PLANO DE RISCOS DE TIC

ENTIC-JUD E PJAC

REVISÃO Abril de 2025

PRESIDENTE
Desembargador Laudivon Nogueira

VICE-PRESIDENTE
Desembargadora Regina Ferrari

CORREGEDOR GERAL DE JUSTIÇA
Desembargador Nonato Maia

PLANO DE RISCO DO PODER JUDICIÁRIO RESOLUÇÃO
TPADM - Nº268/2022

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO RESOLUÇÃO
Nº 291/2023

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Elson Correia de Oliveira Neto

Histórico de Alterações

Data	Versão	Descrição	Autor
01/06/2023	1.0	1ª Revisão do Plano de Riscos de TIC 2023	Assessoria de Governança de TIC
05/07/2024	2.0	2ª Revisão do Plano de Riscos de TIC 2024	Assessoria de Governança de TIC
01/04/2025	3.0	3ª Revisão do Plano de Riscos de TIC 2025	Assessoria de Governança de TIC

INTRODUÇÃO

A importância da tecnologia da informação e comunicação (TIC) para atingir os objetivos estratégicos do tribunal de justiça do estado do acre (TJAC) é indiscutível. Portanto, é imperativo gerenciar os riscos relacionados à área de TIC de maneira eficaz e eficiente. Este documento delineia o plano de gestão de riscos de TIC (PGRTIC) a ser implementado na Diretoria de Tecnologia da Informação e Comunicação (DITEC).

De acordo com a resolução nº 370/2021 do conselho nacional de justiça (CNJ), que estabelece a estratégia nacional de tecnologia da informação e comunicação do poder judiciário (ENTIC-JUD) para o período de 2021 a 2026, o art. 37 prescreve:

"cada órgão deve desenvolver um plano de gestão de riscos de TIC, focado na continuidade dos negócios, na manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, com o objetivo de mitigar as ameaças identificadas e agir de maneira preditiva e preventiva diante das incertezas."

Dentro dessa perspectiva, este plano inclui um conjunto de diretrizes que possibilitam a identificação e implementação das medidas de proteção necessárias para reduzir ou eliminar os riscos associados à Tecnologia da Informação e Comunicação. Isso contribui para fortalecer a governança de TIC, facilitar a tomada de decisões e alcançar os objetivos institucionais.

Para elaboração deste plano foram utilizados os seguintes documentos de referência:

• Resolução CNJ 370/2021;

• Resolução CNJ 396/2021;

• Portaria CNJ 162/2021;

•Resolução 268/2022

• Metodologia de Gestão de Riscos do TJSC;

• Manual de Gestão de Riscos do TCU (2020);

• Manual de Gestão de Riscos do TCU

Plano de Gestão de Riscos para a DITEC/TJAC

1. Introdução

A gestão de riscos é crucial para a DITEC/TJAC, alinhando-se com as melhores práticas e normativas. Este plano visa identificar, avaliar e mitigar riscos de TI, assegurando a continuidade dos serviços e a segurança da informação.

