SECRETARIA DE ESTRUTURA DE
TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PLANO DE GESTÃO DE RISCO DE TIC DO TJAP

Controle de Versões

Versão	Data	Autor	Notas da Revisão
1.0	2023	SETIC	Elaboração

Visão Geral

1. Objetivo do Plano de Gestão de Riscos

Identificar e apontar os passos necessários, de acordo com práticas listadas em literatura e conhecimento prático, para a Gestão de Riscos de TIC no Tribunal de Justiça do Estado do Amapá - TJAP.

2. Gestão de Riscos de TIC

A gestão de riscos visa identificar, avaliar e reduzir continuamente os riscos relacionados a TIC dentro dos níveis de tolerância definidos pela Alta gestão da organização. Nesse sentido, faz-se necessária a definição de políticas e diretrizes para o tratamento de riscos e gerenciamento da segurança da informação.

2.1 Processos Gestão de Riscos

Os Processo de riscos de TIC são determinados pela norma ABNT NBR 27005:2019 compreendido pelas seguintes fases:

I - Estabelecimento do contexto - etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os fatores externo e interno que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.) e os critérios de riscos a serem levados em consideração ao gerenciar riscos;

Compõem os critérios de risco:

1. Escala de probabilidade: define como a probabilidade será medida. A probabilidade está associada às chances de um evento ocorrer;
2. Escala e impacto: define natureza e tipos de consequências e como elas serão medidas nas diversas áreas. Para definir o nível do impacto, é necessário primeiro considerar as dimensões do objetivo do processo de trabalho avaliado;
3. Matriz “impacto X Probabilidade: define como o nível de risco deve ser determinado;
4. Apetite a risco: é o nível em que um risco se torna aceitável ou inaceitável;
5. Matriz de classificação de riscos: define como os riscos serão classificados quanto à significância;

6. Diretrizes para priorização e tratamento: determina como os riscos serão priorizados; e
7. Definição da eficácia dos controles: estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual.

II - Identificação de Riscos - etapa em que são identificados possíveis riscos para os objetivos associados aos processos organizacionais. O propósito da identificação de risco é determinar o que pode causar uma perda e deixar claro como, onde e o por que a perda pode acontecer. A identificação de risco devem incluir os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.

III - Análise de riscos - etapa que se refere ao desenvolvimento da compreensão sobre o risco e à determinação do nível do risco, que é determinado pela Matriz Probabilidade x Impacto.

● Escala de probabilidade (1 a 5):
(1) raro: acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
(2) pouco provável: o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo.
(3) provável: repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.
(4) muito provável: repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte.
(5) praticamente certo: ocorrência quase garantida no prazo associado ao objetivo.

● Escalas de impacto (1 a 5):
(1) muito baixo: compromete minimamente o atingimento do objetivo. Para fins práticos, não altera o alcance do objetivo/resultado.
(2) baixo: compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
(3) médio: compromete razoavelmente o alcance do objetivo/resultado.
(4) alto: compromete a maior parte do atingimento do objetivo/resultado.
(5) muito alto: compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

IV - Avaliação de Riscos - etapa em que são estimados os níveis dos riscos identificados, a fim de determinar se o risco é aceitável.

O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

V - Tratamento de Riscos - etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas.

As opções de tratamento de riscos são:
- Evitar o risco: ação para evitar totalmente o risco.
- Transferir o risco: compartilhar ou transferir uma parte do risco a terceiros
- Mitigar o risco: reduzir o impacto ou a probabilidade de de ocorrência do risco

VI - Aceitação de Riscos - etapa em que se aceita ou tolera o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.

A elaboração e a implementação do Plano de Tratamento de Riscos deve levar em consideração:

- A eficácia das ações já existentes.
- As restrições organizacionais, técnicas e estruturais.
- Os requisitos legais.
- A análise custo/benefício.
- As ações a serem realizadas.
- Os responsáveis.
- As prioridades.
- Os prazos de execução.

