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

ATA DE REUNIÃO N. 23/2020 - CGESTIC

I . Identificação da Reunião

Data	Horário		Local	Coordenador
	Início	Término		
10.08.2020	13h30	16h40	Videoconferência	Marcos Flávio Nascimento Maia

II. Objetivo

Pauta:

1. Apresentação da análise de riscos dos processos a seguir:
    1.1. COINF: Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados
    1.2. COINF: Gerenciamento de Incidentes de TIC
    1.3. COSIS: A critério da Coordenadoria - relativos à Segurança da Informação
2. Ferramenta para facilitar comunicação institucional - Whatsapp Business, Rocket Chat
3. Gestão das Coordenadorias
4. Pendências anteriores:
    4.1. COINF - Validação da versão do windows em todas as zonas eleitorais
    4.2. COINF - Confirmar os números voips disponíveis
    4.3. COINF/SSI - Atualização do Catálogo de Serviços e Catálogo de Soluções de TIC
5. Coordenação do evento do teste em campo - COTEL
6. Gestores dos sistemas
7. Ofício-Circular nº 4 - DTI - CNJ - Acórdão 1613-2020- TCU que trata de uso de tecnologia de blockchain

III. Participantes

Nome	Lotação	Assinatura
Marcos Flávio Nascimento Maia	STIC	MARCOS FLAVIO NASCIMENTO MAIA:30024317 Assinado de forma digital por MARCOS FLAVIO NASCIMENTO MAIA:30024317 Dados: 2020.09.16 19:41:52 -03'00'
Osmar Fernandes de Oliveira Júnior	COSIS	OSMAR FERNANDES DE OLIVEIRA JUNIOR:92440637 Assinado de forma digital por OSMAR FERNANDES DE OLIVEIRA JUNIOR:92440637 Dados: 2020.08.17 10:31:42 -03'00'
Tyronne Dantas de Medeiros	COTEL	TYRONNE DANTAS DE MEDEIROS:92440597 Assinado de forma digital por TYRONNE DANTAS DE MEDEIROS:92440597 Dados: 2020.08.17 18:47:11 -03'00'
Carlos Magno do Rozário Câmara	COINF	CARLOS MAGNO DO ROZARIO CAMARA:30024407 Assinado de forma digital por CARLOS MAGNO DO ROZARIO CAMARA:30024407 Dados: 2020.08.17 16:33:39 -03'00'

Sidnei Costa Souza	SRI/COINF	SIDNEI COSTA SOUZA:30024385 Assinado de forma digital por SIDNEI COSTA SOUZA:30024385 Dados: 2020.09.01 06:45:36 -03'00'
Alexandre Marcio Cavalcanti Machado	SSI/COINF	ALEXANDRE MARCIO CAVALCANTI MACHADO:10024103 Assinado de forma digital por ALEXANDRE MARCIO CAVALCANTI MACHADO:10024103 Dados: 2020.08.31 14:27:00 -03'00'
Dina Márcia Vasconcelos Maranhão da Câmara	GAPSTIC	DINA MARCIA DE VASCONCELOS MARANHAO DA CAMARA:20024230 Assinado de forma digital por DINA MARCIA DE VASCONCELOS MARANHAO DA CAMARA:20024230 Dados: 2020.08.17 20:35:18 -03'00'
Jussara de Gois Borba Melo Diniz	GAPSTIC	JUSSARA DE GOIS BORBA MELO DINIZ:92440668 Assinado de forma digital por JUSSARA DE GOIS BORBA MELO DINIZ:92440668 Dados: 2020.08.17 14:04:57 -03'00'

IV. Discussão da Pauta

Nº	Descrição/Decisão	Responsável
01	1. Apresentação da análise de riscos dos processos a seguir: 1.1. COINF: Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados Conforme reunião do CGesTIC n.21/2020, cuja deliberação foi a de reapresentação da análise para enquadrar o risco final do processo em risco baixo, Sidnei reapresentou a análise realizada. Em um primeiro momento, ele apresentou um comparativo das faixas de risco da norma do TRE/RN e a norma do TCU, demonstrando a forma como as faixas foram enquadradas, como também, uma falha existente na Matriz de Risco Residual do nosso Tribunal, motivo pelo qual Marcos concordou em, a partir da sugestão de Sidnei, levar ao Comitê de Riscos propostas de revisão da norma da casa, para revisão das faixas, inclusive no que diz respeito a uma faixa de riscos residuais que não foi contemplada na nossa norma. Em seguida, Sidnei apresentou os ajustes na análise quando ele implementou novas respostas para mitigação dos riscos que encontravam-se com risco residual médio. Desta forma, a análise de risco do processo "Gerenciamento de Cópias de Segurança (Backup) e de Restauração de Dados" foi aprovado pelos participantes, conforme o Anexo 1 desta ata. 1.2. COINF: Gerenciamento de Incidentes de TIC Em seguida, Alexandre Márcio passou a a apresentar a análise de riscos do processo Gerenciamento de Incidentes de TIC, que resultou em uma média de risco residual de 7,94, considerado baixo pela norma da casa, devidamente aprovado pelos participantes, conforme o Anexo 2 desta ata. 1.3. COSIS: A critério da Coordenadoria - relativos à Segurança da Informação Após explanação, Marcos e Osmar deliberaram que deve ser apresentada a análise de riscos relacionados à Segurança da Informação na próxima reunião do CGesTIC.	Sidnei/ Alexandre

02	2. Ferramenta para facilitar comunicação institucional - Whatsapp Business, Rocket Chat Foi iniciada a discussão em torno da necessidade de instituir uma ferramenta de comunicação institucional que seja independente dos telefones pessoais dos servidores. Marcos relatou também as dificuldades encontradas pelos servidores em se comunicar pelos números VOIP. Ele trouxe para discussão prós e contras das soluções para que seja estudado pelos participantes. Osmar relatou uma experiência positiva com o uso do “Slack” em sua equipe. Informou que a ferramenta possui versão gratuita e versão paga. Entretanto, para fins de uso para contactar todos os servidores, a solução precisa ser simples e que seja de uso institucional. Dina reforçou a necessidade de estabelecer quais os acessos que desejam ser alcançados, ou seja público externo e público interno. Avaliando as soluções, os participantes concluíram que a melhor solução é através do uso do Whatsapp Business, devendo ser recomendado à Administração que em cada seção seria indicado ter pelo menos um número disponível para comunicação interna e externa. Desta forma, Marcos entrará em contato com a Direção Geral para verificar o interesse em implantar a solução de Whatsapp Business nos ramais dos setores, recomendando o uso por parte de um servidor, no mínimo, como forma de melhoria da comunicação interna e por parte do público externo com o Tribunal, principalmente em razão do isolamento social.	Todos os participantes
03	3. Gestão das Coordenadorias Marcos iniciou esta parte da reunião explanando que após realização de reunião com o Gabinete, alguns pontos foram relatados como maiores dificuldades no andamento das dificuldades. O primeiro ponto a ser tratado foi sobre a gestão do planejamento das contratações. Apontou as dificuldades que estão sendo encontradas em função das equipes de planejamento não estarem trabalhando de forma uníssona, bem como, pela quantidade de erros que estão sendo encontrados nos artefatos. Assim, deve o processo de planejamento não deve tramitar entre os integrantes da equipe, apenas quando for colher as assinaturas, a equipe tem que trabalhar em conjunto para elaborar o planejamento, o integrante demandante deve elaborar os artefatos do planejamento, reunindo o conteúdo subsidiado pelos integrantes técnico e administrativo, coletando as assinaturas e anexando ao PAE para envio ao titular da área demandante e, por fim, a equipe tem que observar o teor dos documentos, prezando pela escrita e conferindo o cumprimento do manual de contratações de TIC, como forma de evitar retorno dos processos e consequente atraso da licitação. Além disso, deve ser reforçado o cuidado com o cumprimento dos prazos estabelecidos no Plano de Contratações.	Marcos Maia

