TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

ATA DE REUNIÃO N. 002/2020

I. Identificação da Reunião

Data	Horário		Local	Coordenador
	Início	Término		
09.09.20	13h30	15h00	Videoconferência	Marcos Flávio Nascimento Maia

II. Objetivo

Reunião da CPSI para tratar dos seguintes assuntos:

- Análise da revisão dos processos:
  - "Elaboração, Acompanhamento e Revisão da Política de Segurança da Informação"
  - "Classificação da Informação, tratamento e grau de sigilo"
  - "Gerenciamento de Incidentes em Segurança da Informação"
- Apresentação do processo de "Gestão de Riscos da Segurança da Informação"
- Apresentação das análises de riscos dos seguintes processos que interferem em Segurança da Informação (Memorando nº 39/STIE - PAE 6844/2020):
  - Atendimento ao PJe - Problemas Técnicos
  - Gerenciamento de Cópias de Segurança (backup) e de restauração de dados
- Tomada de decisão estratégica com base nos riscos tratados, demonstrados no item anterior
- Avaliação da Política de Segurança da Informação (Res. TRE/RN 20/2019)
- Panorama da Segurança da Informação no TRE/RN
  - Divulgação mensal de informativos de segurança
  - Eventos de Segurança da Informação
  - Curso de disseminação
  - Grupos de estudo para melhoria da segurança da informação

III. Participantes

Nome	Lotação	Assinatura
Marcos Flávio Nascimento Maia - Presidente da CPSI	STIE	
Osmar Fernandes de Oliveira Júnior	COSIS/STIE	
Carlos Magno do Rozário Câmara	COINF/STIE	

Renato Vilar de Lima	ASCOM/ PRES	
Maria Ruth Bezerra Maia de Hollanda	AGE/ PRES	
Fernanda Araújo Cruz Barbosa	GAPDG	
Zeneide Lobato Reis da Silva	GAPSAOF	
Denilson Bastos da Silva	SSI/COINF/ STIC	
Helder Jean Brito da Silva	SSI/COINF /STIC	
Francisco de Assis Paiva Leal	SSI/COINF/ STIC	
Daniel César Gurgel Coelho Ponte	SRI/COINF/ STIC	
Leonardo Dantas de Oliveira	SRI/COINF/ STIC	
Alexandre Márcio Cavalcanti Machado	SMI/COINF/ STIC	
José Wendell de Morais Silva	SBDS/COSIS/ STIC	
Henrique Eduardo Calife de França	SMI/COINF/ STIC	
Jussara de Gois Borba Melo Diniz	GAPSTIC	

IV. Discussão da Pauta

Nº	Descrição/Decisão	Responsável
01	● Análise da revisão dos processos: ○ "Elaboração, Acompanhamento e Revisão da Política de Segurança da Informação" ○ "Classificação da Informação, tratamento e grau de sigilo" ○ "Gerenciamento de Incidentes em Segurança da Informação" A reunião foi iniciada com um panorama geral do que seria tratado na pauta. Em seguida, Marcos, Presidente da Comissão, iniciou pelos processos instituídos no ano de 2019, relacionados à Segurança da Informação. Para cada um dos processos citados, instituídos respectivamente pelas Portarias n.º 182/2019-GP, 184/2019-GP e 185/2019-GP, foram realizadas análises dos desenhos e manuais, ao fim de que concluiu-se que os mesmos estão sendo executados conforme instituídos e que não necessitam de alteração, sendo validado por todos os participantes	Marcos Maia
02	● Apresentação do processo de "Gestão de Riscos da Segurança da Informação" Em seguida, foi apresentada a modelagem do processo de "Gestão de Riscos da Segurança da Informação", pelo servidor da SSI/COINF, Francisco Leal, que demonstrou o fluxo do processo, sendo o mesmo aprovado pelos participantes, conforme Anexo 1 desta ata.	Francisco Leal/ Marcos Maia
03	● Apresentação das análises de riscos dos seguintes processos que interferem em Segurança da Informação (Memorando nº 39/STIE - PAE 6844/2020): ○ Atendimento ao PJe - Problemas Técnicos ○ Gerenciamento de Cópias de Segurança (backup) e de restauração de dados Ato contínuo, foram apresentadas aos participantes as análises de riscos realizadas em dois processos modelados pela STIE relacionados diretamente à Segurança da Informação: "Atendimento ao PJe - Problemas Técnicos" e "Gerenciamento de Cópias de Segurança (backup) e de restauração de dados". Foram apresentados os artefatos produzidos e aprovados pelo CGesTIC que impactam diretamente em medidas de segurança e efetividade da área técnica. O levantamento dos riscos dos processos constam, respectivamente, nos Anexos 2 e 3 desta ata.	Marcos Maia/ Osmar Fernandes
04	● Tomada de decisão estratégica com base nos riscos tratados, demonstrados no item anterior A partir dos riscos identificados pelas unidades técnicas da STIE, foram submetidas aos participantes, os principais direcionamentos para minimizar as chances de ocorrência dos riscos identificados. Desta forma, a Comissão	Todos os participantes

	ratificou o levantamento dos riscos e, visto tratar-se de assunto de suma importância e de alcance estratégico, elencou as decisões conforme o Anexo 4 desta ata.	
05	● Avaliação da Política de Segurança da Informação (Res. TRE/RN 20/2019) Sobre a Política de Segurança da Informação do TRE/RN, instituída pela Resolução TRE/RN n.º 20/2019, a Comissão debruçou-se sobre os seus termos e verificou que, durante este 01 (um) ano de vigência da norma, as ações das comissões e unidades deste Tribunal estão agindo em conformidade com a norma, dando-lhe efetividade, principalmente no que diz respeito aos seguintes pontos: ● Sobre classificação da informação (Art. 8º - conformidade) ● Estrutura normativa (Art. 9º - conformidade) ● Adequação aos tipos documentais (Art. 10º - conformidade) ● Das competências (Arts. 12 a 28 - conformidade)	Todos os participantes
06	● Panorama da Segurança da Informação no TRE/RN Realizando análise sobre a situação da Segurança da Informação no TRE/RN, foram realizadas análises sobre os seguintes pontos: ○ Aquisições de melhorias para o Datacenter Foi destacado o direcionamento do CGovTIC, principalmente, na pessoa do então Presidente do Comitê de Governança, Des. Glauber Rêgo, que demonstrou total apoio, elencando como estratégicas as aquisições que garantam as melhorias técnicas e de segurança relacionadas ao Datacenter deste Tribunal. Objetivando minimizar os riscos e ampliando as garantias, encontram-se em tramitação as aquisições referentes ao site backup, a solução de combate à incêndio e solução de climatização dos racks do Datacenter. ○ Publicação da Portaria n. 75/2020 Dando efetividade ao Plano de Ação aprovado pela CPSI na reunião 01/2020, foi publicada a Portaria n. 75/2020- GP, que dispõe sobre a política de atualização dos sistemas operacionais dos servidores de rede físicos e virtuais, que garantirá, de forma sistematizada, uma camada extra de segurança para os serviços e soluções disponibilizados pela STIE.	Todos os participantes

06	○ Divulgação mensal de informativos de segurança Também de acordo com o Plano de Ação, está em andamento a divulgação dos informativos mensais que levam aos servidores do Tribunal informações, dicas e procedimentos, de forma clara e objetiva, sobre os mais diversos temas relacionados à Segurança da Informação. Já estamos na divulgação da terceira edição do informativo que recebeu o nome de "Segurança em Foco". Todos os informativos encontram-se publicados em http://www.tre-rn.jus.br/transparencia/governanca-e-gestao-de-tic/sistema-de-gestao-da-seguranca-da-informacao/sistema-de-gestao-da-seguranca-da-informacao ○ Eventos de Segurança da Informação Em relação à realização de eventos, no formato de webinar, para o público externo e interno, sobre segurança da informação e segurança do processo eletrônico, programados inicialmente para ocorrer no mês de setembro, em razão da mudança de gestão e necessidade de algumas adaptações, o evento será formatado para ser realizado no mês de outubro/2020, ainda conforme planejado no Plano de Ação da CPSI. ○ Curso de disseminação O Curso de disseminação encontra-se em desenvolvimento (por servidores ligados à CPSI e unidades da STIE), será disponibilizado na plataforma do moodle do TRE/RN, com tempo de realização de 03 meses, carga horária de 10 horas e deverá contar com participação maciça dos servidores do Tribunal. ○ Grupos de estudo para melhoria da segurança da informação Com relação aos grupos de estudo criados no âmbito da STIE, cujos objetivos encontram-se listados abaixo, Marcos apresentou aos participantes como encontra-se o andamento de cada um deles, que estão sendo realizadas reuniões periódicas de acompanhamento e que um dos principais objetivos será a capacitação de servidores em análise de vulnerabilidades e realização de testes exaustivos de modo a verificar as falhas de segurança porventura existentes nos serviços e soluções de TI deste Tribunal, protegendo, de forma mais robusta os ativos de informação. São os temas dos grupos: ➔ 1.Estudar forma de viabilizar o sincronismo do banco Oracle para Postgres na DMZ, como forma de disponibilizar o PAE Consulta com mais segurança. ➔ 2.Estudar forma de disponibilizar o Sistema de Agendamento no portal internet, após as Eleições, sem a necessidade de uso de certificado digital, de forma segura.. ➔ 3.Estudar forma de restringir acesso à Extranet através de certificado digital, de forma que seja autorizado somente servidor do TRE/RN e juiz eleitoral.	Todos os participantes

	➔ 4. Estudar forma de realização de testes exaustivos de invasão nos sistemas desenvolvidos pelo TRE/RN, como forma de identificar as vulnerabilidades.	
07	Como fechamento, tanto Marcos Maia quanto Carlos Magno destacaram a importância da criação da SSI/COINF, que passou por nova revisão de suas competências, aprovadas na Resolução TRE/RN n. 29/2020, que fortaleceu ainda mais a STIE e a Seção, permitindo que os servidores ali lotados dediquem-se ainda mais às questões relacionadas à segurança da informação. Destacaram, por fim, a importância da disseminação das ações técnicas realizadas no âmbito da STIE para os demais componentes da Comissão.	Marcos Maia/ Carlos Magno