VII - Comunicação e Consulta do Risco - etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas.

VII - Monitoramento do Risco - etapa que ocorre durante todo o processo de gerenciamento de riscos onde os riscos são monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças de contexto da organização e de se manter uma visão geral dos riscos.

FLUXOGRAMA DO PROCESSO DE AVALIAÇÃO DE RISCOS

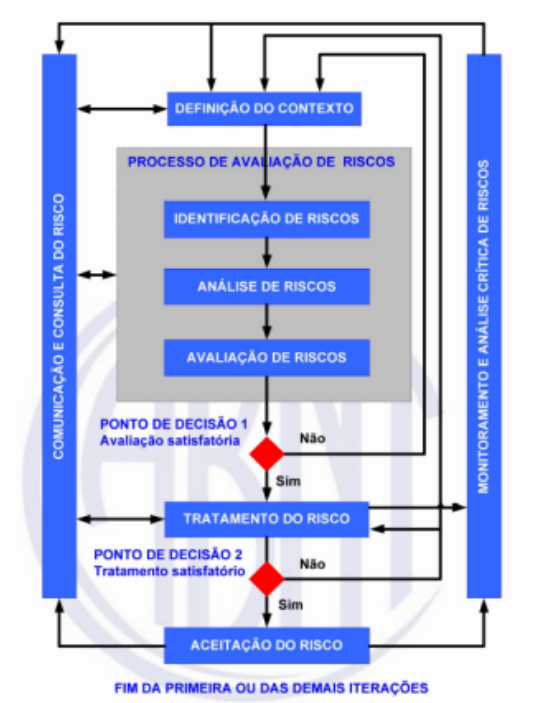


Figura 1. O processo de Gestão de Riscos de TIC - Fonte: ABNT NBR 27005:2019

2.2 Documentos Padronizados de Risco

Documento	Descrição
Plano de gerenciamento dos riscos	O Plano de Gerenciamento dos Riscos tem como objetivo aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto e orientar a equipe do projeto sobre como os processos de riscos serão executados.
Registro dos Riscos	O registro dos riscos é iniciado no processo de Identificar os riscos e é atualizado conforme os outros processos de gerenciamento dos riscos (análise qualitativa, quantitativa, planejar as respostas aos riscos e monitorar e controlar os riscos) são conduzidos, resultando em um aumento no nível e no tipo de informações contidas no registro dos riscos ao longo do tempo.

2.3 Responsabilidade dos Risco da Equipe do Projeto

Membro da Equipe	Responsabilidade
Gestor do Projeto	● Certificar que os riscos foram identificados e tratados de modo a aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto. ● Monitorar os riscos conforme descrito neste plano. ● Divulgar informações pertinentes aos riscos do projeto
ASSEJUR	Assessorar juridicamente o GP em relação às decisões contratuais relacionadas aos riscos.

Comitê de Sustentação Riscos e Segurança do TJAP	● Aprovar o plano de gerenciamento de riscos e suas reservas de contingências. ● Aprovar o uso das reservas de contingência.

São considerados gestores de riscos de TI em seus respectivos âmbitos e escopos de atuação o Comitê de Sustentação Riscos e Segurança de TIC, Gestor de Segurança e Riscos, Secretários de TI (SETIC / SEGES), os Coordenadores, os Chefes de Seção e demais servidores responsáveis pelos processos de trabalho, projetos e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais das Secretarias de TI, independentemente da ocupação de cargo ou função de confiança.

