



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

ATA DE REUNIÃO N. 10/2021 - CGESTIC

I . Identificação da Reunião

Data	Horário		Local	Coordenador
	Início	Término		
27.05.2021	17h00	19h15	Videoconferência	Marcos Flávio Nascimento Maia

II. Objetivo

Reunião do CGesTIC para tratar dos seguintes assuntos:

1. Sensibilização LGPD;;
2. Análises das pendências anteriores;
3. Apresentação da análise de riscos do processo "Gerenciamento de Escopo e Requisitos" da COSIS.
4. Acompanhamento dos Planos de Ação dos Protocolos de Segurança Cibernética
 - 4.1 - Portaria CNJ nº 290/2020 - Protocolo de Gerenciamento de Crises Cibernéticas
 - 4.2 - Portaria CNJ nº 291/2020 - Protocolo de Investigação de Ilícitos Cibernéticos
 - 4.3 - Portaria CNJ nº 292/2020 - Protocolo de Prevenção a Incidentes Cibernéticos
5. COINF - Providências oriundas das reuniões de Avaliação das Eleições 2020:
 - 5.1. Preparação de treinamento, palestra sobre recursos do Google Suits, incluindo criação de filtros no Gmail
 - 5.2. Prestar suporte na criação de filtros no Gmail de todos os servidores das ZEs para atender necessidade de convocação de mesários
6. Fechamento do Índice de Governança e Gestão do TCU (IGG)
7. Outros assuntos

III. Participantes

Nome	Lotação	Assinatura
Marcos Flávio Nascimento Maia	STIE	<p>MARCOS FLAVIO NASCIMENTO MAIA:30024317 Assinado de forma digital por MARCOS FLAVIO NASCIMENTO MAIA:30024317 Dados: 2021.06.16 19:06:34 -03'00'</p>
Carlos Magno do Rozário Câmara	COINF	<p>CARLOS MAGNO DO ROZARIO CAMARA:30024407 Assinado de forma digital por CARLOS MAGNO DO ROZARIO CAMARA:30024407 Dados: 2021.06.14 17:18:26 -03'00'</p>
Tyronne Dantas de Medeiros	COELE	<p>TYRONNE DANTAS DE MEDEIROS:92440597 Assinado de forma digital por TYRONNE DANTAS DE MEDEIROS:92440597 Dados: 2021.06.15 18:41:49 -03'00'</p>
Osmar Fernandes de Oliveira Júnior	COSIS	<p>OSMAR FERNANDES DE OLIVEIRA JUNIOR:92440637 Assinado de forma digital por OSMAR FERNANDES DE OLIVEIRA JUNIOR:92440637 Dados: 2021.06.15 15:51:01 -03'00'</p>



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

Jussara de Gois Borba Melo Diniz	GAPSTIE	JUSSARA DE GOIS BORBA MELO DINIZ:92440668	Assinado de forma digital por JUSSARA DE GOIS BORBA MELO DINIZ:92440668 Dados: 2021.06.09 13:35:42 -03'00'
Ana Karla Tomaz da Costa	GAPSTIE		

IV . Discussão

Nº	Descrição/Decisão	Responsável
1	<p>1.Sensibilização LGPD (com a participação dos chefes ou substitutos das seções da STIE) - Apresentação realizada por videoconferência das primeiras tratativas sobre a Lei nº 13.709/2018 para viabilizar a implementação da proteção dos dados no TRE-RN - estiveram presentes os coordenadores e chefias/substitutos das unidades da Secretaria de Tecnologia da Informação e Eleições:</p> <ul style="list-style-type: none">• Denilson Bastos da Silva (SSI/COINF)• Daniel Cesar Gurgel Coelho Ponte (SRI/COINF)• Sidnei Costa Souza (SRI/COINF)• João Paulo Marques de Oliveira (SRI/COINF)• Carlos André de Azevedo Moura (SMI/COINF)• George Melo de Freitas Barbalho (SDS/COSIS)• Thiago Fernandes Silva Dutra (SBDS/COSIS)• José Wendell de Moraes Silva (SBDS/COSIS)• José Frank Viana da Silva (SNT/COSIS)• Theresa Regina Pereira Padilha (SSAE/COELE)• Antônio Klaus Vilas Boas de Souza Silva (SUE/COELE)	Marcos Maia Coordenadores Chefes/substitutos das chefias das unidades da STIE
2	<p>2. Pendência:</p> <p>2.1. GAPSTIE - Auditoria - Política Formal de Comunicação de TIC e de Divulgação dos Resultados : ficou reagendado para apresentação no 1º CGESTIC de julho.</p>	Marcos Maia
3	<p>3. COSIS - Apresentação da análise de riscos do processo "Gerenciamento de Escopo e Requisitos" da COSIS: Apresentado a análise de risco do processo, sendo aprovada pelos participantes, sem ajustes (ANEXO I).</p> <p>Enviar os artefatos produzidos para AGE, junto com a análise de riscos do processo da COINF.</p> <p>PRAZO: início de julho.</p>	Marcos Maia Osmar Fernandes



