1.10. Portaria (Presidência) Nº 2124/2022 - PJPI/TJPI/SECPRE, de 30 de setembro de 2022

Dispõe sobre a instituição do **Plano de Gestão de Continuidade de Negócios de TIC** no Âmbito do Poder Judiciário do Estado do Piauí.
O **PRESIDENTE DO EGRÉGIO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ**, Desembargador JOSÉ RIBAMAR OLIVEIRA, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a Resolução nº 370, do Conselho Nacional de Justiça, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);
CONSIDERANDO a Resolução nº 232/2021, de 05 de julho de 2021, que dispõe, no âmbito do Tribunal de Justiça do Estado do Piauí - TJPI, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política de Segurança da Informação - PSI;
CONSIDERANDO a Tecnologia de Informação (TIC) como ferramenta indispensável à realização das funções institucionais do TJPI e como instrumento para viabilizar soluções que conduzam ao alcance dos objetivos estratégicos do Tribunal;
CONSIDERANDO o disposto no Levantamento iGovTIC-Jud-2021 do CNJ, referente à formalização e cumprimento do Plano de Gestão de Continuidade de Negócios de TIC;
R E S O L V E:
Art. 1º Fica instituído o o Plano de Gestão de Continuidade de Negócios de TIC no Tribunal de Justiça do Estado do Piauí.
Art. 2º Para os fins deste Ato, entende-se como:
I - Ameaça: qualquer atividade maliciosa, intencional ou acidentalmente, seja através de meios eletrônicos ou não, que possa explorar uma vulnerabilidade e, assim, obter acesso, danificar ou destruir um determinado ativo ou serviço.
II - Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.
III - Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.
IV - Ativos de informação: meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
V - Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções dos negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.
VI - Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.
VII - Estratégia de continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;
VIII - Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.
IX - Incidente: qualquer evento que possa causar a interrupção do negócio.
X - Plano de Continuidade: nome que se dá à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC e é composta por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.
XI - Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.
XII - Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.
XIII - Plano de Administração de Crises (PAC): documento que define as atividades das equipes envolvidas e quais as ações de contingência e comunicação deverão ser executadas durante e após a ocorrência de um desastre, com o intuito de minimizar os impactos, até a superação da crise.
XIV - Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.
XV - RPO (*Recovery Point Objective*): tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.
XVI - RTO (*Recovery Time Objective*): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.
XVII - Sistemas essenciais: sistemas de informação do TJPI definidos como estratégicos e com alto impacto no negócio em caso de indisponibilidade.
Art. 3º O processo definido visa atingir os seguintes objetivos:
I - Reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do TJPI.
II - Manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação jurisdicional do TJPI.
III - Definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.
Art. 4º O Plano de Gestão de Continuidade de Negócios de TIC observará o Anexo Único desta Portaria e dela parte integrante.
Art. 5º A documentação e as demais informações sobre o plano estão disponíveis no Portal da Governança de TIC, na página do TJPI.
Art. 6º Os papéis definidos no plano, relativos aos servidores da STIC, serão designados pelo Secretário da unidade.
Art. 7º Esta Portaria entra em vigor na data de sua publicação.
REGISTRE-SE, PUBLIQUE-SE e CUMPRA-SE.
GABINETE DA PRESIÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ, em Teresina-PI, 30 de setembro de 2022.
DESEMBARGADOR JOSÉ RIBAMAR OLIVEIRA
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ
ANEXO ÚNICO
Portaria (Presidência) Nº 2124/2022 - PJPI/TJPI/SECPRE
PLANO DE CONTINUIDADE DE NEGÓCIOS DE TIC DO TJPI
VERSÃO 1.0.0
PROCESSO SEI Nº 22.0.000093192-0
Histórico de Versões

Versão	Descrição	Data	Responsável	Local
1.0.0	Atualização de papéis e atividades	09/2022	Gildean Alves / Enani Moura	INFRA/SEGINFO

1. Definição
O Plano de Gestão de Continuidade é um documento no qual ficam definidas as estratégias a serem adotadas a fim de que se mantenha o funcionamento das operações da instituição, caso ela venha a enfrentar intempéries causadas por fatores internos ou externos à organização.
2. Objetivo
2.1. Estabelecer as diretrizes e definir o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicação, aplicáveis ao ambiente tecnológico deste Tribunal.
3. Motivações
3.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.
3.2. Correto direcionamento e dimensionamento de recursos tecnológicos para prover a Gestão de Continuidade de TIC.
3.3. Manutenção de um nível aceitável de resiliência dos serviços e sistemas de TIC frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação jurisdicional.
3.4. Estabelecer procedimentos de gestão para assegurar a continuidade das operações de TIC.
4. Escopo
4.1. Serviços de Tecnologia da Informação atinentes à STIC (Secretaria de Tecnologia da Informação e Comunicação) que garantem o pleno funcionamento dos sistemas essenciais do TJPI.
5. Referências normativas
5.1. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.
5.2. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação.
5.3. Norma Técnica ABNT NBR ISO/IEC 22301:2013, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.
6. Conceitos e definições
6.1. Ameaça: qualquer atividade maliciosa, intencional ou acidentalmente, seja através de meios eletrônicos ou não, que possa explorar uma vulnerabilidade e, assim, obter acesso, danificar ou destruir um determinado ativo ou serviço.
6.2. Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e
qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.
6.3. Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.
6.4. Ativos de informação: meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
6.5. Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções dos negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.
6.6. Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.
6.7. Estratégia de continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;
6.8. Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.
6.9. Incidente: qualquer evento que possa causar a interrupção do negócio.
6.10. Plano de Continuidade: nome que se dá à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC e é composta por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.
6.11. Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.
6.12. Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.
6.13. Plano de Administração de Crises (PAC): documento que define as atividades das equipes envolvidas e quais as ações de contingência e comunicação deverão ser executadas durante e após a ocorrência de um desastre, com o intuito de minimizar os impactos, até a superação da crise.
6.14. Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.
6.15. RPO (*Recovery Point Objective*): tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.
6.16. RTO (*Recovery Time Objective*): tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.
6.17. Sistemas essenciais: sistemas de informação do TJPI definidos como estratégicos e com alto impacto no negócio em caso de indisponibilidade.
7. Diretrizes
7.1. A gestão de continuidade de TIC visa:
7.1.1. Reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do TJPI.
7.1.2. Manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação jurisdicional do TJPI.
6.1.3. Definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.
7.2. A gestão de continuidade de TIC deve observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.
7.3. Será elaborado Plano de Continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e comunicações necessárias, bem como o retorno à normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TIC. Devem