03	Em especial, foram destacados os contratos que envolvem terceirização, que, provavelmente não serão renovados, devendo ser os prazos rigorosamente cumpridos. Marcos destacou que não deve haver, de forma alguma, nova situação como a passada pela contratação do backbone secundário, quando houve a necessidade de fazer uma contratação excepcional. Por fim, restou estabelecido que será agendada reunião com as coordenadorias e chefias das seções da COSIS e COINF para sensibilização dos prazos do Plano de Contratações, bem como, sobre a necessidade de observar os acórdãos mais recentes do TCU. O segundo ponto tratado foi sobre a pauta do CGesTIC. Considerando que as reuniões estão sendo semanais e todas as segundas-feiras, foi solicitado que cada Coordenador encaminhe ao Gabinete, até todas as sexta-feiras, no máximo às 9h, para que a pauta seja fechada e encaminhada até às 12h da sexta-feira. Desta forma, as demandas advindas das coordenadorias serão melhor compartilhadas. O terceiro ponto tratado foi sobre o uso do Trello, reforçando a necessidade de uso da ferramenta.Foi verificado com os participantes da necessidade de agendamento de uma explanação da ferramenta com os Coordenadores e chefias das seções, motivo pelo qual foi agendado para 14.08.2020, às 13h, sob a coordenação do Gabinete o momento de disseminação, repasse das principais funcionalidades do Trello e padronização de conduta. Em seguida, o quarto ponto trazido para a reunião foi sobre a necessidade de melhoria de comunicação entre as coordenadorias quando houver evento que envolva mais de uma coordenadoria. Se for o caso, deve ser agendada reunião específica para tratar do assunto, evitando ruídos de comunicação ou falhas no desenvolvimento das atividades. O quinto ponto tratado foi a necessidade de melhorar a comunicação quando da ocorrência de incidentes, não deixando transcorrer espaço de tempo, relatando tão logo seja possível o ocorrido ao Gabinete. É necessário melhorar a comunicação com os usuários.	Marcos Maia
04	4. Pendências anteriores: 4.1. COINF - Validação da versão do windows em todas as zonas eleitorais Carlos Magno informou que foram verificadas que em relação ao Chip TPM, as zonas eleitorais possuem, pelo menos uma máquina, inclusive com Windows 10. É possível migrar a versão do Windows em outras máquinas do cartório, entretanto, não terão o chip. Para solucionar, serão enviadas máquinas novas às zonas eleitorais. Ou seja, em cada zona eleitoral, ficarão pelo menos duas máquinas com as configurações estabelecidas pelo TSE. Restou ainda como pendência o envio, pela COINF, de tabela com as informações de cada zona eleitoral.	Todos os participantes

04	4.2. COINF - Confirmar os números voips disponíveis Carlos Magno confirmou que os ramais VOIP das centrais de suporte, tanto do suporte Jeconnect e Central de Suporte estão reservados, conforme a eleição passada. Serão utilizados os mesmos números, 6300 e 6330, respectivamente. 4.3. COINF/SSI - Atualização do Catálogo de Serviços e Catálogo de Soluções de TIC Além da configuração do arquivo com o Catálogo de Serviços, resta necessário o ajuste dos gestores técnicos questionados pelas unidades após a publicação da portaria da DG.	Todos os participantes
05	5. Coordenação do evento do teste em campo - COTEL Será realizada reunião entre a COINF e a COTEL na sexta-feira, 14.08.2020, para tratar especificamente sobre	Tyronne e Carlos Magno
06	6. Gestores dos sistemas Em virtude de questionamentos de diversas unidades, após a publicação da Portaria XX/2020-DG, restou verificada a necessidade de realização de nova reunião para fechamento - quarta 16h	Todos os participantes
07	7. Ofício-Circular nº 4 - DTI - CNJ - Acórdão 1613-2020- TCU que trata de uso de tecnologia de blockchain Osmar e Carlos Magno informaram que verificaram no acórdão e que não há necessidade de providências por parte de sua Coordenadorias em relação ao uso de tecnologia de blockchain.	Todos os participantes

V. Pendências Identificadas

Nº	Pendências	Responsável	Data limite
01	Apresentação da análise de risco relacionados à Segurança da Informação	Osmar	17.08.2020
02	Elaborar memorando sugerindo ajuste da norma, conforme estudo realizado por Sidnei Costa Souza, para revisão das faixas, inclusive no que diz respeito a uma faixa de riscos residuais não contemplada.	GAPSTIC	12.08.2020
03	Elaborar memorando encaminhando análises de riscos dos processos da STIC.	GAPSTIC	20.08.2020
04	Contactar a Diretoria-Geral sobre o uso da ferramenta do Whatsapp Business	Marcos	14.08.2020
05	Agendamento de reunião com a COSIS e COINF (coordenadores e chefes de seção) para tratar sobre o planejamento das contratações.	GAPSTIC	14.08.2020
06	Contato com Hermann sobre indicação de integrante administrativo para os planejamentos de contratação de TIC	GAPSTIC	14.08.2020

07	Envio de tabela resumo com as informações dos computadores das zonas eleitorais com as versões dos sistemas operacionais.	COINF	12.08.2020
08	Contactar a Diretoria Geral sobre as Mesas Receptoras de Justificativas	Marcos	14.08.2020

VI. Fechamento da Ata

Data	Nome do relator	Assinatura
10.08.2020	Dina Márcia Vasconcelos Maranhão da Câmara	DINA MARCIA DE VASCONCELOS MARANHAO DA CAMARA:20024230 Assinado de forma digital por DINA MARCIA DE VASCONCELOS MARANHAO DA CAMARA:20024230 Dados: 2020.08.17 20:35:56 -03'00'

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

ANEXO I

REUNIÃO N. 23/2020 - CGesTIC

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

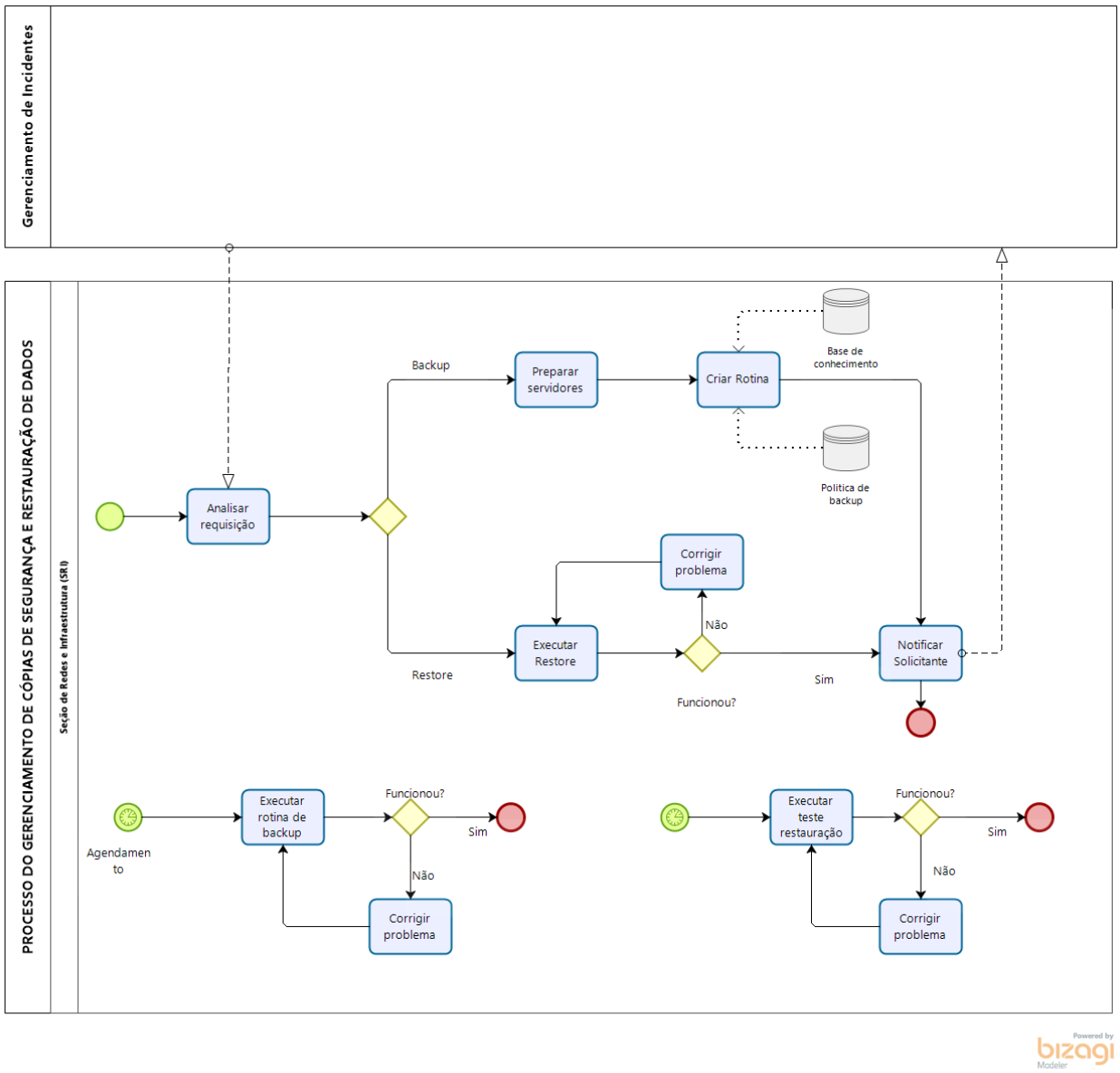
1.2. Objetivo

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
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ANEXO II

REUNIÃO N. 23/2020 - CGesTIC

Tribunal Regional Eleitoral
do Rio Grande do Norte

GESTÃO DE RISCOS

PROCESSO: 10.1.8 GERENCIAMENTO DE INCIDENTES DE TIC

Versão 1.0

NATAL, 10/08/2020

SUMÁRIO

APRESENTAÇÃO

O Gerenciamento de Incidentes, conforme descrito na ITIL, é o processo cujo propósito é restaurar a operação normal do serviço o mais rápido possível de modo a minimizar o impacto adverso nas operações de negócio, garantindo que os níveis acordados de qualidade do serviço sejam mantidos. A operação normal do serviço é definida como a operação de serviço dentro dos limites estabelecidos no ANS (Acordo de Nível de Serviço). Com isso, o gerenciamento de incidentes visa contribuir para melhorar a satisfação dos usuários com a qualidade dos serviços de TI.

