Tribunal Regional Eleitoral
do Rio Grande do Norte

Gestão de Riscos

Processo: 10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados

Versão 1.0

EPOR
Escritório de Processos
Organizacionais e Riscos
AGE / PRES

Natal, Abril/2021.

2021 Tribunal Regional Eleitoral do Rio Grande do Norte

Presidente do TRE-RN

Desembargador Gilson Barbosa de Albuquerque

Diretora-Geral da Secretaria

Yvette Bezerra Guerreiro Maia

Assessoria de Apoio à Governança e Gestão Estratégica – AGE / Presidência

Maria Ruth Bezerra Maia de Hollanda

Preparação, organização, revisão e edição

Escritório de Processos Organizacionais e Riscos - EPOR

Iaperi Gábor Damasceno Árbocz

Participantes das unidades envolvidas no processo

Marcos Flávio Nascimento Maia STIE
Osmar Fernandes de Oliveira Júnior COSIS
Tyronne Dantas de Medeiros COTEL
Carlos Magno do Rozário Câmara COINF
Dina Márcia Vasconcelos Maranhão da Câmara GAPSTIE
Jussara de Gois Borba Melo Diniz GAPSTIE
Daniel César Gurgel Coelho Ponte – SRI/COINF
Sidnei Costa Souza – SRI/COINF

Controle de Versões

Versão	Data	Responsável	Descrição
0.1	02/09/2020	Daniel César Gurgel Coelho Ponte – SRI/COINF/STIE	Versão inicial encaminhada no PAE nº 6844/2020.
0.2	24/09/2020	Iaperi Árbocz – EPOR (edição e consolidação)	Versão inicial com correções e adequações ao disposto no manual do Processo de Gestão de Riscos.
0.3	07/12/2020	Daniel César Gurgel Coelho Ponte – SRI/COINF/STIE	Versão com as correções sugeridas.
0.4	19/03/2021	Carlos Magno do Rozário Câmara (COINF)	Complementações da COINF/STIE.
1.0	22/03/2021	Iaperi Árbocz – EPOR (edição e consolidação final)	Versão inicial aprovada pelo Comitê de Gestão de Riscos em 07/04/2021.

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 “10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados” da Cadeia de Valor, conforme escopo delimitado na etapa preliminar de Estabelecimento do Contexto.

A execução do processo de gestão de riscos envolveu os responsáveis pelas unidades envolvidas no processo de Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados 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.

Com a metodologia supracitada foi descrito o processo de "Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados no TRE-RN" (Portaria nº 130-GP, de 24 de abril de 2017), cuja finalidade é evitar ou minimizar a perda de dados na organização. A principal unidade responsável do processo, a SRI (Seção de Redes e Infraestrutura), elaborou o documento original que foi submetido à validação pelo CGesTIC (Comitê de Gestão de Tecnologia da Informação e Comunicação) e, posteriormente, à EPOR (Escritório de Processos Organizacionais e Riscos).

O objetivo desse trabalho é fornecer informações sobre o processo, riscos e oportunidades, para auxiliar a tomada de decisões gerenciais, em busca do cumprimento da missão institucional e objetivos do TRE-RN.

Marcos Flávio Nascimento Maia
Secretário de Tecnologia da Informação e Eleições

Sumário

Declaração de Apetite a Risco: “10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados”

Referências na Cadeia de Valor / Arquitetura de Processos:

Macroprocesso de Suporte

10. Gestão de Tecnologia da Informação e Comunicação

10.3. Gerenciamento da Disponibilidade da Capacidade

10.3.1. Gestão da Disponibilidade e da Capacidade

10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados

10.3.1.3.1. Requisição de cópia e/ou restauração

10.3.1.3.2. Execução de cópia

10.3.1.3.3. Execução de testes de restauração

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: 10.3.1.3. 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:

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)
Demandante	1	1	4
SRI	9	5	8
Total Geral / Média Geral	**10**	**6**	**6**

Tabela – Nível de Risco Residual (Média) por atividade e ator

	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.

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**
10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados	Baixo (6 pontos)
Aprovação: Comitê de Gestão de Riscos, em 07/04/2021.	

Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte

Estabelecimento do Contexto

Responsável: Daniel César Gurgel Coelho Ponte, SRI/COINF/STIE.	Vigência: 02 (dois) anos, a partir da data de aprovação (07/04/2021).	Versão: 1.0

- Processo Organizacional: ***10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados.***

Referências na Cadeia de Valor / Arquitetura de Processos:

Macroprocesso de Suporte
10. Gestão de Tecnologia da Informação e Comunicação
10.3. Gerenciamento da Disponibilidade da Capacidade
10.3.1. Gestão da Disponibilidade e da Capacidade
10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
10.3.1.3.1. Requisição de cópia e/ou restauração
10.3.1.3.2. Execução de cópia
10.3.1.3.3. Execução de testes de restauração