ser fornecidos recursos humanos, tecnológicos e financeiros para a manutenção e melhoria contínua da gestão de continuidade de TIC.

8. Processo de Gestão de Continuidade de TIC

8.1. O processo de Gestão de Continuidade de TIC é composto pelas seguintes etapas:

8.1.1. Planejamento - compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades da STIC são essenciais para prestação jurisdicional, quais deverão ser tratadas na Continuidade de TIC e quais estratégias serão utilizadas durante a ocorrência de um incidente. Compreende também a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças na infraestrutura, procedimentos ou testes realizados.

8.1.2. Execução - abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a aprovação dos planos, seu armazenamento e divulgação.

8.1.3. Verificação - abrange a realização de testes periódicos dos Planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres) a fim de subsidiar a etapa de Melhoria.

8.1.4. Melhoria - compreende a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, com vistas a dar início ao novo ciclo do processo.

8.2. O desenho do processo de Gestão de Continuidade de TIC, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos e indicadores definidos para o processo serão publicados no Portal da Transparência do TJPI na seção de Governança de TIC, após aprovação pela Presidência.

8.3. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TJPI, objeto de imediata divulgação na forma do item anterior.

9. Plano de Continuidade de TIC

9.1. O Plano de Continuidade de TIC é composto pelos Plano de Continuidade Operacional, Plano de Administração de Crises e Planos de Recuperação de Desastres.

9.2. O Plano de Continuidade de TIC deve ser periodicamente testado, de forma a garantir sua efetividade.

9.3. O Plano de Continuidade de TIC deve ser revisado no mínimo uma vez por ano ou, ainda, em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades etc).

9.4. O Plano de Continuidade de TIC será acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas do TJPI.

9.5. Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para a manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre para retorno das atividades à normalidade.

9.6. A comunicação às partes interessadas observará as orientações contidas nos Planos de Continuidade Operacional.

9.7. Os ativos e serviços afetados pelo incidente serão monitorados pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações à autoridade superior.

9.8. A ativação do Plano de Continuidade de TIC será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos afetados.

10. Serviços essenciais do TJPI

Abrange todos os sistemas do TJPI definidos como essenciais, cujos valores dos parâmetros são definidos abaixo:
Criticidade: Alta, baixa
RPO/RTO: horas, dias, semanas, último backup válido
Impacto: baixo, médio, alto, irrelevante e baixo
Tabela 01 - Parametrização do serviços essenciais de TIC em relação à continuidade de negócios.

	Serviço	Criticidade	RPO	RTO		Impacto		
					Financeiro	Legal	Imagem	Operacional
1	PJe 2g	alta			baixo	alto	alto	alto
2	e-TJPI	baixa			baixo	baixo	baixo	baixo
3	Diário da Justiça	alta			baixo	alto	alto	alto
3	Gestor RH	alta			médio	alto	médio	alto
4	BNMP	baixa			baixo	alto	baixo	baixo
5	Microsoft Teams 2g	baixa			baixo	baixo	alto	médio
6	SEI	alta			baixo	médio	alto	alto
7	COBJUD	alta			alto	alto	alto	alto
8	SEEU	baixa			baixo	alto	médio	médio
9	Selo Digital	alta			alto	alto	alto	alto
10	ThemisWeb	baixa			baixo	baixo	baixo	baixo
11	PJe 1g	alta			baixo	alto	alto	alto
12	Projudi	baixa			baixo	baixo	baixo	baixo
13	Portal do Advogado	baixa			baixo	baixo	alto	baixo
14	DRS Audiência	média			baixo	alto	médio	médio
15	PJe Mídias	baixa			baixo	médio	médio	médio
16	Microsoft Teams 1g	baixa			baixo	baixo	alto	médio
17	CPTEC	baixa			baixo	médio	médio	baixo