Um incidente é qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado. Incidentes podem ser reportados à Central de Serviços pelos usuários, pelo próprio pessoal da TI ou, automaticamente, pelas ferramentas de monitoramento. Alguns exemplos de incidentes são: falta de acesso à Internet, problemas de hardware ou problemas de impressão. É importante diferenciar incidentes de requisições de serviços, já que ambos são reportados à Central de Serviços. Requisição de serviço é uma requisição formal de um usuário por algo a ser fornecido, por exemplo, uma requisição de informações ou aconselhamento, solicitações para redefinir uma senha ou para instalar uma estação de trabalho para um novo usuário. As requisições de serviço são gerenciadas pelo processo de cumprimento de requisição. Por fim, vale ressaltar que não faz parte do escopo do gerenciamento de incidentes investigar a causa raiz dos incidentes (isso faz parte do escopo do gerenciamento de problemas). O objetivo do gerenciamento de incidentes é restaurar a operação do serviço o mais rápido possível. Para tanto, deverá utilizar as soluções de contorno disponíveis na base de erros conhecidos.

Declaração de Apetite a Risco: Processo: Gestão de TIC: 10.1.8 Gerenciamento de Incidentes de TIC

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 cinco atores do "Processo: 10.1.8 Gerenciamento de Incidentes de TIC", restaram identificados, avaliados e tratados 26 (vinte e seis) riscos, vinculados às 26 (vinte e seis) atividades do referido processo. Todos os riscos identificados foram classificados como operacionais.

Ator do Processo	Quantidade de Atividades	Quantidade de Riscos Identificados	Nível de Risco Residual das Atividades (Média)(*)
Equipe de Serviço – 1º Nível de Atendimento (Central de Serviços)	16	15	7,73
Equipe de Serviço – 2º Nível de Atendimento	4	4	8
Equipe de Serviço – 3º Nível de Atendimento	4	4	8
Gerente de Incidentes	1	2	8
Equipe de Serviço – Incidente Grave	1	1	8
Total Geral / Média Geral	**26**	**26**	**7,94**

(*) cálculo baseado na soma dos níveis de riscos residuais dividindo-se pela quantidade de riscos de cada raia.

Majoritariamente, o Nível de Risco Residual das atividades do processo restou classificado como baixo conforme tabela anterior. Em termos da média das atividades verificou-se um resultado de 7,94 pontos, classificando o conjunto das atividades do processo com um nível baixo de riscos.

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**
10.1.8 Gerenciamento de Incidentes de TIC	Baixo (7,94 pontos)
Aprovação: Comitê Gestor de Riscos, em xx/11/2019	

2. Estabelecimento do Contexto

2.1 Identificação do Processo

Processo de Gestão de TIC: **10.1.8 Gerenciamento de Incidentes de TIC**

Responsável: Chefe da SSI - Denilson Bastos da Silva

Referências na Cadeia de Valor / Arquitetura de Processos:

III. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

2.2 Objetivos do processo

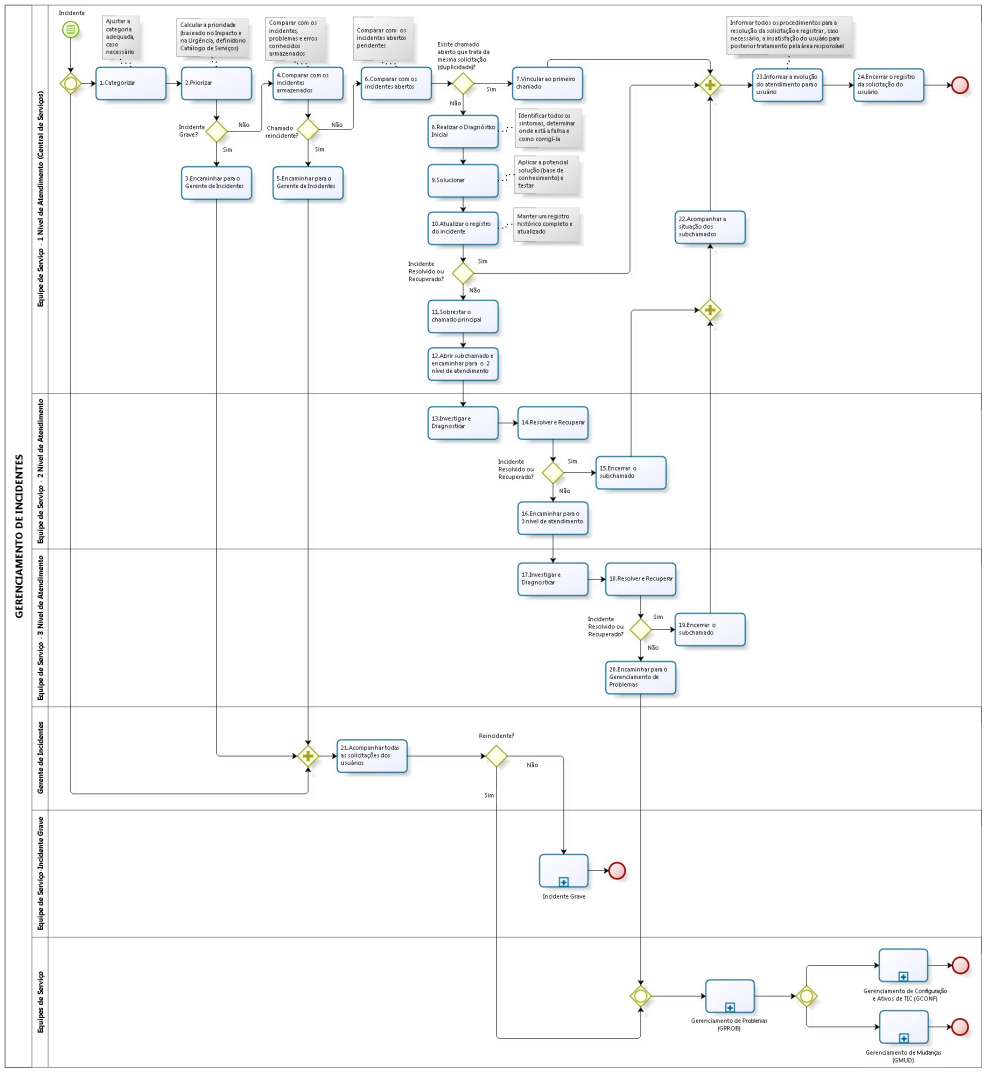
O processo de Gerenciamento de Incidentes de TIC na Justiça Eleitoral do Rio Grande do Norte foi incluído no Catálogo de Processos da STIC, através da ação/projeto de elaboração de proposta desse catálogo no Plano Diretor de Tecnologia da Informação e Comunicação de 2016/2017. Para subsidiar a confecção deste catálogo, foi considerada, inicialmente, a Cadeia de Valor do TRE-RN (instituída por meio da Portaria nº 250/2015 – GP), estando a Gestão de Tecnologia da Informação e Comunicação classificada como um Macroprocesso de Suporte.

O Gerenciamento de Incidente "foca na restauração de falhas de serviços, o mais rápido possível, para os usuários, de forma a minimizar o impacto no negócio, atividade que inclui a detecção e registro dos incidentes, classificação e suporte inicial, investigação e diagnóstico, resolução e recuperação, acompanhamento e monitoramento do atendimento de incidente até seu fechamento. O Incidente é qualquer evento que não é parte do serviço acordado, muitas vezes interrompendo, e ocasionalmente, reduzindo um serviço. Eles também incluem os eventos reportados pelos clientes (usuários de TIC), que sejam abertos via Central de Serviços de TIC ou de outra forma (telefone, sistema de bate-papo, email, etc)" (definição dada pela ITIL, versão 3).

A *Information Technology Infrastructure Library – ITIL* é um framework para as "melhores práticas" de Gerenciamento de Serviços de TIC. A ITIL oferece uma abordagem sistemática para a entrega de serviços de TIC com qualidade (definição dada pela ITIL, versão 3).