2.4 Ferramentas usadas

Ferramenta	Descrição	Quando Aplicar	Responsável
Brainstorming	Será usado para identificar riscos	No início do projeto e sempre que for necessário revisar os riscos identificados	Gestor do Projeto
Planilha de Identificação dos riscos	Riscos já mapeados e conhecidos	No início do projeto	Gestor do Projeto

3. Identificar os Riscos

3.1 Estrutura Analítica dos Riscos

3.2 Riscos

As principais ameaças e fatores que compõem os cenários de riscos em TI estão mapeados nas tabela abaixo:

Ameaças	Descrição
Ameaças ambientais	● Condições climáticas; ● Alagamentos; ● Tsunamis; ● Incêndios; ● Tempestades e raios; ● Poeira; ● Fumaça; ● Contato com água por meio de vazamentos em encanamentos, telhados, condensação ou ativação de sprinklers; ● Vibração; ● Interferências eletromagnéticas.
Ameaças Físicas	● Acesso não autorizado; ● Roubo; ● Vandalismo; ● Sabotagem; ● Terrorismo; ● Guerra; ● Transporte inadequado; ● Ação externa danosa como exposição à chuva ou aparelhos de raios-X; ● Colisões; ● Quedas.
Ameaças de Infra-estrutura ou de suporte	● Quedas de fornecimento de energia; ● Falha no controle de temperatura; ● Falha no controle de umidade; ● Manutenção inadequada; ● Falta de pessoal; ● Falhas no controle de descarte de material.
Ameaças de ordem técnica	● Procedimentos inadequados; ● Operações inadequadas; ● Configurações de hardware ou software diferentes das recomendadas; ● Modificações de hardware ou software sem autorização; ● Cópia de software, dados ou outras informações;

	● Quantidade de acessos superior ao previsto; ● Classificação de segurança de equipamentos equivocada; ● Falhas de hardware, software, mídia ou serviços de comunicação; ● Reutilização de de objetos (como pen-drives ou discos com informações); ● Modificação acidental de dados (edição, remoção ou inclusão);

Fatores	**Descrição**
Externos	● Fatores de mercado/econômicos ● Velocidade de mudança ● Setor/concorrência ● Situação geopolítica ● Ambiente regulatório ● Status e evolução de tecnologia
Internos	● Importância estratégica de TI ● Complexidade da TI ● Complexidade da entidade ● Grau de mudança ● Capacidade de gestão de mudanças ● Gestão de riscos filosofia e valores ● Modelo operacional ● Prioridades estratégicas
Capacidade de Gestão de Riscos	● Governança de riscos ● Avaliação de riscos ● Resposta ao risco
Capacidade de TI	● Planejar e organizar ● Adquirir e implementar ● Entregar e suportar ● Monitorar e avaliar
Capacidade Corporativa relativa a TI	● Governança de valor ● Gestão de portfólio ● Gestão de investimento

Fonte: ISACA, The Risk IT Practitioner Guide, EUA, 2009

O Anexo I traz a planilha para ser usada na identificação e classificação dos riscos.

4. Análise Qualitativa dos Riscos

4.1 Probabilidade e Impacto dos Riscos

Probabilidade	% de certeza
1-Muito baixa	0 a 20%
2-Baixa	20 a 40%
3-Média	40 a 60%
4-Alta	60 a 80%
5-Muito Alta	>80%