11. Identificação inicial de ameaças:

Eventos	Probabilida	Possíveis causas

	de	
Interrupção de energia elétrica no data center	baixa	Interrupção do fornecimento de energia elétrica pela concessionária; Rompimento dos circuitos elétricos internos; Falha no grupo de UPS; Falha simultânea do gerador da sala cofre e do gerador do prédio, causada por problemas técnicos ou por falta de combustível.
Falha na climatização do data center	baixa	Falha em um ou mais equipamentos/elementos do grupo de climatização.
Indisponibilidade de internet e/ou rede de comunicação no data center	baixa	Interrupção do serviço de fornecimento de internet pela operadora de telecomunicação contratada; Rompimento de fibra óptica interna; Falha em equipamento de rede do data center ou em dispositivo que faz a interconexão com este.
Ataque cibernético interno	baixa	Vulnerabilidades nos softwares/hardwares; Engenharia social; Vazamento de acessos privilegiados; Ausência de ferramentas específicas de segurança;
		Ferramentas de segurança mal configuradas.
Ataque cibernético externo	Alta	Vulnerabilidades nos softwares/hardwares; Engenharia social; Vazamento de acessos privilegiados; Ausência de ferramentas específicas de segurança;
		Ferramentas de segurança mal configuradas.
Falha de hardware em dispositivos do data center	baixa	Falha em hardware que necessite de reparo ou substituição.
Incêndio	baixa	Curto circuito; Sobrecarga de equipamentos; Superaquecimento de equipamentos;
Desastres naturais	baixa	Enchentes, alagamentos, descargas elétricas causadas por raios, terremotos, erosão.
Colapso estrutural	baixa	Queda estrutural.
Conflito bélico	baixa	Bombardeio, em casos de guerra.

12. Papéis e Responsabilidades

Define a responsabilidade das equipes e de seus líderes quanto à execução de itens deste plano.

PAPEL	DESCRIÇÃO	RESPONSABILIDADES
Presidência	Órgão diretivo máximo do TJPI.	Aprovar os planos de continuidade de serviços essenciais de TIC encaminhados pelo Comitê Gestor de Segurança da Informação e garantir os recursos necessários para o sucesso dos mesmos.
Comitê Gestor de Segurança da Informação	Comitê multidisciplinar formado por magistrados e servidores, de assessoramento da Administração na área de segurança da informação.	Analisar e manifestar-se sobre a documentação de Continuidade de Serviços Essenciais de TIC produzida pela área de TIC, apoiando a Presidência na avaliação do processo.
Comitê Gestor de TIC	Grupo formado pelo titular da área de TIC, gestores das unidades e servidores responsáveis pelos macroprocessos de TIC.	Validar a lista de serviços essenciais de TIC, validar os planos elaborados pelas unidades da área da TIC e definir os testes a serem realizados.
		Avaliar as proposições e documentos encaminhados pela Área de Segurança da Informação.
		Encaminhar as proposições às instâncias superiores, para avaliação e aprovação. Quando necessário, retornar avaliação à Área de SI, indicando pontos de melhorias a serem realizados.
Comitê de Desastre/Recuperação	Grupo formado pelo titular da área de TIC, gestores das unidades e servidores responsáveis pelos macroprocessos de TIC.	Ativar e Supervisionar a execução dos planos de continuidades de serviços essenciais de TIC na ocorrência de desastres ou incidentes de segurança da informação.
		Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
Sessão de Segurança da Informação	Unidade responsável pelo macroprocesso de segurança da informação e pelo Processo de Gestão de Continuidade de TIC.	Elaborar e atualizar modelos de documentos utilizados na gestão de continuidade de serviços essenciais de TIC.
		Assessorar o Comitê Gestor de Segurança da Informação
		e o Comitê de Gestão de TIC na análise e na tomada de decisões a respeito de situações decorrentes de incidentes e

		desastres de segurança da informação.
		Gerenciar os Processos de Gestão de Continuidade de TIC e manter a documentação relacionada atualizada.
Coordenação de Infraestrutura de TIC	Unidade técnica da área de TIC responsável pela infraestrutura de TIC.	Executar os procedimentos do PCTIC relacionados à infraestrutura de TIC.
Sessão de Segurança da Informação	Unidade responsável pelo macroprocesso de segurança da informação e pelo Processo de Gestão de Continuidade de TI.	Consolidar os planos e documentos que integram o PCTI.
Coordenação de Sistemas	Unidade técnica da área de TIC responsável pelos sistemas essenciais.	Executar os procedimentos do PCTIC relacionados aos sistemas essenciais.
Superintendência de Engenharia e Arquitetura	Unidade técnica responsável pela infraestrutura predial.	Executar os procedimentos do PCTIC relacionados à infraestrutura predial.
Assessoria de Comunicação	Unidade responsável pela comunicação institucional.	Realizar as comunicações institucionais referentes ao PCTIC.
Unidades de TIC e de outras áreas	Compreende as unidades técnicas da área de TIC, responsáveis por administrar os serviços essenciais de TIC da instituição e outras áreas do tribunal das quais os serviços essenciais dependam.	Preencher e revisar os Planos de Continuidade, de Recuperação de Desastres; Executar, quando necessário, os testes e ensaios periódicos; Executar os planos de sua competência na ocorrência de incidentes em cumprimento a determinação do Comitê de Gestão de TIC; Apoiar a Área de Segurança da Informação no processo.

13. Contatos

Papel	Telefone	Email
Coordenação de Infraestrutura de TIC	(86) 3215-7419	stic.infra@tjpi.jus.br
Sessão de Segurança da Informação	(86) 3215-7419	stic.infra@tjpi.jus.br
Coordenação de Sistemas	(86) 3218-0800	stic.judicial@tjpi.jus.br stic.admin@tjpi.jus.br
Superintendência de Engenharia e Arquitetura	(86) 3221-8284	engenharia@tjpi.jus.br
Assessoria de Comunicação	(86) 3216-7435 Ramal 2113	ascom@tjpi.jus.br

14. Comunicações

As comunicações internas entre os envolvidos na execução do PCTIC serão realizadas por meio dos telefones e emails disponibilizados na sessão Contatos.