Serviço é definido como “um meio de entregar valor para o cliente através da facilitação de resultados que os clientes desejam obter sem incorrer em específicos custos ou riscos” (definição dada pela ITIL, versão 3).Conforme escopo estabelecido no mapeamento acima/abaixo identificado, o objetivo do presente processo é planejar e controlar, com base nas boas práticas preconizadas pela ITIL, as atividades que garantam o restabelecimento do serviço prestado pela área de TIC o mais rápido possível, minimizando o impacto negativo no funcionamento do negócio, no tempo e na forma definidos pelo respectivo Catálogo de Serviços de TIC.

A ilustração a seguir, destaca as etapas deste processo (Gerenciamento de Incidentes de TIC) que constituem o escopo deste trabalho, bem como as suas principais entregas (Termo de Referência ou Projeto Básico, Edital e Contrato ou Nota de Empenho), que proporcionam o resultado almejado, ou seja, o serviço regularmente prestado ou o material entregue em conformidade.



O mapeamento realizado detalha as atividades de cada unidade funcional que atua no processo, dentro de cada etapa do diagrama acima, de modo a permitir a identificação dos pontos frágeis que são passíveis de riscos, visando à aplicação do Processo de Gestão de Riscos.

Já numa análise dos fatores críticos para o sucesso deste processo, assim entendidos aqueles documentos (entregas) cuja qualidade interfere diretamente no sucesso da contratação/aquisição, ou seja, na obtenção do objeto correspondente a necessidade que iniciou o processo, identifica-se os seguintes fatores: (1) Estudos Técnicos Preliminares, (2) Termo de Referência ou Projeto Básico, (3) Edital e (4) a correta identificação da disponibilidade orçamentária.

ANÁLISE DO CONTEXTO
Quadro Resumo

Processo: Gerenciamento de Incidentes de TIC

- Objetivos e Metas:
- Está alinhada às necessidades de negócio e requisitos tecnológicos.
- Necessidade de alcance dos seguintes objetivos estratégicos, elencados no:
- Plano Estratégico da Justiça Eleitoral do RN 2016-2020 (PEJERN):
- Aprimorar a infraestrutura, a gestão e a governança de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 09 (nove).
- Plano Estratégico de Tecnologia da Informação e Comunicação 2016-2020 (PETIC):
- Prover soluções efetivas de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 02 (dois).
- Primar pela satisfação dos usuários de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 06 (seis).

Legislação e normas associadas:

- Constituição Federal (Art. 37, inciso XXI);
- Lei nº 8.666/1993 e alterações;
- Lei nº 10.520/2002 e alterações;
- Decreto nº 10.024, de 23 de setembro de 2019;
- Portaria Nº 220/2015-GP/TRE-RN;
- Revisão da Portaria Nº 220/2015-GP (Revisão da Portaria nº 220/2015-GP - PAE nº 3867/2019); e
- Portaria Nº 104/2014-GP.
- Instrução Normativa nº 04, de 12 de novembro de 2010 – SLTI – Nova Instrução Normativa para contratações de Soluções de Tecnologia da Informação e Manual de Contratação de Soluções de Tecnologia da Informação - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
- Acórdão 667/05 – TCU – Determinações quanto à insuficiência de servidores do quadro para execução dos serviços.

Sistemas utilizados:

- Processo Administrativo Eletrônico – PAE (TRE-RN);
- Sistema de Gerenciamento de Serviço de TI – GLPI

Partes interessadas:

- Internas (Seção de Suporte e Segurança da Informação e demais unidades do TRE-RN.

Matriz SWOT – Processo: **10.1.8. Gerenciamento de Incidentes de TIC**

FATORES INTERNOS

FORÇAS	FRAQUEZAS
Mapeamento dos incidentes	Técnicos terceirizados em pequena quantidade
Ferramenta de Gerenciamento de Serviço – GLPI	Muitos equipamentos com defeito

FATORES EXTERNOS

OPORTUNIDADES	AMEAÇAS
Padronização na aquisição de equipamentos de informática	Contingenciamento orçamentário.
Aumento do número de técnicos terceirizados para atendimento às demandas de chamados	
Contrato de manutenção dos equipamentos de informática	

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

O processo de Gerenciamento de Incidentes de TIC na Justiça Eleitoral do Rio Grande do Norte está ramificado num conjunto que vai desde o "Processo licitatório: fase interna", 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: Gerenciamento de Incidentes de TIC.					
Responsável:		Data: 31/10/2019.			
Papel(raias) **Responsabilidade (atividades)**	Equipe de Serviço - 1º Nível de Atendimento (Central de Serviços)	Equipe de Serviço - 2º Nível de Atendimento	Equipe de Serviço - 3º Nível de Atendimento	Equipe de Serviço - Gerente de Incidentes	Incidente Grave
1. Categorizar	R/I				
2. Priorizar	R/I				
3. Encaminhar para o Gerente de Incidentes	R/I/C			A/I	
4. Comparar com os incidentes armazenados	R/C				
5. Comparar com os incidentes abertos	R/C				
6. Vincular ao primeiro chamado	R/C/I	I	I	I	I
7. Realizar o diagnóstico inicial	R				
8. Solucionar	R				
9. Atualizar o registro do incidente	R/I				
10. Sobrestar o chamado principal	R/I				
11. Abrir subchamado e encaminhar para o 2º nível de atendimento	R/I	A			
12. Investigar e Diagnosticar		R/I		C	
13. Resolver e Recuperar		R/I			
14. Encerrar o subchamado		R/I			
15. Encaminhar para o 3º nível de atendimento		R/I	A		
16. Encaminhar para o Gerenciamento de Problema			R		
17. Acompanhar todas as solicitações dos usuários	I			R	
18. Informar a evolução do atendimento para o usuário	R				
19. Incidente Grave					R

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.1 – Equipe de Serviço – 1 Nível de Atendimento (Central de Serviços)

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

Responsável:	Aprovação:	Vigência:	Versão:
Chefia da SSI, Denilson Bastos da Silva	Comitê Gestor de Riscos, em xx/xx/2019	02 (dois) anos, a partir da data de aprovação	1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 04/12/2019 | Unidade: SSI | Gestor de Riscos: Unidade Demandante / Seção de Suporte e Segurança da Informação

