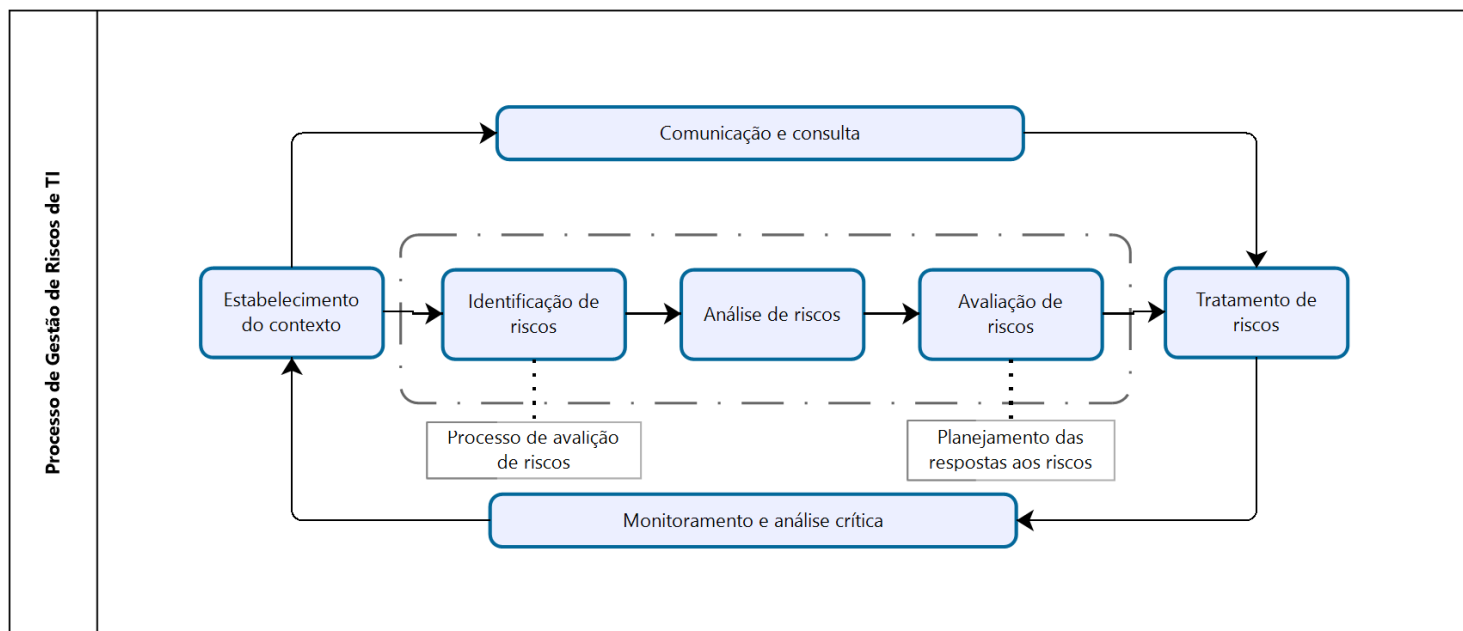


Figura 1 – Visão geral do fluxo do Processo de Gestão de Riscos de TI

## 5.2. Escopo

O escopo do presente processo se refere a orientar as demandas a serem executadas durante o Gerenciamento dos Riscos. Nesta etapa são definidos os parâmetros internos e externos, a definição de critérios básicos avaliativos, bem como escopo e limites, visando estruturar o Plano de Gestão de Riscos de TI. A definição dos critérios básicos dependerá das características e restrições adotadas pelo Tribunal.



### 5.2.2. Escala de Probabilidades

A escala de probabilidades define como a probabilidade será medida. A escala utilizada neste processo é apresentada no quadro a seguir:

| Probabilidade | Descrição                                                                                                                       | % de certeza | Nível |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-------|
| 1-Muito baixa | Evento extraordinário para os padrões conhecidos da gestão e operação do processo, ou seja, não há histórico de sua ocorrência. | 0 a 20%      | 1     |
| 2-Baixa       | Evento casual inesperado, porém, há histórico conhecido de sua ocorrência.                                                      | 20 a 40%     | 2     |
| 3-Média       | Evento esperado que possui frequência reduzida e de conhecimento da maioria dos gestores do processo.                           | 40 a 60%     | 3     |
| 4-Alta        | Evento usual com ocorrência habitual, com histórico amplamente conhecido pelos gestores do processo.                            | 60 a 80%     | 4     |
| 5-Muito Alta  | Evento com reprodução frequente de modo acelerado, interferindo de modo claro no ritmo das atividades.                          | > 80%        | 5     |

