PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PGRTIC 2024

Data: *05/03/2024*

Versão 3.0

Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário do Estado de Pernambuco

Presidente do Tribunal de Justiça do Estado de Pernambuco (gestão 2022- 2024)
Desembargador Ricardo Paes Barreto

1° Vice-Presidente
Desembargador Fausto Campos

2° Vice-Presidente
Desembargador Eduardo Sertório

Corregedor-Geral da Justiça
Desembargador Francisco Bandeira de Mello

Secretaria de Tecnologia da Informação e Comunicação
Juliana Neiva de Gouvêa Ribeiro

Equipe Técnica na elaboração deste documento (servidores do SETIC)

Diego Augusto de Araújo Madeira
Iveruska Carmem Jatobá Basto
Justiniano Frederico Saraiva Vasconcelos
Marcelo Ferreira de Lima
Moisés Neves Camêlo

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Autor(es)	Descrição
1.0	23/03/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Criação do Documento
1.1	02/03/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Sugestão do processo de gestão de riscos e inserir matriz RPCI.
1.2	14/03/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Validar sugestões de alterações no processo de gestão de riscos.
1.3	10/04/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Ajustar processo de gestão de riscos e suas atividades.
1.4	07/06/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Ajuste final para aumentar fonte do processo, corrigir nome da tarefa e inserir texto introdutório sobre os perfis e reponsabilidades.
1.5	10/08/2023	AGTIC – Assessoria de Governança de Tecnologia da Informação	Mudança de nomenclatura de G7 para G9.
1.6		AGTIC – Assessoria de Governança de Tecnologia da Informação	Apresentado ao G9 o plano de gestão de riscos, correções com os apontamentos do G9 e publicação.
3.0	05/03/2024	AGSI – Assessoria de Gestão de Segurança da Informação	Atualizar o documento para o ano de 2024, como: nova composição da mesa diretora do TJPE, responsáveis e atores.

SUMÁRIO

TABELAS

FIGURAS

1. APRESENTAÇÃO

Este documento está estruturado da seguinte forma:

- Objetivos;
- Benefícios e resultados no processo de gestão de riscos;
- Abreviações e definições;
- Referências normativas;
- Fluxo do processo;
- Responsabilidades;
- Metodologia do processo de gestão de riscos de TIC;
- Principais tratados;
- Plano de ação sobre riscos de TIC;
- Considerações finais;
- Anexos

Como também os demais aspectos do **Plano de Gestão de Riscos de TIC**, de forma alinhada às diretrizes institucional de Política de Segurança da Informação e Gestão de Riscos do TJPE, além de servir de referência na sua execução.

Diante disso, os riscos associados à área de TI devem ser gerenciados de forma eficiente e eficaz. Este documento define o Plano de Gestão de Riscos de TIC (PGRTIC) que deverá ser aplicado na Secretaria de Tecnologia da Informação e Comunicação (SETIC).

A Resolução nº 370/2021 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), para o período 2021 a 2026, dispõe no Art. 37 que “Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas”

Nesse contexto, o presente plano contempla um conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos associados à Tecnologia da Informação e Comunicação, contribuindo para o fortalecimento da governança de TIC, a tomada de decisões e o alcance dos objetivos institucionais.

2. OBJETIVO

Este documento visa direcionar as ações da Secretaria de Tecnologia da Informação e Comunicação (SETIC), em cumprimento às diretrizes da Instrução de Serviço para tratamento da Gestão de Riscos de Tecnologia da Informação e Comunicação do Tribunal de Justiça de Pernambuco de Nº001 de 05 de outubro de 2017.

Estabelecendo conceitos, obrigações, responsabilidades e definição de diretrizes para processo de gerenciamento de riscos de uso interno da Secretaria de Tecnologia da Informação e Comunicação (SETIC).

Como também visa a aplicabilidade em toda a SETIC do TJPE, e abrange todas as áreas: infraestrutura de TI, redes, segurança da informação, suporte técnico, manutenção de equipamentos e soluções de TI, desenvolvimento de sistemas, governança e gestão de TI.

O escopo da Gestão de Riscos de TIC é o de analisar os possíveis riscos relacionados aos processos e aos ativos de TIC que podem afetar os objetivos estratégicos da organização.

Este documento está alinhado com o Planejamento Estratégico Institucional e o Plano Diretor de TIC, referente ao ciclo de 2022 - 2024, sendo objeto de revisão periódica anual, buscando adequações à realidade do órgão e da sociedade e de mudanças do Judiciário.

3. BENEFÍCIOS E RESULTADOS NO PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos de segurança da informação é fundamental para garantir a proteção adequada de dados e sistemas contra ameaças externas e internas. A gestão de riscos envolve a identificação, avaliação e tratamento dos riscos de segurança que podem afetar o TJPE.

Existem vários benefícios e resultados associados à implementação de um processo de gestão de riscos de segurança da informação, incluindo:

- Melhoria da segurança da informação: ajuda a garantir que as informações estejam protegidas adequadamente contra ameaças e permite que o TJPE identifique áreas de vulnerabilidade e tome medidas proativas para mitigar os riscos.
- Conformidade regulatória: muitas regulamentações, como a LGPD, exigem que as organizações implementem medidas de segurança adequadas para proteger dados pessoais e informações sensíveis. Um processo de gestão de riscos de segurança da informação pode ajudar o TJPE a cumprir essas regulamentações e evitar sanções.
- Melhoria da eficiência operacional: pode ajudar na identificação áreas onde os processos podem ser melhorados. Isso pode resultar em maior eficiência operacional e redução de custos.