Risco	Causa(s)	Classe(s)	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	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(1) Definição ou ajuste incorreto da categoria dos incidentes	(1) Falta de conhecimento sobre a distinção de cada categoria (2) Ausência de documentação de categorias (3) Falta de conhecimento sobre quais tipos de serviços existentes no Catálogo de Serviços (4) Falta de conhecimento sobre o tipo de item de configuração afetado no incidente (hardware / software) (5) Falta de atenção do operador	Operacional	Médio (6)	Média (6)	36	Alto	(1) Possível abertura do chamado com erro na categorização do incidente, gerando a necessidade de ajuste no chamado (2) Possível abertura de chamado com erro de tipos de serviços gerando a necessidade de ajuste no chamado (3) Possível abertura de chamado com erro sobre o tipo de item de configuração afetado no incidente hardware /software gerando a necessidade de ajuste no chamado	Mitigar/Eliminar o Risco	Baixo (4)	Baixa (4)	16	Médio	Não	SSI	Unidade Demandante / Chefia da SSI
(2) Priorização incorreta	(1) Ausência de matriz de impacto x urgência pré-definida no catálogo de serviços (2) Falta de conhecimento sobre o tipo de item de configuração afetado no incidente (hardware/soft	Operacional	Baixo (4)	Baixa (4)	16	Médio	(1) Possível abertura de chamado com erro ou ausência de priorização gerando a necessidade de ajuste no chamado (2) Possível abertura de chamado com erro sobre o tipo de item de configuração afetado no	Mitigar o Risco	Baixo (4)	Muito Baixa (2)	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	ware) (3) Ausência de tempo requerido para a resolução definido no catálogo de serviços (4) Falta de atenção do operador						incidente hardware / software								
(3) Não atendimento de incidente grave	(1) O incidente não foi identificado (classificado) como grave (mais alta prioridade) (2) O incidente grave não foi encaminhado para o Gerente de Incidentes (3) Não estava estabelecida uma equipe separada para lidar com incidentes graves (3) Gerente de Incidentes não tem o perfil adequado (4) O Gerente de Problemas não foi envolvido para auxiliar na resolução quando foi necessário (5) Gerente de Problemas não tem o perfil adequado (6) Não atualizar a equipe de serviço responsável pelo suporte de 1º nível de atendimento (Central de Serviços) através dos	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento ao chamado por erro na classificação “como grave” e, consequentemente, o não encaminhamento à equipe de incidentes graves (2) Falta de comunicação sobre o andamento do chamado entre equipe de suporte e usuários (feedback)	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	registros de todas as atividades de forma que os usuários também possam ser atualizados.														
(4) Aumento de tempo de atendimento	(1) Não é feita a comparação do incidente atual com os já encerrados (2) Não é feita consulta para identificar se o incidente atual está relacionado a um problema existente (3) Não é feita consulta para identificar se há uma solução de contorno conhecida (erros conhecidos) (4) Não registrar a informação sobre a existência de incidente já aberto (pendente) (5) Não informar ao usuário que a solicitação será atendida através do chamado aberto anteriormente e não encerrar o chamado (6) Não atualizar o registro no chamado atual informando sobre a abertura de novo chamado para a mesma	Operacional	Baixo (4)	Baixo (4)	16	Médio	(1) Demora no atendimento ao chamado por não ter sido realizada a comparação com os chamados já existentes e não ter sido realizada nenhuma solução de contorno para resolução do chamado com base nos registros da base de conhecimento. (2) Falha na atualização na base de conhecimento (3) Falta de comunicação sobre o andamento do chamado entre equipe de suporte e usuários (feedback)	Mitigar/Eliminar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	solicitação e, caso necessário, não acrescentar as informações adicionais e/ou relevantes descritas no novo chamado para o chamado aberto (pendente)														
(5) Atender ao mesmo incidente mais de uma vez	(1) Não é feita a comparação do incidente atual com os já abertos (pendentes) através de consulta aos dados armazenados na base de dados, de forma a verificar a existência de mesmo(s) sintoma(s) ou similar(es). (2) Não é feita a vinculação do incidente atual ao primeiro incidente aberto (pendente) (3) Não registrar a informação sobre a existência de incidente já aberto (pendente) (4) Não informar ao usuário que a solicitação será atendida através do chamado aberto anteriormente e não encerrar	Operacional	Baixo (4)	Baixa (4)	16	Médio	(1) Atendimento ao chamado em duplicidade, visto que, provavelmente, não foi realizada a consulta a base de conhecimento nos registros dos chamados já atendidos, estejam eles encerrados ou pendentes. falha na atualização dos registros na base de dados em relação a existência de mesmo(s) sintoma(s) ou similar(es) (2) Falha na consulta a base de dados em relação a existência de mesmo(s) sintoma(s) ou similar(es) (3) Falha em não registrar a informação de chamados já abertos e pendentes (4) Falha na comunicação sobre o andamento do chamado entre equipe de suporte e usuários (feedback)	Mitigar o Risco	Muito Baixo 2	Muito Baixo 2	4	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	o chamado atualizadas (5) Não atualizar o registro no chamado atual informando sobre a abertura de novo chamado para a mesma solicitação e, caso necessário, não acrescentar as informações adicionais e/ou relevantes descritas no novo chamado para o chamado aberto (pendente)														
(6) Incidente não ser solucionado	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise) (2) Não realizar consulta a Base de Conhecimento de TIC para determinar a causa provável do incidente	Operacional	Alto (8)	Baixa (4)	32	Alto	(1) Demora no atendimento ao chamado devido a não identificação da causa do defeito, gerando, provável, necessidade em se encaminhá-lo ao segundo nível. (2) Possível despreparo do operador (3) Retorno do usuário com feedback negativo	Mitigar/Eliminar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(7) Atender aos chamados abertos em duplicidade	(1) Não registrar informação de chamado já aberto (2) Não foi identificada se há informação adicional no chamado aberto anteriormente	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento por não ser verificado a base de chamados abertos. (2) Demora no atendimento ao chamado	Mitigar o Risco	Muito Baixo 2	Muito Baixo 2	4	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(8) Não identificar a possível solução do incidente	(1) Não identificar todos os	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento ao chamado por não	Mitigar o Risco	Muito Baixo 2	Muito Baixo 2	4	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	sintomas do incidente (2) Não determinar a causa provável do incidente, através de consulta à base de conhecimento (3) Não corrigir a falha do incidente						ter sido consultada a base de conhecimento ou tratar-se de situação (ocorrência) nova. (2) Falha na identificação dos sintomas do incidente (3) Demora no atendimento ao chamado (4) Falta de conhecimento do operador								
(9) Usuário não satisfeito	(1) Não aplicar a solução disponível, conforme procedimentos descritos na base de conhecimento e TIC (2) Não testar (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento ao chamado, ou a ineficácia da solução aplicada gerando, provavelmente, o registro da insatisfação do usuário. (2) Falha na identificação dos sintomas do incidente (3) Falha de atualização da base de conhecimento (4) Falta de conhecimento do operador	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(10) Manter histórico de incidentes atualizado	(1) Não manter o registro de histórico completo e atualizado de todas as etapas e ações efetuadas para resolução e recuperação das atividades	Operacional	Baixo (4)	Média (6)	24	Médio	(1) Impossibilidade de recuperar procedimentos de incidentes resolvidos e impossibilidade em se consultar e gerar relatórios para fins de estatísticos.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(11) Dar prosseguimento ao chamado principal	(1) Não sobrestar o chamado (principal) e acompanhá-lo até que seja solucionado pelas outras equipes de	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento ao chamado e, provável, registro de insatisfação pelo usuário.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	suporte														
(12) Dar seguimento ao chamado para o 2º nível	(1) Não abrir o subchamado (vinculado ao principal) e e não o encaminhar para o 2º nível de atendimento	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora no atendimento ao chamado e, provável, registro de insatisfação pelo usuário. (2) Perda de controle do chamado principal	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(22) Acompanhar a situação dos subchamados	(1) Não acompanhar a situação dos subchamados abertos	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Perda de controle do subchamado e chamado principal	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(23) Informar a evolução do atendimento para o usuário	(1) Não informar a evolução do atendimento para o usuário	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Insatisfação do usuário por falta de feedback	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(24) Encerrar o registro da solicitação do usuário	(1) Não encerrar o registro da solicitação do usuário	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Não encerramento do chamado	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.1. Categorizar [Unidade Demandante] (Risco 1)

10.1.8.2. Priorizar [Unidade Demandante] (Risco 2)

10.1.8.3. Encaminhar para o Gerente de Incidentes [Unidade Demandante] (Risco 3)

10.1.8.4. Comparar com os incidentes armazenados [Unidade Demandante] (Risco 4)

10.1.8.5. Comparar com os incidentes abertos [Unidade Demandante] (Risco 5)

10.1.8.6. Vincular ao primeiro chamado [Unidade Demandante] (Risco 6)

10.1.8.7. Realizar o diagnóstico inicial [Unidade Demandante] (Risco 7)

10.1.8.8. Solucionar [Unidade Demandante] (Risco 8)

10.1.8.9. Atualizar o registro do incidente [Unidade Demandante] (Risco 9)

10.1.8.10. Sobrestar o chamado principal [Unidade Demandante] (Risco 10)

10.1.8.11. Abrir subchamado e encaminhar para o 2º nível de atendimento [Unidade Demandante] (Risco 11)

10.1.8.12. Investigar e Diagnosticar [Unidade Demandante] (Risco 12)

10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)

10.1.8.23. Informar a evolução do atendimento ao usuário e encerrar o registro da solicitação do usuário [Unidade Demandante] (Risco 23 e Risco 24)

Anexo I.2 – Equipe de Serviço – 2 Nível de Atendimento

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Chefia da SSI, Denilson Bastos da Silva	Aprovação: Comitê Gestor de Riscos, em xx/xx/2019	Vigência: 02 (dois) anos, a partir da data de aprovação	Versão: 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 04/12/2019 | Unidade: SSI | Gestor de Riscos: Unidade Demandante / Seção de Suporte e Segurança da Informação

Risco	Causa(s)	Classe(s)	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	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(13) Investigar e Diagnosticar	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise); (2) Não determinar a causa provável do incidente; (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora na solução do chamado devido a não recuperação dos dados do incidente não resolvido. (2) Possível necessidade de encaminhamento do chamado ao nível presencial	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(14) Resolver e Recuperar	(1) Não aplicar a solução definitiva, e caso não seja possível, a solução de contorno ou redução da abrangência (2) Não atualizar o registro do incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Provável não resolução do chamado (2) Não recuperação dos dados do registro do incidente e consequente não recuperação das etapas e ações efetuadas para a resolução e recuperação das atividades.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	a resolução e recuperação das atividades.														
(15) Encerrar o Subchamado	(1) Não encerrar o subchamado	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Necessidade de ter que encerrar o subchamado para a finalização do chamado principal.???	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(16) Dar seguimento ao chamado para o 3º nível	(1) Não encaminhar o subchamado para o 3º nível de atendimento	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Provável sobrestamento do chamado no 2º nível. (2) Demora no atendimento do chamado.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.13. Resolver e Recuperar [Unidade Demandante] (Risco 13)

10.1.8.14. Encerrar o subchamado [Unidade Demandante] (Risco 14)

10.1.8.15. Encaminhar para o 3º nível de atendimento [Unidade Demandante] (Risco 15)

10.1.8.16. Encaminhar para o Gerenciamento de Problema [Unidade Demandante] (Risco 16)

Anexo I.3 – Equipe de Serviço – 3 Nível de Atendimento

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Chefe da SSI, Denilson Bastos da Silva	Aprovação: Comitê Gestor de Riscos, em xx/xx/2019	Vigência: 02 (dois) anos, a partir da data de aprovação	Versão: 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 04/12/2019 | Unidade: SSI | Gestor de Riscos: Unidade Demandante / Seção de Suporte e Segurança da Informação