Impacto
1 - Muito Baixo
2 - Baixo
3 - Médio
4 - Alto
5 - Muito Alto

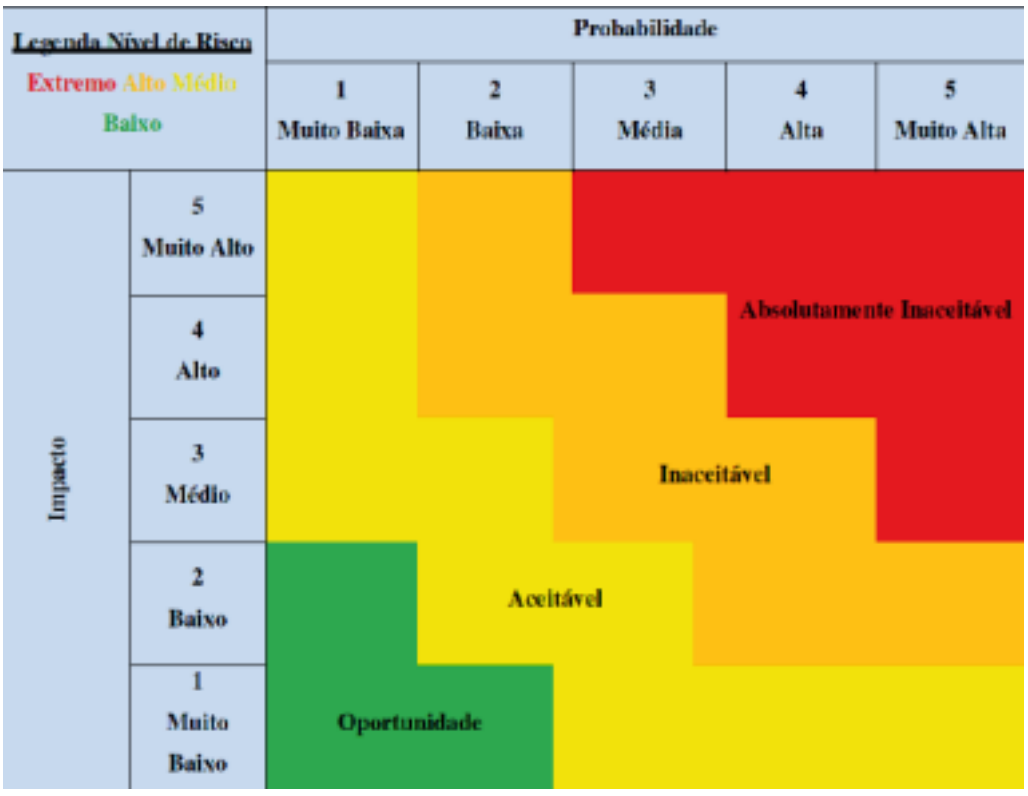
O impacto varia de acordo com a área impactada. Veja o quadro abaixo orientando como classificar o impacto.

Quando um risco impactar mais de uma área, deverá ser usada a área mais impactada.