Como:

- Gerir os riscos de TIC do TJPE;
- Plano de Riscos de TIC atualizado, sendo realizadas revisões periodicamente;
- Propiciar a melhoria contínua na SETIC;
- Reduzir as surpresas e os prejuízos operacionais;
- Aproveitar oportunidades;
- Dinamismo e interatividade durante todo o processo;

4. ABREVIAÇÕES E DEFINIÇÕES

ABREVIAÇÕES:

- **CNJ**: Conselho Nacional de Justiça
- **SETIC**: Secretaria de Tecnologia da Informação e Comunicação
- **ENTIC-JUD**: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
- **PCSTIC**: Plano de Contratações de Solução de TIC
- **PCTIC**: Plano de Capacitação de TIC
- **PDTIC**: Plano Diretor de Tecnologia da Informação e Comunicação
- **PSI**: Política de Segurança da Informação
- **PTD**: Plano de Transformação Digital
- **SEI**: Sistema Eletrônico de Informações
- **SIC**: Segurança da Informação e Comunicação
- **TCU**: Tribunal de Contas da União
- **TIC**: Tecnologia da Informação e Comunicação

DEFINIÇÕES:

Ameaça: causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades.

Apetite a risco: nível de risco que a instituição está disposta a aceitar para atingir os objetivos identificados no contexto analisado.

Ativos de TIC: qualquer elemento de valor para organização, seja tangível ou intangível, que esteja relacionado à Tecnologia da Informação e Comunicação.

Causa de Risco: razão que pode promover a ocorrência do risco.

CGTIC – Comitê de Governança de Tecnologia da Informação e Comunicação: comitê responsável por apoiar e orientar as iniciativas, projetos e investimentos em Tecnologia da Informação e Comunicação, observando a estratégia institucional, dentre outros.

CGESTIC – Comitê Gestor de Tecnologia da Informação e Comunicação: comitê responsável pelos planos táticos e operacionais, análise de demandas, acompanhamento da execução de planos, estabelecimento de indicadores operacionais, dentre outros.

CGSI – Comitê de Gestão de Segurança da Informação: comitê responsável por apreciar, assessorar e aprovar a implementação das ações de segurança da

informação e garantir a implementação da Política de Segurança de Tecnologia da Informação.

Consequências: resultado de um evento que afeta os objetivos estabelecidos.

Escopo: é a soma total de todos os produtos do processo de trabalho e seus requisitos ou características.

Evento: incidente ou ocorrência originada a partir de fontes internas ou externas que afetem a implementação da estratégia ou a realização dos objetivos.

Fonte de Risco: elemento que, individualmente ou combinado, tem potencial para dar origem a um risco específico, podendo ou não estar sob controle.

Impacto: efeito da ocorrência do evento nos objetivos.

Gestão de Riscos: processo contínuo aplicado a toda a instituição que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, tratar e monitorar eventos em potencial, contribuindo para a sua redução ou neutralização.

Matriz de Riscos: representação formal na qual são registrados os riscos identificados, considerando as probabilidades e os impactos, de forma a permitir a definição das ações necessárias ao seu gerenciamento.

Nível de Risco: representação numérica da magnitude do risco, que é expressa pelo produto das variáveis “impacto” e “probabilidade”.

Parte interessada (*Stakeholder*): pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Plano de Contingência: documento que apresenta detalhadamente os procedimentos e recursos a serem utilizados em caso de ocorrência de eventos que possam afetar a segurança de pessoas, do patrimônio ou de sistemas de informação, bem como outros que possam interromper a continuidade da prestação de serviços jurisdicionais.

Probabilidade: possibilidade de ocorrência do evento.

Risco: evento capaz de afetar positiva ou negativamente os objetivos e metas do Poder Judiciário do Estado de Pernambuco.

Risco-Chave: risco com elevado impacto nos objetivos da instituição.

Risco Inerente: é aquele ao qual a instituição está exposta, considerando os controles existentes, mas quando não são estabelecidos nem adotados tratamentos para alterar a probabilidade ou o impacto dos eventos.

Risco Residual: risco remanescente após estabelecimento e adoção de tratamento.

5. REFERÊNCIAS NORMATIVAS

ID	Documento	Descrição
RN01	CNJ - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD), no período de 2021-2026.	Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD), no período de 2021-2026. Resolução nº 370 do CNJ, 28/01/2021.
RN02	CNJ - Política de Governança das Contratações Públicas no Poder Judiciário.	Dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário. Resolução nº 347 do CNJ, 13/10/2020.
RN03	Política de Segurança de Tecnologia da Informação do TJPE.	Dispõe sobre a Política de Segurança de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado de Pernambuco, e estabelece competências administrativas aos seus órgãos integrantes. Objetiva instituir responsabilidades e diretrizes corporativas para a proteção dos ativos de Tecnologia da Informação e a prevenção de responsabilidade legal para todas as autoridades judiciais, servidores e usuários do Poder Judiciário do Estado do Pernambuco. Resolução nº 349 de 04 de março de 2013, publicado no Diário de Justiça Eletrônico no dia 05 de março de 2013 na edição nº42/2013.
RN04	Instrução de serviço para tratamento de gestão de riscos de tecnologia de informação e comunicação do TJPE.	Estabelecimento de conceitos, obrigações e responsabilidades e definição de diretrizes para processo de gerenciamento de riscos de uso interno da Secretaria de Tecnologia da Informação e Comunicação (SETIC). Instrução de serviço de nº 001/2017, publicado no Diário de Justiça Eletrônico no dia 10 de outubro de 2017 na edição nº186/2017.

