PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina
Diretoria-Geral Administrativa
Diretoria de Tecnologia da Informação

PLANO DE GESTÃO DE RISCOS DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PGRTIC

Versionamento do documento

Versão	Atividade	Data	Responsável
2	Criação da nova versão revisada	Jan/2025	Assessoria Técnica
	Aprovação da v2	Abr/2025	Diretor de TI
3	Revisão anual do plano	Fev/2026	Assessoria Técnica
	Aprovação da v3	Mar/2026	Diretor de TI

Introdução

A gestão de riscos de Tecnologia da Informação e Comunicação (TIC) é essencial para assegurar a segurança, continuidade e sucesso das organizações num ambiente cada vez mais tecnológico. A elaboração de um plano de gestão de riscos de TIC é vital para garantir a resiliência e sustentabilidade dos principais serviços prestados pela Diretoria de Tecnologia da Informação (DTI), oferecendo uma abordagem estruturada para lidar com a complexidade e incertezas futuras.

O risco é normalmente expresso em termos de fatores de risco, eventos potenciais, consequências e probabilidades. Os gestores precisam reconhecer e administrar a incerteza em um mundo em constante mudança. Estratégias eficazes de gestão de riscos, aprendizado contínuo e flexibilidade são cruciais para navegar em ambientes incertos. A importância da gestão de riscos se destaca por vários motivos:

a) Fornecimento de informações valiosas para decisões estratégicas;
b) Prevenção e minimização de perdas financeiras e de imagem;
c) Antecipação e gerenciamento proativo de riscos em ambientes complexos;
d) Fortalecimento da continuidade operacional;
e) Adaptação e recuperação rápida diante de adversidades.

Este documento apresenta o Plano de Gestão dos Riscos de TIC em conformidade com o artigo 37 da Resolução CNJ n. 370/2021, que estabelece a Estratégia Nacional de Tecnologia e Comunicação do Poder Judiciário (ENTIC-JUD).

Na elaboração do plano, foram consideradas as diretrizes para a gestão de riscos previstas na ABNT NBR ISO 31000:2018, cujo processo é dividido nas seguintes etapas:

a) Estabelecimento do contexto;
b) Identificação dos riscos;
c) Análise dos riscos;
d) Avaliação dos riscos;
e) Tratamento dos riscos;
f) Monitoramento.

O plano atual apresenta a abordagem de gestão de riscos que será adotada no âmbito tecnológico do Tribunal de Justiça de Santa Catarina (TJSC), particularmente para os sistemas críticos, alinhando-se à determinação do Comitê de Governança de Tecnologia da Informação (COVTI), que o classificou como um sistema crítico. A adoção dessa abordagem possibilita uma gestão de riscos mais eficaz, promovendo a tomada de decisões informadas, o uso eficiente de recursos e o fortalecimento da resiliência organizacional frente a ameaças internas e externas.

Declaração de apetite ao risco

A declaração de apetite ao risco de TIC estabelece o nível de risco que a organização está disposta a aceitar para alcançar seus objetivos estratégicos e operacionais. A inovação e a transformação digital são essenciais para a eficiência e eficácia de nossos serviços, mas isso deve ser equilibrado com a segurança e a continuidade operacional.

A partir do entendimento da cultura de risco e dos valores da instituição, pode ser iniciado o processo de identificação do Apetite ao Risco. É imprescindível que o apetite esteja alinhado ao Planejamento Estratégico Institucional, uma vez que precisa ser definido no nível estratégico da organização.

A declaração de apetite ao risco foi aprovada pelo Comitê de Governança de TI, em reunião ordinário, dia 17/9/2025, e tem por objetivo definir as diretrizes para a resposta, em conformidade com a exposição ao nível do risco definido na matriz NRI.

Exposição	Nível	Diretriz
Muito alto	25	Risco inaceitável. Atuar imediatamente para cessar o fator de risco.
Alto	12-20	Risco inaceitável. Atuar com monitoramento e controle.
Médio	4-10	Risco inaceitável. Atuar apenas com monitoramento.
Baixo	1-2	Risco aceitável.

Escopo

O âmbito da gestão de riscos de TIC engloba a avaliação dos riscos potenciais ligados aos ativos, estrutura, redes, segurança e desenvolvimento que possam impactar a operacionalidade dos sistemas críticos, conforme o agrupamento das áreas demonstrado na tabela a seguir.

ID	Área	Ativo
1	Datacenter	Sala cofre e grupo moto gerador (GMG) do PJSC Monitoramento e sustentação Ambiente de replicação no CIASC
2	Conectividade e segurança	Core de rede Cisco Links de internet Links de comunicação com as comarcas Links de comunicação com o CIASC Firewall Palo Alto
3	Arquitetura física	Primário: 2x servidores HPE DL560 (master e slave) 2x servidores HPE DL560 (VMWare servidores de aplicação) 2x storages HPE 3Par 8450 Secundário: 1x servidor HPE DL560 (slave) 2x servidores HPE DL380 (master e slave) 1x servidor HPE DL380 (slave) 1x storage HPE 3Par 8450

4	Arquitetura lógica	Hypervisor VMWare Servidores de aplicação, balanceamento, sessão, download entre outros Sistema Gerenciador de Banco de Dados (SGBD) MySQL Enterprise Sistema operacional Oracle Linux Server Monitoramento via Zabbix e Grafana
5	Desenvolvimento	Desenvolvimento de novas funcionalidades Manutenção da operação Realização de deploys Integrações com sistemas externos Monitoramento e performance

Papéis e responsabilidades

Todos aqueles que participam dos processos de trabalho do sistema eproc têm a responsabilidade conjunta de gerenciar os riscos. Cada participante, sem distinção de cargo ou atribuição formal, deve contribuir para o reconhecimento e a mensuração dos riscos, bem como para a aplicação de controles internos para redução dos riscos nos processos de trabalho em que opera.