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

4	<p>4. Acompanhamento dos Planos de Ação dos Protocolos de Segurança Cibernética - foram definidos os responsáveis e prazo para realização das atividades, conforme planilhas (ANEXO II).</p> <p>4.1 - Portaria CNJ nº 290/2020 - Protocolo de Gerenciamento de Crises Cibernéticas (Anexo I)</p> <p>4.2 - Portaria CNJ nº 291/2020 - Protocolo de Investigação de Ilícitos Cibernéticos (Anexo II)</p> <p>4.3 - Portaria CNJ nº 292/2020 - Protocolo de Prevenção a Incidentes Cibernéticos (Anexo III)</p>	Todos os participantes
5	<p>5. COINF - Providências oriundas das reuniões de Avaliação das Eleições 2020:</p> <p>5.1. Preparação de treinamento, palestra sobre recursos do Google Suits, incluindo criação de filtros no Gmail.</p> <p>5.2. Prestar suporte na criação de filtros no Gmail de todos os servidores das ZEs para atender a necessidade de convocação de mesários.</p> <p>Ficou definido o seguinte:</p> <ul style="list-style-type: none">• Serão dois encontros por videoconferência, nos dias 11.06.2021 e 30.07.2021, ambos, numa sexta-feira, das 9h - 10h.• Enviar e-mail convidando os participantes (usuários secretaria e zonas eleitorais)• Solicitar para ASCOM uma matéria sobre o evento• Conteúdo da oficina: e-mail e filtros, calendário, driver, Meet e aplicativos mais úteis no Google Workspace.• Publicar os vídeos feitos sobre o G Suits na intranet (solicitar para Frank)	Marcos Maia
6	<p>6. Fechamento do Índice de Governança e Gestão do TCU (IGG):</p> <p>6.1. Item 3132</p> <p>6.2. Item 4263</p> <p>Traçar um plano para todos os itens que não atingiram 100% no questionário do Índice de Governança e Gestão, a fim que sejam atendidos na integralidade.</p>	Todos os participantes



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

	<p>7. Outros assuntos:</p> <p>O Coordenador de Eleições (Tyronne Medeiros) solicitou alguns ajustes nas datas de apresentação dos processos de trabalho da SSA e SUE, em relação à análise de risco; como também demonstrou preocupação de não ter sido iniciado o levantamento de requisitos para implementação do Sistema de Logística de Eleições. Foi discutido junto com o coordenador de Sistemas Corporativos - COSIS (Osmar Fernandes), a necessidade de reescalonamento dos projetos previstos no Plano de Ação da COSIS, devido ao grande número de projetos e poucos desenvolvedores para atender a demanda crescente de sistemas.</p>	
7	<ul style="list-style-type: none">● Processos internos da SSAE:<ul style="list-style-type: none">○ Transferência de Seções Eleitorais De-PARA○ Agregação de Seções EleitoraisA proposta das modelagens dos processos acima será apresentada no 2º CGestIC junho 2021, se aprovada, será feita a análise de riscos.● Sistema de Logística de Eleições - será definido novo prazo para início do levantamento de requisitos.● Processos internos da SUE: a revisão da modelagem e análise de riscos do processo da SUE - será apresentado no 1º CGestic julho.	Tyronne Medeiros

V. Pendências

Nº	Pendências	Responsável	Data limite
01	Apresentação da Política Formal de Comunicação de TIC e de Divulgação dos Resultados.	GAPSTIE	1º CGESTIC de julho
02	Elaborar memorando para AGE enviando as análises de riscos, um processo de cada coordenadoria.	GAPSTIE	início de julho
03	Memorando para criar o Comitê Gestor de Crise	Carlos Magno	07.06.2021
04	Definir os pré-requisitos e parâmetros para identificação de uma crise cibernética	Carlos Magno	21.06.2021
05	Definição das atividades críticas para criar o protocolo de Crises Cibernéticas	Carlos Magno	21.06.2021
06	Revisar a norma de instituição da ETIR	Daniel Pontes	21.06.2021
07	Instituir o protocolo de investigação para ilícitos cibernéticos	Denilson Bastos	21.06.2021
08	Eventos para apresentação das ferramentas do G Suits	Carlos Magno Daniel Pontes	1º evento - 11.06.2021 2º evento - 30.07.2021
09	Levantamento dos ativos de informação que não permitem registro de eventos	Carlos Magno	21.06.2021



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

10	Adequar o nível de registro dos eventos no monitoramento dos sistemas e redes de comunicação	Carlos Magno	21.06.2021
11	Adequar o nível de registro dos eventos no monitoramento dos sistemas e redes de comunicação	Carlos Magno	21.06.2021
12	Instituição formal de política de senhas	Daniel Pontes	21.06.2011
13	Revisar os registros históricos de eventos dos servidores de hospedagem de página eletrônica	Osmar Júnior Daniel Pontes Frank Viana	21.06.2021

VI. Fechamento da Ata

Data	Nome do relator	Assinatura
27.05.2021	Jussara de Gois Borba Melo Diniz	 JUSSARA DE GOIS BORBA MELO DINIZ:92440668 Assinado de forma digital por JUSSARA DE GOIS BORBA MELO DINIZ:92440668 Dados: 2021.06.09 13:38:52 -03'00'



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ANEXO I

REUNIÃO N. 010/2021 - CGESTIC

Gestão de Riscos

Processo: 10.2.1.2. Gerenciamento de Escopo e Requisitos

Versão 1.0



Natal, 24/05/2021

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	XXXXXXX	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 **10.2.1.2. Gerenciamento de Escopo e Requisitos** da Cadeia de Valor¹.

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 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	5
2. Estabelecimento do Contexto	7
2.1. Referências na Cadeia de Valor / Arquitetura de Processos	7
2.2. Objetivos do Processo	7
2.3. Quadro Resumo	9
3. Matriz SWOT	10
4. Matriz RACI	11

Anexo I - Formulário Padrão de Identificação e Avaliação de Riscos

Anexo II - Formulário Padrão de Tratamento de Riscos

Anexo III - Formulário Perfil de Riscos

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 dois atores do processo **10.2.1.2. Gerenciamento de Escopo e Requisitos**, restaram identificados, avaliados e tratados cinco riscos, vinculados às cinco 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 elaboração do Plano de Contratações de Soluções de TIC.