### 5.2.2. Escala de Impactos

A escala de impactos define a natureza e o tipo de consequências, e como serão medidas nas diversas áreas de objetivos impactados.

| Probabilidade | Descrição                                                                                                                                                 | Nível |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Muito Alto    | Interrupção das atividades/processos, projetos ou programas da organização, causando impactos irreversíveis nos objetivos.                                | 5     |
| Baixo         | Degradação das atividades/processos, projetos ou programas da organização, porém com impactos pequenos nos objetivos.                                     | 2     |
| Médio         | Interrupção das atividades/processos, projetos ou programas da organização, causando impactos significativos nos referidos objetivos, porém recuperáveis. | 3     |
| Alto          | Interrupção das atividades/processos, projetos ou programas da organização, causando impactos de reversão muito difíceis nos objetivos.                   | 4     |



### 5.2.3. Matriz Probabilidade X Impacto

A matriz Probabilidade x Impacto define como o nível de risco deve ser determinado.

| Legenda Nível de Risco<br><b>Extremo</b><br><b>Alto</b><br><b>Médio</b><br><b>Baixo</b> |                  | Probabilidade    |            |            |        |                 |
|-----------------------------------------------------------------------------------------|------------------|------------------|------------|------------|--------|-----------------|
|                                                                                         |                  | 1<br>Muito Baixa | 2<br>Baixa | 3<br>Média | 4 Alta | 5<br>Muito Alta |
| I<br>M<br>P<br>A<br>C<br>T<br>O                                                         | 5<br>Muito Alto  | 5                | 10         | 15         | 20     | 25              |
|                                                                                         | 4<br>Alto        | 4                | 8          | 12         | 16     | 20              |
|                                                                                         | 3<br>Médio       | 3                | 6          | 9          | 12     | 15              |
|                                                                                         | 2<br>Baixo       | 2                | 4          | 6          | 8      | 10              |
|                                                                                         | 1<br>Muito Baixo | 1                | 2          | 3          | 4      | 5               |

### 5.2.4. Escala para Avaliação de Controles

A escala de Avaliação de Controles define os critérios objetivos para análise dos controles implementados e para cálculo do risco residual.

| Avaliação        | Situação do Controle Existente                                                                                                      | Multiplicador do Risco Inerente |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| 1 – Inexistente  | Ausência completa de controle.                                                                                                      | 1,00                            |
| 2 – Fraco        | O controle depende do conhecimento pessoal dos operadores do processo, em geral de maneira manual.                                  | 0,80                            |
| 3 – Mediano      | O controle pode falhar por não contemplar todos aspectos relevantes do risco ou por ferramentas que o suportam não serem adequadas. | 0,60                            |
| 4 – Satisfatório | Controle normatizado e passível de aperfeiçoamento, sendo sustentado por ferramentas adequadas que mitigam o risco razoavelmente.   | 0,40                            |
| 5 - Forte        | Controle mitiga os riscos associados em todos os aspectos relevantes.                                                               | 0,20                            |



### 5.3. Analisar e Avaliar os Riscos

Após a definição do escopo, dos limites e da organização do processo de gestão de riscos de segurança da informação, a próxima etapa é a de análise e avaliação de riscos. Nesta fase são identificadas as ameaças, os controles existentes e que devem ser implementados, as vulnerabilidades e consequentes ameaças relacionadas. Após o levantamento das ameaças e vulnerabilidades é necessário identificar e categorizar os riscos envolvidos e realizar o planejamento de tratamento necessário.

Com os resultados da Análise/Avaliação de Riscos será possível implementar os controles de proteção para estes riscos de acordo com o direcionamento e a determinação de ações gerenciais e suas prioridades na Gestão de Riscos de Segurança da Informação.

#### 5.3.1. Identificar os riscos

Compreende-se por identificar, reconhecer, registrar riscos que possam afetar as operações do Tribunal Regional Eleitoral do Acre. A identificação dos riscos é constituída pelas seguintes atividades:

**5.3.1.1. Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido** – a quantidade de informações reunidas nesta etapa influenciará durante o subprocesso de Análise e Avaliação dos Riscos.