Na ocorrência de uma crise, a ASCOM deverá ser imediatamente informada dos seus motivos, devendo ser consultada antes que sejam tomadas decisões que impliquem ações específicas de comunicação, como o contato com os públicos estratégicos. Cabe a ASCOM estabelecer critérios de postura junto ao público externo. Porém, para eventuais comunicados escritos à imprensa por parte da ASCOM, as dúvidas técnicas pertinentes deverão ser relacionadas antes de qualquer publicação, sem exceção. No caso de detalhamento técnico do problema à imprensa falada ou televisiva, o porta-voz da instituição deverá ser assessorado por uma pessoa do corpo técnico de TIC, designado pelo gestor da área de TIC em exercício.

15. Invocação do Plano de Continuidade

O PCTI será acionado pelo Comitê de Desastre/Recuperação quando a ocorrência de algum dos eventos de ameaças gerar indisponibilidade de algum dos sistemas essenciais por período superior ao RTO definido ou na ocorrência de um risco desconhecido que também gere esta mesma indisponibilidade.

O plano poderá também ser invocado em casos de testes ou por determinação do Comitê de DR.

16. Protocolo de Tratamento do PCTIC

É composto de fases ou macroprocessos que se encontram definidos e desmembrados em subplanos específicos para cada área de atuação, quando da ocorrência de um desastre. A sequência de atividades está listada abaixo:

i - Identificação e declaração de desastres;
ii - Ativação do processo de DR;
iii - Comunicar o desastre;
iv - Avaliação da corrente e prevenção de mais danos;
v - Ativação da solução de Contingência;
vi - Estabelecer operações de TI;
vii - Reparação e reconstrução da instalação principal;
viii - Retorno das operações para Ambiente principal.

Os subplanos do PCTIC juntamente com seus objetivos estão assim organizados:

Plano de Continuidade Operacional (PCO): Seu objetivo é garantir a continuidade dos serviços críticos de TIC na ocorrência de um desastre, enquanto recupera-se o ambiente principal. O PCO é fortemente orientado aos processos(sistemas) e serviços**.**

Plano de Administração de Crise (PAC): Definir as atividades das equipes envolvidas e gerenciar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos, até a superação da crise.

Plano de Recuperação de Desastre (PRD): Planejar e agir para que, uma vez controlada a contingência e passada a crise, a Secretaria de Tecnologia do TJPI retome seus níveis originais de operação no ambiente principal.

Plano de Testes e Validação (PTV): Um plano de Continuidade de Negócios só está apto a funcionar após ser testado e exercitado. Este plano define a periodicidade e tipos de teste que serão realizados.

17. SUBPLANOS DO PCTIC

Define os subplanos específicos para cada área de atuação, quando da ocorrência de um desastre.

17.1. Plano de Continuidade Operacional (PCO)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

17.1.2. Objetivo e Escopo

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia.

São objetivos do PCO:

i - Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais.

ii - Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre.

iii - Estabelecer uma equipe para cada plano PCO, PRD e PAC

iv - Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

17.1.2. Execução do PCO

17.1.2.1 Avaliação do impacto: Identificada a ocorrência de um incidente ou crise, o chefe da sessão competente deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Em seguida, todas as equipes envolvidas devem receber informações sobre o ocorrido.

17.1.2.2 Acionamento do plano: Dado o aval pelo COMITÊ DE DR sobre o acionamento do plano, a equipe responsável convocará reunião de emergência com os líderes do PRD e PAC com o intuito de:

i - Coordenar prazos e orquestrar as ações de contingência.

ii - Informar às equipes ações de contingência com a priorização dos serviços essenciais.

17.1.2.3 Ações de contingência: Devem ser adotadas para cada processo ou serviço essencial.

17.1.2.4 Encerramento do PCO: Uma vez validado o retorno dos sistemas essenciais e estabilidade do data center deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO. Informar à equipe de comunicação o retorno das atividades.

17.2 Plano de Administração de Crise (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

17.2.1 Objetivo: O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe. São objetivos específicos do PAC:

i - Garantir a segurança à vida das pessoas;

ii - Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.

iii - Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta.

iv - Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

17.2.2 Execução do PAC

17.2.2.1 Comunicação na ocorrência de um Desastre

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento.

A comunicação com cada parte ocorrerá da seguinte forma:

17.2.2.1.1 Comunicar às Autoridades

A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre.

Autoridade	Número	Data/hora	Num. Ocorrência
Polícia	190		
Bombeiros	193		
Samu	192		

17.2.2.2 Comunicação após um Desastre

Após reunião com líderes do PRD e PCO, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos bem informados e passar a todos a perspectiva dos esforços necessários para o reestabelecimento dos serviços inativos.

17.2.2.2.1 Comunicação com os funcionários

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que as unidades do TJPI mantenham-se informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

Números de contatos a serem disponibilizados:

Telefone: (86) 3215-7419

Email: stic.infra@tjpi.jus.br

Central de serviços: https://glpi.tjpi.jus.br

17.2.2.2.2 Comunicar unidades e setores do TJPI

Acionar diretamente às unidade afetadas pelo desastre e fornecer contato

Natureza, impacto e abrangência da catástrofe

Ações de contingência em andamento

Processos/sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

17.2.2.2.3 Comunicar fornecedores e prestadores de serviços 17.2.2.2.4 Comunicar Colaboradores externos, cidadãos e mídia. A equipe de comunicação, em consonância com a Assessoria de Comunicação do TJPI, deverá fornecer informações pertinentes aos colabores externos: Advogados, cidadãos e outros órgãos.