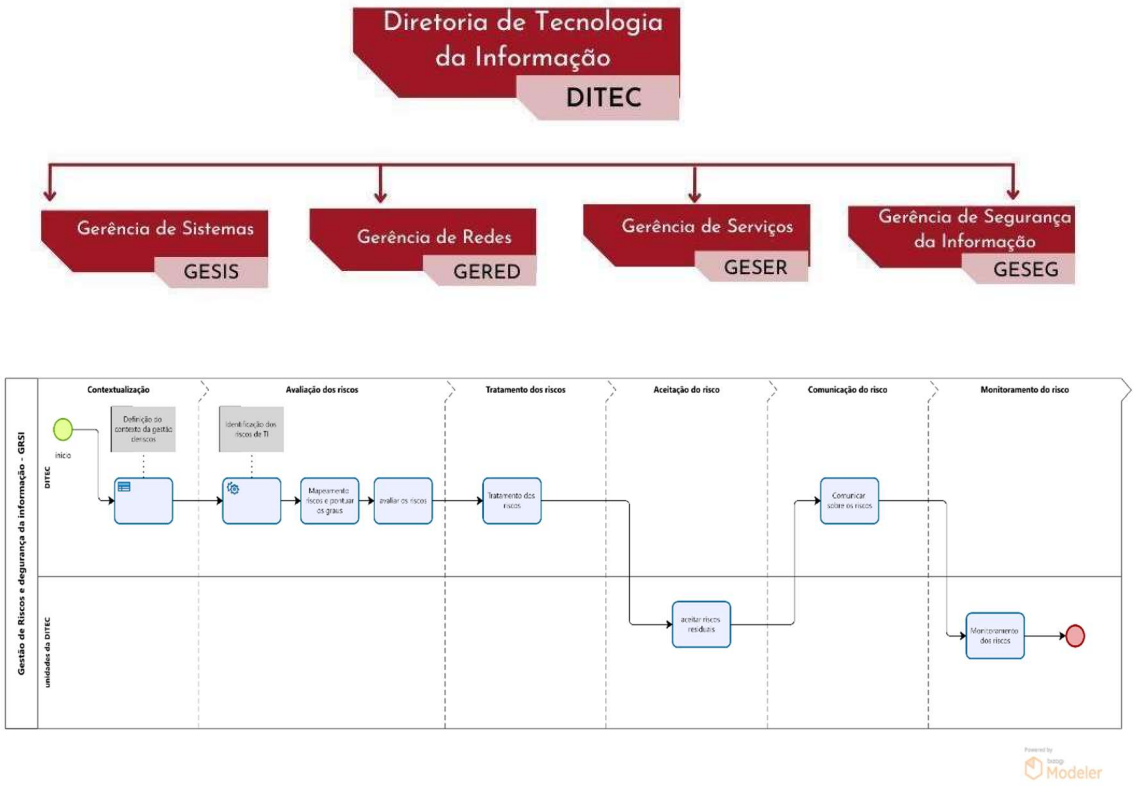

Figura 01 – macroprocesso de gestão de riscos DITEC

2. Objetivos Específicos

- Identificar os riscos de TI que podem impactar os objetivos da DITEC/TJAC.
- Avaliar a probabilidade e o impacto desses riscos.
- Definir ações de tratamento para mitigar ou evitar os riscos.
- Monitorar continuamente os riscos e a eficácia das ações de tratamento.

3. Gestão de Riscos

A gestão de riscos na DITEC/TJAC seguirá as fases estabelecidas pela Resolução Nº 268, 23 de fevereiro de 2022, adaptadas para a realidade do TJAC.

"O Plano de Gestão de Riscos da diretoria de Tecnologia da Informação e comunicação - DITEC do Tribunal de Justiça do Estado do Acre está alinhado com as diretrizes estabelecidas pela Resolução nº 268, 23 de fevereiro de 2022."

3.1 Gestor de Risco da TI

O Secretário (ou Diretor) de Tecnologia da Informação e Comunicação da DITEC/TJAC será o gestor de riscos, responsável por:

- Escolher os processos de trabalho que terão os riscos gerenciados.
- Propor níveis aceitáveis de exposição ao risco.
- Definir as ações de tratamento a serem implementadas.
- Supervisionar o processo e comunicar-se com as partes interessadas.

"Gestor de riscos da TI é representado pelo diretor de Tecnologia da Informação, que possui a responsabilidade de escolher os processos de trabalho e fornecer informações essenciais sobre os riscos durante as etapas subsequentes da metodologia."

3.2 Processos de Gestão de Riscos de TI

"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."

Os processos de gestão de riscos de TI na DITEC/TJAC compreendem as seguintes fases:

I - Estabelecimento do Contexto

- Identificar os objetivos da DITEC/TJAC.
- Definir os fatores externos e internos que podem afetar o alcance dos objetivos (pessoas, sistemas, infraestrutura, legislação, etc.).
- Definir os critérios de riscos a serem considerados:
- Escala de probabilidade: como a probabilidade será medida.
- Escala de impacto: natureza e tipos de consequências.
- Matriz impacto X probabilidade: como o nível de risco será determinado.

Apetite a risco: nível em que um risco se torna aceitável ou inaceitável.

Matriz de classificação de riscos: como os riscos serão classificados.

Diretrizes para priorização e tratamento: como os riscos serão priorizados.

Definição da eficácia dos controles: critérios para análise dos controles.