**5.3.1.2. Identificar as ameaças e suas fontes** – a utilização do catálogo de ameaças deve ser necessária cautela ao usar catálogos de ameaças, pois estas estão sempre mudando de acordo com o ambiente ou sistemas de informações.

**5.3.1.3. Identificar as ações de Segurança da Informação adotadas (controles existentes e planejados)** – a importância desta etapa é para evitar trabalhos desnecessários e seus referentes custos, bem como a duplicação de controles.

**5.3.1.4. Identificar as vulnerabilidades existentes nos ativos** – nesta etapa as vulnerabilidades em que não foram detectadas ameaças correspondentes, devem ser identificadas e monitoradas.

**5.3.1.5. Mesmo as vulnerabilidades que não tem uma ameaça correspondente** devem ser identificadas e monitoradas, no caso de haver mudanças.



**5.3.1.6. Identificar as consequências dos riscos** – é importante identificar o impacto das falhas de segurança, de acordo com os critérios definidos durante a etapa de definições do contexto.

### **5.3.2. Analisar os riscos**

Entender os riscos, sua probabilidade de ocorrência e as consequências para os eventos identificados são realizados neste processo, bem como analisar informações que contribuam com as decisões estratégicas sobre os riscos. A análise dos riscos pode ser qualitativa (exemplo: pequena, média e grande) ou quantitativa (valores numéricos), formada pelas seguintes etapas:

**5.3.2.1. Avaliar as consequências** – podem ser expressas em função dos critérios monetários, técnicos ou humanos de impacto ou de outro critério relevante para o Tribunal.

**5.3.2.2. Avaliar a probabilidade dos incidentes** – nesta etapa é levada em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas;

**5.3.2.3. Estimar o nível do risco** – se refere à combinação da probabilidade em um cenário de incidentes e suas consequências.

**5.3.3. Avaliar Riscos** – compreender a natureza do risco para a melhor tomada de decisão sobre ações futuras.

**5.3.4. Tratar Riscos** – criar um plano para o tratamento dos riscos identificados, selecionar uma ou mais ações para modificar os riscos e a implementação dessas ações;

**5.3.5. Monitoramento e Análise de Riscos** – revisar e analisar periodicamente a gestão de riscos, para o aprimoramento contínuo desse processo pelo Tribunal Regional Eleitoral do Acre.

## **6. Planilha contendo o Plano de Gestão de Riscos de TI**

A planilha a seguir contém o Plano de Gestão de Risco de TI do TRE-AC.