Risco	Causa(s)	Classe(s)	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	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(17) Investigar e Diagnosticar	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise); (2) Não determinar a causa provável do incidente; (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora na solução do chamado (2) Possível necessidade de encaminhamento do chamado ao nível presencial	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(18) Resolver e Recuperar	(1) Não aplicar a solução definitiva, e caso não seja possível, a solução de contorno ou redução da abrangência (2) Não atualizar o registro do incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Provável não resolução do chamado (2) Não recuperação dos dados do registro do incidente e consequente não recuperação das etapas e ações efetuadas para a resolução e recuperação das atividades.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

	a resolução e recuperação das atividades.														
(19) Encerrar o subchamado	(1) Não encerrar o subchamado	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Necessidade de ter que encerrar o subchamado para a finalização do chamado principal.???	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI
(20) Encaminhar o subchamado para o gerente de problemas	(1) Não encaminhar o subchamado para o Gerente de Problemas	Operacional	Baixo (4)	Baixa (4)	16	Médio	(1) O chamado não vai chegar na equipe de incidentes graves.	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.17. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 17)

10.1.8.18. Informar a evolução do atendimento para o usuário [Unidade Demandante] (Risco 18)

10.1.8.19. Encerrar subchamado [Unidade Demandante] (Risco 19)

10.1.8.20. Encaminhar o subchamado para o Gerente de Problemas [Unidade Demandante] (Risco 20)

Anexo I.4 – Gerente de Incidentes

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Chefia da SSI, Denilson Bastos da Silva	Aprovação: Comitê Gestor de Riscos, em xx/xx/2019	Vigência: 02 (dois) anos, a partir da data de aprovação	Versão: 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 04/12/2019 | Unidade: SSI | Gestor de Riscos: Unidade Demandante / Seção de Suporte e Segurança da Informação

Risco	Causa(s)	Classe(s)	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	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(21) Acompanhar todas as solicitações dos usuários	(1) Não acompanhar a situação de todos as solicitações dos usuários que se encontram pendentes (subchamados abertos)	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Desconhecimento dos chamados pendentes, reincidentes e graves	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)

Anexo I.5 – Equipe de Serviço – Incidente Grave

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Identificação e Avaliação de Riscos			
Responsável: Chefia da SSI, Denilson Bastos da Silva	Aprovação: Comitê Gestor de Riscos, em xx/xx/2019	Vigência: 02 (dois) anos, a partir da data de aprovação	Versão: 1.0

Formulário Padrão de Identificação e Avaliação de Riscos

Data: 04/12/2019 | Unidade: SSI | Gestor de Riscos: Unidade Demandante / Seção de Suporte e Segurança da Informação

Risco	Causa(s)	Classe(s)	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	Probabilidade	Nível de Risco (IxP)				Impacto	Probabilidade	Nível de Risco (IxP)				
(25) Incidente grave	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise) (2) Não Determinar a causa provável do incidente; (3) Não Localizar uma solução definitiva, e caso não seja possível, uma solução de contorno.	Operacional	Médio (6)	Baixa (4)	24	Médio	(1) Demora na solução do chamado devido a não recuperação dos dados do incidente não resolvido. (2) Possível necessidade de encaminhamento do chamado ao nível presencial	Mitigar o Risco	Baixo 4	Muito Baixo 2	8	Baixo	Não	SSI	Unidade Demandante / Chefia da SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.25. Incidente grave [Unidade Demandante] (Risco 25)

Anexo II.1 – Equipe de Serviço – 1 Nível de Atendimento (Central de Serviços)

Tribunal Regional Eleitoral do Rio Grande do Norte
Formulário Padrão de Tratamento de Riscos

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(1) Definição ou ajuste incorreto da categoria dos incidentes.	
Probabilidade: Média (6)	**Impacto:** Muito Baixo (2)	**Nível do Risco:** Médio (12)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações inerentes ao chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas serão implantadas em 2020.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Baixa (4)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (4)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Unidade Demandante / Seção de Suporte e Segurança da Informação
Gestor de Risco Setorial

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(2) Priorização incorreta	
Probabilidade: Baixo (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações inerentes ao chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 2020.	
Planos de Contingência Recomendados:	Não foi identificada a necessidade de estabelecer um Plano de Contingência.	
Probabilidade Risco Residual: Baixa (2)	**Impacto Risco Residual:** Baixo (4)	**Nível de Risco Residual:** Baixo (8)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Unidade Demandante / Seção de Suporte e Segurança da Informação
Gestor de Risco Setorial

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(3) Não atendimento de incidente grave	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações inerentes ao chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s)	Não foram identificados.	

(geradas pelas respostas adotadas):		

Unidade Demandante / Seção de Suporte e Segurança da Informação
Gestor de Risco Setorial

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(4) Aumento de tempo de atendimento	
Probabilidade: Baixo (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Checar se todos os sintomas foram identificados e se a solução foi aplicada. (3) Acompanhar o andamento do chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Unidade Demandante / Seção de Suporte e Segurança da Informação
Gestor de Risco Setorial

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(5) Atender ao mesmo incidente mais de uma vez	
Probabilidade: Baixo (4)	**Impacto:** Baixo (4)	**Nível do Risco:** Médio (16)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consulta aos registros de chamados abertos e/ou fechados.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(6) Incidente não ser solucionado	
Probabilidade: Baixo (4)	**Impacto:** Alto (8)	**Nível do Risco: Alto** (32)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Verificar se todos os sintomas do incidente foram identificados e se foi consultada a base de conhecimento.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(7) Atender aos chamados abertos em duplicidade	

Probabilidade: Baixo (4)	**Impacto:** Alto (8)	**Nível do Risco:** Alto (32)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consultar os registros de chamados já abertos.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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:** Muito Baixo (4)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(8) Não identificar a possível solução do incidente	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consultar a base de conhecimento para tentar identificar os sintomas. (3) Consultar supervisor dos técnicos, buscando dicas para solucionar o incidente.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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:** Muito Baixo (4)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(9) Usuário não satisfeito	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Consultar o chamado (2) Consultar o histórico do chamado e verificar os procedimentos realizados (2) Abrir um novo chamado, caso necessário.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(10) Não Manter histórico de incidentes atualizado	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(11) Dar prosseguimento ao chamado principal	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado. (3)	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(12) Dar seguimento ao chamado para o 2º nível	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(22) Acompanhar a situação dos subchamados	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(23) Informar a evolução do atendimento para o usuário	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)

Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	
Formulário Padrão de Tratamento de Riscos		
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação
Risco: Operacional	(24) Encerrar o registro da solicitação do usuário	
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;	
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.1. Categorizar [Unidade Demandante] (Risco 1)
10.1.8.2. Priorizar [Unidade Demandante] (Risco 2)
10.1.8.3. Encaminhar para o Gerente de Incidentes [Unidade Demandante] (Risco 3)
10.1.8.4. Comparar com os incidentes armazenados [Unidade Demandante] (Risco 4)
10.1.8.5. Comparar com os incidentes abertos [Unidade Demandante] (Risco 5)
10.1.8.6. Vincular ao primeiro chamado [Unidade Demandante] (Risco 6)
10.1.8.7. Realizar o diagnóstico inicial [Unidade Demandante] (Risco 7)
10.1.8.8. Solucionar [Unidade Demandante] (Risco 8)
10.1.8.9. Atualizar o registro do incidente [Unidade Demandante] (Risco 9)
10.1.8.10. Sobrestar o chamado principal [Unidade Demandante] (Risco 10)
10.1.8.11. Abrir subchamado e encaminhar para o 2º nível de atendimento [Unidade Demandante] (Risco 11)
10.1.8.12. Investigar e Diagnosticar [Unidade Demandante] (Risco 12)
10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)
10.1.8.23. Informar a evolução do atendimento ao usuário e encerrar o registro da solicitação do usuário [Unidade Demandante] (Risco 23 e Risco 24)

Anexo II.2 – Equipe de Serviço – 2 Nível de Atendimento

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(13) Investigar e Diagnosticar		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(14) Resolver e Recuperar		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(15) Encerrar o Subchamado		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(16) Dar seguimento ao chamado para o 3º nível		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		

Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.13. Resolver e Recuperar [Unidade Demandante] (Risco 13)

10.1.8.14. Encerrar o subchamado [Unidade Demandante] (Risco 14)

10.1.8.15. Encaminhar para o 3º nível de atendimento [Unidade Demandante] (Risco 15)

10.1.8.16. Encaminhar para o Gerenciamento de Problema [Unidade Demandante] (Risco 16)

Anexo II.3 – Equipe de Serviço – 3 Nível de Atendimento

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(17) Investigar e Diagnosticar		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(18) Resolver e Recuperar		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(19) Encerrar o subchamado		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(20) Encaminhar o subchamado para o gerente de problemas		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		

Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.	