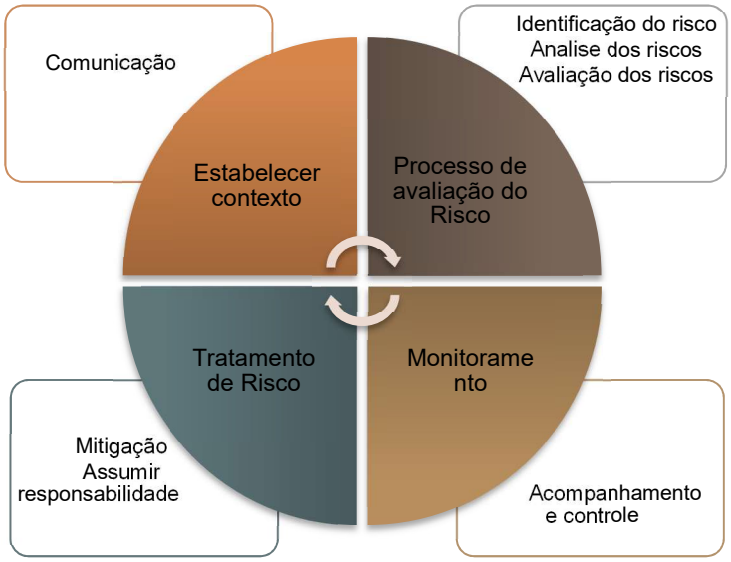

Figura: diagrama do processo

II - Identificação de Riscos

Identificar os riscos que podem causar perdas e como, onde e por que a perda pode acontecer.

Considerar riscos cujas fontes estejam ou não sob controle da organização.

III - Análise de Riscos

Desenvolver uma compreensão detalhada sobre cada risco.

Determinar o nível de risco utilizando a Matriz Probabilidade x Impacto.

Escala de probabilidade: atribuir um grau de probabilidade a cada evento de risco.

Escala de impacto: atribuir um grau de impacto a cada evento de risco.

Calcular o Nível de Risco Inerente (NRI):

- NRI = GP x GI (Grau de Probabilidade x Grau de Impacto)
- Calcular o Nível de Risco Residual (NRR):
- NRR = NRI x FC (Nível de Risco Inerente x Fator de Avaliação dos Controles)

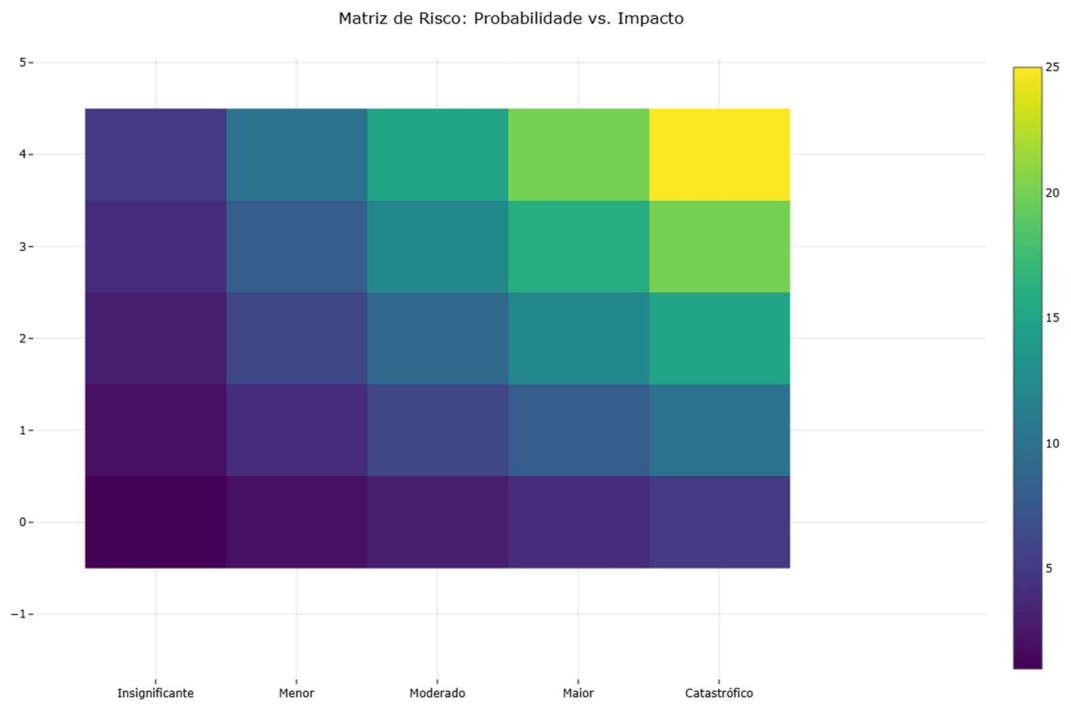

Figura 2 – matriz de risco probabilidade vs. Impacto

"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."