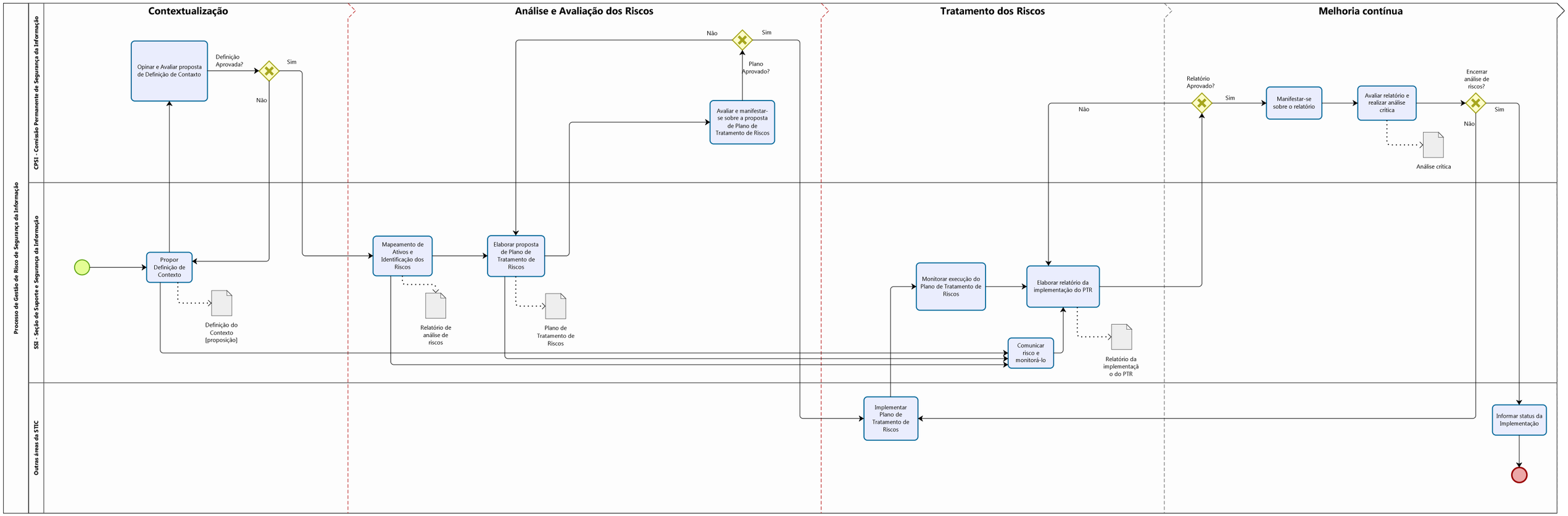
V. <u>Fechamento da Ata</u>

Data	Nome do relator	Assinatura
09.09.2020	Jussara de Gois Borba Melo Diniz	

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

ANEXO I

REUNIÃO N. 02/2020 - CPSI


Processo de Gestão de Risco da Segurança da Informação
CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Suporte e Segurança da Informação
Outras áreas da STIC
Contextualização
Análise e Avaliação dos Riscos
Tratamento dos Riscos
Melhoria contínua
Opinar e Avaliar proposta de Definição de Contaxto
Definição Aprovada?
Sim
Não
Propor Definição de Contexto
Definição do Contexto [proposição]
Mapeamento de Ativos e Identificação dos Riscos
Relatório de análise de riscos
Elaborar proposta de Plano de Tratamento de Riscos
Plano de Tratamento de Riscos
Não
Sim
Plano Aprovado?
Avaliar e manifestar-se sobre a proposta de Plano de Tratamento de Riscos
Implementar Plano de Tratamento de Riscos
Monitorar execução do Plano de Tratamento de Riscos
Comunicar risco e monitorá-lo
Elaborar relatório da implementação do PTR
Relatório da implementação do PTR
Não
Relatório Aprovado?
Sim
Manifestar-se sobre o relatório
Avaliar relatório e realizar análise crítica
Análise crítica
Encerrar análise de riscos?
Não
Sim
Informar status da Implementação

ANEXO II

REUNIÃO N. 02/2020 - CPSI

Tribunal Regional Eleitoral
do Rio Grande do Norte

Gestão de Riscos

Processo: 10.1.x. Atendimento ao PJe - Problemas Técnicos

Versão 1.0

Natal, 02/08/2020

2020 Tribunal Regional Eleitoral do Rio Grande do Norte
Presidente do TRE-RN
Desembargador Glauber Antônio Nunes Rêgo

Diretora-Geral da Secretaria
Simone Maria de Oliveira Soares Mello

Assessoria de Planejamento e Gestão Estratégica – ASPLAN / Presidência
Yvette Bezerra Guerreiro Maia

Preparação, organização, revisão e edição
Escritório de Processos Organizacionais - EPO
Iaperi Gábor Damasceno Árbocz

Participantes das unidades envolvidas no processo
Marcos Flávio Nascimento Maia - STIC
Dina Márcia Vasconcelos de Maranhão Câmara - GAPSTIC
Jussara de Gois Borba Melo Diniz - GAPSTIC
Ana Karla Tomaz Costa - GAPSTIC
Mônica Paim Veppo dos Santos - GAPSTIC
Osmar Fernandes de Oliveira Júnior - COSIS
Carlos Magno do Rozário Câmara - COINF
Tyronne Dantas de Medeiros - COTEL
José Frank Viana da Silva - SNT
George Melo de Freitas Barbalho - SDS
Thiago Fernandes Silva Dutra - SBDS

Controle de Versões

Versão	Data	Responsável	Descrição
1.0	XXXXXXXX	Iaperi Árbocz – EPO (Consolidação)	Versão inicial aprovada pelo Comitê de Gestão de Riscos.

Apresentação

O presente documento reúne o trabalho de aplicação do Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte, que foi aprovado pela Resolução Nº 17/2017 (DJe, 29/12/2017), ao processo "10.1.x. Atendimento ao PJe - Problemas Técnicos" da Cadeia de Valor[1].

A execução do processo de gestão de riscos envolveu os responsáveis pelas unidades envolvidas no processo de solicitação de demandas de sistemas e abrangeu a aplicação de todas as etapas previstas no manual do processo, a saber: Identificação de riscos, Análise de riscos, Avaliação de riscos e Tratamento de riscos.

A elaboração do presente estudo teve por base o trabalho desenvolvido pela Secretaria de Tecnologia da Informação e Comunicação aplicado ao processo "6.1.3.4. Elaboração e Gestão do Plano de Contratações de Soluções TIC", realizado com o apoio do Escritório de Processos Organizacionais – EPO.

A proposta é disseminar a aplicação da Política de Gestão de Riscos a outros processos de trabalho já modelados pela STIC, buscando-se efetivar a implantação da política de gestão de riscos da instituição, o modelo de Gestão de Riscos vigente e o papel dos gestores operacionais, que se constituem na 1ª linha de defesa do gerenciamento de riscos dentro de uma organização.

Marcos Flávio Nascimento Maia
Secretário de Tecnologia da Informação e Comunicação

[1] Cadeia de Valor da Justiça Eleitoral do Rio Grande do Norte, aprovada pela Portaria Nº 179/2018-GP (DJe de 08/08/2018).

Sumário

1. Declaração de Apetite a Risco

Após a aplicação do Modelo de Gestão de Riscos estabelecido pela Resolução Nº 17/2017, conforme as disposições do "Manual do Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte", nos quatro atores do "Processo: 10.1.x. Atendimento ao PJe - Problemas Técnicos", restaram identificados, avaliados e tratados 9 (nove) riscos, vinculados às 14 (catorze) atividades do referido processo. Os riscos identificados foram classificados como Operacionais.

A tabela a seguir apresenta os quantitativos já indicados e explicita o "Nível de Risco Residual" das atividades analisadas, segundo a avaliação realizada pelos responsáveis das unidades que atuam no processo de atendimento técnico ao PJe.

Tabela – Quantidades de Atividades, Riscos e o Nível de Risco Residual (Média)

Ator do Processo	Quantidade de Atividades	Quantidade de Riscos Identificados	Nível de Risco Residual das Atividades (Média)
1. Solicitante	1	1	8 (Baixo)
2. Central de Serviço	4	2	6 (Baixo)
3. SBDS - Seção de Banco de Dados e Sistemas	8	5	7,2 (Baixo)
4. TSE - Tribunal Superior Eleitoral	1	1	8 (Baixo)
Total Geral / Média Geral	**14**	**8**	7,3 (Baixo)

Convenções de cores adotadas: (Verde) nível baixo de riscos e (Amarela) nível médio de riscos.

Em todos os riscos levantados, o Nível de Risco Residual das atividades do processo restou classificado como baixo, o que, em termos da média das atividades, resultou em um resultado de 7,3 (sete vírgula três) pontos, classificando o conjunto das atividades do processo com um nível baixo de riscos.

Ante o exposto e tendo em vista especialmente o item 11 do *Manual do Processo de Gestão de Riscos* sobre o Apetite a Risco, o Tribunal deve fixar o nível de risco considerado institucionalmente razoável para a execução de suas competências e atribuições legais. No presente caso, a fixação do nível de Apetite a Risco que orienta a execução das atividades e a manutenção do nível de riscos declarado pelos responsáveis, refletindo a eficácia da Gestão de Riscos, ou seja, o alcance dos resultados planejados, resultou, em termos da média do conjunto das atividades (7,3 pontos), portanto, no nível baixo (7,3).

Tabela – Apetite a Risco do Processo

Apetite a Risco	
Processo	**Nível de Risco**
10.1.x. Atendimento ao PJe - Problemas Técnicos	Baixo (7,3 pontos)
Aprovação: Comitê de Gestão de Riscos, em 02/07/2020.	