| Plano de Gestão de Riscos de TI do TRE-AC                                                                              |                    |                                                                                                                                                                                                                             |                                                                                                                                                    | Avaliação dos Riscos |         |                | Identificação e definição do controle existente                                                                                                                                                                                                                                                                               | Plano de Contingência de Riscos                                                                                                                                                                                                                                                                                                         | Unidade Responsável |
|------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Evento de Risco                                                                                                        | Categoria do Risco | Causas                                                                                                                                                                                                                      | Impactos                                                                                                                                           | Probabilidade        | Impacto | Nível do risco | Descrição do controle existente                                                                                                                                                                                                                                                                                               | O que fazer?<br>(Antes do risco acontecer = contenção; ou<br>Depois do risco acontecer = contingência)                                                                                                                                                                                                                                  |                     |
| Indisponibilidadd e do Data Center em virtude de falha na rede elétrica                                                | Operacional        | Falta de energia elétrica no prédio sede;<br>Mau funcionamento do Gerador de Energia;<br>Exaurimento da autonomia do nobreak do prédio sede;<br>Exaurimento da autonomia dos nobreaks do Data Center.                       | Paralisação de todos os serviços disponibilizados na rede de dados enquanto durar a pane elétrica.                                                 | 1                    | 5       | 5              | Monitoramento constante do fornecimento de energia elétrica para o prédio sede;<br>Monitoramento do nível de combustível no tanque do gerador de energia;<br>Manutenção periódica do nobreak e do gerador de energia do prédio sede;<br>Monitoramento constante dos no-breaks do Data Center.                                 | Contenção:<br>Manter tanque de combustível do gerador de energia sempre totalmente abastecido;<br>Manter combustível reserva para o caso de alto consumo pelo gerador de energia.<br>Contingência: Ativar o Data Center secundário, na CAE, para que a paralisação dos serviços seja mínima.                                            | SEREDE              |
| Indisponibilidadd e do Data Center em virtude de falha na refrigeração ou aumento excessivo da umidade                 | Operacional        | Mau funcionamento dos aparelhos redundantes de ar condicionado de precisão;<br>Falta de energia elétrica no prédio sede;<br>Mau funcionamento do Gerador de Energia;<br>Exaurimento da autonomia do nobreak do prédio sede. | Paralisação de todos os serviços disponibilizados na rede de dados enquanto durar a falah de refrigeração.                                         | 1                    | 5       | 5              | Monitoramento constante do fornecimento de energia elétrica para o prédio sede;<br>Monitoramento do nível de combustível no tanque do gerador de energia;<br>Manutenção periódica do nobreak e do gerador de energia do prédio sede;<br>Monitoramento constante dos aparelhos de acr condicionado de precisão do Data Center. | Contenção:<br>Manter tanque de combustível do gerador de energia sempre totalmente abastecido;<br>Manter combustível reserva para o caso de alto consumo pelo gerador de energia.<br>Contingência: Ativar o Data Center secundário, na CAE, para que a paralisação dos serviços seja mínima.                                            | SEREDE              |
| Indisponibilidadd e do Data Center em virtude de falha de hardware de equipamentos críticos                            | Operacional        | Falha de hardware de equipamentos críticos do Data Center.                                                                                                                                                                  | Paralisação parcial ou total dos serviços disponibilizados na rede de dados enquanto durar a falha de hardware.                                    | 1                    | 5       | 5              | Monitoramento constante de todos os equipamentos, dispositivos e componentes do Data Center que possam ocasionar interrupção dos serviços.                                                                                                                                                                                    | Contenção:<br>Substituição imedita, se possível, do item de hardware que estiver apresentando falha.<br>Contingência: Ativar o Data Center secundário, na CAE, para que a paralisação dos serviços seja mínima.                                                                                                                         | SEREDE              |
| Indisponibilidadd e do Data Center em virtude de falha ou mau funcionamento de software(programas e sistemas críticos) | Operacional        | Mau funcionamento ou falha dos softwares instalados nos computadores servidores do Data Center.                                                                                                                             | Paralisação parcial ou total dos serviços disponibilizados na rede de dados enquanto durar a pane elétrica.                                        | 1                    | 5       | 5              | Monitoramento constante da necessidade de atualização periódica de drivers e patches de segurança dos sistemas operacionais e aplicativos críticos instalados nos computadores servidores do Data Center.                                                                                                                     | Contenção: atualização periódica de drivers e patches de segurança dos sistemas operacionais e aplicativos críticos instalados nos computadores servidores do Data Center.<br>Contingência: restauração da última imagem válida, no caso de servidores virtuais ou reinstalação, no caso de servidores físicos.                         | SEREDE              |
| Exploração de vulnerabilidade do sistema operacional ou programas instalados nos computadores                          | Operacional        | Falta de atualização do sistema operacional.                                                                                                                                                                                | Paralisação parcial ou total dos serviços disponibilizados na rede de dados enquanto durar a pane elétrica.                                        | 1                    | 5       | 5              | Monitoramento constante da necessidade de atualização imediata de patches de segurança dos sistemas operacionais instalados nos computadores servidores do Data Center.                                                                                                                                                       | Contenção: atualização imediata de patches de segurança do tipo 0 day.<br>Contingência: restauração da última imagem válida, no caso de servidores virtuais ou reinstalação, no caso de servidores físicos.                                                                                                                             | SEREDE              |