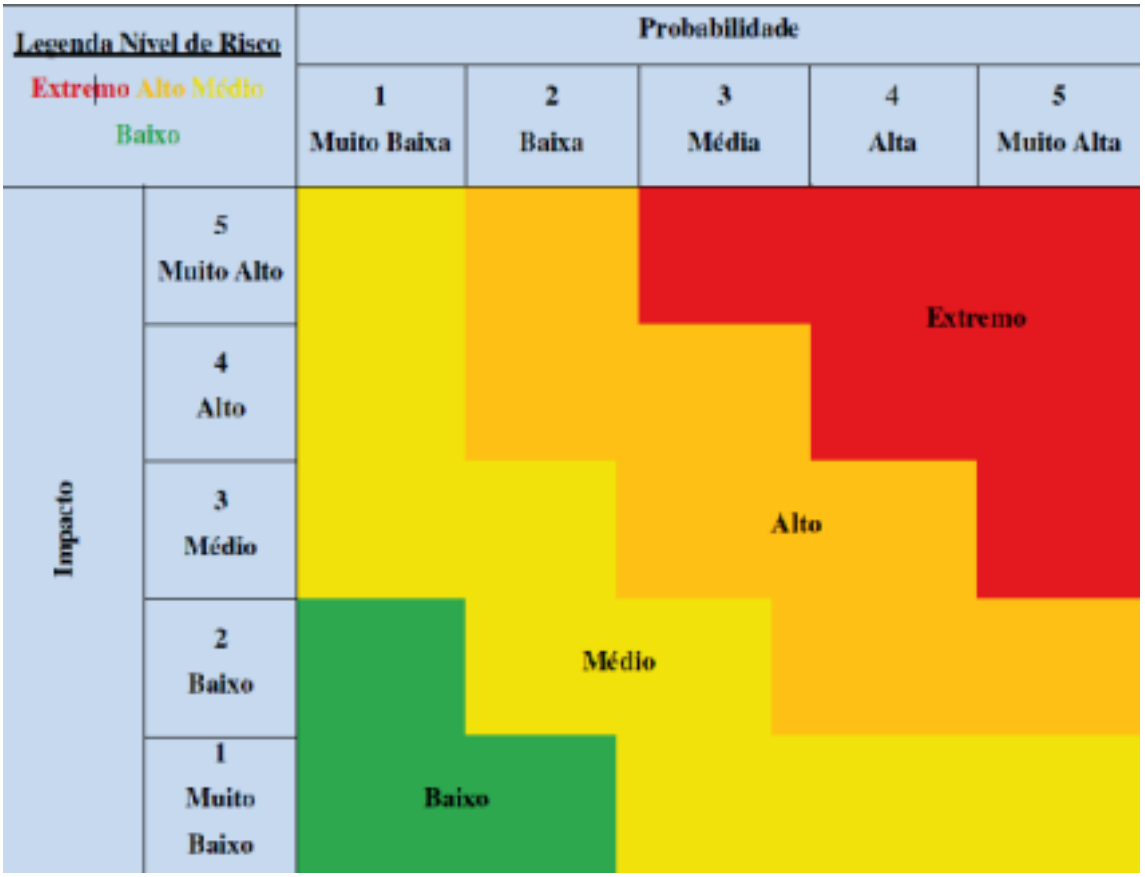
	Muito baixo (Nota = 1)	Baixo (Nota = 2)	Médio (Nota = 3)	Alto (Nota = 4)	Muito alto (Nota = 5)
Custo	Até 2% no orçamento	De 2 a 5% no orçamento	De 5 a 8% no orçamento	De 8 a 10% no orçamento	Acima de 10% no orçamento
Tempo	Até 2% no prazo total	De 2 a 5% no prazo	De 5 a 8% no prazo	De 8 a 10% no prazo	Acima de 10% no prazo
Escopo		Mudança impactará no custo	Mudança impactará no custo e no tempo	Mudança impactará no custo, tempo e qualidade	

O grau do risco (G = I x P) está definido na matriz demonstrada abaixo.

4.2 Matriz Apetite de Risco



4.3 Matriz de Classificação de Riscos



5. Respostas aos riscos

5.1 Estratégias para Riscos Negativos ou Ameaças

Estratégia	Descrição	Exemplo
Eliminar	Remover em 100% a probabilidade que a ameaça ocorra.	Cancelar o projeto;
Transferir	Transferir total ou parcial o impacto em relação a uma ameaça para um terceiro.	Fazer um seguro;
Mitigar	Reduzir a probabilidade e/ou impacto de um risco	Redundância de recursos;

Aceitar	De forma ativa, estabelecendo plano de contingência caso o evento ocorra; ou de forma passiva, o risco será tratado quando ocorrer.	

5.2 Estratégias para Riscos Positivos ou Oportunidades

Estratégia	Descrição
Explorar	Garantir que a oportunidade ocorra para explorar seus benefícios;
Compartilhar	Transferir total ou parcial a propriedade da oportunidade para um terceiro que tem maior capacidade de explorá-la;
Melhorar	Aumentar probabilidade e/ou impacto de uma oportunidade;
Aceitar	Tirar proveito caso a oportunidade ocorra.

6. Controlar os Riscos

O GP e os responsáveis definidos na matriz de responsabilidade (modelo anexo I) devem acompanhar os riscos identificados, monitorar os riscos residuais, identificar novos riscos, executar os planos de respostas a riscos e avaliar sua eficácia durante todo o ciclo de vida do projeto.

O gerente de projeto executa o que foi planejado na análise de riscos e controla os riscos novos identificados durante a execução do projeto.