2. Estabelecimento do Contexto

Responsável:	**Vigência:**	**Versão:**
Coordenador de Sistemas Corporativos	02 (dois) anos, a partir da data de aprovação.	1.0

Processo Organizacional: **10.1.x. Atendimento ao PJe - Problemas Técnicos**

2.1. Referências na Cadeia de Valor / Arquitetura de Processos

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.x. Atendimento ao PJe - Problemas Técnicos

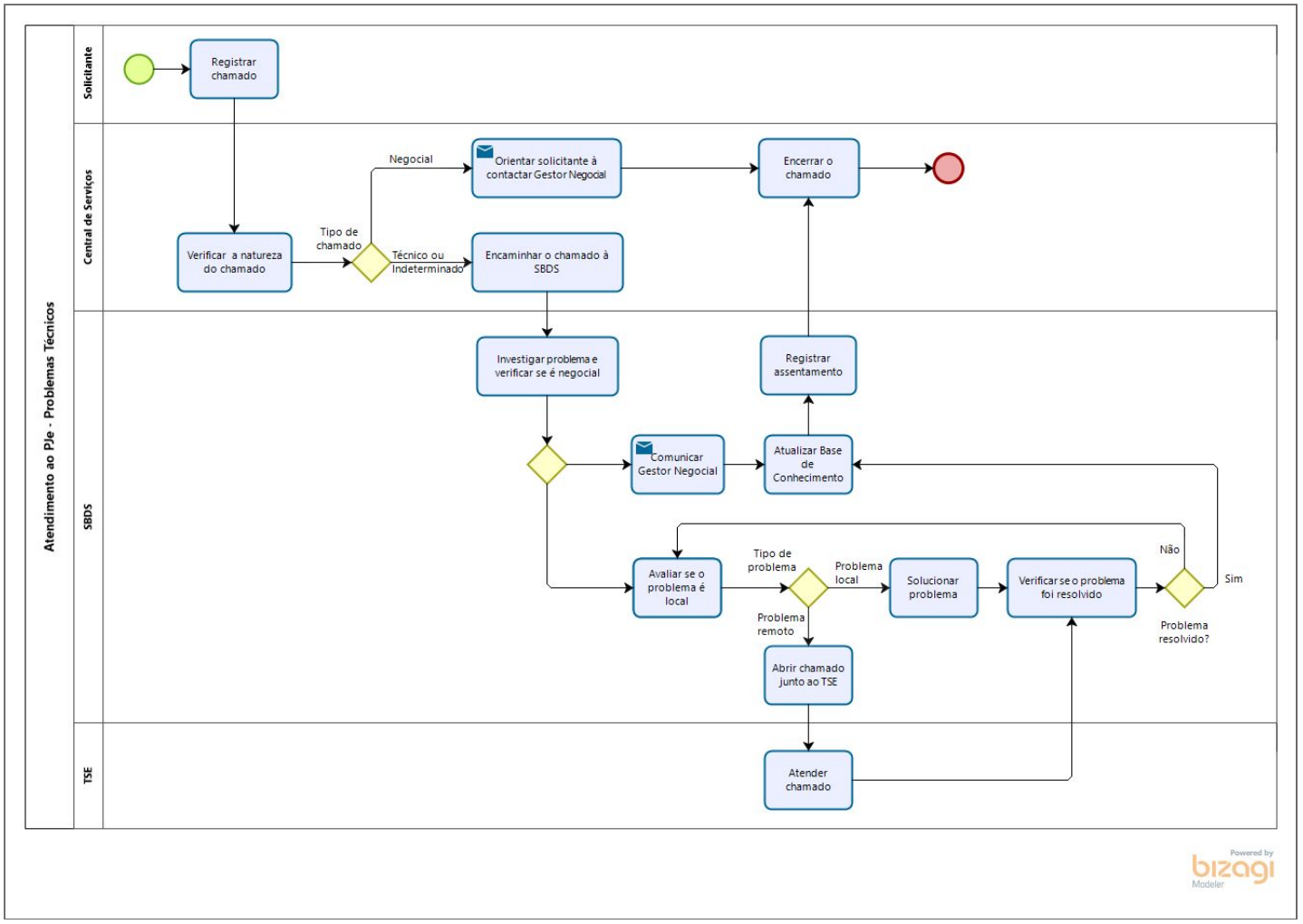
2.2. Objetivos do Processo

O sistema PJe é utilizado pela Justiça Eleitoral do RN para gerenciamento e tramitação de processos judiciais eletrônicos no âmbito do 1º e 2º graus de jurisdição. Ele é utilizado por advogados, servidores dos Cartórios e da Secretaria do TRE-RN, além de ser acessível à qualquer cidadão, via Internet, para consulta de processos públicos. Eventuais problemas na utilização do sistema podem ser de natureza negocial ou técnica, sendo este último tipo, objeto da modelagem do processo "Atendimento ao PJe - Problemas Técnicos".

O presente processo foi instituído formalmente a partir da Portaria n.º xxx/xxx-GP, devendo ser revisto anualmente, visando ganhos de eficiência e eficácia para o processo como um todo.

A representação do processo em *Business Process Model Notation* (BPMN) é apresentada na figura a seguir, onde é possível verificar o detalhamento das atividades de cada um dos oito atores funcionais que atuam no processo, de modo a permitir a identificação dos pontos frágeis que são passíveis de riscos, visando à aplicação do Processo de Gestão de Riscos.

Figura – Representação BPMN do Processo



Na representação gráfica do processo, acima, é possível identificar os artefatos que são produzidos em cada atividade, ressaltando-se a importância de sua padronização para a garantia de homogeneidade e fluidez do processo, minimizando erros de interpretações que possam comprometer a sua execução.

2.3. Quadro Resumo

ANÁLISE DO CONTEXTO Quadro Resumo
Processo: **10.1.x. Atendimento ao PJe - Problemas Técnicos**
Objetivos e Metas: ● Disciplinar a forma como demandas relacionadas à problemas técnicos no sistema PJe (1º e 2º graus) são apresentados pelos solicitantes. ● Plano Estratégico da Justiça Eleitoral do Rio Grande do Norte – PEJERN 2016-2020 - Objetivo Estratégico 09: Aprimoramento da infraestrutura, da gestão e da governança de TIC ● Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) - 2016/2020 - Objetivo Estratégico 02: Prover Soluções Efetivas de TIC
Processos de Gestão e Governança associados: ● Plano Estratégico da Justiça Eleitoral do Rio Grande do Norte – PEJERN 2016-2020 ● Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) - 2016/2020 ● Plano Diretivo de Tecnologia da Informação e Comunicação (PDTIC) ● Comitê de Governança de Tecnologia da Informação e Comunicação (CGovTIC) ● Comitê Gestor de Tecnologia da Informação e Comunicação (CGesTIC)
Sistemas utilizados: ● Processo Judicial Eletrônico – PJE (TRE-RN).
Partes interessadas: ● Internas (SJ, CRE-RN, Cartórios Eleitorais); e ● Externas (Advogados, Cidadãos em geral).

3. Matriz SWOT

A análise das fraquezas, forças, ameaças e oportunidades relativas ao processo "10.1.x. Atendimento ao PJe - problemas Técnicos" encontra-se apresentada na matriz SWOT (*Strenghts, Weaknesses, Opportunities* e *Threats*) a seguir:

Tabela – Matriz SWOT do Processo

FATORES INTERNOS	**FORÇAS**	**FRAQUEZAS**
	Padronização do processo de trabalho.	Necessidade de maior organização envolvendo atores internos do Tribunal envolvidos no atendimento às demandas do PJe.
	Alimentação contínua da base de conhecimentos sobre o tratamento de problemas relacionados ao PJe.	Falta de um sistema formal para controle e registro de demandas de natureza negocial.
FATORES EXTERNOS	**OPORTUNIDADES**	**AMEAÇAS**
	Maior agilidade no atendimento de demandas do PJe, garantindo maior satisfação de usuários externos, como os Advogados.	Susceptibilidade e dependência técnica do Tribunal Superior Eleitoral, responsável pela implantação nacional do sistema.
		Eventuais conflitos relacionadas à natureza técnica ou negocial de dúvidas demandadas.

4. Matriz RACI

A matriz de designação de responsabilidades responsável pela atribuição de funções e responsabilidades relacionadas ao processo "10.1.x. Atendimento ao PJe - Problemas Técnicos" encontra-se representada na Matriz RACI (*Responsible*, *Accountable*, *Consulted* e *Informed*) a seguir:

Tabela – Matriz RACI do Processo

MATRIZ RACI				
Processo Organizacional: 10.2.1.x. Solicitação de Demandas de Sistemas				
Responsável: Coordenador de Sistemas Corporativos			**Data:** 27/07/2020	
Papel **Responsabilidade**	Solicitante	Central de Serviço	SBDS	TSE
1. Registrar Chamado	R			
2. Verificar a Natureza do Chamado		R	C	
3. Orientar Solicitante à Procurar Gestor Negocial		R		
4. Encaminhar chamado à SBDS		R		
5. Encerrar o chamado		R		
6. Investigar Problema e Verificar se é Negocial			R	
7. Comunicar Gestor Negocial			R	
8. Atualizar Base de Conhecimento			R	
9. Registrar Assentamento	I		R	
10. Avaliar se o problema é local			R	
11. Abrir chamado junto ao TSE			R	I
12. Solucionar o Problema			R	C
13. Verificar se o problema foi resolvido	A		R	
14. Atender Chamado			C	R

Legenda	
R – Responsável	É quem executa a atividade efetivamente.
A – Aprovado	É quem aprova ou valida formalmente a atividade ou produto dela resultante.
C – Consultado	É quem gera uma informação que agrega valor para execução de uma atividade ou quem apoia à sua execução.
I – Informado	É quem precisa ser notificado do resultado da atividade.

O Processo de Gestão de Riscos aprovado pela Resolução Nº 17/2017-TRE/RN estabelece a Matriz de Riscos com as escalas de probabilidade e impacto, os critérios de avaliação da frequência (análise quantitativa) e os critérios de avaliação qualitativa dos riscos por eventos, as classes de risco e os critérios de priorização. Todos os atores, conceitos e procedimentos estão detalhados no “Manual do Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte”, anexo à referida resolução.

Outras diretrizes que forem estabelecidas pelo Comitê de Gestão de Riscos, caso impactem na análise desenvolvida, poderão implicar na revisão dos documentos das etapas da gestão de riscos aplicadas ao presente processo, sendo devidamente registradas as circunstâncias e as alterações.