ID	Documento	Descrição
RN 05	Política de Proteção aos Dados Pessoais, conforme a Lei nº 13.709/2018 (LGPD).	Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.
RN 06	Comitê de Gestão de Segurança da Informação	Instituir o Comitê de Gestão da Segurança da Informação no âmbito do poder judiciário do Estado de Pernambuco. Publicado na portaria de nº16 de 16 de julho de 2022.
RN 07	Comitê de Governança e Tecnologia da Informação e Comunicação (CGTIC)	Institui o Comitê Governança de Tecnologia da Informação e Comunicação (CGTIC) do Poder Judiciário de Pernambuco. Resolução de nº388, de 25 de agosto de 2016.
RN 08	Comitê Gestor de Proteção de Dados (CGPD)	Institui o Comitê Gestor de Proteção de Dados e define suas diretrizes no âmbito do Tribunal de Justiça do Estado de Pernambuco. DJE nº 166/2020 de 15 de setembro de 2020
RN 09	ABNT NBR ISO/IEC 31000:2018	ABNT NBR ISO/IEC 31000:2018 – Gestão de riscos – Diretrizes.
RN 10	ABNT NBR ISO/IEC 27005:2019	ABNT NBR ISO/IEC 27005:2019 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.
RN 11	Manual de Gestão	Manual de Gestão de Riscos do TCU (2020). Disponível em: https://portal.tcu.gov.br/, acessado em 07/03/2023.

	de Riscos do TCU.	
RN 13	Processo de Gestão de Riscos do STJ	Disponível no link https://www.stj.jus.br/static_files/STJ/Institucional/Gest%C3%A3o%20estrat%C3%A9gica/6_gestao_riscos_21jun.pdf , acessado em 08/06/2023.

Tabela 1 - Documentos de Referência para elaborar o PGRTIC do TJPE

6. FLUXO DO PROCESSO

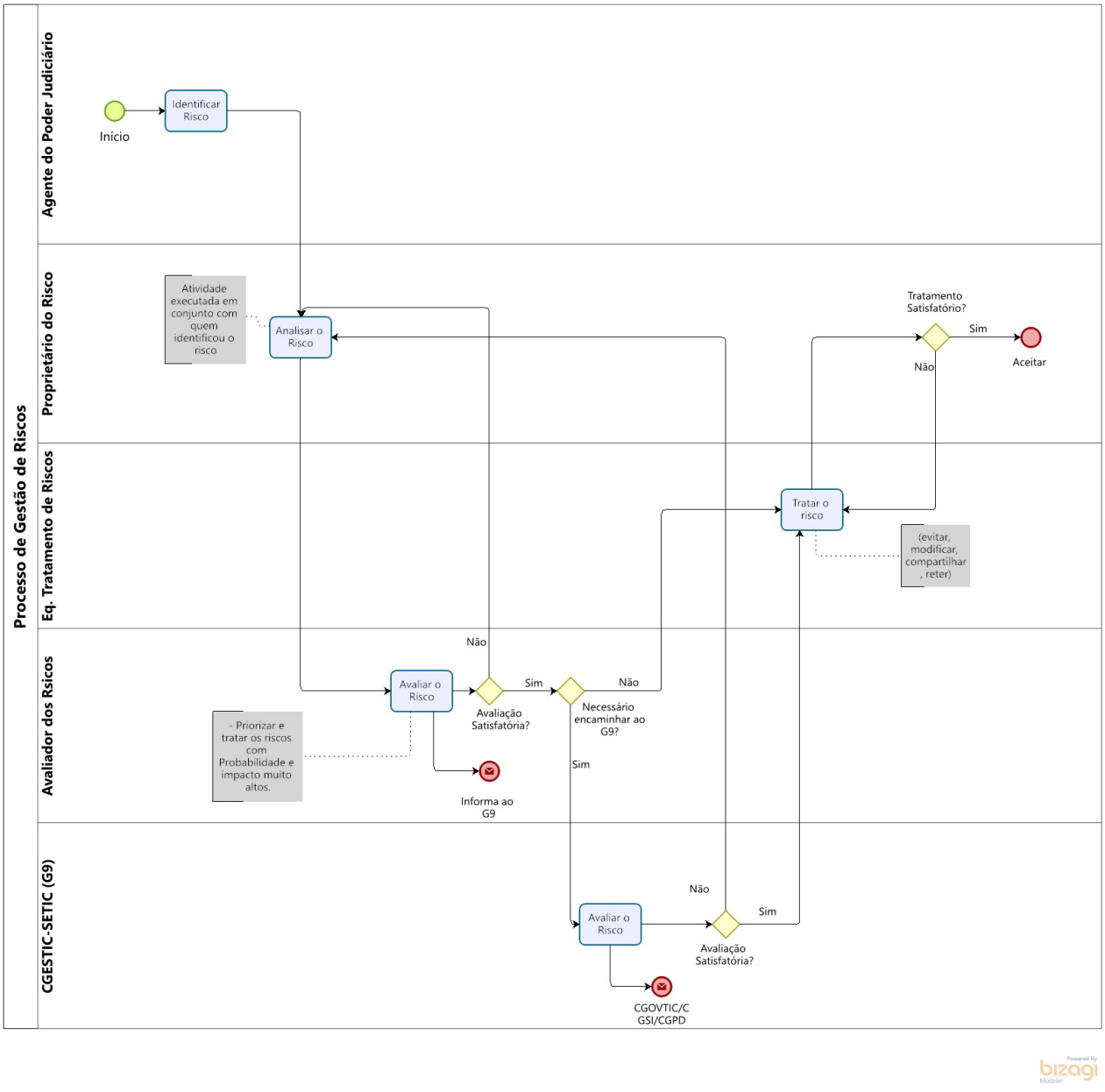


Figura 1 – Fluxo de atividades no processo de gestão de riscos do TJPE (aumentar fonte)

6.1. Descritivo do processo de Gestão de riscos de TIC

Atividade: Identificar Risco (escopo e cenários)	
Objetivo	Realizar a identificação dos riscos, estabelecer qual será o escopo de aplicação (determinando produto ou processo ou projeto) e cenários (ambientes interno e externo além de cenários político, econômico, sociocultural, tecnológico, sustentabilidade etc.).
Responsável	Agente do Poder Judiciário
Entradas	-
Saídas	Proposta de contexto
Descrição	É uma atividade de realizar a identificação dos riscos do âmbito de sua unidade, conforme contexto definido. Como também se define a estratégia de gestão de riscos, que se concretiza com o estabelecimento de diversos elementos, tais como: parâmetros internos e externos; equipe responsável; escopo de aplicação, acompanhamento e monitoramento. Essa atividade pode ser iniciada por qualquer agente do Poder Judiciário de Pernambuco.