Critérios de impacto	**Critérios de impacto**			
	Financeiro	**Operacional**	**Imagem**	**Legal/regulatório**
Insignificante	Perda financeira insignificante	Redução pequena na eficiência operacional	Impacto ligeiramente negativo	Sem implicações legais ou regulatórias
Menor	Perda financeira moderada	Redução significativa na eficiência operacional	Impacto negativo	Violação legal ou regulatório
Moderado	Perda financeira moderada	Interrupção principal nas operações	Impacto significativamente negativo	Impacto extremamente negativo
Catastrófico	Perda financeira substancial	Interrupção das atividades	Impacto severamente negativo	Consequências legais e regulatórias severas
Nível de impacto	Falha total das operações	Falha total das operações	Sem implicação	

Figura 3 – critérios de impactos

IV - Avaliação de Riscos

Estimar os níveis dos riscos identificados para determinar se o risco é aceitável.

Comparar o nível de risco com o limite de exposição a riscos estabelecido.

V - Tratamento de Riscos

Definir as respostas aos riscos para adequar seus níveis ao apetite estabelecido.

Escolher as medidas de controle associadas a essas respostas:

Evitar o risco: impedir o início ou descontinuar atividades que geram os riscos.

Compartilhar o risco: transferir ou compartilhar o risco com outra parte interessada.

Mitigar o risco: reduzir o impacto ou a probabilidade de ocorrência do risco.

Aceitar o risco: tolerar o risco sem ações específicas.

"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."

VI - Aceitação de Riscos

Aceitar ou tolerar o risco quando o nível é considerado baixo, a capacidade de tratamento é limitada ou o custo é desproporcional ao benefício.

VII - Comunicação e Consulta do Risco

Integrar todas as instâncias envolvidas durante todo o processo de gerenciamento de riscos.

VIII - Monitoramento do Risco

Monitorar e analisar criticamente os riscos para identificar mudanças no contexto e manter uma visão geral dos riscos.

"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."

4. Modelos de Documentos

A DITEC/TJAC deverá adaptar os modelos de documentos utilizados no plano de gestão de riscos, incluindo:

- Relatório de identificação de riscos.
- Matriz de riscos.
- Plano de tratamento de riscos.
- Relatório de monitoramento de riscos.

A gestão de riscos é essencial para a DITEC/TJAC, contribuindo para a melhoria das operações, o atendimento às expectativas da sociedade e a sustentabilidade dos resultados. A implementação eficaz deste plano reduzirá surpresas e prejuízos, garantindo a continuidade e a segurança dos serviços de TI.

5. Comunicação e Treinamento

"Sua principal função é reduzir perdas e impactos negativos, além de identificar oportunidades para viabilizar projetos e alcançar resultados sustentáveis."

A comunicação e o treinamento são essenciais para garantir que todos os membros da DITEC compreendam o plano de gestão de riscos e suas responsabilidades. Isso inclui:

Comunicação: Comunicar o plano de gestão de riscos a todos os membros da DITEC, explicando seus objetivos, processos e responsabilidades.

Treinamento: Fornecer treinamento adequado aos membros da DITEC sobre os princípios da gestão de riscos, a metodologia de avaliação de riscos e as ações de tratamento.

Conscientização: Promover a conscientização sobre a importância da gestão de riscos e seus benefícios para a DITEC.

"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."

6. Integração com Outros Processos

O plano de gestão de riscos deve ser integrado com outros processos da DITEC, como:

Gestão de Projetos: Considerar os riscos em todas as fases do ciclo de vida dos projetos.

Gestão de Mudanças: Avaliar os riscos associados a todas as mudanças na infraestrutura e nos sistemas.

Gestão de Incidentes: Utilizar as informações sobre riscos para prevenir e responder a incidentes de segurança da informação.

Continuidade de Negócios: Integrar o plano de gestão de riscos com o plano de continuidade de negócios para garantir a resiliência da DITEC.

7. Exemplos de Riscos Comuns na DITEC/TJAC

Para ilustrar a aplicação do plano de gestão de riscos, é útil identificar alguns exemplos de riscos comuns na DITEC/TJAC:

Falha de Infraestrutura: Falha de servidores, redes, sistemas de armazenamento ou outros componentes críticos da infraestrutura de TI.