Anexo I - Formulário Padrão de Identificação e Avaliação de Riscos

1. Solicitante

2. Central de Serviços

3. SBDS - Seção de Banco de Dados e Sistemas

4. TSE - Tribunal Superior Eleitoral

Anexo I - 1. Solicitante

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 02/08/2020 | **Unidade:** Unidade do solicitante | **Gestor de Riscos:** Solicitante

Risco	Causa	Classe	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Demanda não solicitada através do sistema de chamados.	Desconhecimento da necessidade de abertura de chamado, ou por se tratar de um usuário da alta administração.	Operacional	Médio (6)	Média (6)	36	Alto	Falta de padronização no atendimento das demandas, e eventual falha na consulta e registro das lições aprendidas.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	Unidade solicitante	Solicitante

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    - 10.1. Processo: Gerenciamento de Serviços de TIC
      - 10.1.X. Atendimento ao PJe - Problemas Técnicos
        - **10.1.x.1. Registrar Chamado *(Risco 1)***

Anexo I - 2. Central de Serviços

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Identificação e Avaliação de Riscos														
Data: 02/08/2020			**Unidade:** Central de Serviços					**Gestor de Riscos:** Coordenador da Central de Serviços						
Risco	Causa	Classe	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Identificação incorretamente a natureza do chamado.	Base de conhecimento mal alimentada ou incompleta.	Operacional	Baixo (4)	Baixa (4)	16	Médio	O demandante pode ser comunicado incorretamente que o problema seria de natureza negocial.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	Central de Serviços	Coordenador da Central de Serviços
(2) Demora na comunicação com o demandante.	Sobrecarga de atividades na Central.	Operacional	Baixo (4)	Muito Baixa (2)	8	Baixo	O demandante pode buscar outros canais para sanar o seu questionamento.	Mitigar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	Central de Serviços	Coordenador da Central de Serviços

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    - 10.1. Processo: Gerenciamento de Serviços de TIC
      - 10.1.X. Atendimento ao PJe - Problemas Técnicos
        - **10.1.x.2. Verificar a Natureza do Chamado *(Risco 1)***
        - **10.1.x.3. Orientar Solicitante à Procurar Gestor Negocial *(Risco 2)***

Anexo I - 3. SBDS - Seção de Banco de Dados e Sistemas

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 02/08/2020 | **Unidade:** SBDS | **Gestor de Riscos:** Chefe da SBDS

Risco	Causa	Classe	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Classificar o chamado incorretamente como negocial.	Base de conhecimento mal alimentada ou incompleta.	Operacional	Baixo (4)	Baixa (4)	16	Médio	Repasse da demanda indevidamente para a área de negócios.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SBDS	Chefe da SBDS
(2) Repasse incompleto para a área de negócios.	Sobrecarga de atividades na unidade.	Operacional	Baixo (4)	Muito Baixa (2)	8	Baixo	A área de negócios receberia informações incompletas sobre o problema relatado.	Mitigar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	SBDS	Chefe da SBDS
(3) Não realização do registro na base de conhecimento.	Esquecimento por parte da unidade técnica.	Operacional	Baixo (4)	Baixa (4)	16	Médio	Empobrecimento da base de conhecimento.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SBDS	Chefe da SBDS
(4) Não realização do assentamento no sistema de chamados.	Esquecimento por parte da unidade técnica.	Operacional	Baixo (4)	Baixa (4)	16	Médio	Falta de rastreabilidade das ações executadas ao longo do atendimento do chamado.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SBDS	Chefe da SBDS
(5) Demora na solução do problema.	Desconhecimento técnico sobre a infraestrutura do PJe	Operacional	Alto (8)	Média (6)	48	Alto	Atraso na solução do problema, com repercussões junto ao demandante.	Mitigar o risco	Muito Baixo (2)	Baixa (4)	8	Baixo	Não	SBDS	Chefe da SBDS

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.6. Investigar Problema e Verificar se é Negocial *(Risco 1)*
            10.1.x.7. Comunicar Gestor Negocial *(Risco 2)*
            10.1.x.8. Atualizar Base de Conhecimento *(Risco 3)*
            10.1.x.9. Registrar Assentamento *(Risco 4)*
            10.1.x.12. Solucionar o Problema *(Risco 5)*

Anexo I - 4. TSE - Tribunal Superior Eleitoral

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Identificação e Avaliação de Riscos														
Data: 02/08/2020			**Unidade:** SEDESC1/TSE					**Gestor de Riscos:** Chefe da SEDESC1/TSE						
Risco	Causa	Classe	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Demora no atendimento do chamado.	Sobrecarga de atividades junto à área técnica responsável no TSE.	Operacional	Médio (6)	Média (6)	36	Alto	Impacto nas atividades do demandante em que é necessário utilizar o PJe.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SEDESC1 /TSE	Chefe da SEDESC1/TSE

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação

10.1. Processo: Gerenciamento de Serviços de TIC

10.1.X. Atendimento ao PJe - Problemas Técnicos

10.1.x.14. Atender Chamado *(Risco 1)*

Anexo II - Formulário Padrão de Tratamento de Riscos

1. Solicitante

2. Central de Serviços

3. SBDS - Seção de Banco de Dados e Sistemas

4. TSE - Tribunal Superior Eleitoral

Anexo II - 1. Solicitante

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Tratamento de Riscos		
Data: 02/08/2020	**Área Funcional:** Unidade solicitante	**Proprietário do Risco:** Solicitante
Risco:	(1) Demanda não solicitada através do sistema de chamados.	
Probabilidade: Média (6)	**Impacto:** Médio (6)	**Nível do Risco:** Alto (36)
Resposta a ser implantada:	Publicar Comunicado da STIE informando aos usuários da Secretaria e Zonas Eleitorais da necessidade de abertura de chamado junto à STIE para atendimento de demandas relacionadas ao PJe.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Solicitante
Gestor de Risco Setorial

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.1. Registrar Chamado *(Risco 1)*

Anexo II - 2. Central de Serviços

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Tratamento de Riscos		
Data: 02/08/2020	**Área Funcional:** Central de Serviços	**Proprietário do Risco:** Coordenador da Central de Serviços
Risco:	(1) Identificação incorretamente a natureza do chamado.	
Probabilidade: Baixa (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	A área técnica realizará uma revisão da Base de Conhecimentos de modo a deixar mais claro a identificação da natureza da demanda no PJe, se técnica ou negocial.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020, até Novembro/2020.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Data: 02/08/2020	**Área Funcional:** Central de Serviços	**Proprietário do Risco:** Coordenador da Central de Serviços
Risco:	(2) Demora na comunicação com o demandante.	
Probabilidade: Muito baixa (2)	**Impacto:** Baixo (4)	**Nível do Risco:** Baixo (8)
Resposta a ser implantada:	Estabelecer junto à Central de Serviços uma priorização para o atendimento de chamados relacionados ao PJe.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (4)
Riscos Secundários:	Não foram identificados.	

Coordenador da Central de Serviços
Gestor de Risco Setorial

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.2. Verificar a Natureza do Chamado *(Risco 1)*
            10.1.x.3. Orientar Solicitante à Procurar Gestor Negocial *(Risco 2)*

Anexo II - 3. SBDS - Seção de Banco de Dados e Sistemas

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Tratamento de Riscos		
Data: 02/08/2020	**Área Funcional:** SBDS	**Proprietário do Risco:** Chefe da SBDS
Risco:	(1) Classificar o chamado incorretamente como negocial.	
Probabilidade: Baixa (4)	**Impacto:** Baixa (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	Atualizar continuamente a Base de Conhecimentos reportando as lições aprendidas em atendimentos anteriores.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Data: 02/08/2020	**Área Funcional:** SBDS	**Proprietário do Risco:** Chefe da SBDS
Risco:	(2) Repasse incompleto para a área de negócios.	
Probabilidade: Muito Baixa (2)	**Impacto:** Baixo (4)	**Nível do Risco:** Baixa (8)
Resposta a ser implantada:	Revisitar os assentamentos do chamado e as informações constantes na base de conhecimentos antes de enviar e-mail para a área negocial, reportando o problema informado pelo solicitante e pedindo providências.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (4)
Riscos Secundários:	Não foram identificados.	

Data: 02/08/2020	**Área Funcional:** SBDS	**Proprietário do Risco:** Chefe da SBDS
Risco:	(3) Não realização do registro na base de conhecimento.	
Probabilidade: Baixa (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Média (16)
Resposta a ser implantada:	Estabelecer uma rotina de revisão do chamado antes seu encerramento, garantindo que todas as informações relevantes sejam lançadas ou alteradas na base de conhecimento.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro de 2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Data: 02/08/2020	**Área Funcional:** SBDS	**Proprietário do Risco:** Chefe da SBDS
Risco:	(4) Não realização do assentamento no sistema de chamados.	
Probabilidade: Baixa (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Média (16)
Resposta a ser implantada:	Estabelecer uma rotina de revisão do chamado antes seu encerramento, garantindo que todas os assentamentos relevantes sejam lançados na ferramenta de chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Data: 02/08/2020	**Área Funcional:** SBDS	**Proprietário do Risco:** Chefe da SBDS
Risco:	(5) Demora na solução do problema.	
Probabilidade: Média (6)	**Impacto:** Alto (8)	**Nível do Risco:** Alto (48)
Resposta a ser implantada:	Priorizar, no âmbito da SBDS, o atendimento dos chamados técnicos relativos à problemas do PJe.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Baixa (4)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Chefe do SBDS
Gestor de Risco Setorial

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.6. Investigar Problema e Verificar se é Negocial *(Risco 1)*
            10.1.x.7. Comunicar Gestor Negocial *(Risco 2)*
            10.1.x.8. Atualizar Base de Conhecimento *(Risco 3)*
            10.1.x.9. Registrar Assentamento *(Risco 4)*
            10.1.x.12. Solucionar o Problema *(Risco 5)*

Anexo II - 4. TSE - Tribunal Superior Eleitoral

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Data: 02/08/2020	**Área Funcional:** SEDESC1/TSE	**Proprietário do Risco:** Chefe do SEDESC1/TSE
Risco:	(1) Demora no atendimento do chamado.	
Probabilidade: Média (6)	**Impacto:** Médio (6)	**Nível do Risco:** Alta (36)
Resposta a ser implantada:	(1) Acompanhar, no âmbito da SBDS, o atendimento dos chamados abertos junto ao TSE, reiterando-os quando necessários. (2) Em casos de demora excessiva, reportar a situação à COSIS, para tomada de providências junto à CSCOR/TSE.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A partir de Setembro/2020	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Riscos Secundários:	Não foram identificados.	