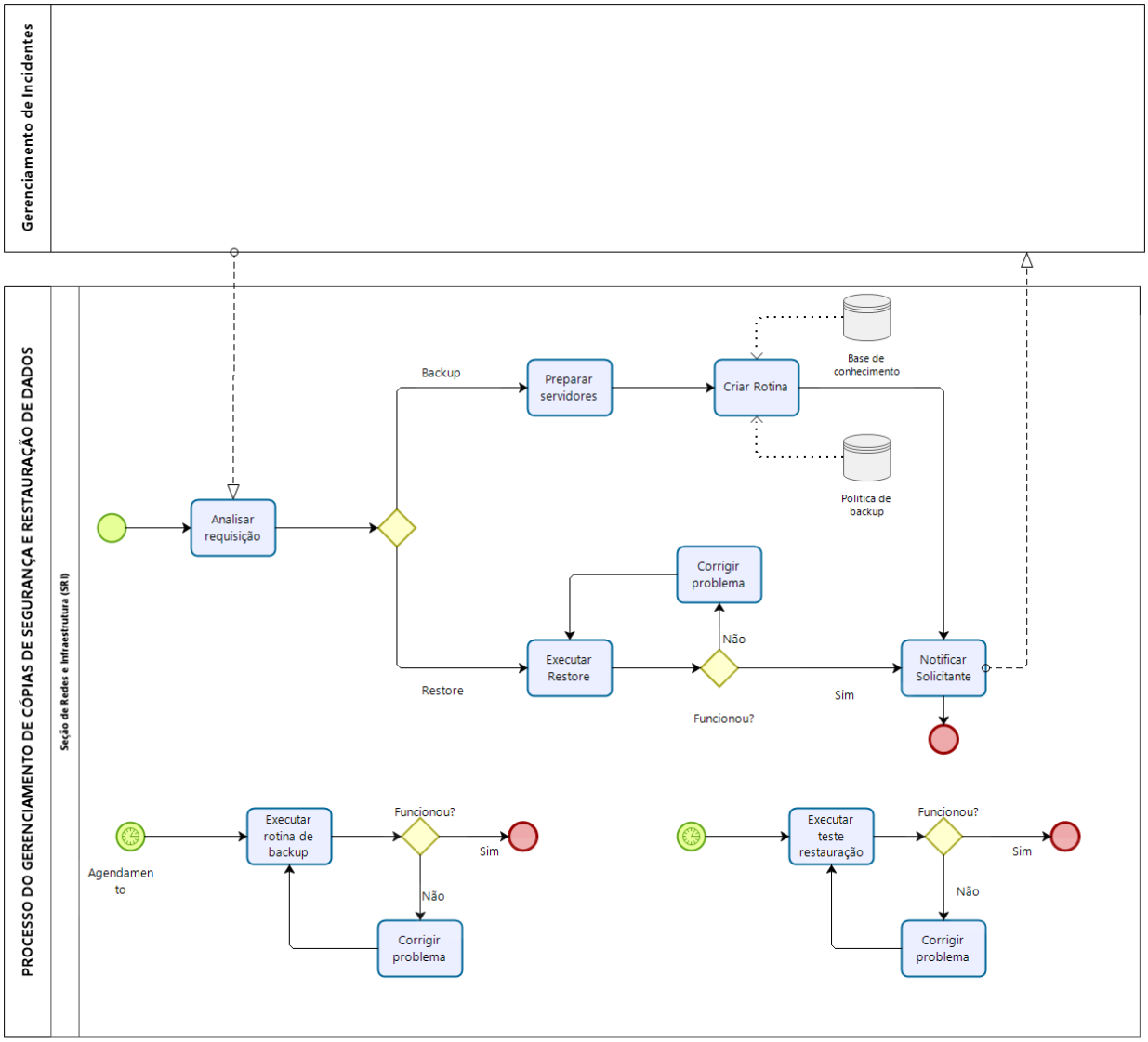
1. Objetivos do processo

O Processo "10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dado" 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: ***10.3.1.3. 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: • Resolução CNJ Nº 182/2013; • TRE-RN Portaria GP n.º 174, de 06 de setembro de 2019; • TRE-RN Portaria GP n.º 130, de 24 de abril de 2017; e • TRE/RN Portaria GP n.º 111, de 25 de maio de 2016.
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; e
- 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: 10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados**

FATORES INTERNOS

FORÇAS	FRAQUEZAS
Ferramentas automatizadas.	Defeitos em equipamentos.
	Volume de dados.

FATORES EXTERNOS

OPORTUNIDADES	AMEAÇAS
Contratos de prestação de serviços (e-mail, por exemplo) que podem transferir a responsabilidade/risco de perda de dados.	Ataques cibernéticos / vírus.

2. **Identificar os elementos relevantes para o alcance dos objetivos/resultados (atores envolvidos no processo)**

   - Análise das partes interessadas e seus interesses, com o uso da ferramenta matriz RACI.