Contudo, no âmbito da gestão de riscos de TIC, para formalizar os controles da primeira linha de defesa da gestão dos riscos de TIC, são definidos os papeis e responsabilidades. A gestão dos riscos é uma responsabilidade compartilhada entre os servidores da DTI cada um em sua área de responsabilidade, devendo atuar na identificação e avaliação dos riscos bem como na implementação de controles internos para mitigação. Para formalizar os controles, são designados como Gestores dos Riscos de TIC os ocupantes dos cargos de Assessores Técnicos e Chefes de Divisão da diretoria

Gestores de Risco de TIC

a) Identificar, analisar, avaliar e gerir os riscos dos processos de trabalho que possuam relação com suas respectivas unidades;
b) Estabelecer e propor procedimentos de controle interno proporcionais aos riscos identificados, observada a relação custo-benefício;
c) Reportar ao NSEC os riscos identificados que eventualmente extrapolem sua competência e capacidade de gerenciamento; e
d) Sempre que necessário e possível criar indicadores para controle dos riscos identificados.

Núcleo de Segurança Cibernética

a) Validar e aprimorar o Plano de Gestão dos Riscos;
b) Validar e aprimorar o Mapa dos Riscos consolidado para que tenha cobertura holística e integrada dos processos de TIC bem como dos objetivos táticos e estratégicos de TIC;
c) Avaliar a probabilidade, o impacto e a resposta adequada de cada risco do Mapa consolidado de Gestão do Riscos em relação aos Objetivos Estratégicos e Táticos de

TIC, garantindo que os controles internos propostos sejam proporcionais ao risco e observem a relação custo-benefício; e

d) Apoiar o gabinete do Diretor de TI na gestão de riscos utilizando-se das metodologias de abordagem do risco.

Diretor de TI

a) Validar o Plano de Gestão de Riscos de TIC;
b) Apoiar as áreas técnicas da DTI na construção do Mapa de Riscos; e
c) Apoiar o NSEC na construção do Plano de Gestão de Riscos de TIC.

Comitê de Governança de Segurança da Informação (CGOVSI)

a) Aprovar o Apetite a Risco da Instituição;

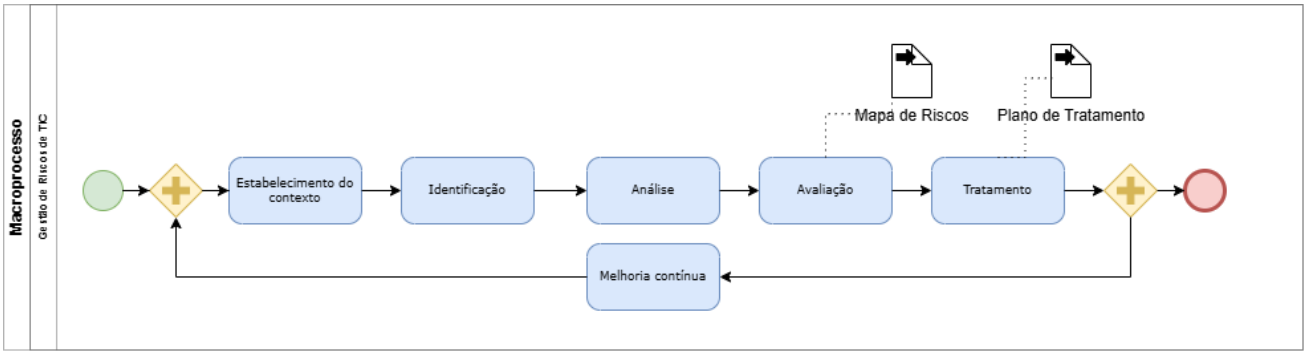
Processo de Gestão de Riscos de TIC

Para o processo de gestão de riscos de TIC no âmbito do TJSC, adotou-se como referência a metodologia descrita na norma ABNT NBR ISO 31000:2018, que estabelece princípios e diretrizes para a gestão de riscos aplicáveis a qualquer tipo de organização. A escolha dessa norma se deu em razão de sua ampla aceitação internacional, abordagem sistemática e flexível, bem como pela aderência às necessidades institucionais de governança, conformidade e melhoria contínua da segurança da informação.

A metodologia da ISO 31000:2018 estrutura o processo de gestão de riscos de forma cíclica e integrada, contemplando as seguintes etapas: estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, monitoramento e revisão, além da comunicação e consulta ao longo de todo o processo. Cada uma dessas etapas é aplicada de maneira contínua e iterativa, promovendo uma visão dinâmica dos riscos e permitindo o aprimoramento das medidas de controle.

No contexto do TJSC, essas diretrizes são aplicadas de forma alinhada ao planejamento estratégico institucional, de modo a garantir que os riscos relacionados aos ativos de informação, processos críticos de TIC e serviços essenciais à atividade jurisdicional sejam devidamente identificados, analisados e tratados. O objetivo é assegurar a continuidade dos serviços, a confidencialidade, integridade e disponibilidade das informações, bem como a conformidade com as normas e regulamentos aplicáveis, incluindo os requisitos de auditoria, controle interno e legislação vigente.