| Utilização de técnicas de phising para descobrir senhas dos usuários ou instalação de programas maliciosos             | Operacional        | Falta de conhecimento dos usuários das técnicas utilizadas em ataques de phising.                                                                                                                                           | Instalação de vírus e programas maliciosos nos computadores da rede de dados.                                                                      | 1                    | 5       | 5              | Monitoramenteo constante e manutenção de sistema de antivírus e anti spam para o servidor de correio eletrônico;                                                                                                                                                                                                              | Contenção: realização de campanhas de conscientização sobre phising e outras técnicas utilizadas para o furto de senhas e tentativas de ataques cibernéticos.<br>Contingência: isolamento dos computadores infectados, varredura na rede, alteração das senhas de todos os usuários envolvidos e adoção de outras medidas de segurança. | SCSEG               |
| Criptografia dos dados institucionais por meio de um ataque do tipo ransomware                                         | Operacional        | Invasão da rede de dados com escalção de privilégios para permitir ao atacante criptografar todos os dados institucionais.                                                                                                  | Possibilidade de perda de todos os dados institucionais.                                                                                           | 1                    | 5       | 5              | Monitoramenteo constante dos acessos na rede de dados;<br>Restrição do acesso às contas de tipo administrador;<br>Utilização de duplo fator de autenticação para acesso administrador, mesmo na rede interna.                                                                                                                 | Contenção: Utilização de backup em fita, além do backup em disco. Testes periódicos de restauração para garantir a integridade dos backups realizados;<br>Contingência: restauração do último backup válido gravado em fita.                                                                                                            | SEREDE              |
| Infecção da rede de dados por vírus e pragas virtuais                                                                  | Operacional        | Falta de conhecimento dos usuários que utilizam pendrives, arquivos ou mensagens infectadas.                                                                                                                                | Instalação de vírus e programas maliciosos nos computadores da rede de dados.                                                                      | 1                    | 5       | 5              | Monitoramenteo constante e manutenção de sistema de antivírus.                                                                                                                                                                                                                                                                | Contenção: realização de campanhas de conscientização. Instalação de antivírus em todas as máquinas conectadas à rede lógica;<br>Contingência: isolamento dos computadores infectados, varredura na rede, alteração das senhas de todos os usuários envolvidos e adoção de outras medidas de segurança.                                 | SEREDE              |
| Indisponibilidade de algum serviço/ativo de TI em virtude de ataques do tipo DOS                                       | Operacional        | Envio de uma quantidade massiva de requisições de acesso a um serviço/aplicação fazendo com que o mesmo fique indisponível.                                                                                                 | Paralisação do serviço/aplicação causando transtornos e contratempos.                                                                              | 1                    | 4       | 4              | Monitoramento constantes do tráfego na rede de dados, principalmente os oriundos de origem externa;<br>Contratação de links de comunicação com serviço anti-DDOS ativo;                                                                                                                                                       | Contenção: utilização de firewall e balanceadores de carga;<br>Contingência: Reativação do serviço no menor tempo possível.                                                                                                                                                                                                             | SEREDE              |
| Paralisação de um serviço por falta de espaço no storage                                                               | Operacional        | Falta de planejamento para expansão da capacidade do storage.                                                                                                                                                               | Paralisação do serviço/aplicação causando transtornos e contratempos.                                                                              | 1                    | 4       | 4              | Monitoramento constante da capacidade do storage com envio de alertas quando o espaço superar 80% de utilização.                                                                                                                                                                                                              | Contenção: planejamento prévio das expansões necessárias para a aquisição de mais espaço ou novo storage;<br>Contingência: Exclusão de informações não críticas/históricas já armazenadas via backup em disco e fita.                                                                                                                   | SEREDE              |
| Paralisação do banco de dados devido ao exaurimento de espaço de uma tablespace crítica do SGBD Oracle                 | Operacional        | Falta de monitoramento da expansão do tamanho das tablespaces                                                                                                                                                               | Paralisação do serviço/aplicação causando transtornos e contratempos.                                                                              | 1                    | 4       | 4              | Monitoramento constante do tamanho das tablespaces do banco de dados com envio de alertas quando o espaço superar 80% de utilização.                                                                                                                                                                                          | Contenção: realização de estimativa da progressão de utilização das tablespaces para assegurar o redimensionamento das mesmas antes de seu exaurimento;<br>Contingência: Expansão do tamanho das tablespaces.                                                                                                                           | SEREDE/SDBD         |
| Erro na realização dos backups ou inconsistência nas cópias de segurança                                               | Operacional        | Fita com problema; Storage cheia; erro na gravação do backup etc                                                                                                                                                            | Comprometimento dos dados que deveriam ser armazenados para futura recuperação e/ou falha na recuperação dos dados em função de alguma necessidade | 1                    | 2       | 2              | Alertas da solução de backup sobre a execução dos backups<br>Quanto à inconsistências nas cópias de segurança, não há controle                                                                                                                                                                                                | Contenção: SEREDE deve monitorar os alertas para verificar caso ocorra erros na execução dos backups.<br>E, estabelecer processo de restauração para validar dados backupados.<br>Contingência: Resolver o erro e realizar novo backup.                                                                                                 | SEREDE              |