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.17. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 17)

10.1.8.18. Informar a evolução do atendimento para o usuário [Unidade Demandante] (Risco 18)

10.1.8.19. Encerrar subchamado [Unidade Demandante] (Risco 19)

10.1.8.20. Encaminhar o subchamado para o Gerente de Problemas [Unidade Demandante] (Risco 20)

Anexo II.4 – Gerente de Incidentes

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(21) Acompanhar todas as solicitações dos usuários		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) (geradas pelas respostas adotadas):	Não foram identificados.		

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)

Anexo II.5 – Equipe de Serviço – Incidente Grave

Tribunal Regional Eleitoral do Rio Grande do Norte Formulário Padrão de Tratamento de Riscos			
Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão:** 1.0
Formulário Padrão de Tratamento de Riscos			
Data: 04/12/2019	**Área Funcional:** SSI	**Proprietário do Risco:** Unidade Demandante / Seção de Suporte e Segurança da Informação	
Risco: Operacional	(25) Incidente grave		
Probabilidade: Baixo (4)	**Impacto:** Médio (6)	**Nível do Risco:** Médio (24)	
Resposta a ser implantada:	(1) Necessidade de um treinamento da ferramenta GLPI;		
Tipo de Resposta: Mitigar o risco	**Prazo para implantação:** As respostas (4) serão implantadas em 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)	
Risco(s) Secundário(s) **(geradas pelas respostas adotadas):**	Não foram identificados.		

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.25. Incidente grave [Unidade Demandante] (Risco 25)

Anexo III.1 – Equipe de Serviço – 1 Nível de Atendimento (Central de Serviços)

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

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

Formulário Perfil de Riscos

Gestor de Risco Setorial: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva | **Área Funcional:** SSI | **Data:** 13/11/2019

Risco (Descrição)	Classe(s)	Causa(s)	Consequências	Resposta(s)	Nível de Riscos (IxP)		Tipos de Resposta(s)	Proprietário do Risco
(1) Definição ou ajuste incorreto da categoria dos incidentes.	Risco Operacional	(1) Falta de conhecimento sobre a distinção de cada categoria (2) Ausência de documentação de categorias (3) Falta de conhecimento sobre quais tipos de serviços existentes no Catálogo de Serviços (4) Falta de conhecimento sobre o tipo de item de configuração afetado no incidente (hardware / software) (5) Falta de atenção do operador	(1) Possível abertura do chamado com erro na categorização do incidente, gerando a necessidade de ajuste no chamado (2) Possível abertura de chamado com erro de tipos de serviços gerando a necessidade de ajuste no chamado (3) Possível abertura de chamado com erro sobre o tipo de item de configuração afetado no incidente hardware /software gerando a necessidade de ajuste no chamado	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações inerentes ao chamado.	Nível de Risco Inerente = 6 x 6 = 36 (Alto))	Nível de Risco Residual = 4 x 4 = 16 (Médio)	Mitigar o risco	Unidade Demandante / SSI
(2) Priorização incorreta	Risco Operacional	(1) Ausência de matriz de impacto x urgência pré-definida no catálogo de serviços (2) Falta de conhecimento sobre o tipo de item de configuração afetado no incidente (hardware/software) (3) Ausência de tempo requerido para a resolução definido no catálogo de serviços (4) Falta de atenção do operador	(1) Possível abertura de chamado com erro ou ausência de priorização gerando a necessidade de ajuste no chamado (2) Possível abertura de chamado com erro sobre o tipo de item de configuração afetado no incidente hardware / software	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações inerentes ao chamado.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(3) Não atendimento de incidente grave	Risco Operacional	(1) O incidente não foi identificado (classificado) como Grave (mais alta	(1) Possível abertura de chamado com erro ou ausência de priorização gerando a necessidade	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Em caso de dúvida sobre o preenchimento das informações do chamado realizar consulta ao manual ou ao supervisor imediato; (3) Criar um *checklist* para preenchimento das informações	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

		prioridade) (2) O incidente grave não foi encaminhado para o Gerente de Incidentes (3) Não estava estabelecida uma equipe separada para lidar com incidentes graves (3) Gerente de Incidentes não tem o perfil adequado (4) O Gerente de Problemas não foi envolvido para auxiliar na resolução quando foi necessário (5) Gerente de Problemas não tem o perfil adequado (6) Não atualizar a equipe de serviço responsável pelo suporte de 1º nível de atendimento (Central de Serviços) através dos registros de todas as atividades de forma que os usuários também possam ser atualizados.	de ajuste no chamado (2) Possível abertura de chamado com erro sobre o tipo de item de configuração afetado no incidente hardware / software	inerentes ao chamado.				
(4) Aumento do tempo de atendimento	Risco Operacional	(1) Não é feita a comparação do incidente atual com os já encerrados (2) Não é feita consulta para identificar se o incidente atual está relacionado a um problema existente (3) Não é feita consulta para identificar se há uma solução de contorno conhecida (erros conhecidos) (4) Não registrar a informação sobre a existência de incidente já aberto (pendente) (5) Não informar ao usuário que a solicitação será	(1) Possível demora no atendimento ao chamado por não ter sido realizada a comparação com os chamados já existentes e não ter sido realizada nenhuma solução de contorno para resolução do chamado com base nos registros da base de conhecimento. (2) Possível falha na atualização na base de conhecimento (3) Falta de comunicação sobre o andamento do chamado entre equipe de suporte e usuários (feedback)	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Checar se todos os sintomas foram identificados e se a solução foi aplicada. (3) Acompanhar o andamento do chamado.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

		atendida através do chamado aberto anteriormente e não encerrar o chamado. (6) Não atualizar o registro no chamado atual informando sobre a abertura de novo chamado para a mesma solicitação e, caso necessário, não acrescentar as informações adicionais e/ou relevantes descritas no novo chamado para o chamado aberto (pendente)						
(5) Atender ao mesmo incidente mais de uma vez	Risco Operacional	(1) Não é feita a comparação do incidente atual com os já abertos (pendentes) através de consulta aos dados armazenados na base de dados, de forma a verificar a existência de mesmo(s) sintoma(s) ou similar(es). (2) Não é feita a vinculação do incidente atual ao primeiro incidente aberto (pendente) (3) Não registrar a informação sobre a existência de incidente já aberto (pendente) (4) Não informar ao usuário que a solicitação será atendida através do chamado aberto anteriormente e não encerrar o chamado atualizadas. (5) Não atualizar o registro no chamado atual informando sobre a abertura de novo chamado para a mesma solicitação e, caso necessário, não acrescentar as informações adicionais e/ou relevantes descritas	(1) Possível atendimento ao chamado em duplicidade, visto que, provavelmente, não foi realizada a consulta a base de conhecimento nos registros dos chamados já atendidos, estejam eles encerrados ou pendentes. falha na atualização dos registros na base de dados em relação a existência de mesmo(s) sintoma(s) ou similar(es) (2) Possível falha na consulta a base de dados em relação a existência de mesmo(s) sintoma(s) ou similar(es) (3) Possível falha em não registrar a informação de chamados já abertos e pendentes (4) Possível falha na comunicação sobre o andamento do chamado entre equipe de suporte e usuários (feedback)	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consulta aos registros de chamados abertos e/ou fechados.	Nível de Risco Inerente = 4 x 4 = 16 (Médio)	Nível de Risco Residual = 2 x 2 = 4 (Muito Baixo)	Mitigar o risco	Unidade Demandante / SSI

		no novo chamado para o chamado aberto (pendente)						
(6) Incidente não ser solucionado	Risco Operacional	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise) (2) Não realizar consulta a Base de Conhecimento de TIC para determinar a causa provável do incidente	(1) Possível demora no atendimento ao chamado devido a não identificação da causa do defeito, gerando, provável, necessidade em se encaminhá-lo ao segundo nível. (2) Possível despreparo do operador (3) Possível retorno do usuário com feedback negativo	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Verificar se todos os sintomas do incidente foram identificados e se foi consultada a base de conhecimento. (3) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 8 x 4 = 32 (Alto)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(7) Atender aos chamados abertos em duplicidade	Risco Operacional	(1) Não registrar informação de chamado já aberto. (2) Não foi identificada se há informação adicional no chamado aberto anteriormente	(1) Possível demora no atendimento por não ser verificado a base de chamados abertos. (2) Possível demora no atendimento ao chamado	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consultar os registros de chamados já abertos. (3) Acompanhar o andamento do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 2 x 2 = 4 (Muito Baixo)	Mitigar o risco	Unidade Demandante / SSI
(8) Não identificar a possível solução do incidente	Risco Operacional	Não identificar todos os sintomas do incidente Não determinar a causa provável do incidente, através de consulta à base de conhecimento Não corrigir a falha do incidente	(1) Possível demora no atendimento ao chamado por não ter sido consultada a base de conhecimento ou tratar-se de situação (ocorrência) nova. (2) Possível falha na identificação dos sintomas do incidente (3) Possível demora no atendimento ao chamado (4) Possível falta de conhecimento do operador	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Consultar a base de conhecimento para tentar identificar os sintomas. (3) Consultar supervisor dos técnicos, buscando dicas para solucionar o incidente.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 2 x 2 = 4 (Muito Baixo)	Mitigar o risco	Unidade Demandante / SSI
(9) Usuário não satisfeito	Risco Operacional	(1) Não aplicar a solução disponível, conforme procedimentos descritos na base de conhecimento e TIC (2) Não testar (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	(1) Possível demora no atendimento ao chamado, ou a ineficácia da solução aplicada gerando, provavelmente, o registro da insatisfação do usuário. (2) Possível falha na identificação dos sintomas do incidente (3) Possível falha de atualização da base de conhecimento	(1) Consultar o chamado (2) Consultar o histórico do chamado e verificar os procedimentos realizados (2) Abrir um novo chamado, caso necessário.	Nível de Risco Inerente = 6 x 4 = 24 (M4édia)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