Chefe da SDS
Gestor de Risco Setorial

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.13. Atender Chamado *(Risco 1)*

Anexo III - Formulário Perfil de Riscos

1. Solicitante

2. Central de Serviços

3. SBDS - Seção de Banco de Dados e Sistemas

4. TSE - Tribunal Superior Eleitoral

Anexo III - 1. Solicitante

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Solicitante					**Área Funcional:** Unidade solicitante			**Data:** 02/08/2020
Risco (Descrição)	**Classe**	**Causa**	**Consequências**	**Resposta**	**Nível de Riscos (IxP)**		**Tipos de Resposta**	**Proprietário do Risco**
(1) Demanda não solicitada através do sistema de chamados.	Operacional	(1) Demanda não solicitada através do sistema de chamados. Desconhecimento da necessidade de abertura de chamado, ou por se tratar de um usuário da alta administração.	Falta de padronização no atendimento das demandas, e eventual falha na consulta e registro das lições aprendidas.	Publicar Comunicado da STIC informando aos usuários da Secretaria e Zonas Eleitorais da necessidade de abertura de chamado junto à STIC para atendimento de demandas relacionadas ao PJe.	Nível de Risco Inerente = 6 x 6 = 36 (Alto)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Solicitante

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação

10.1. Processo: Gerenciamento de Serviços de TIC

10.1.X. Atendimento ao PJe - Problemas Técnicos

10.1.x.1. Registrar Chamado *(Risco 1)*

Anexo III - 2. Central de Serviços

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Coordenador da Central de Serviços					**Área Funcional:** Central de Serviços			**Data:** 02/08/2020
Risco (Descrição)	**Classe**	**Causa**	**Consequências**	**Resposta**	**Nível de Riscos (IxP)**		**Tipos de Resposta**	**Proprietário do Risco**
(1) Identificação incorretamente a natureza do chamado.	Operacional	Base de conhecimento mal alimentada ou incompleta.	O demandante pode ser comunicado incorretamente que o problema seria de natureza negocial.	A área técnica realizará uma revisão da Base de Conhecimentos de modo a deixar mais claro a identificação da natureza da demanda no PJe, se técnica ou negocial.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Coordenador da Central de Serviços
(2) Demora na comunicação com o demandante.	Operacional	Sobrecarga de atividades na Central.	O demandante pode buscar outros canais para sanar o seu questionamento.	Estabelecer junto à Central de Serviços uma priorização para o atendimento de chamados relacionados ao PJe.	Nível de Risco Inerente = 4 x 2 = 8 (Baixo)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Mitigar o risco	Coordenador da Central de Serviços

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    - 10.1. Processo: Gerenciamento de Serviços de TIC
      - 10.1.X. Atendimento ao PJe - Problemas Técnicos
        - **10.1.x.2. Verificar a Natureza do Chamado *(Risco 1)***
        - **10.1.x.3. Orientar Solicitante à Procurar Gestor Negocial *(Risco 2)***

Anexo III - SBDS - Seção de Banco de Dados e Sistemas

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Chefe da SBDS					**Área Funcional:** SBDS			**Data:** 02/08/2020
Risco (Descrição)	**Classe**	**Causa**	**Consequências**	**Resposta**	**Nível de Riscos (IxP)**		**Tipos de Resposta**	**Proprietário do Risco**
(1) Classificar o chamado incorretamente como negocial.	Operacional	Base de conhecimento mal alimentada ou incompleta.	Repasse da demanda indevidamente para a área de negócios.	Atualizar continuamente a Base de Conhecimentos reportando as lições aprendidas em atendimentos anteriores.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SBDS
(2) Repasse incompleto para a área de negócios.	Operacional	Sobrecarga de atividades na unidade.	A área de negócios receberia informações incompletas sobre o problema relatado.	Revisitar os assentamentos do chamado e as informações constantes na base de conhecimentos antes de enviar e-mail para a área negocial, reportando o problema informado pelo solicitante e pedindo providências.	Nível de Risco Inerente = 4 x 2 = 8 (Baixo)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Mitigar o risco	Chefe da SBDS
(3) Não realização do registro na base de conhecimento.	Operacional	Esquecimento por parte da unidade técnica.	Empobrecimento da base de conhecimento.	Estabelecer uma rotina de revisão do chamado antes seu encerramento, garantindo que todas as informações relevantes sejam lançadas ou alteradas na base de conhecimento.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SBDS
(4) Não realização do assentamento no sistema de chamados.	Operacional	Esquecimento por parte da unidade técnica.	Falta de rastreabilidade das ações executadas ao longo do atendimento do chamado.	Estabelecer uma rotina de revisão do chamado antes seu encerramento, garantindo que todas os assentamentos relevantes sejam lançados na ferramenta de chamado.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SBDS
(5) Demora na solução do problema.	Operacional	Desconhecimento técnico sobre a infraestrutura do PJe	Atraso na solução do problema, com repercussões junto ao demandante.	Priorizar, no âmbito da SBDS, o atendimento dos chamados técnicos relativos à problemas do PJe.	Nível de Risco Inerente = 8 x 6 = 48 (Alto)	Nível de Risco Residual = 2 x 4 = 8 (Baixo)	Mitigar o risco	Chefe da SBDS

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
    10.1. Processo: Gerenciamento de Serviços de TIC
        10.1.X. Atendimento ao PJe - Problemas Técnicos
            10.1.x.6. Investigar Problema e Verificar se é Negocial *(Risco 1)*
            10.1.x.7. Comunicar Gestor Negocial *(Risco 2)*
            10.1.x.8. Atualizar Base de Conhecimento *(Risco 3)*
            10.1.x.9. Registrar Assentamento *(Risco 4)*
            10.1.x.12. Solucionar o Problema *(Risco 5)*

Anexo III - 4. TSE - Tribunal Superior Eleitoral

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Coordenador de Sistemas Corporativos	**Aprovação:** Comitê Gestor de Riscos, em 02/08/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Perfil de Riscos							
Gestor de Risco Setorial: Chefe da SEDESC1/TSE					**Área Funcional:** SEDESC1/TSE		**Data:** 02/08/2020
Risco (Descrição)	**Classe**	**Causa**	**Consequências**	**Resposta**	**Nível de Riscos (IxP)**		**Tipos de Resposta**	**Proprietário do Risco**
((1) Demora no atendimento do chamado.	Operacional	Sobrecarga de atividades junto à área técnica responsável no TSE.	Impacto nas atividades do demandante em que é necessário utilizar o PJe.	(1) Acompanhar, no âmbito da SBDS, o atendimento dos chamados abertos junto ao TSE, reiterando-os quando necessários. (2) Em casos de demora excessiva, reportar a situação à COSIS, para tomada de providências junto à CSCOR/TSE	Nível de Risco Inerente = 6 x 6 = 36 (Alto)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SEDESC1/TSE

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação

10.1. Processo: Gerenciamento de Serviços de TIC

10.1.X. Atendimento ao PJe - Problemas Técnicos

10.1.x.14. Atender Chamado *(Risco 1)*

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

ANEXO III

REUNIÃO N. 02/2020 - CPSI

Tribunal Regional Eleitoral
do Rio Grande do Norte

GESTÃO DE RISCOS

PROCESSO: 10.3.1 GERENCIAMENTO DE CÓPIAS DE SEGURANÇA (BACKUP) E DE RESTAURAÇÃO DE DADOS

Versão 1.0

NATAL, 31/07/2020

SUMÁRIO

INTRODUÇÃO

A tecnologia da informação está cada vez mais presente nas organizações como meio de auxiliar seus processos e contribuir para o alcance dos seus objetivos. Nesse ambiente, a cada dia é maior o volume de dados e informações digitais da organização e a preservação e segurança digital torna-se essencial para operação da empresa.

A perda de dados pode ocasionar desde retrabalho até a parada de operações e comprometimento da organização e pode ocorrer por diversos fatores:

- Ambiental: temperatura e umidade que danificam equipamentos;
- Físico/hardware: defeito em equipamentos, discos, fitas e mídias de armazenamento;
- Humano: o usuário pode acidentalmente apagar algum arquivo, parte de documento;
- Ameaças digitais: vírus que podem ocasionar a perda total dos dados ou, cada vez mais comum, vírus do tipo *ransomware*, que sequestra dados da organização e solicita pagamento de resgate.

Com o objetivo de evitar ou minimizar a perda de dados na organização, foi estabelecido o processo Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados no TRE-RN (Portaria GP n.º 130, de 24 de abril de 2017 (http://www.tre-rn.jus.br/legislacao/legislacao-compilada/portarias-gp/portarias-gp-por-ano/2017/tre-rn-portaria-gp-n-o-130-de-24-de-abril-de-2017).

Outra referência importante nas regras de execução das cópias de segurança é a “regra de backup 3-2-1”, a qual recomenda:

- ter pelo menos 3 (três) cópias dos seus dados (incluindo o dado original, ou seja, no mínimo dois backups);
- armazenar estas cópias em 2 (duas) mídias diferentes;
- manter (1) uma cópia de backup em outro local externo.

1. ESTABELECIMENTO DO CONTEXTO

1.1. Identificação do Processo

Processo: 10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados

Gestor: CIT

Responsável: Daniel César Gurgel Coelho Ponte

Referências na Cadeia de Valor / Arquitetura de Processos:

Macroprocesso de Suporte (S)