O processo de Elaboração e Gestão do Plano de Contratações de TIC na Justiça Eleitoral do Rio Grande do Norte está ramificado num conjunto que vai desde a "Consolidação das demandas", aí incluído o "Planejamento da Contratação", a "Gestão de contratos administrativos", processos que se ramificam até o nível das atividades nas unidades responsáveis, conforme detalhamento a seguir demonstrado:

MATRIZ RACI		
Processo Organizacional: **10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados**		
Responsável: Daniel César Gurgel Coelho Ponte, Seção de Redes e Infraestrutura (SRI/COINF/STIC).	Data: 22/07/2020.	
Papel / **Responsabilidade**	Demandante	SRI
Subprocesso: Requisição de cópia e/ou restauração	A / C / I	R
1. Analisar requisição	C	R / A
2. Preparar servidor		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
Subprocesso: Cópia automatizada		
7. Executar rotina de backup		R / A
8. Corrigir problema		R / A
Subprocesso: Testes de recuperação		
9. Executar teste de recuperação		R / A
10. Corrigir problema		R / A

Legenda	
R – Responsável	É quem executa a atividade efetivamente.
A – Aprovador	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.

3. **Enumerar o conjunto de critérios mais importantes para analisar e avaliar os níveis de risco: escalas de probabilidade; escalas de consequências ou impactos; como será determinado se o nível de risco é tolerável ou aceitável e se novas ações de tratamento são necessárias, isto é, diretrizes para priorização e tratamento de riscos.**

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 avalição 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. Unidade Demandante / SRI/COINF/STIE

2. Seção de Redes e Infraestrutura – SRI

Anexo I – 1. Unidade Demandante / SRI/COINF/STIE

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário de Identificação e Avaliação de Riscos			
Responsável: Chefe da SRI/COINF/STIC, Daniel César Gurgel Coelho Ponte.	Aprovação: Comitê de Gestão de Riscos, em 07/04/2021.	Vigência: 02 (dois) anos, a partir da data de aprovação.	Versão: 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 30/07/2020	**Unidade:** Seção de Redes e Infraestrutura – SRI	**Gestor de Riscos: Unidade Demandante / Chefe da Seção de Redes e Infraestrutura**

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	Unidade Demandante / Chefe da SRI/COINF/STIE

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

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.1. Requisição de cópia e/ou restauração (Risco 1)

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).

Anexo I – 2. Seção de Redes e Infraestrutura – SRI

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 de Gestão de Riscos, em 07/04/2021.	02 (dois) anos, a partir da data de aprovação.	1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 30/07/2020 | **Unidade:** Seção de Redes e Infraestrutura – SRI | **Gestor de Riscos:** Chefe da Seção de Redes e Infraestrutura – 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)				
(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
(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	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

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).

	acesso)														
(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 (**Subprocessos ou Atividades**):

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.2. Execução de cópia (Riscos 2, 3, 4, 5 e 6)
                10.3.1.3.3. Execução de testes de restauração

Anexo II - Formulário Padrão de Tratamento de Riscos

1. Unidade Demandante / SRI/COINF/STIE

2. Seção de Redes e Infraestrutura – SRI

Anexo II – 1. Unidade Demandante / SRI/COINF/STIE

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 de Gestão de Riscos em 07/04/2021.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Tratamento de Riscos		
Data: 30/07/2020	**Área Funcional:** SRI	**Proprietário do Risco:** Demandante / Chefe da SRI/COINF/STIE
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**		

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

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.1. Requisição de cópia e/ou restauração (Risco 1)

Anexo II – 2. Seção de Redes e Infraestrutura – SRI

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 de Gestão de Riscos em 07/04/2021.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

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:** (1) Treinamento efetuado somente com uma pessoa; e (2) A documentação dos procedimentos necessários está registrada no Google Drive institucional da SRI, já com relação a migração da ferramenta de Backup, o processo é complexo e deve ser concluído até o mês de julho de 2021.	
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**		

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; e (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**		

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; e (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". O plano de contingencia (procedimentos de recuperação de estrutura de backup) depende em parte da conclusão da migração e deve ser finalizado e disponibilizado no Google Drive institucional da SRI até o final de maio de 2021.	
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**		

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:	(1) 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 necessária.	
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**		

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 (**Subprocessos ou Atividades**):

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.2. Execução de cópia (Riscos 2, 3, 4, 5 e 6)
                10.3.1.3.3. Execução de testes de restauração

Anexo III - Formulário Perfil de Riscos

1. Unidade Demandante / SRI/COINF/STIE

2. Seção de Redes e Infraestrutura – SRI

Anexo III – 1. Unidade Demandante / SRI/COINF/STIE

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 de Gestão de Riscos, em 07/04/2021.	**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 / Chefe da SRI/COINF/STIE

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

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.1. Requisição de cópia e/ou restauração (Risco 1)

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

Anexo III – 2. Seção de Redes e Infraestrutura – SRI

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 de Gestão de Riscos, em 07/04/2021.	**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
(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; e (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; e (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; e (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; e (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
(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.	(1) 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

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

(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 (**Subprocessos ou Atividades**):

10. Macroprocesso de Suporte: Gestão de Tecnologia da Informação e Comunicação
    10.3. Gerenciamento da Disponibilidade da Capacidade
        10.3.1. Gestão da Disponibilidade e da Capacidade
            10.3.1.3. Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
                10.3.1.3.2. Execução de cópia (Riscos 2, 3, 4, 5 e 6)
                10.3.1.3.3. Execução de testes de restauração