Este processo consiste em:

- Identificar, analisar, e planejar para riscos novos;
- Monitorar os riscos identificados;
- Analisar novamente os riscos existentes de acordo com as mudanças de contexto;
- Monitorar condições para ativar planos de contingência;
- Monitorar riscos residuais;
- Rever a execução do plano de respostas aos riscos para avaliar sua eficácia;
- Determina se as premissas do projeto ainda são válidas;
- Determinar se as políticas e os procedimentos de gestão de risco estão sendo seguidas;

- Determinar se as reservas de contingência de custo e prazo devem ser modificadas com os riscos do projeto.

Checklist

- Implementar a análise de risco aprovada.
- Identificar novos riscos e gerenciá-los adequadamente.
- Atualizar o plano de resposta de riscos com os riscos novos.

Anexos

Anexo I - Matriz RACI

	CSRS-TIC	Secretários de TI (SETIC / SEGES)	Gerente do Projeto	# Nome1	# Nome 2	#Nome 3
Estabelecer o Contexto Específico						
Identificar os Riscos						
Analisar os Riscos						
Avaliar os Riscos						
Tratar os Riscos						
Elaborar o Plano de Tratamento de Riscos						
Monitoramento e Análise Crítica						
Comunicar e Consultar						
Capacitar Envolvidos						

R - Responsável; A - aprovador; C - consultado; I - informado

Anexo II - Formulário de Identificação e Avaliação dos Riscos

Processo de Trabalho:							Compilado por: Data:				
Objetivo do Processo de Trabalho:							Analisado por: Data:				
Riscos Identificados				Avaliação Risco Inerente			Controles Existentes			Risco Residual	Recomendação para Tratamento do Risco	
ID	Eventos	Causas	Consequências	Probabilidade	Impacto	Nível	Descrição	Eficácia*			Diretriz**	Resposta ao risco
1												
2												

Detalhes sobre Eficácia: Tabela 8 – Definição da Eficácia dos Controles **Detalhes sobre as diretrizes:* Tabela 7 – Diretrizes para Priorização do Tratamento de Riscos

Diretriz
Extremo
Alto
Médio
Baixo

Resposta
Evitar
Mitigar
Aceitar
Transferir

Anexo III - Formulário para Monitoramento e Análise Crítica

Processo de Trabalho:									**Compilado por:** **Data:**		
Objetivo do Processo de Trabalho:									**Analisado por:** **Data:**		
Risco				**Categoria do Risco**	**Controles Existentes***	**Novos Controles***	**Nível do Risco**	**Risco Residual**	**Tendência**	**Melhoria**		
ID	**Eventos**	**Causas**	**Consequências**							**Requerida**	**Responsável**	**Status**
1												
2												
3												
4												
5												

** Se aplicável*

Status da Melhoria
Completo
Em Implementação
Atrasado
Não Aplicável

Tendência
↑ Aumento
↔ Estável
↓ Diminuição

Anexo IV - Formulário para comunicação de Riscos

Processo de Trabalho:				**Compilado por:** **Data:**		
Objetivo do Processo de Trabalho:				**Analisado por:** **Data:**		
Parte Interessada	**Comunicador**	**Propósito**	**Descrição do Risco**	**Método de Comunicação**	**Data da Comunicação**	**Frequência**