10. Gestão de Tecnologia da Informação e Comunicação (GTIC)

10.3. Gerenciamento da Disponibilidade da Capacidade (GDC)

10.3.1. Gerenciamento de Cópias de Segurança e Restauração de Dados

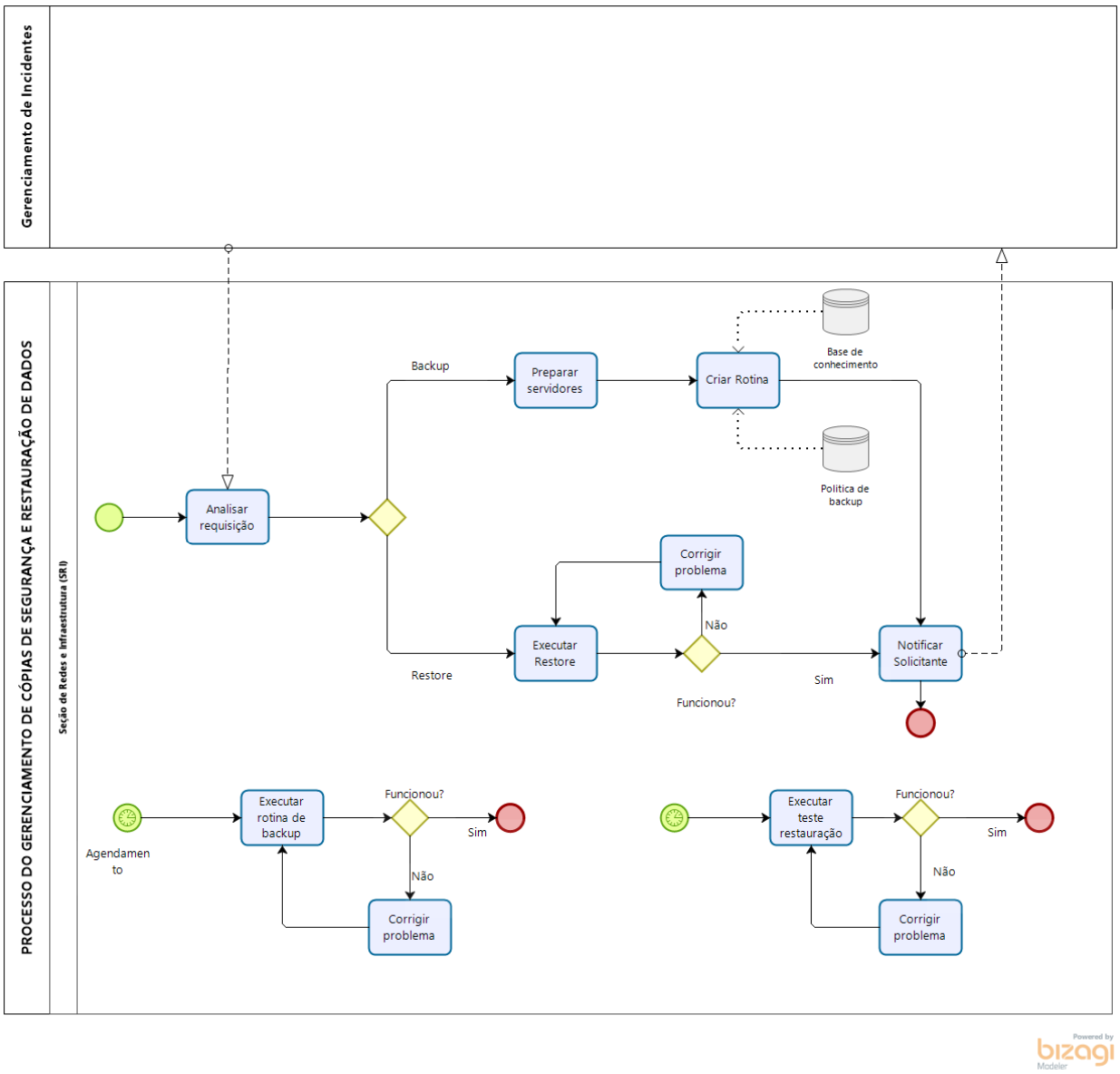
1.2. Objetivo

O Processo "10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados" tem por finalidade planejar e controlar as cópias de segurança e de restauração de dados essenciais a manutenção do funcionamento dos sistemas utilizados no TRE/RN, abrangendo a sua elaboração, utilização e manutenção, com base nas boas práticas preconizadas pela ITIL, para evitar ou minimizar o risco de perda de dados.

Conforme a modelagem do processo, 3 subprocessos podem ser definidos:

- Requisição de cópia e/ou restauração: ocorre quando existe um incidente de perda de dados e o usuário do TRE (no processo de gerenciamento de incidentes) solicita a recuperação ou quando o usuário solicita que determinado dado seja incluído na rotina de backup;
- Execução de cópia: rotina automatizada, gerenciado pela Seção de Redes e Infraestrutura (SRI), de acordo com os parâmetros pré-estabelecidos de periodicidade e retenção;
- Execução de testes de restauração: consiste em efetuar testes periódicos de recuperação para verificar a integridades dos dados (em geral semestralmente, de acordo com a política de backup).

A ilustração a seguir mostra a modelagem do processo. Como responsável pela execução do processo a Seção de Redes e Infraestrutura (SRI) e como solicitante temos todas as unidades/setores/usuários do Tribunal, pois armazenam dados digitais e informações necessárias da organização.



O fator crítico para o sucesso da execução do processo de cópia de segurança é a correta definição da rotina de backup, definindo quais são os dados importantes, qual o volume, periodicidade e retenção.

ANÁLISE DO CONTEXTO Quadro Resumo
Processo: ***10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados***
Objetivos e Metas: • Evitar ou minimizar o risco de perda de dados. • Plano Estratégico da Justiça Eleitoral do Rio Grande do Norte – PEJERN 2016-2020 (IA21, IA38, IA39 e IA41).
Legislação e normas associadas: • TRE-RN Portaria GP n.º 130, de 24 de abril de 2017 – Política de backup; • ABNT NBR ISO/IEC 27001:2013 – Sistemas de gestão de segurança da informação; • ABNT NBR ISO 22301:2020 – Segurança e resiliência - Sistema de gestão de continuidade de negócios.
Sistemas utilizados: • Atendimento STIC – GLPI; • HP Data Protector; • Commvault Complete™ Backup & Recovery.
Partes interessadas: • Internas: SRI e demais unidades do TRE-RN; • Externas: Fornecedores de serviços com armazenamento, TSE.

A seguir foi realizada a análise das forças, fraquezas, oportunidades e ameaças ao Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados. Deve-se considerar que o próprio processo foi criado para minimizar e/ou evitar o risco de perda de dados na instituição. Desta forma, considera-se:

- fator/agente interno para o processo: o próprio TRE-RN;
- fatores externos, que podem ocasionar alterações no processo: (a) fornecedores de serviços que prestam armazenamento de dados; (b) o TSE – Tribunal Superior Eleitoral e; (c) ameaças cibernéticas.

Para a análise, foi utilizada a matriz SWOT (Strengths, Weaknesses, Opportunities and Threats) ou FOFA (Forças, Oportunidades, Fraquezas e Ameaças).

Matriz SWOT

Processo: 10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados

	FATORES POSITIVOS	FATORES NEGATIVOS
FATORES INTERNOS	**FORÇAS** • Ferramentas automatizadas.	**FRAQUEZAS** • Defeitos em equipamentos. • Volume de dados.
FATORES EXTERNOS	**OPORTUNIDADES** • Contratos de prestação de serviços (e-mail, por exemplo) que podem transferir a responsabilidade/risco de perda de dados.	**AMEAÇAS** • Ataques cibernéticos / vírus.

1.3. Responsabilidades

A Para identificar os elementos relevantes para o alcance dos objetivos/resultados e atores envolvidos no processo, segue a análise das partes interessadas e seus interesses, com o uso da ferramenta matriz RACI.

Matrix RACI

Processo: 10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados

Responsável: Seção de Redes e Infraestrutura (SRI/COINF/STIC)

Data: 22/07/2020

		PAPEL	
	Responsabilidade	**Demandante**	**SRI**
	Requisição de cópia e/ou restauração		
1	Analisar requisição	A C I	R
2	Preparar servidor	C	R A
3	Criar rotina		R A
4	Executar restauração		R A
5	Corrigir problema de recuperação		R A
6	Notificar solicitante	I	R A
	Cópia automatizada		
7	Executar rotina de backup		R A
8	Corrigir problema		R A
	Testes de recuperação		
9	Executar teste de recuperação		R A
10	Corrigir problema		R A

Legenda:

R	Responsável
A	Aprovador
C	Consultado
I	Informado

2. IDENTIFICAÇÃO DOS RISCOS

Segue a identificação dos riscos para o processo 10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados, levando em conta as principais fontes de riscos de infraestrutura, pessoal, processos e tecnologia e as tarefas executadas no processo.

	TAREFA	OBJETIVO	RISCO	CONSEQUÊNCIA
	Requisição de cópia e/ou restauração			
1	Analisar requisição	Determinar qual a ação desejada (cópia ou restauração) e obter informação suficiente para a execução.	1.1) falta de informação sobre o que restaurar (o nome e localização do objeto); 1.2) informações insuficientes sobre qual servidor deve ser feito cópia de segurança, periodicidade e retenção (temporalidade).	1.1 e 1.2) Processo postergado pois exige novo contato com o demandante para esclarecimentos.
2	Preparar servidor	Deixar o computador/servidor pronto para a execução da cópia automática.	2.1) não ter pessoal disponível para a operação. 2.2) Volume de cópia de dados alto.	2.1) Adiamento do processo até que tenha pessoal com conhecimento disponível. Demora na execução. 2.2) Necessário que o demandante priorize / refine a solicitação.
3	Criar rotina	Configurar o software de backup com os parâmetros adequados.	3.1) parametrização inadequada.	3.1) Não há cópia de dados.
4	Executar restauração	Obter os dados demandados.	4.1) Inexistência dos dados. 4.2) Defeito no equipamento. 4.3) Defeito na mídia de backup.	4.1) Não há cópia: dados não encontrados ou cópia inexistente. Exige novo contato com o demandante para esclarecimentos. Comprovada a existência do dado demandado, verificação/criação de rotina de backup. 4.2) Processo não pode ser realizado, é necessário a manutenção/substituição do equipamento de backup. 4.3) Não há cópia e é necessário a substituição da mídia de backup.

5	Corrigir problema de recuperação	Os dados restaurados estejam acessíveis para o demandante.	5.1) Mídia de backup não encontrada. 5.2) Recuperação inacessível ao demandante (local, permissão de acesso)	5.1) É necessário localizar fisicamente mídia de backup; 5.2) É necessário copiar os dados para destino correto e corrigir permissão.
6	Notificar solicitante	Informar resultado do processo.	6.1) Não ser efetuado o registro do resultado do processo no sistema de ocorrências (Atendimento STIC/GLPI).	6.1) Notificação adiada até que o demandante entre em contato.
	Cópia automatizada			
7	Executar rotina de backup	Executar todas as rotinas de cópia agendadas.	7.1) Rotina não completada por causa da origem estar indisponível; 7.2) Rotina não completada por problema na mídia; 7.3) Rotina não completada até a próxima execução da rotina. 7.4) Defeito no equipamento	7.1) Cópia não efetuada, é necessário averiguar o servidor origem dos dados; 7.2) Cópia não efetuada, necessário verifica equipamento e mídia de cópia; 7.3) Cópia incompleta, necessário averiguar a causa: problemas de hardware, volume de dados ou parâmetros da rotina de cópia. 7.4) Processo não pode ser realizado, é necessário a manutenção/substituição do equipamento de backup.
8	Corrigir problema da cópia	Eliminar problemas das rotinas agendadas	8.1) Impossibilidade de correção imediata do defeito em equipamento.	8.1) Aguardar manutenção externa e/ou necessidade de aquisição de novo equipamento.
	Testes de recuperação			
9	Executar teste de recuperação	Correta restauração de cópia executada.	9.1) Não há cópia dos dados; 9.2) Mídia de backup danificada.	9.1) reavaliar a rotina de backup, fonte de dados / parâmetros. 9.2) Substituir mídia e avaliar causa.
10	Corrigir problema encontrado no teste	Eliminar problemas encontrados no teste	10.1) Impossibilidade de substituição de mídia de backup danificada. 10.2) Rotina de backup inválida por mudança da fonte de origem.	10.1) necessário aquisição da mídia; 10.2) reavaliar a rotina de backup, fonte de dados / parâmetros.

3. ANÁLISE DOS RISCOS

O objetivo do processo Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados é evitar ou minimizar o risco de perda de dados. Consequentemente, o principal risco é a inexistência da cópia de segurança o que implica na perda de dados.

Um fato a ser observado na modelagem do processo é que já há uma política de backup estabelecida e já existe um tratamento de alguns riscos (a rotina de teste de restauração, por exemplo).

Os principais riscos elencados são:

1. Falta de informação na solicitação;
2. Falta de pessoal técnico para executar a operação;
3. Extrapolação dos recursos disponíveis;
4. Não há cópia dos dados:
5. Restauração inacessível;
6. Falha de comunicação com o demandante.