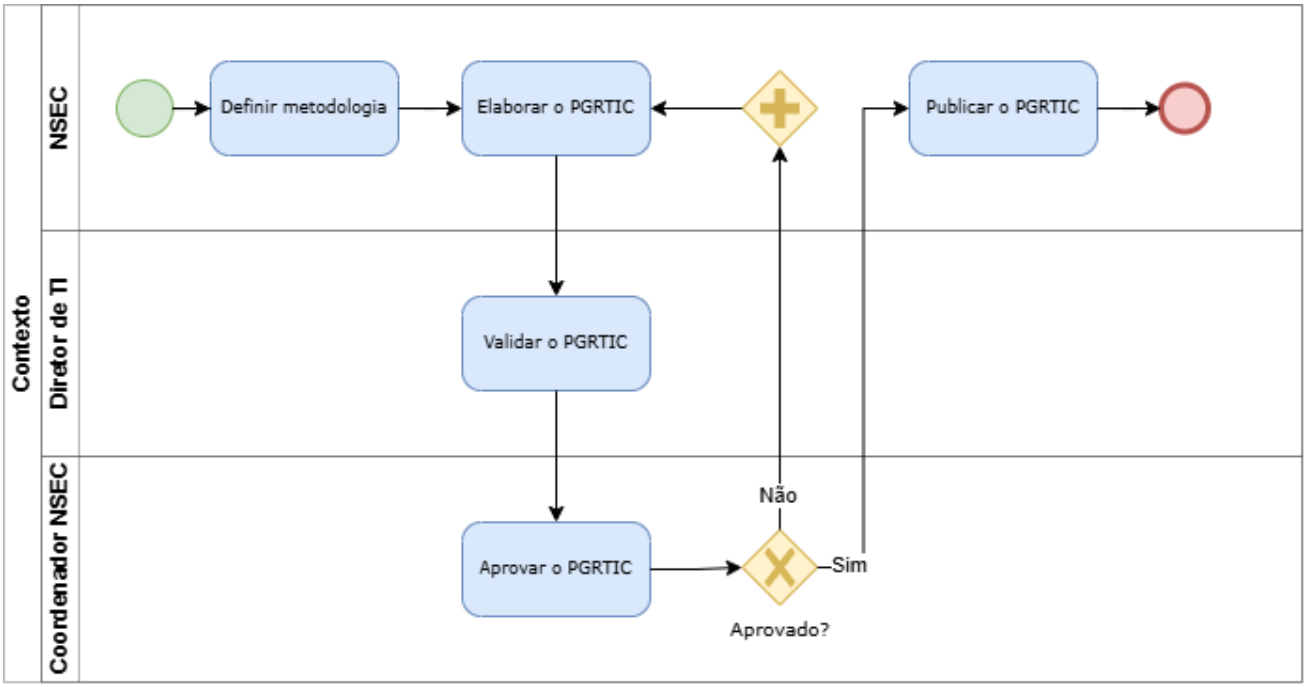
Macroprocesso



Contexto

O processo de contextualização envolve o entendimento tanto do cenário interno quanto externo que circunda o objeto de gerenciamento de riscos, e o reconhecimento dos parâmetros e critérios essenciais ao procedimento de administração de riscos.

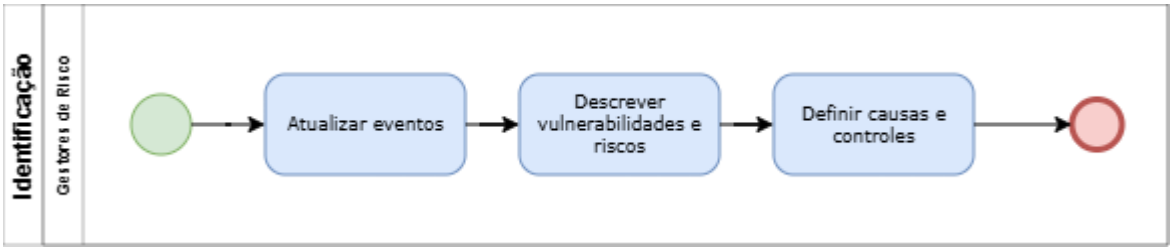
Uma das metodologias de administração mais prevalentes adotadas para essa análise é a técnica SWOT, que delimita forças (*Strengths*), fraquezas (*Weaknesses*), oportunidades (*Opportunities*) e ameaças (*Threats*). Esta técnica contribui significativamente no levantamento dos fatores de risco atrelados à acessibilidade do sistema eproc.



Identificação

A etapa de identificação de riscos envolve reconhecer eventos que podem impactar o eproc e seus processos relacionados. Ela inclui a análise de origens, vulnerabilidades, pontos

fortes, além de elementos concretos e abstratos e fatores temporais. A identificação deve listar e descrever os riscos de TIC, incluindo suas causas potenciais, independentemente de estarem sob o controle do TJSC ou não.



Análise

Envolve a análise da característica do risco e a avaliação do seu nível correspondente, por meio de uma análise da probabilidade de acontecimento e dos potenciais impactos, considerando os controles já em vigor. A probabilidade refere-se à frequência com que se espera que o risco se concretize e ao grau de efeito que ele pode ter. Já o impacto relaciona-se com as possíveis consequências do evento quando o risco se torna realidade.

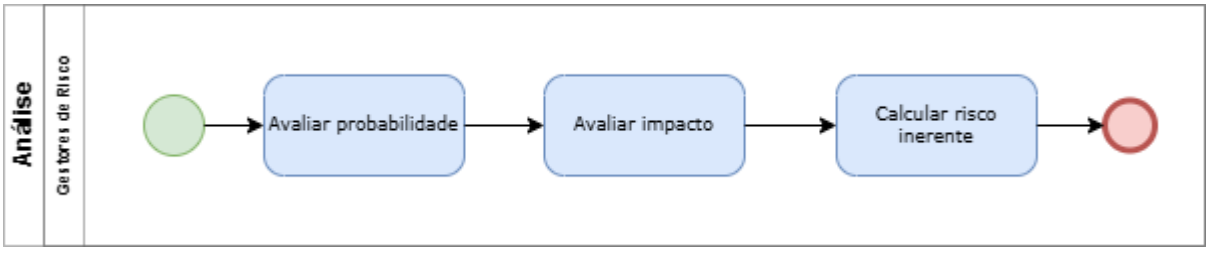


Tabela de probabilidades:

Nível	Probabilidade	Descrição
1	Muito baixa	Evento sem histórico de ocorrência, que pode ocorrer em circunstâncias excepcionais.
2	Baixa	Evento sem histórico de ocorrência, que pode ocorrer ocasionalmente, dependendo das circunstâncias.
3	Média	Evento com histórico de ocorrência, com uma frequência reduzida ou mínima.
4	Alta	Evento com histórico de ocorrência, com uma frequência relativamente baixa.
5	Muito alta	Evento com histórico de ocorrência, com uma alta frequência e que provavelmente irá ocorrer.