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

Autor do Processo	Quantidade de Atividades	Quantidade de Riscos Identificados	Nível de Risco Residual das Atividades (Média)
1. Time Scrum	4	4	07 (Baixo)
2. Dono do Produto	1	1	08 (Baixo)
Total Geral / Média Geral	5	5	7,5 (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 7,5 (sete vírgula cinco) pontos, classificando o conjunto das atividades do processo com um nível *Baixo* de riscos. Após os tratamentos de mitigação dos riscos aplicados, verificou-se que três dos riscos relacionados aos dois atores do processo apresentaram um impacto residual *Baixo* (4), enquanto outros dois riscos apresentaram impacto residual *Muito Baixo* (2). Quanto à probabilidade residual, chegamos ao resultado de quatro riscos *Muito Baixo* (2) e um risco *Baixo* (4), após 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, 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 (7,5 pontos), portanto, no nível Baixo.

Tabela – Apetite a Risco do Processo

Apetite a Risco	
Processo	Nível de Risco
10.2.1.2. Gerenciamento de Escopo e Requisitos	Baixo (7,5 pontos)
Aprovação: Comitê de Gestão de Riscos, em xx/xx/2021 .	

2. Estabelecimento do Contexto

Responsável:	Vigência:	Versão:
Coordenador de Sistemas Corporativos	02 (dois) anos, a partir da data de aprovação (xx/xx/2021).	1.0

Processo Organizacional: **10.2.1.2. Gerenciamento de Escopo e Requisitos**

2.1. Referências na Cadeia de Valor / Arquitetura de Processos

Referências na Cadeia de Valor / Arquitetura de Processos:

Macroprocesso de Suporte:

10. Gestão da Tecnologia da Informação e Comunicação

 10.2. Gerenciamento do Desenvolvimento de Soluções

 10.2.1. Desenvolvimento de Sistemas Administrativos

10.2.1.2. Gerenciamento de Escopo e Requisitos

10.2.1.2.1. Estabelecer o Escopo a ser Desenvolvido na Sprint

10.2.1.2.2. Analisar e Especificar os Requisitos da Sprint

10.2.1.2.3. Realizar Planejamento da Sprint

10.2.1.2.4. Desenvolver Protótipo

10.2.1.2.5. Validar Protótipo

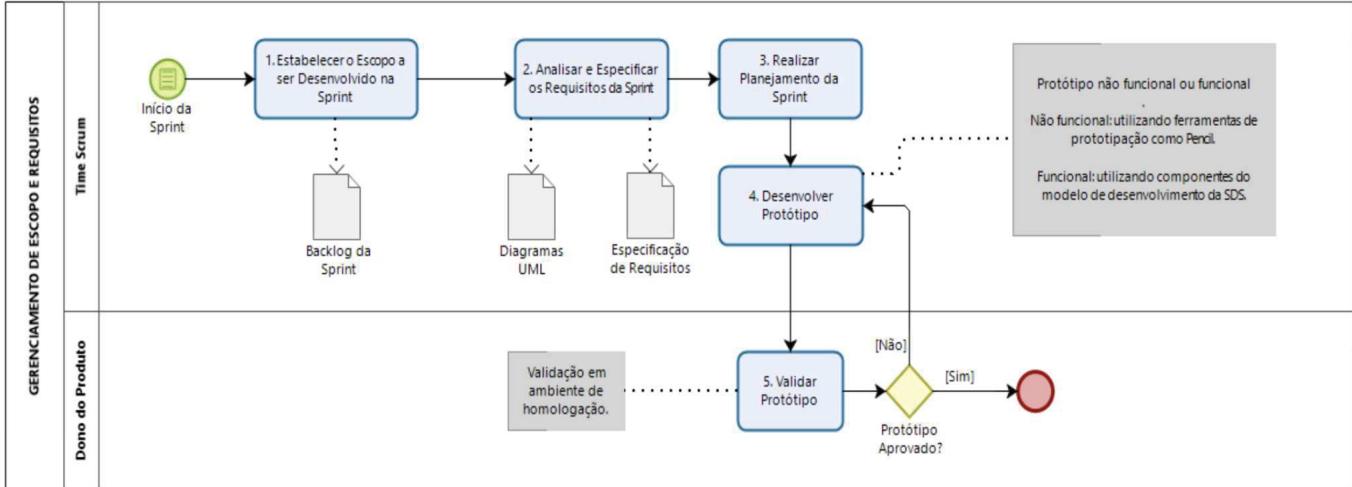
2.2. Objetivos do Processo

O gerenciamento de escopo e requisitos de demandas de sistemas é um processo fundamental para garantir que o projeto solicitado atenda a todas as expectativas da área de negócios, e que todas as funcionalidades pleiteadas sejam atendidas e mantidas pela equipe técnica. Importante ressaltar que apesar de ser um processo fortemente relacionado à área de desenvolvimento de sistemas, a gestão adequada de requisitos e estabelecimento de escopo se aplica também à iniciativas de implantação de soluções de software externas, assim como a implementação de soluções Web.