Buscar publicar em meios oficiais e de ampla divulgação as informações sobre o ocorrido.

17.2.2.2.5 Comunicar o retorno das operações

Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

17.2.3 Encerramento do PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter a equipe de comunicação entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência do desastre como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

17.3. Plano de Recuperação de Desastre (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para

reestabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.
17.3.1. Objetivo e Escopo
É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.
São objetivos PRD:
Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.
Evitar desdobramentos de outros incidentes na facilidade principal.
Reestabelecer o datacenter dentro do prazo tolerável
17.3.1.1 Execução do PRD
17.3.1.1.1 Identificar ativos danificados: As sessões vinculadas à Coordenação de Infraestrutura de TI deverão identificar e listar todos os ativos danificados da ocorrência do desastre.
17.3.1.1.2 A sessão de redes deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.
17.3.1.1.3 Listar serviços descontinuados
A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do COMITÊ DE DR. O relatório deverá abranger todos os componentes necessários à plena operação das aplicações como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, dns, rotas, vlans etc.
17.3.1.1.4 Elaborar cronograma de recuperação
O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:
? A priorização dos serviços essenciais, ou determinação de nível institucional;
? O RTO definido para cada serviço essencial; ? A força de trabalho disponível.
17.3.1.1.4.1 Substituição de ativos e equipamentos
Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao COMITÊ DE DR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.
A coordenação de infraestrutura de TI deve verificar quais ativos de TI que foram danificados estão cobertos por garantia e se pode ser acionada com os fornecedores.
As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.
17.3.1.1.4.2 Reconfiguração de ativos e equipamento
As configurações dos ativos reparados ou substituídos deverão ser verificadas para garantir que estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à equipe de comunicação e ao COMITÊ DE DR.
17.3.1.1.4.3 Teste do ambiente
O ambiente principal do datacenter antes do recovery dos dados do backup deverá ser testado afim de garantir que o processo de recuperação ocorra conforme o planejado Os testes incluem:
Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
Validar configurações que precisaram ser refeitas tanto em sistemas como em equipamentos;
17.3.1.1.4.4 Recuperar dados do backup
Proceder com a recuperação dos dados para as aplicações.
17.3.1.2 Encerramento do PRD
Ao término do procedimento de *recovery*, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.
18. Validação e teste de PCTIC
O PCTI será testado e validado em reunião entre os líderes de cada subplano a cada semestre ou com a insurgência de novos fatores de risco, mudança na análise de impacto ou com a inclusão de um novo serviço no plano de continuidade.

Data	Tipo	Motivo	Status

Data: Refere-se ao dia da execução ou validação do teste;
Tipo: de mesa, caminho percorrido, simulação, entre outros;
Motivo: motivo pelo qual o teste foi necessário;
Status: programado, executado, planejado, agendado.
19. Atualização da Norma
19.1. As diretrizes previstas na presente norma serão atualizadas na forma do art. 14 § 1º da Política de Segurança da Informação vigente sempre que alterados os procedimentos de Gestão de Continuidade de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.

Documento assinado eletronicamente por **José Ribamar Oliveira**, **Presidente**, em 30/09/2022, às 14:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **3669007** e o código CRC **52DD45B0**.

1.11. Portaria (Presidência) Nº 2126/2022 - PJPI/TJPI/SECPRE, de 30 de setembro de 2022

Dispõe sobre a instituição do Processo de Gestão de Riscos de Segurança da Informação no Âmbito do Poder Judiciário do Estado do Piauí.
O **PRESIDENTE DO EGRÉGIO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ**, Desembargador JOSÉ RIBAMAR OLIVEIRA, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a Resolução Nº 370 do Conselho Nacional de Justiça, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);
CONSIDERANDO a Resolução Nº 232/2021, de 05 de julho de 2021, que dispõe, no âmbito do Tribunal de Justiça do Estado do Piauí - TJPI, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política de Segurança da Informação - PSI;
CONSIDERANDO a Tecnologia de Informação (TIC) como ferramenta indispensável à realização as funções institucionais do TJPI e como instrumento para viabilizar soluções que conduzam ao alcance dos objetivos estratégicos do Tribunal;
CONSIDERANDO o disposto nos itens 3.5 e 24, do Levantamento iGovTIC-Jud-2021 do CNJ, referente à formalização e cumprimento do processo de Plano de Gestão de Riscos de TIC;
CONSIDERANDO as recomendações das boas práticas de gerenciamento de Gestão de Riscos contidos nas Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação, Norma Técnica ABNT NBR ISO

31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos, Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação, Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização e Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

R E S O L V E:

Art. 1º Fica instituído o processo de Gestão de Riscos de Segurança da Informação no Âmbito do Poder Judiciário do Estado do Piauí.

Art. 2º Para os fins deste Ato, entende-se como:

I - Ameaça - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

II - Análise de riscos - uso sistemático de informações para identificar fontes e estimar o risco;

III - Análise/avaliação de riscos - processo completo de análise e avaliação de riscos;

IV - Ativos de Informação - os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V - Avaliação de riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

VI - Comunicação do risco - troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;

VII - Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

VIII - Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

IX - Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC-TJPI) - conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

X - Gestão de Riscos em Projetos de TIC - conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

XI - Gestão de Riscos em Processos de TIC - conjunto de atividades estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

XII - Identificação de riscos - processo para localizar, listar e caracterizar elementos do risco.