Tabela de impactos:

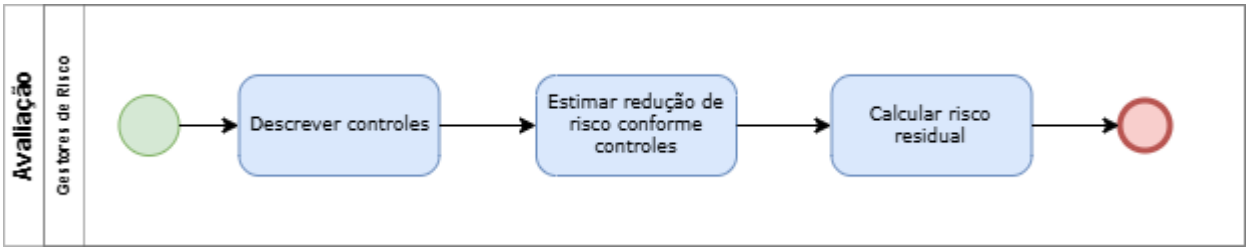
Nível	Impacto	Descrição
1	Muito baixo	Impacto insignificante com danos leves, sem perda de dados, ou paralisação que afete um único usuário ou equipamento.
2	Baixo	Impacto mínimo com danos leves, perda de dados recuperados rapidamente ou paralisação que afete um pequeno grupo.
3	Médio	Impacto médio com perda de dados recuperados em poucas horas ou paralisação que afete um grande grupo sem paralisação total.
4	Alto	Impacto significativo com perda de dados recuperados em até um dia ou paralisação total por algumas horas.
5	Muito alto	Impacto catastrófico com perdas de dados recuperados em dois dias ou mais, paralisação total por mais de um dia em sistemas essenciais.

Após estabelecer os níveis de probabilidade e impacto, conforme tabelas acimas, será possível obter o Nível de Risco Inerente (NRI) de cada evento identificado, a partir do resultado da multiplicação da Probabilidade (P) pelo Impacto (I). A título de exemplo, a depender do apetite a risco da instituição, a tabela NRI resultante seria:

Impacto/ Probabilidade	Muito baixa (1)	Baixa (2)	Média (3)	Alta (4)	Muito alta (5)
Muito alto (5)	(5)	(10)	(15)	(20)	(25)
Alto (4)	(4)	(8)	(12)	(16)	(20)
Médio (3)	(3)	(6)	(9)	(12)	(15)
Baixo (2)	(2)	(4)	(6)	(8)	(10)
Muito baixo (1)	(1)	(2)	(3)	(4)	(5)

Avaliação

Subsequente à análise de riscos, procede-se para a etapa de avaliação. Esta etapa envolve determinar quais riscos exigem atenção e em que ordem devem ser abordados, levando em consideração o apetite ao risco da instituição; isto é, o grau de exposição ao risco que a entidade está preparada para tolerar e a estratégia de mitigação a ser aplicada.



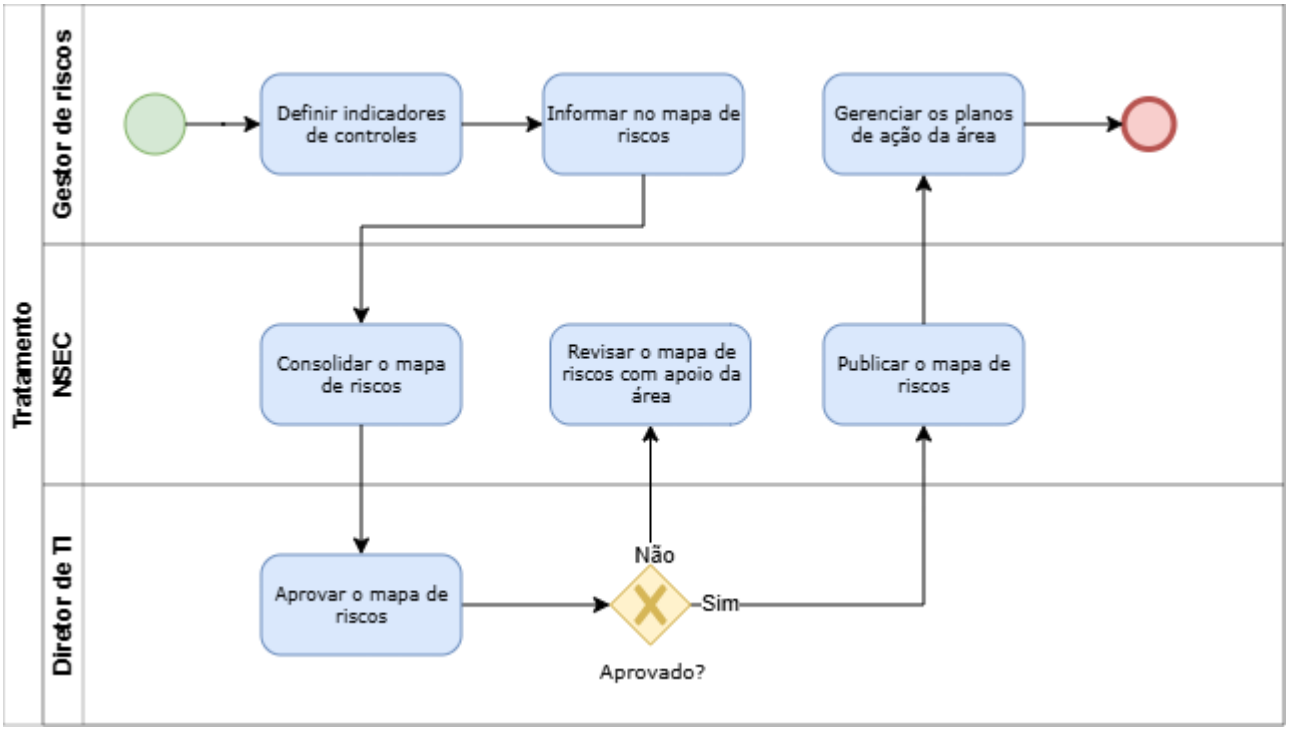
O nível de risco para cada evento identificado se dará de acordo com a classificação da tabela de nível de risco inerente (NRI) e o nível conforme as diretrizes aprovadas pelo apetite à risco da instituição.