O presente processo foi instituído formalmente a partir da Portaria n.^º 187/2019-GP, de 11/09/2019, posteriormente alterada pela Portaria n.^º 190/2020-GP, de 14/09/2020. A revisão anual é necessária para que sejam garantidos os 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 dois 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



Ainda 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:	10.2.1.2. Gerenciamento de Escopo e Requisitos
Objetivos e Metas:	<ul style="list-style-type: none">• Disciplinar a forma como os requisitos de demandas de sistemas são repassados para as equipes técnicas.• Garantir a prioridade de atendimento de requisitos considerados mais relevantes pela área demandante.• Viabilizar a implementação de todas as funcionalidades elencadas no escopo da demanda.• 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
Processos de Gestão e Governança associados:	<ul style="list-style-type: none">• Plano Estratégico da Justiça Eleitoral do Rio Grande do Norte – PEJERN• 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:	<ul style="list-style-type: none">• Processo Administrativo Eletrônico – PAE (TRE-RN).
Partes interessadas:	<ul style="list-style-type: none">• Internas (Unidades Administrativas que demandam soluções de TIE – STIE, SAOF, SJ, SGP, NSPRES, ASCOM, AGE, EJE, CRE); e• Externas (Sociedade - Eleitores, Advogados, Mesários, etc.).

3. Matriz SWOT

A análise das fraquezas, forças, ameaças e oportunidades relativas ao processo **10.2.1.2. Gerenciamento de Escopo e Requisitos** encontra-se apresentada na matriz SWOT (*Strengths, Weaknesses, Opportunities e Threats*) a seguir:

Tabela – Matriz SWOT do Processo

FATORES INTERNOS	FORÇAS	FRAQUEZAS
	Priorização dos requisitos da solução por parte da área de negócios.	Necessidade maior de atuação da área de negócios no processo de estabelecimento e priorização de requisitos.
	Gerenciamento padronizado de mudanças de requisitos.	Maior formalismo no gerenciamento de alterações de escopo ou de funcionalidades demandadas.
	Estabelecimento dos controles de escopo dos projetos de sistemas.	
FATORES EXTERNOS	OPORTUNIDADES	AMEAÇAS
	Adoção de premissas de gerenciamento amplamente utilizadas por outras instituições.	Necessidade de revisões de processo visando adequá-lo às evoluções das metodologias de desenvolvimento.

4. Matriz RACI

A matriz de designação de responsabilidades relacionada ao processo **10.2.1.5. Gerenciamento de Escopo e Requisitos** encontra-se representada na Matriz RACI (*Responsible, Accountable, Consulted e Informed*) a seguir:

Tabela – Matriz RACI do Processo

MATRIZ RACI			
Processo Organizacional: 10.2.1.2. Gerenciamento de Escopo e Requisitos			
Responsável: Coordenador de Sistemas Corporativos	Data: 27/05/2021		
	Papel	I ..	C C D
Responsabilidade			
1. Estabelecer o Escopo a ser Desenvolvido na <i>Sprint</i>	R	A/C	
2. Analisar e especificar os Requisitos da <i>Sprint</i>	R	A	
3. Realizar o Planejamento da <i>Sprint</i>	R		
4. Desenvolver Protótipo	R	I	
5. Validar Protótipo	I		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.		

O Processo de Gestão de Riscos aprovado pela Resolução n.^º 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. Time Scrum**
- 2. Dono do Produto**

Anexo I - 1. Time Scrum

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 xx/xx/2021				Vigência: 02 (dois) anos, a partir da data de aprovação.			Versão: 1.0	

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 27/05/2021			Unidade: COSIS					Gestor de Riscos: Chefe da SDS							
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) Backlog do Produto incompleto ou com informações desatualizadas.	Alimentação da planilha de Backlog do Produto feita de forma inadequada pelo Dono do Produto.	Operacional	Alto (8)	Média (6)	48	Alto	Priorização inadequada do Backlog da Sprint, impactando na ordem de implementação das funcionalidades.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SDS	Chefe da SDS
(2) Requisitos mal definidos ou inconsistentes.	Inexperiência do Dono do Produto na definição das funcionalidades.	Operacional	Médio (6)	Baixa (4)	24	Médio	Perda de tempo decorrente da necessidade de ajuste dos requisitos junto ao demandante.	Mitigar o risco	Muito Baixo (2)	Muito Baixa (2)	4	Baixo	Não	SDS	Chefe da SDS
(3) Impossibilidade de atendimento das funcionalidades selecionadas para o Backlog da Sprint.	Excesso de funcionalidades selecionadas para o Backlog da Sprint.	Operacional	Médio (6)	Média (6)	36	Alto	Não implementação de todas as funcionalidades elencadas para serem realizadas ao longo da Sprint.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SDS	Chefe da SDS
(4) Atraso na realização dos protótipos.	Excesso de atividades atribuídas ao membro do Time Scrum.	Operacional	Médio (6)	Baixa (4)	24	Médio	Baixa qualidade na elaboração dos protótipos a serem validados junto ao demandante.	Mitigar o risco	Muito Baixo (2)	Baixa (4)	8	Baixo	Não	SDS	Chefe da SDS

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

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

10.2. Processo: Gerenciamento do Desenvolvimento de Soluções

10.2.1. Desenvolvimento de Sistemas Administrativos

10.2.1.2. Gerenciamento de Escopo e Requisitos

10.2.1.2.1. Estabelecer o Escopo a ser Desenvolvido na Sprint (Risco 1)

10.2.1.2.2. Analisar e Especificar os Requisitos da Sprint (Risco 2)

10.2.1.2.3. Realizar Planejamento da Sprint (Risco 3)

10.2.1.2.4. Desenvolver Protótipo (Risco 4)

Anexo I - 2. Dono do Produto

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 xx/xx/2021			Vigência: 02 (dois) anos, a partir da data de aprovação.			Versão: 1.0		

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 27/05/2021			Unidade: COSIS					Gestor de Riscos: Servidor Demandante							
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) Os protótipos elaborados não atendem aos requisitos das funcionalidades selecionadas para a Sprint.	Erro de entendimento por parte do Time Scrum quanto aos requisitos solicitados.	Operacional	Médio (6)	Muito Baixa (2)	12	Médio	Perda de tempo decorrente da necessidade de reimplementação dos protótipos.	Mitigar o risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SDS	Servidor Demandante