Atividade: Analisar os riscos de TIC	
Objetivo	O principal objetivo da análise de riscos é **antecipar as situações que possam representar ameaças para um negócio**. Além disso, ela também aponta oportunidades e as probabilidades de que essas situações ocorram. A partir desse conhecimento, se consegue elaborar planos de ação para enfrentar cada uma delas.
Responsável	Proprietário do Risco
Entradas	- Riscos de TIC identificados. - Insulmos ou elementos necessários das unidades
Saídas	- Riscos de TIC analisados
Descrição	Essa atividade pode ser executada em conjunto com quem identificou o risco. As partes envolvidas deverão realizar a análise dos riscos conforme a metodologia institucional do TJPE.

Atividade: Avaliar riscos de TIC (Avaliador)	
Objetivo	Sumarizar os resultados da avaliação dos riscos segundo metodologia institucional de gestão de riscos, após as tarefas de identificação e análise.
Responsável	Avaliador dos Riscos
Entradas	- Riscos de TIC analisados pelo proprietário dos riscos
Saídas	- Resultado da avaliação dos riscos
Descrição	Após realizar a análise e avaliação dos riscos segundo metodologia institucional e documentar em proposta de planilha para análise posterior em grupo. A avaliação é feita da probabilidade e do impacto do risco. Qualquer dúvida deve ser encaminhada ao Proprietário de riscos de TIC. Por se tratar de uma avaliação de riscos, que não há necessidade de decisão estratégica do CGESTIC (G9), este é apenas informado sobre o risco avaliado. E esta a avaliação é encaminhada para equipe competente para tratar os riscos.

Atividade: Avaliar riscos de TIC (CGESTIC – SETIC G9)	
Objetivo	Sumarizar os resultados da avaliação dos riscos segundo metodologia institucional de gestão de riscos, após as tarefas de identificação e análise.
Responsável	CGESTIC – SETIC (G9)
Entradas	- Riscos de TIC levantados por todas as unidades
Saídas	- Resultado da avaliação dos riscos
Descrição	Quando a atividade de avaliar os riscos transcender os limites de competência do avaliador de riscos, essa atividade deverá ser encaminhada ao CGESTIC (G9). Após realizar a análise e avaliação dos riscos segundo metodologia institucional e documentar em proposta de planilha para análise posterior em grupo. A avaliação é feita da probabilidade e do impacto do risco. Qualquer dúvida deve ser encaminhada ao Proprietário de riscos de TIC.

Atividade: Tratar o Risco	
Objetivo	Encaminhar os resultados consolidados após a identificação, análise e avaliação dos riscos, a equipe de tratamento de riscos.
Responsável	Equipe de tratamento de riscos
Entradas	- Planilha de riscos e controles ajustada pelos representantes das unidades. - Uma lista de riscos priorizada, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos
Saídas	- Planilha de riscos homologada pelo CGESTIC (G9).
Descrição	Subsidiar ao proprietário do risco com informações sobre riscos de TIC e deliberar sobre os riscos considerados altos e extremos que, eventualmente, lhes forem apresentados pelos proprietários de risco. Convém que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e o plano de tratamento do risco seja definido.

Atividade: Aceitar Riscos	
Objetivo	Convém que a decisão de aceitar os riscos seja feita e formalmente registrada, juntamente com a responsabilidade pela decisão (isso se refere ao parágrafo 4.2.1 h) da ABNT NBR ISO/IEC 27001:2006).
Responsável	Proprietário do Risco
Entradas	O plano de tratamento do risco e o processo de avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação do mesmo.
Saídas	Uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.
Descrição	O CGESTIC (G9) e o Proprietário do Risco é quem tem autoridade, dentro da SETIC, para submeter o Processo de Riscos de TIC para aprovação e publicação.

7. RESPONSABILIDADES

Com relação ao assunto Riscos de TIC, reforçamos abaixo as principais atribuições e responsabilidades citados em outros normativos:

Atividades	Papéis				
	Agente do Poder Judiciário	Proprietário do Risco	Equipe de Tratamento de Riscos	Avaliador de riscos	CEGESTIC – SETIC (G9)
Identificar Risco	R		I		I
Analisar Risco	I/C	R/A	I	I	I
Avaliar Risco	I	I/C	I	R/A	R/A/C/I
Tratar o Risco	I	I/C	R/A	I	I
Aceitar Risco	I	R/A	I		I/C

Tabela 2 – Matriz RACI com papeis e responsabilidades

R = Responsável – Unidades responsáveis por executar as etapas.
A = Autoridade – Unidade que deve responder pelo cumprimento/conclusão da etapa.
C = Consultado – Unidades que devem ser consultadas e participar da decisão ou execução das etapas.
I = Informado – Unidades as quais o trabalho depende das etapas realizadas e/ou que devem ser atualizadas acerca dos progressos alcançados com a execução das etapas.

Durante a execução do nosso projeto, a matriz de responsabilidades tem como principal função promover o alinhamento entre as pessoas envolvidas. Por meio dessa técnica, consegue-se esclarecer o que cabe e o que não cabe à cada um dos agentes, o que facilita a cobrança por resultados e evita desentendimentos. Abaixo descrevemos os principais papéis e responsabilidades no contexto da SETIC-TJPE.

Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC)
CGTIC

- Normatizar, fomentar e acompanhar a implementação e operação do processo de gestão de riscos de TIC, exceto de riscos de segurança da informação;
- Definir e acompanhar a manutenção de nível de risco tolerável (“apetite a risco”) de TIC;
- Aprovar o objetivo e o escopo das análises e avaliação de riscos de TIC, exceto de riscos de segurança da informação;
- Deliberar sobre priorização de ações cuja necessidade resulte de planos de tratamento de riscos de TIC, exceto de riscos de segurança da informação.

Comitê de Gestão de Segurança da Informação (CGSI)

- Normatizar, fomentar e acompanhar a implementação e operação do processo de gestão de riscos de TIC exclusivamente sobre o escopo dos riscos de segurança da informação, inclusive quando da sua aplicação no SGSI (Sistema de Gestão de Segurança da Informação);
- Definir e acompanhar a manutenção de nível de risco tolerável ("apetite a risco") para segurança da informação;
- Aprovar o objetivo e o escopo das análises e avaliação de riscos de segurança da informação;
- Deliberar sobre priorização de ações cuja necessidade resulte de planos de tratamento de riscos de segurança da informação.

Comitê Gestor de Proteção de Dados Pessoais (CGPD)

- Subsidiar o processo de gestão de gestão de riscos com informações a respeito da legislação, normas do poder judiciário e normas internas pertinentes a análise e avaliação de riscos relacionados aos dados pessoais sob responsabilidade do TJPE;
- Definir e acompanhar a manutenção de nível de risco tolerável ("apetite a risco") para os titulares de dados pessoais sob responsabilidade do TJPE;
- Aprovar o objetivo e o escopo das análises e avaliação de riscos para titulares de dados pessoais sob responsabilidade do TJPE;
- Deliberar sobre priorização de ações cuja necessidade resulte de planos de tratamento de riscos que impliquem na proteção de dados pessoais.

Encarregado pelo Tratamento de Dados Pessoais

- Participar da execução de todas as fases do processo de gestão de risco quando este envolver análise e avaliação de riscos para titulares de dados pessoais sob responsabilidade do TJPE;
- Definir o objetivo e o escopo das avaliações de risco para titulares de dados pessoais e submeter ao CGPD;
- Definir critérios/controles para a análise e avaliação de riscos para titulares de dados pessoais;
- Reportar resultados de avalições de risco para o CGPD.

Comitê de Gestão de Tecnologia da Informação e Comunicação da SETIC (CGESTIC-SETIC) G9

- Implantar, manter e acompanhar a operacionalização e melhorias do processo de gestão de riscos de TIC;
- Avaliar e revisar continuamente a adequação, a suficiência e a eficácia da estrutura de gestão de riscos de TIC;
- Submeter alterações da estrutura de gestão de riscos de TIC ao CGTIC e ao CGSI;
- Subsidiar os CGTIC, CGSI e CGPD com informações sobre riscos de TIC;

- Gerir os riscos da área de TIC;
- Operacionalizar a aplicação dos recursos disponibilizados para a gestão de riscos de TIC na SETIC;
- Dirimir eventuais dúvidas dos proprietários de risco, na execução da Gestão de Riscos de TIC;
- Deliberar sobre os riscos considerados altos e extremos que, eventualmente, lhes forem apresentados pelos proprietários de risco;
- Submeter aos Comitês CGTIC, CGSI e CGPD, após sua apreciação e manifestação, os riscos de se considerados altos e extremos;
- Subsidiar os Comitês CGTIC, CGSI e CGPD com informações técnicas, visando auxiliá-los no processo de tomada de decisão;
- Conscientizar os gestores sobre a importância da gestão de riscos de TIC e as responsabilidades dos proprietários dos riscos;
- Submeter aos Comitês CGTIC e CGSI, nos seus respectivos âmbitos de atuação, os objetivos e escopos dos processos de análise e avaliação de riscos sobre os processos de trabalho que envolvam recursos de TIC.

Proprietário de Risco de TIC /Agente do Poder Judiciário / Gestor de Risco de TIC / Gestor de Unidade da SETIC

- Identificar, analisar, avaliar, tratar, monitorar e comunicar os Riscos de TIC dos seus respectivos processos de trabalho, atividades, sistemas, serviços, projetos, contratos ou iniciativas sob sua responsabilidade;
- Realizar a seleção dos riscos que deverão ser priorizados para tratamento por meio de ações de caráter imediato ou de aperfeiçoamento contínuo;
- Definir e implementar as ações de tratamento de riscos, estabelecendo prazos, responsáveis e meios para avaliação dos resultados;
- Reportar para Assessoria de Governança de TIC os riscos considerados altos ou extremos;
- Garantir que as informações sobre o risco estejam disponíveis para tomada de decisões;
- Realizar reuniões periódicas com envolvidos para monitorar os riscos de TIC identificados com alto ou extremo;
- Acompanhar a Gestão de Riscos de TIC e comunicar ao gestor imediato e Assessoria de Governança de TIC.

Assessoria de Governança de TIC

- Propor diretrizes para compor o Plano de Gestão de Riscos de TIC;
- Acompanhar os riscos classificados como de nível alto e extremo, ou seja, fora do apetite a riscos da instituição, de forma a verificar se as ações de tratamento e monitoramento estão sendo cumpridas pelos responsáveis dentro dos prazos estabelecidos;

- Reportar Riscos de TIC (altos e extremos) aos comitês (CGESTIC, CGSI e ao CGTIC);
- Manter interlocução com o Núcleo de Governança, Riscos e Compliance deste Tribunal sobre os Riscos de TIC.

Núcleos de Gestão de Projetos e Processos da SETIC

- Coordenar e monitorar a execução das atividades relativas à gestão de riscos em projetos de TIC;
- Coordenar e monitorar a execução das atividades relativas à gestão de riscos em processos de TIC, considerando inclusive aqueles presentes na cadeia de valor institucional.