3.1. Matriz de Riscos

		Probabilidade				
		2 Muito Baixa	4 Baixa	6 Média	8 Alta	10 Muito Alta
Impacto	10 Muito Alto	**20**	**40** (4) Não há cópia dos dados	**60**	**80**	**100**
	8 Alto	**16**	**32**	**48**	**64**	**80**
	6 Médio	**12**	**24** (3) Extrapolação dos recursos	**36**	**48**	**60**
	4 Baixo	**8**	**16** (2) Falta de pessoal	**24**	**32**	**40**
	2 Muito Baixo	**4** (5) Restauração inacessível; (6) Falha de comunicação	**8** (1) Falta de informação	**12**	**16**	**20**

Legenda: Extremo Alto Médio Baixo

4. AVALIAÇÃO DOS RISCOS

A avaliação dos riscos anteriormente identificados consta no documento “Anexo I – Identificação e Avaliação de Riscos”.

5. TRATAMENTO DOS RISCOS

O tratamento dos riscos anteriormente identificados consta no documento “Anexo II – Formulário Padrão de Tratamento de Riscos”.

Um resumo da análise e tratamento dos riscos foi sintetizado no “Anexo III – Formulário Perfil de Riscos”.

6. APETITE A RISCO

Após a aplicação do Modelo de Gestão de Riscos estabelecido pela Resolução Nº 17/2017, conforme as disposições do "Manual do Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte", nos dois atores do "Processo: 10.3.1 Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados", restaram identificados, avaliados e tratados 6 (seis) riscos, vinculados às 10 (dez) atividades do referido processo. Todos os riscos identificados foram classificados como "Risco Operacional", a exceção de um que também recebeu as classes "Risco de Imagem" e "Risco de Segurança da Informação".

Conforme descrito no “Anexo II – Formulário Padrão de Tratamento de Riscos”, a tabela a seguir mostra o nível dos riscos residuais, após o tratamento, do processo de gerenciamento de cópias de segurança (Backup) e de restauração de dados:

	RISCO	Nível de Risco Residual (IxP)	Ator do Processo
1	Falta de informação na solicitação	4	Demandante
2	Falta de pessoal técnico para executar a operação	8	SRI
3	Extrapolação dos recursos disponíveis	8	SRI
4	Não há cópia dos dados	16	SRI
5	Restauração inacessível	4	SRI
6	Falha de comunicação com o demandante	4	SRI

Risco Baixo Risco Médio

Observando-se os riscos residuais, a maioria ficou classificada como risco baixo e somente um como médio. O risco “(4) Não ter cópia dos dados”, embora após o tratamento do erro tem uma probabilidade muito baixa (=2), continua possuir um impacto alto (=8) na ocorrência da falha. Como o objetivo do processo em si é ter cópia dos dados para evitar/minimizar as perdas, esse é o risco de maior importância no tratamento.

Segue abaixo a análise dos atores do processo, riscos identificados e residuais:

Ator do Processo	Quantidade de Atividades	Quantidade de Riscos Identificados	Nível de Risco Residual das Atividades (Média)
Demandante	1	1	4
SRI	9	5	8
Total Geral / Média Geral	**10**	**6**	**6**

Ante o exposto e tendo em vista especialmente o item 11 do Manual do Processo de Gestão de Riscos sobre o Apetite a Risco, o Tribunal deve fixar o nível de risco considerado institucionalmente razoável para a execução de suas competências e atribuições legais, no presente caso, aquelas relativas às atividades do presente processo em termos da média do conjunto das atividades (6 pontos), portanto, no nível baixo.

Assim, a fixação do nível de Apetite a Risco que orienta a execução das atividades e a manutenção do nível de riscos declarado pelos responsáveis, refletindo a eficácia da Gestão de Riscos, ou seja, o alcance dos resultados planejados.

Apetite a Risco	
Processo	**Nível de Risco**
10.3.1 Gerenciamento de cópias de Segurança (Backup) e de Restauração de Dados	Baixo (6 pontos)
Aprovação: Comitê de Gestão de Riscos, em ##/##/2020.	

ANEXOS

Anexo I –Identificação e Avaliação de Riscos

Tribunal Regional Eleitoral do Rio Grande do Norte
Formulário de Identificação e Avaliação de Riscos

Responsável:	Aprovação:	Vigência:	Versão:
Chefe da SRI/COINF/STIC, Daniel César Gurgel Coelho Ponte	Comitê Gestor de Riscos, em xx/xx/2020.	02 (dois) anos, a partir da data de aprovação.	1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 30/07/2020 | **Unidade:** SRI | **Gestor de Riscos:** SRI

Risco	Causa(s)	Classe(s)[1]	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência(s)	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto[2]	Proba-bilidade[3]	Nível de Risco (IxP)[4]				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Falta de informação na solicitação	(1) falta de informação sobre o que restaurar (o nome e localização do objeto); (2) informações insuficientes sobre o que deve ser feito cópia, periodicidade e retenção (temporalidade).	Operacional	Muito Baixo (2)	Baixa (4)	8	Baixo	(1) Processo postergado até esclarecimento / fornecimento de novas informações pelo demandante.	Mitigar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	SRI	Demandante
(2) Falta de pessoal técnico para executar a operação	(1) não ter pessoal com conhecimento técnico disponível.	Operacional	Baixo (4)	Baixa (4)	16	Médio	(1) Adiamento do processo até que tenha pessoal com conhecimento disponível. Demora na execução.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SRI	Chefe da SRI/COINF/STIC
(3) Extrapolação dos recursos disponíveis	(1) Volume de cópia de dados alto.	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Necessário que o demandante priorize os dados importantes. (2) Necessidade de mais recursos (equipamentos e mídias)	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SRI / Unidade Demandante	Chefe da SRI/COINF/STIC

1 Utilizar parâmetros constantes da tabela 4 (p. 22).
2 Utilizar parâmetros constantes da tabela 3 (p. 21).
3 Utilizar parâmetros constantes da tabela 2 (p. 20).
4 Nível de Risco (NR): NR ≤ 8 = baixo; NR ≤ 24 = médio; 24 < NR ≤ 48 = alto; NR ≥ 60 = extremo (v. Tabela 1 – Matriz de Riscos).

Tribunal Regional Eleitoral do Rio Grande do Norte
Formulário de Identificação e Avaliação de Riscos

Responsável:	Aprovação:	Vigência:	Versão:
Chefe da SRI/COINF/STIC, Daniel César Gurgel Coelho Ponte	Comitê Gestor de Riscos, em xx/xx/2020.	02 (dois) anos, a partir da data de aprovação.	1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 30/07/2020 | **Unidade:** SRI | **Gestor de Riscos:** SRI

Risco	Causa(s)	Classe(s)[1]	Avaliação Riscos Inerentes			Categoria de Priorização	Consequência(s)	Tratamento	Avaliação Riscos residuais			Categoria de Priorização	Plano de Contingência	Área Funcional Responsável	Proprietário do Risco
			Impacto[2]	Proba-bilidade[3]	Nível de Risco (IxP)[4]				Impacto	Probabilidade	Nível de Risco (IxP)				
(4) Não há cópia dos dados	(1) defeito no equipamento que realiza o backup; (2) defeito na mídia de backup indisponível; (3) problemas na execução da rotina de cópia.	Operacional, Imagem e de Segurança da Informação	Muito Alto (10)	Baixa (4)	40	Alto	(1) Perda de dados, é necessário a manutenção/substituição do equipamento de backup e/ou da mídia. (2) Necessidade de análise da causa do defeito e correção. A causa pode ser de estrutura (temperatura do ambiente e umidade), bem como operacional (mudança do objeto de backup sem comunicação) e pessoal.	Mitigar o risco	Alto (8)	Muito Baixa (2)	16	Médio	Sim	SRI	Chefe da SRI/COINF/STIC
(5) Restauração inacessível	(1) dado recuperado inacessível ao demandante (local, permissão de acesso)	Operacional	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	(1) É necessário copiar os dados para destino correto e corrigir permissão.	Aceitar/tolerar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	SRI	Chefe da SRI/COINF/STIC
(6) Falha de comunicação com o demandante	(1) não ser efetuado o registro do resultado do processo no sistema de ocorrências (Atendimento STIC/GLPI).	Operacional	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	(1) Notificação adiada até que o demandante entre em contato.	Aceitar/tolerar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	SRI	Chefe da SRI/COINF/STIC

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):
Macroprocesso de Suporte (S)
10. Gestão de Tecnologia da Informação e Comunicação (GTIC)
    10.3. Gerenciamento da Disponibilidade da Capacidade (GDC)
        10.3.1. Gerenciamento de Cópias de Segurança e Restauração de Dados
            1. Falta de informação na solicitação (Risco 1);
            2. Falta de pessoal técnico para executar a operação (Risco 2);
            3. Extrapolação dos recursos disponíveis (Risco 3);
            4. Não há cópia dos dados (Risco 4):
            5. Restauração inacessível (Risco 5);
            6. Falha de comunicação com o demandante (Risco 6).

Anexo II – Formulário Padrão de Tratamento de Riscos

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Chefe da SRI/COINF/STIC, Daniel César Gurgel Coelho Ponte	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2020	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

1

Tratamento de Riscos		
Data: 30/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Demandante
Risco: Operacional	(1) Falta de informação na solicitação	
Probabilidade: Baixa (4)	**Impacto:** Muito Baixo (2)	**Nível do Risco:** Baixo (8)
Resposta a ser implantada:	(1) Documentação das informações necessárias do demandante para o processo de backup, para que desta forma a solicitação já tenha todos os dados necessários.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** Até o dezembro/2020.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (4)
Risco(s) Secundário(s) **(geradas pelas respostas adotadas):**	Não foram identificados.	
Chefe da SRI/COINF/STIC **Gestor de Risco Setorial**		

2

Tratamento de Riscos		
Data: 28/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Chefe da SRI/COINF/STIC
Risco: Operacional	(2) Falta de pessoal técnico para executar a operação	
Probabilidade: Baixa (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	(1) Treinamento de pessoal técnico. (2) Documentação de procedimentos necessários.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** Treinamento efetuado somente com uma pessoa. Ainda não há documentação sobre procedimentos.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Risco(s) Secundário(s) **(geradas pelas respostas adotadas):**	Não foram identificados.	
Chefe da SRI/COINF/STIC **Gestor de Risco Setorial**		

3

Tratamento de Riscos		
Data: 28/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Chefe da SRI/COINF/STIC
Risco: Operacional	(3) Extrapolação dos recursos disponíveis	
Probabilidade: Baixa (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Monitoramento frequente da execução da rotina de cópia de segurança, para informações sobre tempo de execução e volume de dados; (2) Aquisição de mídias sobressalentes; (3) Revisão da rotina de cópia com a unidade demandante, em caso de falha.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (1) e (2) já estão implementadas. A resposta (3) é somente dada quando houver incidente.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Chefe da SRI/COINF/STIC **Gestor de Risco Setorial**		