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

10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
 - 10.2. Processo: Gerenciamento do Desenvolvimento de Soluções
 - 10.2.1. Desenvolvimento de Sistemas Administrativos
 - 10.2.1.2. Gerenciamento de Escopo e Requisitos
 - 10.2.1.2.5. Validar Protótipo (Risco 1)**

Anexo II - Formulário Padrão de Tratamento de Riscos

- 1. Time Scrum**
- 2. Dono do Produto**

Anexo II - 1. Time Scrum

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 xx/xx/2021	Vigência: 02 (dois) anos, a partir da data de aprovação.	Versão: 1.0
---	---	--	-----------------------

Formulário Padrão de Tratamento de Riscos

Data: 27/05/2021	Área Funcional: SDS	Proprietário do Risco: Chefe da SDS
Risco:	(1) Backlog do Produto incompleto ou com informações desatualizadas.	
Probabilidade: Média (6)	Impacto: Alto (8)	Nível do Risco: Alto (48)
Resposta a ser implantada:	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do Backlog do Produto pelo Dono do Produto.	
Tipo de Resposta: Mitigar o risco	Prazo para implantação: Até 1 semana após o início do projeto.	
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: 27/05/2021	Área Funcional: SDS	Proprietário do Risco: Chefe da SDS
Risco:	(2) Requisitos mal definidos ou inconsistentes.	
Probabilidade: Baixa (4)	Impacto: Médio (6)	Nível do Risco: Médio (24)
Resposta a ser implantada:	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do Backlog do Produto pelo Dono do Produto.	
Tipo de Resposta: Mitigar o risco	Prazo para implantação: Até 1 semana após o início do projeto.	
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: 27/05/2021	Área Funcional: SDS	Proprietário do Risco: Chefe da SDS
Risco:	(3) Impossibilidade de atendimento das funcionalidades elencadas no prazo estabelecido pela Sprint.	
Probabilidade: Médio (6)	Impacto: Médio (6)	Nível do Risco: Alto (36)
Resposta a ser implantada:	Negociar com o Dono do Produto uma revisão dos requisitos elencados para compor o Backlog da Sprint.	
Tipo de Resposta: Mitigar o risco	Prazo para implantação: Até 1 semana após o início da Sprint.	
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: 27/05/2021	Área Funcional: SDS	Proprietário do Risco: Chefe da SDS
Risco:	(4) Atraso na realização dos protótipos.	

Probabilidade: Baixa (4)	Impacto: Médio (6)	Nível do Risco: Médio (24)
Resposta a ser implantada:	Realizar uma revisão na priorização das atividades associadas aos servidores integrantes <i>Time Scrum</i> .	
Tipo de Resposta: Mitigar o risco	Prazo para implantação: Até 1 semana após a reunião de revisão da <i>Sprint</i> .	
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 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
 - 10.2. Processo: Gerenciamento do Desenvolvimento de Soluções
 - 10.2.1. Desenvolvimento de Sistemas Administrativos
 - 10.2.1.2. Gerenciamento de Escopo e Requisitos
 - 10.2.1.2.1. Estabelecer o Escopo a ser Desenvolvido na Sprint (Risco 1)**
 - 10.2.1.2.2. Analisar e Especificar os Requisitos da Sprint (Risco 2)**
 - 10.2.1.2.3. Realizar Planejamento da Sprint (Risco 3)**
 - 10.2.1.2.4. Desenvolver Protótipo (Risco 4)**

Anexo II - 2. Dono do Produto

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 xx/xx/2021	Vigência: 02 (dois) anos, a partir da data de aprovação.	Versão: 1.0

Formulário Padrão de Tratamento de Riscos			
Data: 27/05/2021	Área Funcional: SDS	Proprietário do Risco: Servidor Demandante	
Risco:	(1) Os protótipos elaborados não atendem aos requisitos das funcionalidades selecionadas para a Sprint.		
Probabilidade: Muito Baixa (2)	Impacto: Médio (6)	Nível do Risco: Médio (12)	
Resposta a ser implantada:	Realizar reunião para esclarecimentos dos requisitos, entre o Time Scrum e o Dono do Projeto.		
Tipo de Resposta: Mitigar o risco	Prazo para implantação: Até 1 semana após a reunião de revisão da Sprint.		
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
 - 10.2. Processo: Gerenciamento do Desenvolvimento de Soluções
 - 10.2.1. Desenvolvimento de Sistemas Administrativos
 - 10.2.1.2. Gerenciamento de Escopo e Requisitos
 - 10.2.1.2.5. Validar Protótipo (Risco 1)**

Anexo III - Formulário Perfil de Riscos

- 1. Time Scrum**
- 2. Dono do Produto**

Anexo III - 1. Time Scrum

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Perfil de Riscos			
Responsável: Coordenador de Sistemas Corporativos	Aprovação: Comitê Gestor de Riscos, em xx/xx/2021	Vigência: 02 (dois) anos, a partir da data de aprovação.	Versão: 1.0