XIII - Reduzir risco - forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

XIV - Reter risco - forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

XV - Riscos de Segurança da Informação e Comunicações - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XVI - Transferir risco - uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

XVII - Tratamento dos riscos - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

XVIII - Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

Art. 3º O processo definido visa atingir os seguintes objetivos:

I - Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações;

II - Definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TJPI (GRSIC-TJPI).

Art. 4º O processo de Gestão de Riscos de Segurança da Informação observará o manual do processo, constante no Anexo Único desta Portaria e dela parte integrante.

Art. 5º Os fluxos, o manual, a documentação e as demais informações sobre o processo estão disponíveis no Portal da Governança de TIC, na página do TJPI.

Art. 6º Os papéis definidos no manual do processo, relativos aos servidores da STIC, serão designados pelo Secretário da unidade.

Art. 7º Esta Portaria entra em vigor na data de sua publicação.

REGISTRE-SE, PUBLIQUE-SE e CUMPRA-SE.

GABINETE DA PRESIÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ, em Teresina-PI, 30 de setembro de 2022.

DESEMBARGADOR JOSÉ RIBAMAR OLIVEIRA

PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ

ANEXO ÚNICO

PORTARIA (PRESIDÊNCIA) Nº 2126/2022 - PJPI/TJPI/SECPRE

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO TJPI

VERSÃO 1.0.0

PROCESSO SEI Nº 22.0.000070110-0

Histórico de Versões

Versão	Descrição	Data	Responsável	Local
1.0.0	Criação do documento	09/2022	Gildean Alves / Enani Moura	INFRA/SEGINFO

Gestão de Riscos de Segurança da Informação e Comunicações

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos relacionadas ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações, e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TJPI (GRSIC-TJPI).

2. Aplicabilidade

2.1. Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TJPI.

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.2. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.3. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.
4.4. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.
4.5. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

4. Conceitos e definições

4.1. Ameaça - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;
4.2. Análise de riscos - uso sistemático de informações para identificar fontes e estimar o risco;
4.3. Análise/avaliação de riscos - processo completo de análise e avaliação de riscos;
4.4. Ativos de Informação - os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
4.5. Avaliação de riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;
4.6. Comunicação do risco - troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;
4.7. Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;
4.8. Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;
4.9. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC-TJPI) - conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;
4.10. Gestão de Riscos em Projetos de TIC - conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.
4.11. Gestão de Riscos em Processos de TIC - conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.
4.12. Identificação de riscos - processo para localizar, listar e caracterizar elementos do risco.
4.13. Reduzir risco - forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;
4.14. Reter risco - forma de tratamento de risco pela qual se decide realizar a
atividade, assumindo as responsabilidades caso ocorra o risco identificado;
4.15. Riscos de Segurança da Informação e Comunicações - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
4.16. Transferir risco - uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;
4.17. Tratamento dos riscos - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;
4.18. Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

5. Escopo

5.1. A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados à área de TIC, que suportam os principais processos de negócio do TJPI.

6. Diretrizes

6.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação deste Tribunal.
6.2. Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.
6.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

7. Gestão de riscos em projetos de TIC

7.1. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Secretaria de Tecnologia da Informação de Comunicações.

8. Gestão de riscos em processos de TIC

8.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.
8.1.1. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.
8.2. A gestão de riscos em processos de TIC é monitorada pelo Escritório de Processos de TIC.

9. Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC-TJPI)

9.1. O processo de GRSIC-TJPI é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação e da Gestão de Continuidade de Negócios.
9.2. O processo de GRSIC-TJPI está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 31000:2018;
9.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.
9.5. Considerando as políticas praticadas pelo TJPI, não há riscos passíveis de serem tratados através da estratégia de transferência de riscos.

10. Processo da Gestão de Riscos de Segurança da Informação e Comunicação

O processo de Gestão de Riscos do TJPI possui as seguintes etapas: Estabelecimento do Contexto, Processo de Avaliação de Riscos, Tratamento de Riscos, Monitoramento e Análise Crítica e Comunicação e Consulta.

10.1 Estabelecimento do Contexto

Ao iniciar as atividades para a elaboração do plano de gestão de riscos, a primeira tarefa consiste em compreender o ambiente no qual o trabalho será desenvolvido, definir o escopo e critérios a serem considerados no processo de gestão de riscos. Nesta etapa, a equipe que realiza a gestão de risco deve identificar todos os processos e atividades críticas sujeitas a vulnerabilidades de forma que os riscos possam ser gerenciados.
Nesse sentido, a Resolução 370 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 20212026, define o Índice de Serviços Críticos com Gestão de Risco como um dos indicadores do objetivo estratégico "Aprimorar Segurança da Informação e a Gestão de Dados". A intenção é avaliar se os serviços identificados como críticos possuem gestão de risco e se são aplicados.