| Plano de Gestão de Riscos de TI do TRE-AC                                                                                                                                                                                   |                    |                                                                                                                                                                                       |                                                                                                                                                                    | Avaliação dos Riscos |         |                | Identificação e definição do controle existente                                                                                                                                                                                                                                         | Plano de Contingência de Riscos                                                                                                                                                                                                                                                                                                                                       | Unidade Responsável |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Evento de Risco                                                                                                                                                                                                             | Categoria do Risco | Causas                                                                                                                                                                                | Impactos                                                                                                                                                           | Probabilidade        | Impacto | Nível do risco | Descrição do controle existente                                                                                                                                                                                                                                                         | O que fazer?<br>(Antes do risco acontecer = contenção; ou<br>Depois do risco acontecer = contingência)                                                                                                                                                                                                                                                                |                     |
| Falha na comunicação entre o TRE e o TSE e entre o TRE e os Cartórios Eleitorais                                                                                                                                            | Operacional        | Rompimento de fibra ou falha no firewall ou nos elementos ativos da rede.                                                                                                             | Indisponibilidade parcial ou total dos serviços essenciais de TI, tanto para usuários internos como para externos (eleitores).                                     | 1                    | 4       | 4              | Monitoramento constante dos links de comunicação (perda de pacote, indisponibilidade etc);<br>Monitoramento do funcionamento dos firewall e elementos ativos de rede, tanto na sede do Tribunal quanto nas zonas eleitorais.                                                            | Contenção: Manutenção de links redundantes de comunicação e de equipamentos reservas necessários para garantir a interligação TSE/TRE/ZE.<br>Contingência: Acionamento da empresa fornecedora do link de comunicação ou substituição imediata dos equipamentos avariados.                                                                                             | SEREDE              |
| Interrupção no funcionamento do Sistema de Chamado Técnicos (GLPI), da Central de Serviços                                                                                                                                  | Operacional        | Falha na infraestrutura que suporta o sistema.                                                                                                                                        | Paralisação do funcionamento do sistema de chamados GLPI, impedindo a abertura, gerenciamento e solução das requisições e incidentes de TI.                        | 1                    | 2       | 2              | Monitoramento constante da infraestrutura que suporta o sistema.                                                                                                                                                                                                                        | Contenção: Monitoramento do funcionamento pela SSU e intervenções da SEREDE, caso necessário.<br>Contingência: reinstalar a aplicação e restaurar backups do banco e filesystem.                                                                                                                                                                                      | SSU/SEREDE          |
| Interrupção dos serviços de manutenção preventiva de urnas eletrônicas devido à encerramento da cobertura contratual                                                                                                        | Operacional        | Falta de planejamento para realizar contratação em tempo hábil                                                                                                                        | As urnas eletrônicas deixarão de passar por ciclos periódicos de verificação, podendo resultar em número elevado de defeitos durante a preparação para as eleições | 1                    | 2       | 2              | Solicitação orçamentária para contratações periódicas                                                                                                                                                                                                                                   | Contenção: fiscalização do contato deve iniciar estudo de nova contratação ou renovação do contrato com antecedência<br>Contingência: fazer o ciclo do STE com a equipe da SEUE e SSU, em forma de mutirão.                                                                                                                                                           | CIE/SEUE            |
| Diminuição da força de trabalho das unidades da STI que suportam os processos críticos de TI do Tribunal.                                                                                                                   | Estratégico        | Ausência de servidores em virtude de férias, licenças médicas, aposentadoria, remoção, mudança de lotação e demais motivos que possam causar falta de servidores nas unidades da STI. | Diminuição ou paralisação de projetos das unidades afetadas; Sobrecarga de trabalho; Aumento do tempo necessário para solucionar as demandas.                      | 2                    | 3       | 6              | Escalonamento/controle das férias dos servidores lotados nas unidades da STI.                                                                                                                                                                                                           | Contenção: solicitação de servidores requisitados para suprir eventuais lacunas; solicitação de concursos públicos para suprir os cargos vagos, contratação de empresas para o fornecimento de mão de obra especializada.<br>Contingência: Realocação de servidores para suprir às áreas com maior carência de pessoal.                                               | STI                 |