Núcleo de Gestão da Segurança da Informação da SETIC

- Coordenar e monitorar a execução das atividades relativas à gestão de riscos de segurança da informação, relacionadas ao ambiente tecnológico da instituição;
- Propor definições na área de TIC que envolvam segurança da informação, proteção de dados, serviços em nuvem, continuidade de serviços essenciais, incidentes e riscos de segurança e assuntos correlatos;
- Promover a utilização de gestão de outros tipos de riscos de TIC junto a outras áreas da SETIC e do TJPE, com o objetivo de difundir o uso do processo para outros fins além da análise e avaliação dos riscos de segurança da informação;
- Propor ações de sensibilização e capacitação em Gestão de Riscos;
- Elaborar, em conjunto com a SETIC e outras áreas da AGTIC, o Manual de Gestão de Riscos de TIC do TJPE;
- Coordenar e monitorar o gerenciamento de riscos de segurança da informação;
- Consolidar a matriz de riscos-chave de segurança da informação;
- Elaborar e encaminhar o Plano de Tratamento de Riscos-Chave de segurança da informação;
- Prestar apoio técnico aos gestores de risco nas atividades afetas ao gerenciamento de riscos.

Assessoria Administrativa de TIC

- Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos em Contratações de TIC;

Avaliador dos Riscos

- Avaliar a eficácia da Gestão de Riscos de TIC;
- Comunicar à Alta Administração os resultados da avaliação da Gestão de Riscos de TIC.

8. METODOLOGIA E PROCESSO DE GESTÃO DE RISCOS DE TIC

A Gestão de Riscos de TIC no TJPE deve seguir as diretrizes da norma ABNT NBR ISO 27005:2019, que propõe um processo cíclico e contínuo que ajuda a identificar, avaliar e gerenciar os riscos de segurança da informação, visando garantir o preparo do tribunal para lidar com potenciais ameaças de segurança e a proteger a confidencialidade, integridade e disponibilidade das informações.

Nesse contexto o TJPE deve adotar em sua metodologia controles estabelecidos pelas principais normas de referência, como a ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27031 e ISO/IEC 27701; além de controles estabelecidos pela legislação vigente e órgãos de regulamentação externa.

A gestão de riscos de TIC no TJPE ocorre da seguinte forma:

1. Contexto da organização: nesta etapa, é importante entender o contexto da organização em termos de objetivos, metas, requisitos legais e regulatórios, e a identificação dos ativos relevantes e suas interdependências.
2. Avaliação de riscos: nesta etapa, os riscos potenciais são identificados e avaliados em termos de probabilidade de ocorrência e impacto potencial. Isso é feito através da análise de ameaças, vulnerabilidades e impactos na confidencialidade, integridade e disponibilidade da informação.
3. Tratamento de riscos: nesta etapa, as opções de tratamento de risco são identificadas, avaliadas e selecionadas. Isso pode incluir a aceitação do risco, a implementação de controles de segurança, a transferência do risco para outra parte ou a redução do risco através de ações preventivas.
4. Implementação de controles de segurança: nesta etapa, os controles de segurança selecionados são implementados e monitorados para garantir sua eficácia na redução dos riscos.
5. Monitoramento e revisão: nesta etapa, o processo de gestão de riscos é continuamente monitorado e revisado para garantir que os riscos sejam gerenciados de forma eficaz e que os controles de segurança sejam mantidos atualizados.