Frequência
Ad hoc
Esporádica
Semanal
Mensal
Trimestral
Semestral
Anual

Método de Comunicação
E-mail
Memorando
Ofício
Intranet
Treinamento
Reunião

Propósito
Informar
Consultar

Anexo V - Riscos Identificados comuns

Contexto	Possibilidade de:
Arquitetura de Software	● falha na percepção de restrições tecnológicas ● componentes previstos podem não estar adequados/ajustados às necessidades do projeto ● solução técnica planejada parece não ser viável de ser implantada ● Não validação por parte dos arquitetos dos padrões tecnológicos
Comunicação	● Ausência de Plano de Comunicação ● Baixo engajamento por parte dos envolvidos no projeto ● Atrasos em processos chave de comunicação ● Partes envolvidas não cientes dos desafios do projeto ● Falta de priorização das funcionalidades/necessidades/características do produto ● Responsabilidades da equipe de projeto não delineadas ● Descobrimento de algumas unidades acerca da abrangência do projeto
Custo	● Cancelamento /sustentação do projeto ● flutuação de câmbio ● Redução do orçamento ● Corte no orçamento do projeto
Escopo	● Áreas chave de negócio não envolvidas na definição do escopo do projeto ● Escopo muda constantemente
Gestão	● Complexidade do projeto não mensurada ● Falta de coordenação entre projetos dependentes
Negócio	● Legislação complexa
Gestão de Configuração	● Perda dos documentos de projeto (documentação, produto, fontes e subprodutos) ● Perda /roubo/sabotagem no código fonte ● Falta de documentação adequada
Político	● Pressão política para antecipar a entrega do projeto antes do prazo acordado ● troca dos stakeholders do projeto ● Baixo comprometimento /envolvimento dos stakeholders do projeto ● Usuários da solução estão contra a implementação da solução

Prazo	● Morosidade pode impactar na validação de produtos e subprodutos

	● Morosidade na definição do escopo ● atraso na completude dos marcos do projeto ● Retrabalhos com produção de massa de dados ● Infraestrutura frequentemente indisponível/manutenção em aviso ● Atraso na disponibilização de recursos necessários a equipe de projeto
Qualidade	● Defeitos no software podem não ser detectados até a sua implementação ● Alta taxa de defeito encontrados durante a homologação do produto/subprodutos ● Qualidade dos produtos ou subprodutos não atingem expectativa do cliente
Recursos Humanos	● Indisponibilidade da equipe de projeto ● Férias de pessoa chave na equipe do projeto ● Saída de pessoa chave na equipe do projeto ● Subestimar necessidade de algum tipo de treinamento necessário aos envolvidos no projeto ● Detentor/aprovador de negócio entra em recesso durante o projeto ● Superlocação de algum integrante em atividades do projeto (excesso de horas extras) ● Dificuldade na alocação ou contratação de recursos necessários ao projeto ● Equipe inexperiente para o nível de complexidade do projeto ● Desentendimento entre membros chave da equipe ● Equipe de projeto insatisfeita com remuneração desigual ● Equipe de projeto dispersa/ falta de entrosamento entre membros de equipe.
Requisitos	● Não avaliação de necessidade de migração de dados de sistema legado ● Necessidade de Interface do sistema negligenciada ● Hardware/equipamento disponível não está adequado às necessidades técnicas do projeto ● Escopo não-funcional não foi documentado a contexto

Contratação	● Inclusão de referência de preço inadequada no TR/PB ● A contratação não atende a uma necessidade real da organização ● Contratos com modelos inadequados (principalmente de execução do objeto e de gestão do contrato). ● Estabelecimento de prazo inicial de duração para contrato para prestação de serviços de natureza continuada insuficiente para que a contratada dilua adequadamente os custos iniciais da prestação dos serviços (e.g., montagem de infraestrutura exclusiva para prestação do serviço) ● Estimativa de quantidades maior ou menor que as necessidades da organização. ● Descontinuidade da solução antes do órgão conseguir desfrutar do investimento feito na solução ● Desconsideração dos riscos existentes na contratação e gestão do contrato ● Dificuldades de contato com a contratada para solução de problemas operacionais nos contratos ● Dependência excessiva em relação à contratada ● Falhas na comunicação entre as partes, e ausência de evidências das ocorrências do contrato. ● Não manutenção das condições contratuais nos contratos de execução continuada ou parcelada ● Impossibilidade de aplicação de penalidades ● Vencimento de contratos de natureza continuada sem licitação iniciada/finalizada. ● Recebimento de bens e serviços que não atendem aos requisitos do contrato