Exposição	Nível	Diretriz
Muito alto	25	Risco inaceitável. Atuar para cessar o fator de risco.
Alto	12-20	Risco inaceitável. Atuar com monitoramento e controle.
Médio	4-10	Risco aceitável. Atuar apenas com monitoramento.
Baixo	1-2	Risco aceitável.

Tratamento

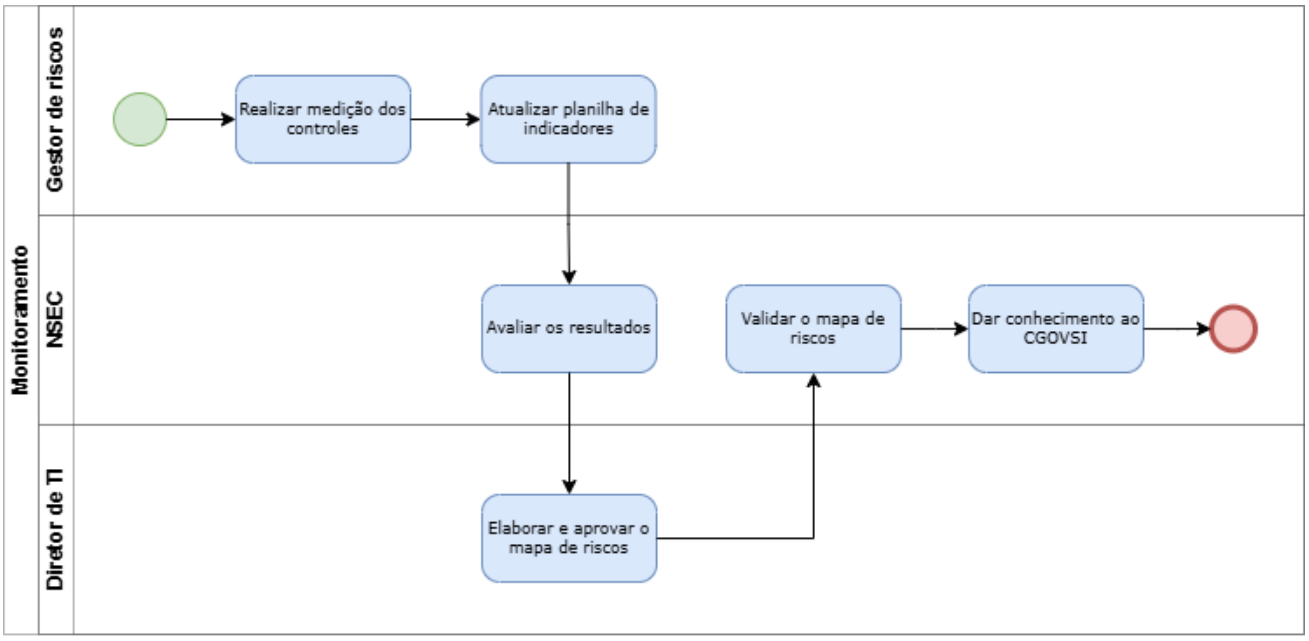
Os riscos identificados serão reportados e compilados no mapa de riscos, identificando os riscos que obtiveram o NRI com exposição alta ou muito alta no apetite a riscos.

Os gestores dos riscos de TIC deverão estruturar um plano de ação visando atividades que possibilitem a reclassificação e projeção futura de probabilidade e/ou impacto. O gestor do risco de TIC gerencia o plano de ação e monitora a evolução do plano de ação até sua conclusão. Após a conclusão do plano de ação é devolvido para o processo de identificar riscos de TIC para a atualização do mapa dos riscos.



Monitoramento

Compreende o acompanhamento e a verificação dos indicadores ou da situação de elementos da gestão dos riscos de TIC, podendo abranger a política, as atividades, os riscos de TIC, os planos de tratamento dos riscos de TIC e os controles.



O monitoramento das ações de tratamento dos riscos envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. O monitoramento deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

O monitoramento consistirá na atualização da análise e avaliação do risco, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas. A medição dos indicadores de controles dos riscos de processos de TIC, unidades e projetos de TIC será realizado pelo respectivo gestor do risco de TIC.

ANEXO I – Descrição dos processos

1. Processo: Contexto

1.2. Objetivo

1.1.1. Estabelecer o contexto interno e externo do gerenciamento de riscos de TIC do PJSC, definindo a metodologia, os critérios e os parâmetros que orientarão todo o processo de administração de riscos, culminando na elaboração, validação, aprovação e publicação do Plano de Gestão de Riscos de TIC (PGRTIC).