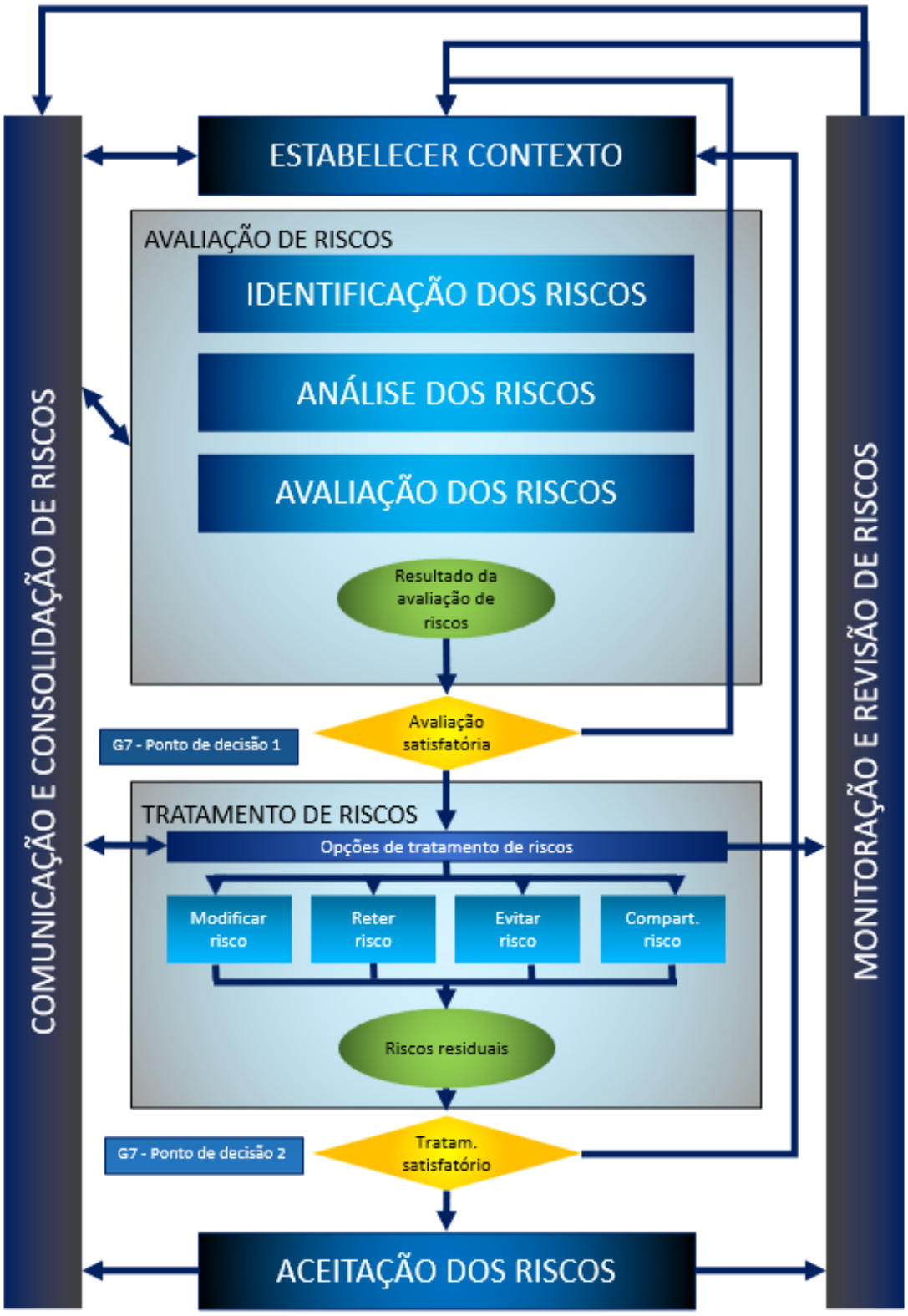


Figura 1 - Fluxo do Processo de Gestão de Riscos do TJPE

Em relação à metodologia adotada para implementação dos controles de risco a SETIC utiliza o NIST (*National Institute of Standards and Technology*) SP 800-30, que fornece orientações sobre a identificação, avaliação e resposta a riscos de segurança da informação e é baseada em um processo iterativo que requer monitoramento contínuo e atualizações regulares para garantir que a organização esteja sempre preparada para lidar com ameaças de segurança da informação.

9. PRINCIPAIS RISCOS TRATADOS

Inicialmente, o presente plano considera os riscos de TIC que envolvem os seguintes “pilares”:

a) **Riscos Estratégicos de TIC**: riscos identificados e analisados no escopo da elaboração dos artefatos e nos sistemas e serviços estratégicos para o Tribunal. Após o levantamento, será atribuído a uma área proprietária, ainda que outras áreas possam estar envolvidas na mitigação e controle. Os gestores destas áreas serão os proprietários destes riscos. Com o término da vigência do PDTIC, os riscos serão avaliados quanto a pertinência em transportá-los para as futuras versões do plano.

b) **Riscos de Segurança da Informação e Comunicação (SIC)**: riscos identificados e analisados no escopo de segurança da informação e comunicação ou normas relacionadas, considerando-se principalmente os sistemas e serviços críticos de TIC para o Tribunal e aqueles identificados no Plano de Continuidade de Serviços de TIC. Os responsáveis pelos sistemas, serviços e pelos ativos que os suportam são identificados juntamente com a avaliação de cada controle, cabendo a estes o monitoramento do risco residual após o tratamento.

c) **Riscos aos Titulares de Dados Pessoais**: riscos identificados e analisados que possam causar impactos para os titulares de dados pessoais, inclusive sensíveis, cujo controle é do Tribunal de Justiça;

d) **Riscos em Contratações de TIC**: riscos identificados, avaliados, tratados e monitorados no âmbito de cada contratação, desde a fase de planejamento até a fase de execução, incluindo a vigência contratual da solução ou serviço de TIC. Com o término da vigência do Contrato, os riscos serão avaliados quanto a pertinência em manter na base de riscos de TIC. A equipe de planejamento da contratação é responsável por identificar e monitorar os riscos referentes ao processo de licitatório (contratação) até etapa de homologação, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato.

e) **Riscos em Projetos de TIC:** são gerenciados no âmbito de cada projeto de TIC, devendo ser identificados pelo PMO ou Líder de Projeto do mesmo. Os riscos em projetos de TIC são monitorados pelos Líderes de Projetos.

f) **Riscos em Processos de TIC:** riscos identificados nos processos mapeados e/ou instituídos pela SETIC.

Assim que todo os riscos citados acima forem contemplados no Processo de Riscos de TIC, outros poderão ser sugeridos.

A Assessoria de Governança de TIC fará reuniões de acompanhamento da execução do processo de gestão de Riscos de TIC, conforme acordado na Matriz dos Riscos de TIC (ver sugestão de modelo de matriz no anexo 11). Os procedimentos operacionais e dinâmica das reuniões serão divulgados em documento específico.

Sugere-se **semestralmente ou quando surgirem novos riscos altos ou extremos** que de demandem uma prestação de contas de Riscos de TIC aos membros do CGESTIC, CGSI e CGTIC.

As ações definidas neste Plano terão a sua execução acompanhada pelos comitês CGESTIC, CGSI e CGTIC, bem como qualquer deliberação que seja necessária daquele fórum, considerando as suas atribuições e responsabilidades, definidas na Política.

10. PLANO DE AÇÃO SOBRE RISCOS DE TIC

Atividades necessárias ou próximas ações para continuidade da análise dos riscos de TIC, a serem realizadas no período de março de 2024 a março de 2025:

ID	Título
1	Revisar a Política de Segurança de TI e seus normativos
2	Definir a Lista de Serviços de Críticos de TIC para o Tribunal
3	Revisar a lista de sistemas e serviços Críticos de TIC para a SETIC
4	Realizar o processo de gestão de riscos de TIC para os serviços críticos de TIC
5	Realizar o processo de gestão de riscos de TIC para os sistemas e serviços críticos de TIC ou originados pelo Plano de Gestão da Continuidade de Serviços de TIC
6	Realizar o processo de gestão de riscos nas Contratações de TIC para exercício 2023 e 2024

7	Realizar o processo de gestão de riscos de TIC nos contratos de TIC vigentes.
8	Realizar o processo de gestão de riscos TIC nos projetos de TIC estratégicos.
9	Realizar o processo de gestão de riscos TIC nos processos de TIC estratégicos.