10.2 Avaliação de Riscos

O processo de Avaliação de Riscos de Tecnologia da Informação possui as seguintes etapas: identificação de riscos, análise de riscos e avaliação de riscos.
11.2.1 Identificação de Riscos

Uma vez definidos os serviços críticos para a estratégia do Tribunal, a ação prática do gestor do ativo nesta etapa deve ser identificar os ativos de TI que suportam a execução desses serviços críticos. Tal atividade dá início a etapa de identificação dos riscos de TI. As ameaças e as vulnerabilidades associadas a cada ativo que suporta um serviço crítico devem ser levantadas conforme o estabelecido na norma ISO 27005, permitindo, assim, uma identificação mais apropriada dos riscos de TI.

11.2.2 Análise de Riscos

Na análise de riscos, para cada um dos riscos identificados na etapa anterior, a ação prática do gestor de risco deve ser definir os seguintes passos: avaliar a probabilidade e o impacto do risco e definir o nível desse risco.

Probabilidade - é a chance de um evento ocorrer dentro do prazo previsto para se alcançar o resultado ou objetivo. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final. Para estimar a probabilidade será usada uma escala qualitativa de cinco níveis, conforme a seguir.

	Escala de Probabilidade
Muito baixa	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
Baixa	o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo
Média	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte
Alta	Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerão nesse horizonte.
Muito alta	Ocorrência quase garantida no prazo associado ao objetivo

Impacto - o impacto mede o potencial comprometimento do objetivo ou resultado. Por exemplo, um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto. Segue abaixo a escala para impacto.

	Escala de Impacto
Muito baixo	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado.
Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
Médio	Compromete razoavelmente o alcance do objetivo/resultado.
Alto	Compromete a maior parte do atingimento do objetivo/resultado
Muito alto	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

Nível de Risco - O nível de risco é calculado a partir da combinação das escalas de probabilidade e de impacto. Para definir o nível de risco, deve ser usada a matriz abaixo.

Apresentaremos uma análise de risco exemplificativa. Consideraremos os seguintes eventos de riscos que poderiam afetar os sistemas essenciais:

Indisponibilidade da rede de dados;

Impacto: alto

Probabilidade: baixa

Perda da base de dados, sem possibilidade de recuperação.

Impacto: muito alto

Probabilidade: média

Olhando para a tabela acima é possível deduzir o nível de risco de cada um dos dois eventos: o nível de risco de (a) é 14 e o de (b) é 22. O nível de risco é dado pelo número inscrito em cada célula da matriz, não sendo obtido por qualquer fórmula matemática. São 25 possíveis níveis de risco, em que cada nível está associado a uma estimativa de probabilidade e de impacto. A matriz ordena os possíveis níveis de risco, desde o mais baixo, ao qual é atribuído o nível 1 (evento muito raro, de impacto muito baixo), até o mais elevado, ao qual se atribui o nível 25 (probabilidade muito alta, evento praticamente certo, e de impacto muito alto)

Algumas considerações importantes sobre o uso no TJPI das matrizes de impacto e probabilidade:

O impacto é a dimensão mais importante: um evento de impacto muito alto e de probabilidade de ocorrência muito baixa deve preocupar o gestor muito mais do que o oposto, um evento de probabilidade muito alta e impacto muito baixo - se o impacto é mínimo, logo a preocupação deve ser menor.

Atribuição de valores arbitrários: deve-se evitar o uso de matrizes que "calculam" o nível do risco pela soma ou multiplicação desses valores, dado o risco de distorção trazido por matrizes simétricas, que consideraram como do mesmo nível os riscos descritos no item anterior. Na matriz acima apresentada, um risco com probabilidade muito baixa e impacto muito alto é classificado como de nível 15, enquanto outro risco de probabilidade muito alta e impacto muito baixo é considerado de nível 11, ou seja, é bem menos prioritário para a ação do gestor do que o de nível 15.

Fazer a avaliação dos riscos considerando a situação real do TJPI (considerando os controles existentes e em funcionamento).

10.2.1 Categorias de riscos

Estratégico: Estão associados à tomada de decisão que pode afetar negativamente o alcance dos objetivos da organização. o **Operacional:** Riscos que afetam o desempenho e a qualidade das atividades operacionais de TI. Os riscos devem ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos.

Reputação ou Imagem: Riscos que podem afetar a imagem da STIC ou do Tribunal. Os riscos **devem** ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos. o **Financeiro: Estão** associados ao não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.

Conformidade: Riscos externos ao controle direto do TJPI, mas que ainda assim podem afetar o sucesso das metas e ações. Os riscos externos podem ser aceitos, pois independem de ação direta do TJPI. o **Tecnologias:** Riscos relacionados a problemas técnicos em hardware, software ou outra solução de informática. o **Infraestrutura de TI:** Riscos relacionados a problemas técnicos em hardware, software, ou demais equipamentos de TI (exige conhecimento técnico para definir esta categoria).

Software: Riscos relacionados a problemas técnicos em um software específico (exige conhecimento técnico para definir esta categoria). o **Escopo:** Riscos relacionados ao assunto escopo de um projeto, exemplo: indefinições, alterações constantes, sem validação. o **Cliente / Usuário:** Riscos relacionados a clientes ou usuários de algum projeto, por exemplo: indefinição, representante ausente, sem comprometimento.

10.2.2 Avaliação de Riscos

A avaliação do risco envolve a comparação do nível de risco dos ativos do TJPI com o limite de exposição a riscos, a fim de determinar que riscos o Tribunal está disposto a aceitar. 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 real fique abaixo do limite de exposição tolerável.