1.3. Entradas

1.1.2. Diretrizes institucionais e normativas aplicáveis.
1.1.3. Análise SWOT do ambiente de TIC do PJSC.
1.1.4. Informações sobre o contexto interno (estrutura organizacional, sistemas críticos, capacidade técnica, recursos disponíveis).
1.1.5. Informações sobre o contexto externo (cenário regulatório, ameaças cibernéticas, benchmarks de outros tribunais).
1.1.6. Políticas e regulamentos internos vigentes.

1.4. Saídas

1.1.7. PGRTIC elaborado, validado, aprovado e publicado.
1.1.8. Metodologia de gestão de riscos formalmente definida.
1.1.9. Registro do processo de aprovação (incluindo eventuais ciclos de revisão).

1.5. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Definir metodologia	NSEC	O NSEC define a abordagem metodológica a ser adotada para o gerenciamento de riscos de TIC, incluindo técnicas de análise (ex.: SWOT, matriz de riscos), critérios de avaliação de probabilidade e impacto, e o escopo do PGRTIC.
2	Elaborar o PGRTIC	NSEC	Com base na metodologia definida e no contexto levantado (interno e externo), o NSEC elabora o Plano de Gestão de Riscos de TIC, contemplando identificação de ativos, ameaças, vulnerabilidades, controles existentes e propostas de tratamento.
3	Validar o PGRTIC	Diretor de TI	O Diretor de TI realiza a análise crítica do documento elaborado, verificando a aderência às diretrizes institucionais, a consistência técnica e a completude das informações.
4	Aprovar o PGRTIC	Coordenador NSEC	O Coordenador do NSEC analisa o plano validado e decide pela aprovação ou rejeição.

5	Decisão: Aprovado?	Coordenador NSEC	Sim: o processo segue para publicação. Não: o plano retorna para reelaboração pelo NSEC, reiniciando o ciclo a partir da etapa de elaboração.
6	Publicar o PGRTIC	NSEC	Após aprovação, o PGRTIC é formalmente publicado e disponibilizado aos stakeholders internos, encerrando o processo de contextualização.

2. Processo: Identificação

2.1. Objetivo

2.1.1. Reconhecer e catalogar todos os eventos de risco que possam impactar o sistema eproc e seus processos relacionados, descrevendo suas origens, vulnerabilidades, causas potenciais e controles existentes de modo a subsidiar as etapas subsequentes de análise e avaliação de riscos de TIC.

2.2. Entradas

2.2.2. PGRTIC publicado (saída do processo de Contextualização).
2.2.3. Catálogo de ativos de TIC relacionados ao eproc (infraestrutura, dados, processos, pessoas).
2.2.4. Registros históricos de incidentes e eventos de segurança anteriores.
2.2.5. Resultados de análise SWOT (forças, fraquezas, ameaças e oportunidades).
2.2.6. Informações sobre o ambiente interno (configurações, controles existentes, dependências sistêmicas).
2.2.7. Informações sobre o ambiente externo (ameaças emergentes, vulnerabilidades conhecidas, CVEs publicados).
2.2.8. Fatores temporais relevantes (sazonalidade, janelas de manutenção, prazos processuais críticos).

2.3. Saídas

2.2.9. Catálogo/registro de eventos de risco atualizado.
2.2.10. Lista descritiva de vulnerabilidades e riscos identificados para o eproc.
2.2.11. Mapeamento de causas potenciais por risco identificado.
2.2.12. Registro dos controles existentes associados a cada risco.
2.2.13. Insumos estruturados para a etapa de análise.

2.4. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Atualizar eventos	Gestores de Risco	Os Gestores de Risco revisam e atualizam o inventário de eventos de risco relevantes para o eproc, considerando novas ameaças identificadas, mudanças no ambiente tecnológico, alterações organizacionais e lições aprendidas de incidentes anteriores. Elementos concretos (falhas de hardware, indisponibilidade

			de rede) e abstratos (erro humano, engenharia social) devem ser contemplados, assim como fatores temporais (ex.: períodos de alta demanda processual).
2	Descrever vulnerabilidades e riscos	Gestores de Risco	Para cada evento identificado, os Gestores de Risco descrevem formalmente as vulnerabilidades exploráveis e os riscos associados ao eproc, abrangendo: origens do risco (técnica, humana, ambiental, regulatória), pontos de exposição do sistema, fraquezas de processo ou controle, e a natureza do impacto potencial (disponibilidade, integridade, confidencialidade).
3	Definir causas e controles	Gestores de Risco	Para cada risco descrito, são identificadas as causas potenciais e os controles já existentes (preventivos, detectivos ou corretivos). Essa etapa consolida o registro de risco com as informações necessárias para a análise de probabilidade e impacto na fase seguinte, encerrando o processo de identificação.

3. Processo: Análise

3.2. Objetivo

3.1.1. Analisar as características de cada risco identificado, determinando seu nível por meio da avaliação combinada da probabilidade de ocorrência e do impacto potencial, considerando os controles já em vigor, de modo a calcular o risco inerente e fornecer insumos qualificados para a etapa de avaliação e priorização dos riscos de TIC do eproc.

3.3. Entradas

3.1.2. Catálogo de riscos identificados (saída do processo de Identificação).
3.1.3. Registro de vulnerabilidades e causas potenciais por risco.
3.1.4. Inventário de controles existentes (preventivos, detectivos e corretivos).
3.1.5. Critérios e escalas de probabilidade definidos na metodologia do PGRTIC.
3.1.6. Critérios e escalas de impacto definidos na metodologia do PGRTIC.
3.1.7. Histórico de incidentes e eventos materializados anteriormente.