Ataques Cibernéticos: Ataques de hackers, malwares, phishing ou outras ameaças cibernéticas que podem comprometer a confidencialidade, integridade ou disponibilidade dos dados.

Erros Humanos: Erros cometidos por funcionários da DITEC que podem causar perdas de dados, interrupções de serviço ou outros incidentes.

Não conformidade: Não cumprimento de leis, regulamentos ou políticas internas que podem resultar em sanções legais ou financeiras.

Perda de Dados: Perda de dados devido a falhas de hardware, erros humanos, ataques cibernéticos ou outros eventos.

Indisponibilidade de Sistemas: Indisponibilidade de sistemas críticos devido a falhas de hardware, software, ataques cibernéticos ou outros eventos.

8. Ações Práticas para Mitigar Riscos

RESPOSTA AOS RISCOS		
Resposta	Risco negativo	Risco positivo
Aceitar	Nada a fazer, aceitar o risco, acompanhar com a alternativa de criar uma reserva de contingência	Não aproveitar a oportunidade
Evitar/explorar	Eliminar incertezas	Eliminar incertezas
Mitigar /melhorar	Reduzir a probabilidades e/ ou o impacto	Identificar e maximizar as oportunidade de ocorrência
Compartilhar	Transferir a responsabilidade para outra área	Repassar a propriedade para terceiros para melhor capturar as oportunidades

Para cada risco identificado, é importante definir ações práticas para mitigar ou evitar o risco. Alguns exemplos de ações práticas incluem:

Implementar Controles de Acesso: Implementar controles de acesso rigorosos para proteger os dados e sistemas contra acesso não autorizado.

Realizar Backups Regulares: Realizar backups regulares dos dados e sistemas para garantir a recuperação em caso de perda de dados.

Implementar Firewalls e Sistemas de Detecção de Intrusão: Implementar firewalls e sistemas de detecção de intrusão para proteger a rede contra-ataques cibernéticos.

Realizar Testes de Segurança: Realizar testes de segurança periódicos para identificar vulnerabilidades nos sistemas e na infraestrutura.

Fornecer Treinamento de Segurança: Fornecer treinamento de segurança regular aos funcionários da DITEC para conscientizá-los sobre as ameaças cibernéticas e as melhores práticas de segurança.

Implementar Políticas de Segurança: Implementar políticas de segurança claras e abrangentes para orientar o comportamento dos funcionários e proteger os dados e sistemas.

Monitorar Logs de Auditoria: Monitorar os logs de auditoria para identificar atividades suspeitas ou não autorizadas.

Implementar Planos de Recuperação de Desastres: Implementar planos de recuperação de desastres para garantir a continuidade dos negócios em caso de eventos catastróficos.

Ao detalhar esses aspectos adicionais, o plano de gestão de riscos da DITEC/TJAC se tornará mais completo, eficaz e adaptado às necessidades específicas do tribunal. Isso garantirá que os riscos de TI sejam gerenciados de forma proativa e que a DITEC possa cumprir sua missão de forma segura e eficiente.

9. Monitoramento e Revisão Contínua

O monitoramento e a revisão contínua são cruciais para garantir que o plano de gestão de riscos permaneça eficaz e relevante ao longo do tempo. Isso inclui:

Monitoramento Regular: Monitorar regularmente os riscos identificados, as ações de tratamento implementadas e os indicadores de desempenho para identificar quaisquer desvios ou problemas.

Revisão Periódica: Revisar periodicamente o plano de gestão de riscos para garantir que ele esteja atualizado e alinhado com as mudanças no ambiente de negócios, nas tecnologias e nas ameaças.

Auditoria Interna: Realizar auditorias internas periódicas para avaliar a eficácia do plano de gestão de riscos e identificar áreas de melhoria.

Relatórios de Desempenho: Elaborar relatórios de desempenho periódicos para comunicar os resultados da gestão de riscos às partes interessadas.

"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."

10. Responsabilidades e Funções

Definir claramente as responsabilidades e funções de cada membro da DITEC em relação à gestão de riscos é fundamental para garantir a eficácia do plano. Isso inclui:

Gestor de Riscos (Secretário/Diretor de TI): Responsável por supervisionar todo o processo de gestão de riscos, definir as políticas e diretrizes, e garantir que o plano seja implementado e monitorado.