A ação prática do gestor de risco nesta fase deve ser: identificar, na matriz probabilidade e impacto, os riscos cujos níveis estão acima do limite de exposição a riscos (faixa vermelha) e, para esses riscos, identificar as respectivas fontes, causas e consequências; os riscos que estão na faixa amarela, abaixo do limite de exposição a riscos, deverão ser monitorados os riscos que estão na faixa verde, também abaixo do limite de exposição, podem ser aceitos sem que nenhuma providência tenha que ser tomada.
Para retratar o exposto neste parágrafo, segue uma tabela na sequência.

10.3 Tratamento de Riscos

O tratamento de riscos está relacionado à resposta a riscos encontrados. Envolve decidir se o risco vai ser tratado ou não, promovendo a priorização de tratamento dos riscos. A estratégia de tratamento de risco adotada pelo TJPI é composta pelas opções: modificar o risco, aceitar o risco, evitar o risco e compartilhar o risco, conforme descrito na tabela a seguir.

RESPOSTA AO RISCO	DESCRIÇÃO
Modificar	O risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e considerado aceitável.
Aceitar	O objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, como: risco de baixo nível ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco.
Evitar	Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho.
Compartilhar	Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.

Conhecendo os riscos envolvidos em suas áreas de atuação e o resultado de suas análises, cada gestor deve levar em consideração o nível de tolerância ao risco e com isso tomar sua decisão sobre o tratamento dos riscos.
No Tratamento de Risco, a ação prática do gestor de risco é prover ações (respostas) para reduzir o nível de risco mapeado nos passos anteriores. Essas ações podem envolver controles, capacitação, redesenho de processo, realocação de pessoas, aperfeiçoamento de soluções de TI, etc. que, ao final, irão modificar, evitar, aceitar ou compartilhar os riscos.

10.4 Monitoramento e Análise Crítica

O monitoramento trata da revisão e avaliação periódica da gestão de riscos, objetivando aprimorar continuamente a instituição. O monitoramento tem finalidade de:
Garantir que os controles sejam eficazes e eficientes no projeto e na operação.
Obter informações adicionais para melhorar a avaliação dos riscos.
Analisar os eventos, as mudanças e aprender com o sucesso ou fracasso do tratamento dos riscos.
Detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que poderão exigir a revisão da forma de tratar os riscos e das prioridades.
Identificar os riscos emergentes, que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo de gestão de riscos.
Convém que os resultados do monitoramento e da análise crítica sejam registrados e reportados periodicamente.

10.5 Comunicação e Consulta

A comunicação e a consulta constituem o fluxo de informações entre as partes envolvidas no processo de gestão de riscos a fim de assegurar a compreensão necessária à tomada de decisão, devendo durante todas as fases do processo de gestão de riscos. As informações devem estar consolidadas e organizadas de forma que seja fácil e inteligível o acompanhamento de todo o processo.
A consulta consiste na disponibilização das informações consolidadas em local de fácil acesso, como o portal corporativo do Tribunal. A comunicação consiste no envio periódico das informações disponibilizadas na consulta para todos os envolvidos.

11. Recursos

Faz-se necessário que o TJPI aloque recursos apropriados para a gestão de riscos. Tais recursos podem ser pessoas, processos, tecnologia da informação, comunicação e treinamento.

13. Papéis e responsabilidades

Para gerenciar o processo de gestão de riscos institucional, os integrantes de governança e gestão de riscos do TJPI serão as seguintes unidades organizacionais:
Gestores das unidades da STIC - representa os chefes das unidades administrativas internas da STIC - Secretaria de Tecnologia da Informação e Comunicação. São responsáveis por identificar, analisar, propor tratamento e
acompanhar o tratamento dos riscos.;
Comitê Gestor de Tecnologia da Informação (CGTI) - responsável pela avaliação das proposições de tratamento de riscos produzidas, chancelando a validade, momento e modo de implementação de cada tratamento.;
Gestores de risco - servidores designados da STIC com aptidão para implantar as medidas definidas no plano de tratamento de riscos.

14. Atualização da Norma

As diretrizes previstas na presente norma serão atualizadas na forma do art. 14 § 1º da Política de Segurança da Informação vigente, sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.

Documento assinado eletronicamente por **José Ribamar Oliveira**, **Presidente**, em 30/09/2022, às 14:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **3669739** e o código CRC **A428066E**.

1.12. Portaria Nº 4227/2022 - PJPI/TJPI/PRESIDENCIA/SECGER, de 30 de setembro de 2022

PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ, Desembargador **JOSÉ RIBAMAR OLIVEIRA**, no uso de suas atribuições legais e regimentais, etc.
CONSIDERANDO a edição da Resolução n. 227, de 15 de junho de 2016, do Conselho Nacional de Justiça, que regulamenta o teletrabalho no âmbito do Poder Judiciário brasileiro;
CONSIDERANDO o Provimento Conjunto Nº 35/2017, de 19 de julho de 2017 que regulamenta o teletrabalho no âmbito do Poder Judiciário do Estado do Piauí e dá outras providências;
CONSIDERANDO a Decisão Nº 12952/2022 - PJPI/TJPI/PRESIDENCIA/SECGER, proferida nos autos do Processo SEI 22.0.000092856-2;
R E S O L V E :
Art. 1º **CONCEDER** o regime de teletrabalho na ESCOLA JUDICIÁRIA DO PIAUÍ - EJUD-PI, em benefício de CLAUDIA JESUS XAVIER DE LIMA, Analista Judicial, área Judiciária, Matrícula 105223-3**,** pelo prazo de 01 (um) ano, a partir da publicação da portaria de concessão do