4

Tratamento de Riscos		
Data: 28/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Chefe da SRI/COINF/STIC
Risco: Operacional, Imagem e de Segurança da Informação	(4) Não há cópia dos dados	
Probabilidade: Baixa (4)	**Impacto:** Muito Alto (10)	**Nível do Risco:** Alto (40)
Resposta a ser implantada:	(1) Execução de teste de restauração, para averiguar funcionamento correto do hardware, mídia e rotina de cópia. (2) Seguir recomendações Política de backup. (3) Implementar recomendação de backup “3-2-1” (3 cópias dos dados, 2 mídias diferentes, 1 cópia armazenada em local externo). (4) redundância de hardware. (5) ativação de cópia de sombreamento para servidores de arquivos.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** A resposta (2) já é realizada. A resposta (5) já está ativada. Respostas (1), (3) e (4) são parcialmente implementadas.	
Planos de Contingência Recomendados:	É necessário plano de contingência, através da aplicação da política (TRE-RN Portaria GP n.º 130, de 24 de abril de 2017) e recomendação de backup “3-2-1”.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Alto (8)	**Nível de Risco Residual:** Médio (16)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Chefe da SRI/COINF/STIC **Gestor de Risco Setorial**		

5

Tratamento de Riscos		
Data: 28/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Chefe da SRI/COINF/STIC
Risco: Operacional	(5) Restauração inacessível	
Probabilidade: Muito Baixa (2)	**Impacto:** Muito Baixo (2)	**Nível do Risco:** Baixo (4)
Resposta a ser implantada:	A consequência, ter que copiar os dados para destino correto e corrigir permissão, é aceitável.	
Tipo de Resposta: Aceitar/tolerar o risco	**Prazo para implantação:** não é necessário.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (4)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Chefe da SRI/COINF/STIC		

Gestor de Risco Setorial

6

Tratamento de Riscos		
Data: 28/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Chefe da SRI/COINF/STIC
Risco: Operacional	(6) Falha de comunicação com o demandante	
Probabilidade: Muito Baixa (2)	**Impacto:** Muito Baixo (2)	**Nível do Risco:** Baixo (4)
Resposta a ser implantada:	A consequência, a notificação adiada até que o demandante entre em contato, é aceitável.	
Tipo de Resposta: Aceitar/tolerar o risco	**Prazo para implantação:** não é necessário.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Muito Baixa (2)	**Impacto Risco Residual:** Muito Baixo (2)	**Nível de Risco Residual:** Baixo (4)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Chefe da SRI/COINF/STIC **Gestor de Risco Setorial**		

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):
Macroprocesso de Suporte (S)
10. Gestão de Tecnologia da Informação e Comunicação (GTIC)
    10.3. Gerenciamento da Disponibilidade da Capacidade (GDC)
        10.3.1. Gerenciamento de Cópias de Segurança e Restauração de Dados
            1. Falta de informação na solicitação (Risco 1);
            2. Falta de pessoal técnico para executar a operação (Risco 2);
            3. Extrapolação dos recursos disponíveis (Risco 3);
            4. Não há cópia dos dados (Risco 4):
            5. Restauração inacessível (Risco 5);
            6. Falha comunicação com o demandante (Risco 6).

Anexo III – Formulário Perfil de Riscos

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Chefe da SRI/COINF/STIC, Daniel César Gurgel Coelho Ponte	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2020.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Chefe da SRI/COINF/STIC					**Área Funcional:** SRI			**Data:** 31/07/2020
Risco (Descrição)	**Classe(s)**	**Causa(s)**	**Consequências**	**Resposta(s)**	**Nível de Riscos (IxP)[1]**		**Tipos de Resposta(s)**	**Proprietário do Risco**
(1) Falta de informação na solicitação	Operacional	(1) falta de informação sobre o que restaurar (o nome e localização do objeto); (2) informações insuficientes sobre o que deve ser feito cópia, periodicidade e retenção (temporalidade).	(1) Processo postergado até esclarecimento / fornecimento de novas informações pelo demandante.	(1) Documentação das informações necessárias do demandante para o processo de backup, para que desta forma a solicitação já tenha todos os dados necessários.	Nível de Risco Inerente = 2 x 4 = 8 (Baixo)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Mitigar o risco	Demandante
(2) Falta de pessoal técnico para executar a operação	Operacional	(1) não ter pessoal com conhecimento técnico disponível.	(1) Adiamento do processo até que tenha pessoal com conhecimento disponível. Demora na execução.	(1) Treinamento de pessoal técnico. (2) Documentação de procedimentos necessários.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SRI/COINF/STIC
(3) Extrapolação dos recursos disponíveis	Operacional	(1) Volume de cópia de dados alto.	(1) Necessário que o demandante priorize os dados importantes. (2) Necessidade de mais recursos (equipamentos e mídias)	(1) Monitoramento frequente da execução da rotina de cópia de segurança, para informações sobre tempo de execução e volume de dados; (2) Aquisição de mídias sobressalentes; (3) Revisão da rotina de cópia com a unidade demandante, em caso de falha.	Nível de Risco Inerente = 6 x 4 = 24 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SRI/COINF/STIC
(4) Não há cópia dos dados	Operacional, Imagem e de Segurança da Informação	(1) defeito no equipamento que realiza o backup; (2) defeito na mídia de backup indisponível; (3) problemas na execução da rotina de cópia.	(1) Perda de dados, é necessário a manutenção/substituição do equipamento de backup e/ou da mídia. (2) Necessidade de análise da causa do defeito e correção. A causa pode ser de estrutura (temperatura do ambiente e umidade), bem como operacional (mudança do objeto de backup sem comunicação) e pessoal.	(1) Execução de teste de restauração, para averiguar funcionamento correto do hardware, mídia e rotina de cópia. (2) Seguir recomendações Política de backup. (3) Implementar recomendação de backup “3-2-1” (3 cópias dos dados, 2 mídias diferentes, 1 cópia armazenada em local externo). (4) redundância de hardware. (5) ativação de cópia de sombreamento para servidores de arquivos.	Nível de Risco Inerente = 10 x 4 = 40 (Alto)	Nível de Risco Residual = 8 x 2 = 20 (Médio)	Mitigar o risco	Chefe da SRI/COINF/STIC

1 Expressar o Nível de Risco (NR) como (probabilidade x impacto) = NR

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Chefe da SRI/COINF/STIC					**Área Funcional:** SRI			**Data:** 31/07/2020
Risco (Descrição)	**Classe(s)**	**Causa(s)**	**Consequências**	**Resposta(s)**	**Nível de Riscos (IxP)[1]**		**Tipos de Resposta(s)**	**Proprietário do Risco**
(5) Restauração inacessível	Operacional	(1) dado recuperado inacessível ao demandante (local, permissão de acesso)	(1) É necessário copiar os dados para destino correto e corrigir permissão.	A consequência, ter que copiar os dados para destino correto e corrigir permissão, é aceitável.	Nível de Risco Inerente = 2 x 2 = 4 (Baixo)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Aceitar/tolerar o risco	Chefe da SRI/COINF/STIC
(6) Falha de comunicação com o demandante	Operacional	(1) não ser efetuado o registro do resultado do processo no sistema de ocorrências (Atendimento STIC/GLPI).	(1) Notificação adiada até que o demandante entre em contato.	A consequência, a notificação adiada até que o demandante entre em contato, é aceitável.	Nível de Risco Inerente = 2 x 2 = 4 (Baixo)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Aceitar/tolerar o risco	Chefe da SRI/COINF/STIC

Referências na Cadeia de Valor / Arquitetura de Processos (**Atividades**):
Macroprocesso de Suporte (S)
11. Gestão de Tecnologia da Informação e Comunicação (GTIC)
    10.4. Gerenciamento da Disponibilidade da Capacidade (GDC)
        10.4.1. Gerenciamento de Cópias de Segurança e Restauração de Dados
            7. Falta de informação na solicitação (Risco 1);
            8. Falta de pessoal técnico para executar a operação (Risco 2);
            9. Extrapolação dos recursos disponíveis (Risco 3);
            10. Não há cópia dos dados (Risco 4):
            11. Restauração inacessível (Risco 5);
            12. Falha de comunicação com o demandante (Risco 6).

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

ANEXO IV

REUNIÃO N. 02/2020 - CPSI

Análise dos riscos identificados e tratados

Atividade/Processo/ Projeto	Principais Riscos (descrição)	Causas	Decisões para mitigar os riscos
Atendimento ao PJe - Problemas Técnicos	Demora na comunicação com o demandante. Não realização do registro na base de conhecimento Demora na solução do problema.	Sobrecarga de atividades na Central Esquecimento por parte da unidade técnica. Desconhecimento técnico sobre a infraestrutura do PJe	Estabelecer junto à Central de Serviços uma priorização para o atendimento de chamados relacionados ao PJe. Estabelecer uma rotina de revisão do chamado antes seu encerramento, garantindo que todas as informações relevantes sejam lançadas ou alteradas na base de conhecimento. Priorizar, no âmbito da SBDS, o atendimento dos chamados técnicos relativos à problemas do PJe.
Gerenciamento de Cópias de Segurança (backup) e de restauração de dados	Falta de pessoal técnico para executar a operação Extrapolação dos recursos disponíveis Não há cópia dos dados	Adiamento do processo até que tenha pessoal com conhecimento disponível. Demora na execução. Necessário que o demandante priorize os dados importantes. Necessidade de mais recursos (equipamentos e mídias) Perda de dados, é necessário a manutenção/substituição do equipamento de backup e/ou da	Treinamento de pessoal técnico. Documentação de procedimentos necessários. Monitoramento frequente da execução da rotina de cópia de segurança, para informações sobre tempo de execução e volume de dados; Aquisição de mídias sobressalentes; Revisão da rotina de cópia com a unidade demandante, em caso de falha. Execução de teste de restauração, para averiguar

		mídia. Necessidade de análise da causa do defeito e correção. A causa pode ser de estrutura (temperatura do ambiente e umidade), bem como operacional (mudança do objeto de backup sem comunicação) e pessoal.	funcionamento correto do hardware, mídia e rotina de cópia. Seguir recomendações Política de backup. Implementar recomendação de backup “3-2-1” (3 cópias dos dados, 2 mídias diferentes, 1 cópia armazenada em local externo). Redundância de hardware. Ativação de cópia de sombreamento para servidores de arquivos.