| Força de trabalho insuficiente para a realização das atividades técnicas de preparação e execução das Eleições (oficiais e comunitárias).                                                                                   | Estratégico        | Quantidade insuficiente de servidores lotados na STI.                                                                                                                                 | Falta de pessoal para realizar as atividades técnicas relacionadas às eleições.                                                                                    | 2                    | 4       | 8              | Identificação prévia da necessidade de contar com apoio temporário de servidores de outras unidades ou requisitados, no período eleitoral.                                                                                                                                              | Contenção: solicitação prévia de servidores requisitados e alocação temporária de servidores de outras unidades do TRE em atividades específicas da STI durante o período eleitoral.                                                                                                                                                                                  | STI                 |
| Manutenção do acesso à rede de dados e aos sistemas administrativos e eleitorais de servidores, magistrados e colaboradores que não mais pertencem ao quadro de pessoal do TRE.                                             | Integridade        | Descumprimento de normas internas                                                                                                                                                     | Existência de contas ativas que deveriam ter sido inativadas quando do desligamento do servidor, magistrado ou colaborador.                                        | 2                    | 2       | 4              | Monitoramento das contas do AD com alertas de contas não utilizadas por mais de 30 dias. Link disponibilizado na INTRANET, com todas as contas ativas no TRIBUNAL                                                                                                                       | Contenção: conscientização dos usuários acerca das normas existentes e sobre as boas práticas em segurança da informação.<br>Contingência: inativação imediata da conta.                                                                                                                                                                                              | COGEP/SEREDE        |
| Subtração de ativos de TI (bens permanentes)                                                                                                                                                                                | Integridade        | Falha de segurança patrimonial ou falha no controle de saída de bens patrimoniais do TRE.                                                                                             | Perda total ou parcial dos bens, uso indevido                                                                                                                      | 1                    | 2       | 2              | Fiscalização rígida da entrada e saída de bens no TRE;<br>Normas de controle de acesso físico às dependências do TRE.                                                                                                                                                                   | Contenção: Contratação de empresa de vigilância e segurança patrimonial; Uso de procedimentos para controlar a saída de bens do órgão; Verificações periódicas acerca da localização dos bens.<br>Contingência: Informação à Polícia Judiciária para a abertura de inquérito policial; Abertura de sindicância para apurar os fatos e identificar eventuais culpados. | DG                  |
| Furto, alteração e/ou inclusão de informações armazenadas nos bancos de dados por meio do uso de sistemas administrativos, eleitorais e e judiciais do TRE, aos quais tenha acesso, para benefício próprio ou de terceiros. | Integridade        | Má fé e desconhecimento da legislação.                                                                                                                                                | Causar alterações indevidas que possam prejudicar a integridade dos dados. Divulgação/mau uso de informações restritas                                             | 1                    | 5       | 5              | Registro de todas as ações que possam inserir, modificar ou excluir dados dos sistemas administrativos, judiciais e eleitorais permitindo identificar quem, quando e por qual via foi realizada a ação.                                                                                 | Contenção: Assinatura de termo de confidencialidade quando da entrada de um novo servidor ou colaborador; Concessão de permissão de acesso mediante pedido justificado da chefia imediata.<br>Contingência: restauração do último backup válido para trazer de volta a informação antes da alteração/modificação/exclusão indevida.                                   | SEREDE/SDBD         |
| Uso indevido ou manipulação de informações diretamente no banco de dados dos sistemas administrativos do TRE.                                                                                                               | Integridade        | Má fé e desconhecimento da legislação. Falta de controle de acesso ao banco de dados                                                                                                  | Causar alterações indevidas que possam prejudicar a integridade dos dados. Divulgação/mau uso de informações restritas                                             | 1                    | 5       | 5              | Restrição de acesso ao banco de dados apenas ao pessoal técnico responsável.<br>Registro de todas as ações que possam inserir, modificar ou excluir dados dos sistemas administrativos, judiciais e eleitorais permitindo identificar quem, quando e por qual via foi realizada a ação. | Contenção: Assinatura de termo de confidencialidade quando da entrada de um novo servidor ou colaborador; Concessão de permissão de acesso mediante pedido justificado da chefia imediata.<br>Contingência: restauração do último backup válido para trazer de volta a informação antes da alteração/modificação/exclusão indevida.                                   | SEREDE/SDBD         |

Legenda Nível de Risco

Baixo

Médio

Alto

Extremo

Legenda Impacto do risco

1 - Muito baixo

2 - Baixo

3 - Médio

4 - Alto

5 - Muito alto

Legenda Probabilidade do risco

1 - Muito baixa

2 - Baixa

3 - Média

4 - Alta

5 - Muito alta