11. CONSIDERAÇÕES FINAIS

A área da Tecnologia da Informação e Comunicação (TIC) se mostra cada vez mais estratégica para o Tribunal, e entender os riscos de TIC que podem afetar os objetivos institucionais é um caminho crucial para uma gestão de excelência e contribui para a tomada de decisão. Tais técnicas podem não ser suficientes para garantir que eventos negativos ocorram, no entanto, o domínio sobre estes eventos serve para reduzir a probabilidade que ocorram ou o impacto ao efetivamente ocorrerem.

Em suma, a adoção da Gestão de Riscos de TIC é parte integrante positiva para a efetividade da gestão governamental

12. ANEXOS

12.1. ESCALA DE VALORES PARA APURAÇÃO DO NÍVEL DE RISCO

- PROBABILIDADE (1 a 5):

TABELA DE PROBABILIDADES

PROBABILIDADE	DESCRIÇÃO	GRAU
Muito baixa	Evento sem histórico de ocorrência, podendo ocorrer em circunstâncias excepcionais.	1
Baixa	Evento sem histórico de ocorrência, mas com possibilidade excepcional.	2
Média	Evento com histórico de ocorrência, mas com frequência mínima.	3
Alta	Evento com histórico de ocorrência, com alta frequência.	4
Muito alta	Evento com histórico de ocorrência. O evento só não ocorre excepcionalmente.	5

Tabela de Probabilidades

- IMPACTO (1 a 5):

TABELA DE IMPACTO

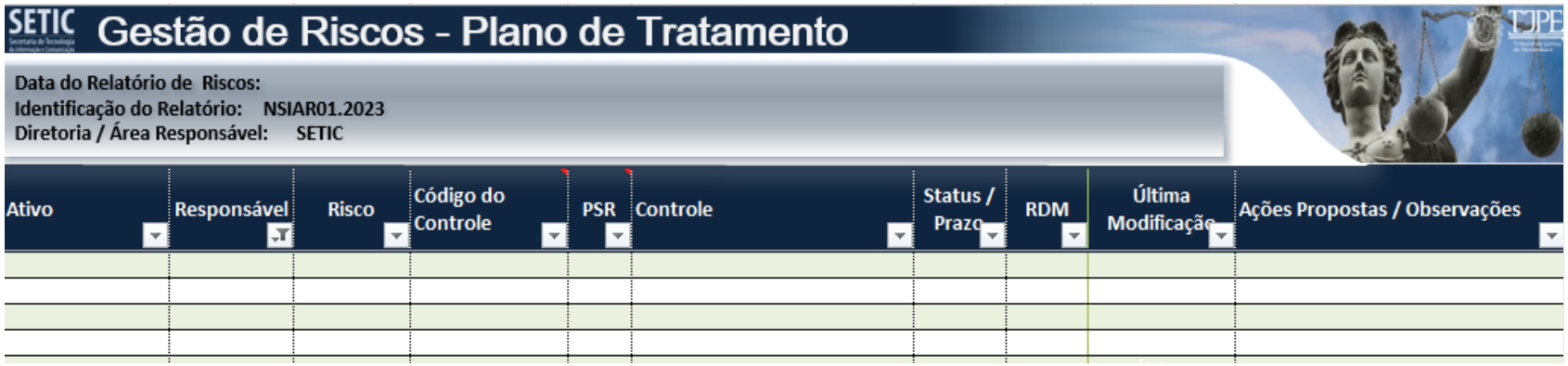
IMPACTO	DESCRIÇÃO	GRAU
Muito baixo	Impacto insignificante no objetivo.	1
Baixo	Impacto pequeno no objetivo.	2
Médio	Impacto moderado no objetivo.	3
Alto	Impacto significativo no objetivo, tornando improvável seu atingimento.	4
Muito alto	Impacto catastrófico no objetivo, impossibilitando seu atingimento.	5

Tabela de Impacto

- NÍVEL DE RISCO, calculado por (probabilidade X impacto):

NÍVEL DE RISCO	
Baixo	1-2
Médio	3-10
Alto	12-16
Extremo	20-25

12.2. Planilha modelo para Gestão de Riscos de TIC (parte 1)



SETIC Gestão de Riscos - Plano de Tratamento

Data do Relatório de Riscos:
Identificação do Relatório: NSIAR01.2023
Diretoria / Área Responsável: SETIC

Ativo	Responsável	Risco	Código do Controle	PSR	Controle	Status / Prazo	RDM	Última Modificação	Ações Propostas / Observações

12.3. Planilha modelo para Gestão de Riscos de TIC (parte 2)

TRATAMENTO DOS RISCOS							MONITORAMENTO	
TIPO DE RESPOSTA AO RISCO *(selecionar o item)*	AÇÃO DE PREVENÇÃO *(descrever várias ações na mesma célula)*	RESPONSÁVEL PELO RISCO (Nome e Cargo) *(pessoa ou unidade)*	PRAZO PARA RESPOSTA *(data limite dd/mm/aaa)*	AÇÃO DE CONTINGÊNCIA *(descrever várias ações na mesma célula)*	RESPONSÁVEL PELA CONTIGÊNCIA (Nome e Cargo) *(pessoa ou unidade)*	PRAZO PARA CONTINGÊNCIA *(data dd/mm/aaa)*	OBSERVAÇÕES GERAIS *(descrições)*	STATUS (selecionar o item)
								0.Não Iniciado