Formulário Perfil de Riscos								
Gestor de Risco Setorial: Chefe da SDS				Área Funcional: SDS		Data: 24/05/2021		
Risco (Descrição)	Classe	Causa	Consequências	Resposta	Nível de Risco (IxP)	Tipos de Resposta	Proprietário do Risco	
(1) Backlog do Produto incompleto ou com informações desatualizadas.	Operacional	Alimentação da planilha de Backlog do Produto feita de forma inadequada pelo Dono do Produto.	Priorização inadequada do Backlog da Sprint, impactando na ordem de implementação das funcionalidades.	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do Backlog do Produto pelo Dono do Produto.	Nível de Risco Inerente = 8 x 6 = 48 (Alto)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SDS
(2) Requisitos mal definidos ou inconsistentes.	Operacional	Inexperiência do Dono do Produto na definição das funcionalidades.	Perda de tempo decorrente da necessidade de ajuste dos requisitos junto ao demandante.	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do Backlog do Produto pelo Dono do Produto.	Nível de Risco Inerente = 6 x 4 = 24 (Médio)	Nível de Risco Residual = 2 x 2 = 4 (Baixo)	Mitigar o risco	Chefe da SDS
(3) Impossibilidade de atendimento das funcionalidades elencadas no prazo estabelecido pela Sprint.	Operacional	Excesso de funcionalidades selecionadas para o Backlog da Sprint.	Não implementação de todas as funcionalidades elencadas para serem realizadas ao longo da Sprint.	Negociar com o Dono do Produto uma revisão dos requisitos elencados para compor o Backlog da Sprint.	Nível de Risco Inerente = 6 x 6 = 36 (Alto)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Chefe da SDS
(4) Atraso na realização dos protótipos.	Operacional	Excesso de atividades atribuídas ao membro do Time Scrum.	Baixa qualidade na elaboração dos protótipos a serem validados junto ao demandante.	Realizar uma revisão na priorização das atividades associadas aos servidores integrantes Time Scrum.	Nível de Risco Inerente = 6 x 4 = 24 (Médio)	Nível de Risco Residual = 2 x 4 = 8 (Baixo)	Mitigar o risco	Chefe da SDS

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

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

10.2. Processo: Gerenciamento do Desenvolvimento de Soluções

10.2.1. Desenvolvimento de Sistemas Administrativos

10.2.1.2. Gerenciamento de Escopo e Requisitos

10.2.1.2.1. Estabelecer o Escopo a ser Desenvolvido na Sprint (Risco 1)

10.2.1.2.2. Analisar e Especificar os Requisitos da Sprint (Risco 2)

10.2.1.2.3. Realizar Planejamento da Sprint (Risco 3)

10.2.1.2.4. Desenvolver Protótipo (Risco 4)

Anexo III - 2. Dono do Produto

Tribunal Regional Eleitoral do Rio Grande do Norte
Formulário Perfil de Riscos

Responsável: Coordenador de Sistemas Corporativos	Aprovação: Comitê Gestor de Riscos, em xx/xx/2021	Vigência: 02 (dois) anos, a partir da data de aprovação.	Versão: 1.0
---	---	--	-----------------------

Formulário Perfil de Riscos

Gestor de Risco Setorial: Chefe da SDS					Área Funcional: SDS		Data: 24/05/2021	
Risco (Descrição)	Classe	Causa	Consequências	Resposta	Nível de Riscos (IxP)	Tipos de Resposta	Proprietário do Risco	
(1) Os protótipos elaborados não atendem aos requisitos das funcionalidades selecionadas para a <i>Sprint</i> .	Operacional	Erro de entendimento por parte do <i>Time Scrum</i> quanto aos requisitos solicitados.	Proposta de alteração não reflete o real cronograma do andamento dos projetos.	Realizar reunião para esclarecimentos dos requisitos, entre o <i>Time Scrum</i> e o <i>Dono do Projeto</i> .	Nível de Risco Inerente = $6 \times 2 = 12$ (Médio)	Nível de Risco Residual = $4 \times 2 = 8$ (Baixo)	Mitigar o risco	Servidor Demandante

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

- 10. Macroprocesso de Suporte: Gestão da Tecnologia da Informação e Comunicação
 - 10.2. Processo: Gerenciamento do Desenvolvimento de Soluções
 - 10.2.1. Desenvolvimento de Sistemas Administrativos
 - 10.2.1.2. Gerenciamento de Escopo e Requisitos
 - 10.2.1.2.5. Validar Protótipo (Risco 1)**

DECISÕES PARA MITIGAR RISCOS

Processo: Gerenciamento de Escopo de Requisitos

Gestor de Risco Setorial: Chefe da SDS

Área Funcional: SDS

Riscos (Descrição)	Classe(s)	Decisões para mitigar o risco	Proprietário do Risco
<i>Backlog do Produto</i> incompleto ou com informações desatualizadas.	Operacional	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do <i>Backlog do Produto</i> pelo <i>Dono do Produto</i> .	Chefe da SDS
Requisitos mal definidos ou inconsistentes.	Operacional	Realizar reunião de conscientização da importância da definição adequada dos requisitos que fazem parte do <i>Backlog do Produto</i> pelo <i>Dono do Produto</i> .	Chefe da SDS
Impossibilidade de atendimento das funcionalidades elencadas no prazo estabelecido pela <i>Sprint</i> .	Operacional	Negociar com o Dono do Produto uma revisão dos requisitos elencados para compor o <i>Backlog da Sprint</i> .	Chefe da SDS
Atraso na realização dos protótipos.	Operacional	Realizar uma revisão na priorização das atividades associadas aos servidores integrantes <i>Time Scrum</i> .	Chefe da SDS

Gestor de Risco Setorial: Servidor Demandante

Área Funcional: SDS

Riscos (Descrição)	Classe(s)	Decisões para mitigar o risco	Proprietário do Risco
Os protótipos elaborados não atendem aos requisitos das funcionalidades selecionadas para a <i>Sprint</i> .	Operacional	Realizar reunião para esclarecimentos dos requisitos, entre o <i>Time Scrum</i> e o <i>Dono do Projeto</i> .	Servidor Demandante



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ANEXO II

REUNIÃO N. 010/2021 - CGESTIC

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS
Resolução CNJ n.º 360/2020 - Portaria n.º 290/2020
versão 1.0