3.4. Saídas

3.1.8. Registro de probabilidade atribuída a cada risco (com justificativa).
3.1.9. Registro de impacto atribuído a cada risco (com justificativa).
3.1.10. Valor do risco inerente calculado para cada risco (Probabilidade X Impacto).
3.1.11. Matriz de riscos inerentes populada.

3.1.12. Insumos estruturados para a etapa de Avaliação de Riscos.

3.5. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Avaliar probabilidade	Gestores de Risco	Os Gestores de Risco analisam a frequência esperada de materialização de cada risco identificado, atribuindo um nível de probabilidade conforme escala definida na metodologia (ex.: Muito Baixa, Baixa, Média, Alta, Muito Alta). A avaliação considera os controles já existentes, o histórico de ocorrências, a exposição do eproc a ameaças e fatores temporais relevantes.
2	Avaliar impacto	Gestores de Risco	Para cada risco, os Gestores de Risco estimam as consequências de sua materialização sobre o eproc e seus processos relacionados, atribuindo um nível de impacto conforme escala metodológica (ex.: Insignificante, Baixo, Moderado, Alto, Crítico). A avaliação abrange dimensões como indisponibilidade do sistema, comprometimento de dados processuais, danos à imagem institucional e impacto à prestação jurisdicional.
3	Calcular risco inerente	Gestores de Risco	Com base nos valores de probabilidade e impacto atribuídos, os Gestores de Risco calculam o risco inerente de cada evento, aplicando a fórmula ou matriz definida na metodologia do PGRTIC (tipicamente: Risco Inerente = Probabilidade × Impacto). O resultado posiciona cada risco em um nível de criticidade (ex.: Baixo, Médio, Alto, Crítico), subsidiando a priorização na etapa seguinte.

4. Processo: Avaliação

4.2. Objetivo

4.1.1. Determinar quais riscos exigem atenção prioritária e em que ordem devem ser tratados, considerando o apetite ao risco institucional do TJSC e a efetividade dos controles já existentes, de modo a calcular o risco residual.

4.3. Entradas

4.1.2. Registro de riscos inerentes calculados (saída do processo de Análise).
4.1.3. Matriz de riscos inerentes populada.
4.1.4. Inventário de controles existentes (preventivos, detectivos e corretivos) por risco.
4.1.5. Apetite ao risco institucional definido no PGRTIC.
4.1.6. Critérios de aceitabilidade e tolerância ao risco estabelecidos na metodologia.

4.1.7. Estratégias de mitigação disponíveis (mitigar, aceitar, transferir, evitar).

4.4. Saídas

4.1.8. Descrição dos controles associados a cada risco.

4.1.9. Estimativa percentual ou qualitativa de redução de risco proporcionada pelos controles vigentes.

4.1.10. Valor do risco residual calculado para cada risco.

4.1.11. Matriz de riscos residuais atualizada.

4.1.12. Lista priorizada de riscos que requerem tratamento adicional.

4.1.13. Insumos estruturados para a etapa de Tratamento de Riscos.

4.5. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Descrever controles	Gestores de Risco	Os Gestores de Risco documentam formalmente os controles já implementados para cada risco identificado, especificando sua natureza (preventivo, detectivo ou corretivo), abrangência, responsável pela execução e grau de maturidade. Exemplos aplicáveis ao eproc incluem: autenticação multifator, backups automatizados, monitoramento de logs, políticas de acesso e procedimentos de resposta a incidentes.
2	Estimar redução de risco conforme controles	Gestores de Risco	Com base nos controles descritos, os Gestores de Risco estimam o quanto cada conjunto de controles reduz a probabilidade de ocorrência e/ou o impacto do risco, aplicando critérios definidos na metodologia do PGRTIC. Essa estimativa pode ser expressa de forma qualitativa ou quantitativa, considerando a efetividade real e a consistência de aplicação de cada controle.
3	Calcular risco residual	Gestores de Risco	Aplicando a redução estimada sobre o risco inerente, os Gestores de Risco calculam o risco residual de cada evento (o nível de exposição remanescente após os controles vigentes). O resultado é comparado ao apetite ao risco institucional: riscos cujo nível residual supera o limiar de tolerância do TJSC são priorizados para tratamento adicional na etapa seguinte; os demais podem ser formalmente aceitos.

5. Processo: Tratamento

5.2. Objetivo

5.1.1. Estruturar e executar respostas formais aos riscos de TIC que apresentem Nível de Risco Inerente (NRI) com exposição alta ou muito alta, por meio da

definição de indicadores de controle, consolidação e aprovação do mapa de riscos, e gerenciamento de planos de ação orientados à reclassificação da probabilidade e/ou impacto, promovendo a redução contínua da exposição ao risco do eproc e retroalimentando o ciclo de gestão de riscos.

5.3. Entradas

5.1.2. Matriz de riscos residuais com NRI calculado (saída do processo de Avaliação).
5.1.3. Lista priorizada de riscos com exposição alta ou muito alta.
5.1.4. Apetite ao risco institucional e critérios de aceitabilidade definidos no PGRTIC.
5.1.5. Inventário de controles existentes e suas respectivas lacunas.
5.1.6. Histórico de planos de ação anteriores e seus resultados.

5.4. Saídas

5.1.7. Mapa de riscos consolidado, aprovado e publicado.
5.1.8. Indicadores de controle definidos por risco.
5.1.9. Planos de ação estruturados e em execução por área.
5.1.10. Registro atualizado de evolução dos planos de ação.
5.1.11. Retroalimentação para o processo de **Identificação de Riscos**.