Equipe de Segurança da Informação: Responsável por identificar e avaliar os riscos de segurança da informação, implementar as medidas de segurança adequadas e monitorar a eficácia dessas medidas.

Equipe de Infraestrutura de TI: Responsável por garantir a disponibilidade, confiabilidade e segurança da infraestrutura de TI, incluindo servidores, redes, sistemas de armazenamento e outros componentes críticos.

Equipe de Desenvolvimento de Sistemas: Responsável por garantir que os sistemas sejam desenvolvidos e mantidos de forma segura, seguindo as melhores práticas de segurança e as políticas internas.

Todos os servidores da DITEC: Responsáveis por seguir as políticas e procedimentos de segurança, relatar quaisquer incidentes de segurança e participar de treinamentos de conscientização sobre segurança.

11. Ferramentas e Tecnologias

A utilização de ferramentas e tecnologias adequadas pode facilitar a implementação e o monitoramento do plano de gestão de riscos. Isso inclui:

Software de Gestão de Riscos: Utilizar software de gestão de riscos para automatizar o processo de identificação, avaliação, tratamento e monitoramento de riscos.

Ferramentas de Análise de Vulnerabilidades: Utilizar ferramentas de análise de vulnerabilidades para identificar vulnerabilidades nos sistemas e na infraestrutura.

Sistemas de Detecção de Intrusão: Utilizar sistemas de detecção de intrusão para monitorar a rede e os sistemas em busca de atividades suspeitas ou maliciosas.

Ferramentas de Monitoramento de Logs: Utilizar ferramentas de monitoramento de logs para coletar e analisar os logs de auditoria dos sistemas e aplicativos.

12. Considerações Finais

A gestão de riscos é um processo contínuo e dinâmico que requer o envolvimento de todos os membros da DITEC. Ao implementar este plano de gestão de riscos adaptado, a DITEC/TJAC estará melhor preparada para proteger seus ativos de informação, garantir a continuidade dos serviços e cumprir sua missão de forma segura e eficiente.

Anexos:

ANÁLISE DE AMBIENTE FIXAÇÃO DOS OBJETIVOS ALINHAMENTO ESTRATÉGICO- PROCESSOS DE TRABALHO Formulário elaborado a partir do plano de risco				
Unidade:				
Estrutura Organizacional: Diretoria de Tecnologia da Informação				
OBJETIVOS ESTRATÉGICOS/ INDICADORES ESTRATÉGICOS				
Objetivo Estratégico	Indicadores Estratégico			
	Descrição	Finalidade	meta	
OBJETIVOS ESTRATÉGICO/CARTEIRA DE TRABALHO				
Objetivo estratégico	Projetos estratégicos			
	Descrição		Objetivo	
Processos de trabalho da unidade (citar todos os processos de trabalho da unidade constante da cadeia de valor)				
Macroprocesso	Processos	Descrição do processo	Entregas por processo	Clientes por processo

PROCESSO DE TRABALHO DA UNIDADE/ALINHAMENTO ESTRATÉGICO (destacar os processos de trabalho constante da cadeia de valor que tem algum indicador e/ou projeto estratégico associado)			
referência	Processo de trabalho	Indicador estratégico associado	Projeto estratégico associado
Processo 1			
Processo 2			
Processo 3			
Processo 4			
Processo 5			

RELATO SINTÉTICO DO CONTEXTO DO PROCESSO DE TRABALHO	
Dados do processo:	Ciclo do gerenciamento de riscos: Unidade: Processo de trabalho:
DOCUMENTAÇÃO DO CONTEXTO DO PROCESSO DE TRABALHO	
Relevância estratégica (importância relativa ou o papel desempenhado pelo processo de trabalho no alcance dos objetivos estratégicos) :	
Estrutura responsável	
Principais rotinas e suas formas de execução	
Materialidade (montante de recursos orçamentários ou financeiros alocados no processo.	
Sistemas informatizados utilizados:	
Controles existentes e suas formas de execução:	
Criticidade (vulnerabilidades, fraquezas, situações críticas efetivas ou potenciais já identificadas):	

TRIBUNAL DE JUSTIÇA
Diretoria de Tecnologia da Informação e Comunicação

www.tjac.jus.br
Rua Tribunal de Justiça, s/n. Via Verde. 69.920-193
Rio Branco-AC | (68) 3302-0360 / 3302-0361