Atividade	Descrição / Objetivo Geral	Responsável	Período limite	CGesTIC 10/2021	Observações	Situação
Definições dos pré-requisitos e parâmetros para identificação de uma crise cibernética	Relacionar possíveis danos que possam ser considerados relevantes para acionar o processo de gerenciamento de crise.	Comitê Gestor de Crises	Junho/2021	Responsável: Carlos Magno Prazo: 21.06		
Definir o mínimo necessário para a continuidade de negócios	<ul style="list-style-type: none"> . Estabelecer e manter o Plano de Continuidade de Serviço de TIC(PCSTIC) e planos de recuperação que suporte a continuidade denegócio de TRE/RN . Realizar exercícios (regulares) de Análise de Impacto no Negócio (AIN) . Conduzir exercícios (de forma regular) de avaliação e gerenciamento de risco . Fornecer aconselhamento e orientação a todas as outras áreas de negócio e de TIC sobre questões relativas à continuidade e recuperação . Assegurar que os mecanismos adequados de continuidade e recuperação sejam implantados para alcançar ou superar as metas acordadas . Avaliar o impacto de todas as mudanças sobre o Plano de Continuidade de Serviço de TIC (PCSTIC) e os planos de recuperação de TIC . Assegurar que medidas proativas para melhorar a disponibilidade de serviços sejam implantadas sempre que o custo de implantação for justificável . Negociar e acordar os contratos necessários com fornecedores para fornecimento de recursos necessários à recuperação 	COINF/STIE e COSIS/STIE	Já realizada		Portaria nº 177/2019 - GP instituiu a Gestão da Continuidade de Serviços Essenciais de TIC, no âmbito da JE/RN, incluindo Plano de Continuidade de Serviços Essenciais de TIC	CONCLUÍDO
Avaliar continuamente os riscos a que atividades críticas estão expostas	<ul style="list-style-type: none"> . Instituir o processo de Gestão de Riscos da Segurança da Informação, no âmbito da Justiça Eleitoral do Rio Grande do Norte . O Processo de Gestão de Riscos da Segurança da Informação tem como objetivo principal minimizar a ocorrência de ameaças que podem interferir (negativamente) no recurso de informação utilizado pela organização para atingir os seus objetivos corporativos 	SSI/COINF/STIE	Já realizada			CONCLUÍDO
definir as atividades críticas	Definir as atividades críticas que são fundamentais para a atividade finalística do órgão	Alta administração	Junho/2021	Responsável: Carlos Magno Prazo: 21.06		
identificar os ativos de informação críticos	Identificar os ativos de informação críticos que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação	Comitê Gestor de Crises	Julho/2021			
Categorizar os incidentes e definir playbooks específicos	Categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente	COINF/STIE e COSIS/STIE	Dezembro/2021			
Definir plano de contingência	Criar um plano de contingência, detalhando atividades críticas e ações necessárias para reestabelecer-las.	COINF/STIE e COSIS/STIE	Já realizada		Portaria nº 177/2019 - GP instituiu a Gestão da Continuidade de Serviços Essenciais de TIC, no âmbito da JE/RN, incluindo Plano de Continuidade de Serviços Essenciais de TIC	CONCLUÍDO
Definir cenários de simulações	Elaborar um cronograma de simulações, definindo cenários e testes para validação dos planos e procedimentos	COINF/STIE e COSIS/STIE	Dezembro/2021			
Criar Comitê de Crise	Criar um Comitê de Crises Cibernéticas formado por representante da Alta Administração e por representantes executivos, suportados pela Equipe de Resposta a Incidentes de Segurança Cibernética e por especialistas das áreas: I – Jurídica; II – Comunicação; III – Tecnologia da Informação; IV – Privacidade de Dados Pessoais; V – Segurança da Informação; VI – Unidades administrativas de apoio à contratação; e VII – Segurança Institucional.	Presidência	Março/2021	Responsável: Carlos Magno Prazo: 07.06		
Estruturar Plano de Gestão de Incidentes Cibernéticos, conforme ANEXO I	Elaborar um plano de gestão de incidentes ciberneticos contendo, no mínimo: Indicação do incidente cibernético, Descrição, Procedimento e Severidade	COINF/STIE e COSIS/STIE	Dezembro/2021			

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO PROTOCOLO DE PREVENÇÃO DE INCIDENTES CIBERNÉTICOS (PPI Ciber/PJ)
Resolução CNJ n.º 361/2020 - Portaria n.º 292/2020
versão 1.0

Atividade	Descrição / Objetivo Geral	Responsável	Período	CGestic	Observações	Situação
Elaborar o protocolo de prevenção a incidentes cibernéticos	definir e implementar controles de segurança críticos para uma defesa cibernética eficaz, estabelecendo as ações prioritárias, ou seja, um conjunto prescritivo e priorizado de práticas recomendadas de segurança cibernética e respostas defensivas que podem ajudar a evitar os ataques mais perigosos e disseminados	COINF/STIE e COSIS/STIE	Dezembro/2021			
Criar o processo de gestão de incidentes de segurança cibernética	. Mapear o processo de Gestão de Incidentes de Segurança Cibernética · Identificar, no processo, as fases de detecção, triagem, análise e resposta aos incidentes de segurança	SSI/COINF/STIE	Agosto/2021			
Instituir a ETIR	. Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, subordinada à Secretaria de Tecnologia da Informação e Comunicação . A ETIR terá como objetivo garantir o cumprimento da missão institucional do TRE/RN, através do tratamento e resposta a incidentes de segurança na rede interna de computadores	Presidência	Já realizada		Instituída através da Portaria n.º 423/2017-GP, alterada pela Portaria n.º 127/2020 - GP	CONCLUÍDO
Revisar a norma de instituição da ETIR	Revisar o documento para que contenha, no mínimo, os seguintes pontos: definição da missão, público-alvo, modelo de implementação, nível de autonomia, designação de integrantes, canal de comunicação de incidentes de segurança e os serviços que serão prestados.	CPSI	Abril/2021	Responsável: Daniel Prazo: 21.06		