5.5. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Definir indicadores de controles	Gestor de Riscos	O Gestor de Riscos define os indicadores que permitirão monitorar a efetividade dos controles associados a cada risco tratado, estabelecendo métricas mensuráveis de acompanhamento (ex.: taxa de disponibilidade do eproc, número de tentativas de acesso não autorizado, tempo médio de resposta a incidentes). Esses indicadores fundamentam a estruturação dos planos de ação.
2	Informar no mapa de riscos	Gestor de Riscos	Os riscos identificados, seus NRIs, controles e indicadores são registrados formalmente no mapa de riscos, garantindo rastreabilidade e visibilidade institucional. Riscos com exposição alta ou muito alta são destacados para tratamento prioritário.
3	Consolidar o mapa de riscos	NSEC	O NSEC consolida as contribuições de todos os Gestores de Risco em um único mapa institucional de riscos de TIC, verificando consistência, completude e alinhamento com a metodologia do PGRTIC.
4	Aprovar o mapa de riscos	Diretor de TI	O Diretor de TI analisa criticamente o mapa consolidado e decide pela aprovação ou rejeição.
5	Decisão: Aprovado?	Diretor de TI	Sim: o processo segue para publicação do mapa. Não: o mapa retorna ao NSEC para revisão com

			apoio das áreas gestoras, reiniciando o ciclo a partir da etapa de revisão.
6	Revisar o mapa de riscos com apoio da área	NSEC	Quando não aprovado, o NSEC realiza revisão colaborativa com os Gestores de Risco das áreas envolvidas, ajustando inconsistências, complementando informações e realinhando os critérios de avaliação antes de nova submissão para aprovação.
7	Publicar o mapa de riscos	NSEC	Após aprovação, o mapa de riscos é formalmente publicado e disponibilizado aos stakeholders institucionais, conferindo transparência e servindo de base para prestação de contas ao CNJ e demais órgãos de controle.
8	Gerenciar os planos de ação da área	Gestor de Riscos	Para os riscos com NRI alto ou muito alto, o Gestor de Riscos estrutura, executa e monitora os planos de ação correspondentes, acompanhando a evolução das atividades até sua conclusão. Após a conclusão, o processo é retroalimentado à etapa de Identificação de Riscos para atualização do mapa e reavaliação do NRI com as novas condições.

6. Processo: Monitoramento

6.2. Objetivo

6.1.1. Acompanhar sistematicamente a efetividade dos controles implementados, a evolução dos indicadores de risco e a situação geral da gestão de riscos de TIC do eproc, por meio da medição periódica, atualização do mapa de riscos e comunicação formal dos resultados ao Comitê de Governança de Segurança da Informação (CGOVSI), assegurando a melhoria contínua e a conformidade com o PGRTIC e as diretrizes do CNJ.

6.3. Entradas

6.1.2. Mapa de riscos publicado (saída do processo de Tratamento).
6.1.3. Planos de ação em execução e seus registros de progresso.
6.1.4. Planilha de indicadores de controles definidos na etapa de Tratamento.
6.1.5. Resultados anteriores de monitoramento (séries históricas de indicadores).
6.1.6. Política de gestão de riscos de TIC e critérios de aceitabilidade do PGRTIC.
6.1.7. Informações sobre novos eventos, incidentes ou mudanças no ambiente de TIC.

6.4. Saídas

6.1.8. Planilha de indicadores atualizada com os resultados das medições.
6.1.9. Avaliação consolidada dos resultados dos controles e planos de ação.

6.1.10. Mapa de riscos revisado, elaborado e aprovado.
6.1.11. Mapa de riscos validado pelo NSEC.
6.1.12. Comunicação formal dos resultados ao CGOVSI.
6.1.13. Insumos para eventual retroalimentação ao ciclo de Identificação ou Tratamento de Riscos.

6.5. Descrição das atividades

Seq.	Atividade	Responsável	Descrição
1	Realizar medição dos controles	Gestor de Riscos	O Gestor de Riscos executa a medição periódica dos controles associados a cada risco monitorado, coletando dados quantitativos e qualitativos sobre sua efetividade. A medição abrange controles técnicos (ex.: disponibilidade do eproc, taxa de falhas de autenticação, cobertura de backups) e controles processuais (ex.: conformidade com procedimentos, execução de treinamentos, cumprimento de prazos dos planos de ação).
2	Atualizar planilha de indicadores	Gestor de Riscos	Com base nas medições realizadas, o Gestor de Riscos registra e atualiza a planilha de indicadores, inserindo os novos valores apurados, comparando-os com as metas e limites estabelecidos no PGRTIC, e sinalizando desvios ou tendências de agravamento que demandem atenção.
3	Avaliar os resultados	NSEC	O NSEC analisa criticamente os indicadores atualizados, avaliando o desempenho geral dos controles, a evolução dos riscos monitorados e o progresso dos planos de ação em execução. Essa avaliação identifica riscos que sofreram alteração de nível, controles ineficazes e necessidades de ajuste na estratégia de tratamento.
4	Elaborar e aprovar o mapa de riscos	Diretor de TI	Com base na avaliação dos resultados, o Diretor de TI elabora e aprova a versão atualizada do mapa de riscos, incorporando as variações identificadas no monitoramento, os novos níveis de risco residual e as recomendações de ajuste nos planos de ação ou controles.
5	Validar o mapa de riscos	NSEC	O NSEC realiza a validação formal do mapa de riscos atualizado e aprovado pelo Diretor de TI, verificando sua consistência metodológica, completude e alinhamento com os critérios do PGRTIC e as exigências do CNJ, antes de sua comunicação ao CGOVSI.

6	Dar conhecimento ao CGOVSI	NSEC	O NSEC apresenta formalmente o mapa de riscos validado ao Comitê de Governança de Segurança da Informação (CGOVSI), garantindo visibilidade institucional sobre o estado da gestão de riscos de TIC, subsidiando decisões estratégicas e registrando o cumprimento dos requisitos de reporte exigidos pelo CNJ e pelo PGRTIC.