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS
Resolução CNJ n.º 362/2020 - Portaria n.º 291/2020
versão 1.0

Etapas	Código da Ação	Item da Portaria CNJ n.º 291/2020	Atividade	Descrição / Objetivo Geral	Responsável	Período	Observações	Situação
Do objetivo	1	Art. 1º e 3º	Instituir o protocolo de investigação para ilícitos ciberneticos	Estabelecer os procedimentos básicos para coleta e preservação de evidências, e comunicar os fatos penalmente relevantes ao órgão de polícia judiciária	CPSI e NSPRES	Junho/2021	Responsável: Denilson Prazo: 21.06	
Das definições	2	Art. 4º, XIV	Definir informação sigilosa	Elaborar Plano de Classificação Documental onde encontra-se a definição de informação sigilosa que necessita ser submetida temporariamente à restrição de acesso público em razão de sua imprecindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.	CPAD	Já realizado		https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/acesso-a-informacao/arquivos_informacoes-sigilosas/classificacao-informacao-grau-de-sigilo-2019-pdf
	3	Art. 4º, XV	Definir e avaliar a gerencia de logs	Criar/configurar um servidor de logs centralizado, para guardar todas as informações de acesso (de rede) relevantes	SRI/COINF/STIE	Já realizado		CONCLUÍDA
	4	Art. 4º, XVIII	Definição de método de geração de resumo criptográfico	Definir e adotar um método de geração de resumo criptográfico (hash) reconhecidamente eficiente para garantir a integridade das informações guardadas	SSI/COINF/STIE	Dezembro/2021		
	5	Art. 5º	Garantir que todos os ativos de informação estejam sincronizados com a Hora Legal Brasileira	Garantir o sincronismo dos registros (logs) de todos os ativos de informação, para permitir maior precisão na verificação de informações	SRI/COINF/STIE	Já realizado		CONCLUÍDA
Dos requisitos para adequação dos ativos de informação	6	Art. 6º	Configurar os ativos de informação de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC)	Configurar os ativos para registrar eventos tais como: I - autenticação, tanto as bem-sucedidas quanto as mal-sucedidas; II – acesso a recursos e dados privilegiados; e III – acesso e alteração nos registros de auditoria.	SRI/COINF/STIE	Já realizado		CONCLUÍDA
	7	Art. 8º	Levantamento dos ativos de informação que não permitem registro de eventos	Mapear e documentar os ativos de informação que não permitem os registros de eventos quanto ao tipo e formato de registros de auditoria permitidos e armazenados.	SRI/COINF/STIE, SBDS/COSIS/STIE, SDS/COSIS/STIE	Junho/2021	Responsável: Carlos Magno Prazo: 21.06	
	8	Art. 9º	Adequar o nível de registro dos eventos no monitoramento dos sistemas e redes de comunicação	Garantir um detalhamento mínimo das informações disponíveis para diversos eventos de segurança, de modo a garantir identificar quem acessou, o que acessou, como e quando	SRI/COINF/STIE, SBDS/COSIS/STIE, SDS/COSIS/STIE	Junho/2021	Responsável: Carlos Magno Prazo: 21.06	
	9	Art. 9º, V	Instituição formal de política de senhas	Elaboração e formalização de política de senhas, com previsão de modificação periódica dos critérios mínimos necessários	CPSI	Junho/2021	Responsável: Daniel Prazo: 21.06	
	10	Art. 9º, VI	Definir arquivos e sistemas críticos	Definir quais arquivos ou sistemas críticos devem ser monitorados, para registro de acessos e modificações	COINF/STIE e COSIS/STIE	Dezembro/2021		
	11	Art. 10	Revisar os registros históricos de eventos dos servidores de hospedagem de página eletrônica	Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que permita a completa identificação dos fluxos de dados. Os registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.	COSIS/STIE	Junho/2021	Osmar informou sobre o Plone da Intranet e da Internet (ver ao lado). Daniel e Frank devem alinhar se é necessária a ativação dos logs de auditoria das máquinas servidores de hospedagem. Prazo: 21.06	<p>Informação de Osmar: o serviço de hospedagem de página eletrônica do TRE-RN faz uso de uma área disponível para usuários externos (Internet) e outra área apenas para uso interno dos servidores (Intranet e Extranet).</p> <p>A infraestrutura da Internet é gerida completamente pelo TSE e questões referentes a como estão atendendo essa norma devem ser encaminhadas para a unidade responsável daquele Tribunal.</p> <p>No caso da Intranet/Extranet, usamos o sistema gerenciador de conteúdo Plone que internamente registra, no nível de aplicação, as modificações que os usuários realizam no conteúdo das páginas e pode gerar um relatório identificando os usuários e data/hora de modificação.</p> <p>Pelo rol de eventos listados acima, pode-se ver que a maioria dos eventos de segurança são gerados no nível do sistema operacional. No entanto, a SNT, unidade responsável pelo Plone, não dispõe de conhecimentos técnicos para habilitar o registro e monitoramento desses eventos de segurança gerados pelo sistema operacional da máquina.</p> <p>Normalmente, a unidade responsável por manter a infraestrutura dos servidores e redes de computadores é a SRI/COINF (Seção de Redes e Infraestrutura) que detém conhecimento mais avançado em relação aos requisitos de segurança do sistema operacional.</p>