			(4) Possível falta de conhecimento do operador					
(10) Manter histórico de incidentes atualizado	Risco Operacional	(1) Não manter o registro de histórico completo e atualizado de todas as etapas e ações efetuadas para resolução e recuperação das atividades	(1) Possível impossibilidade de recuperar procedimentos de incidentes resolvidos e impossibilidade em se consultar e gerar relatórios para fins de estatísticos.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 4 x 6 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(11) Dar prosseguimento ao chamado principal	Risco Operacional	(1) Não sobrestar o chamado (principal) e acompanhá-lo até que seja solucionado pelas outras equipes de suporte	(1) Possível demora no atendimento ao chamado e, provável, registro de insatisfação pelo usuário.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(12) Dar seguimento ao chamado para o 2º nível	Risco Operacional	(1) Não abrir o subchamado (vinculado ao principal) e encaminhá-lo para o 2º nível de atendimento	(1) Possível demora no atendimento ao chamado e, provável, registro de insatisfação pelo usuário. (2) Possível perda de controle do andamento sobre o chamado principal.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(22) Acompanhar a situação dos subchamado	Risco Operacional	(1) Não acompanhar a situação dos subchamados abertos	(1) Possível perda de controle do subchamado e chamado principal	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 16 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(23) Informar a evolução do atendimento para o usuário	Risco Operacional	(1) Não informar a evolução do atendimento para o usuário (2) Não informar a evolução do atendimento para o usuário, esclarecendo todos os procedimentos adotados para a sua resolução ou recuperação, registrando, caso necessário, o nível de satisfação relativo ao atendimento, para posterior tratamento pela unidade responsável	(1) Possível insatisfação do usuário por falta de feedback	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 16 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

(24) Encerrar o registro da solicitação do usuário	Risco Operacional	(1) Não informar a evolução do atendimento para o usuário (2) Não atualizar o registro de incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para a resolução e recuperação	(1) Possível não encerramento do chamado	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 16 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.1. Categorizar [Unidade Demandante] (Risco 1)
10.1.8.2. Priorizar [Unidade Demandante] (Risco 2)
10.1.8.3. Encaminhar para o Gerente de Incidentes [Unidade Demandante] (Risco 3)
10.1.8.4. Comparar com os incidentes armazenados [Unidade Demandante] (Risco 4)
10.1.8.5. Comparar com os incidentes abertos [Unidade Demandante] (Risco 5)
10.1.8.6. Vincular ao primeiro chamado [Unidade Demandante] (Risco 6)
10.1.8.7. Realizar o diagnóstico inicial [Unidade Demandante] (Risco 7)
10.1.8.8. Solucionar [Unidade Demandante] (Risco 8)
10.1.8.9. Atualizar o registro do incidente [Unidade Demandante] (Risco 9)
10.1.8.10. Sobrestar o chamado principal [Unidade Demandante] (Risco 10)
10.1.8.11. Abrir subchamado e encaminhar para o 2º nível de atendimento [Unidade Demandante] (Risco 11)
10.1.8.12. Investigar e Diagnosticar [Unidade Demandante] (Risco 12)
10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)
10.1.8.23. Informar a evolução do atendimento ao usuário e encerrar o registro da solicitação do usuário [Unidade Demandante] (Risco 23 e Risco 24)

Anexo III.2 – Formulário Perfil de Riscos

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

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

(13) Investigar e Diagnosticar	Risco Operacional	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise); (2) Não determinar a causa provável do incidente; (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	(1) Possível demora na solução do chamado devido a não recuperação dos dados do incidente não resolvido. (2) Possível necessidade de encaminhamento do chamado ao nível presencial	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(14) Resolver e Recuperar	Risco Operacional	(1) Não aplicar a solução definitiva, e caso não seja possível, a solução de contorno ou redução da abrangência (2) Não atualizar o registro do incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para a resolução e recuperação das atividades.	(1) Provável não resolução do chamado (2) Provável não recuperação dos dados do registro do incidente e consequente não recuperação das etapas e ações efetuadas para a resolução e recuperação das atividades.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(15) Encerrar o Subchamado	Risco Operacional	(1) Não encerrar o subchamado	(1) Necessidade de ter que encerrar o subchamado para a finalização do chamado principal	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(16) Dar seguimento ao chamado para o 3º nível	Risco Operacional	(1) Não encaminhar o subchamado para o 3º nível de atendimento	(1) Provável sobrestamento do chamado no 2º nível. (2) Possível demora no atendimento do chamado.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

Referências na Cadeia de Valor / Arquitetura de Processos (Atividades):
10. Macroprocesso: Suporte
10. Processo: Gestão de Tecnologia da Informação e Comunicação (GTIC)
10.1. Subprocesso: Gerenciamento de Serviços de TIC
10.1.8. Gerenciamento de Incidentes de TIC
10.1.8.13. Resolver e Recuperar [Unidade Demandante] (Risco 13)
10.1.8.14. Encerrar o subchamado [Unidade Demandante] (Risco 14)
10.1.8.15. Encaminhar para o 3º nível de atendimento [Unidade Demandante] (Risco 15)
10.1.8.16. Encaminhar para o Gerenciamento de Problema [Unidade Demandante] (Risco 16)

Anexo III.3 – Equipe de Serviço – 3 Nível de Atendimento

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

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

Formulário Perfil de Riscos

Gestor de Risco Setorial: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva | **Área Funcional:** SSI | **Data:** 13/11/2019

Risco (Descrição)	Classe(s)	Causa(s)	Consequências	Resposta(s)	Nível de Riscos (IxP)		Tipos de Resposta(s)	Proprietário do Risco
(17) Investigar e Diagnosticar	Risco Operacional	(1) Não Identificar todos os sintomas, avaliando os detalhes do incidente (análise); (2) Não determinar a causa provável do incidente; (3) Não localizar uma solução definitiva, e caso não seja possível, uma solução de contorno	(1) Possível demora na solução do chamado (2) Possível necessidade de encaminhamento do chamado ao nível presencial	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(18) Resolver e Recuperar	Risco Operacional	(1) Não aplicar a solução definitiva, e caso não seja possível, a solução de contorno ou redução da abrangência (2) Não atualizar o registro do incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para a resolução e recuperação das atividades.	(1) Provável não resolução do chamado (2) Provável não recuperação dos dados do registro do incidente e consequente não recuperação das etapas e ações efetuadas para a resolução e recuperação das atividades.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(19) Encerrar o subchamado	Risco Operacional	(1) Não encerrar o subchamado	(1) Necessidade de ter que encerrar o subchamado para a finalização do chamado principal.???	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI
(20) Encaminhar o subchamado para o gerente de problemas	Risco Operacional	(1) Não encaminhar o subchamado para o Gerente de Problemas	(1) O chamado não vai chegar na equipe de incidentes graves.	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 4 x 4 = 16 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

Referências na Cadeia de Valor / Arquitetura de Processos (Atividades):
10. Macroprocesso: Suporte
10. Processo: Gestão de Tecnologia da Informação e Comunicação (GTIC)
10.1. Subprocesso: Gerenciamento de Serviços de TIC
10.1.8. Gerenciamento de Incidentes de TIC
10.1.8.17. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 17)
10.1.8.18. Informar a evolução do atendimento para o usuário [Unidade Demandante] (Risco 18)
10.1.8.19. Encerrar subchamado [Unidade Demandante] (Risco 19)
10.1.8.20. Encaminhar o subchamado para o Gerente de Problemas [Unidade Demandante] (Risco 20)

Anexo III.4 – Gerente de Incidentes

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

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

Formulário Perfil de Riscos

Gestor de Risco Setorial: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Área Funcional:** SSI	**Data:** 13/11/2019

Risco (Descrição)	Classe(s)	Causa(s)	Consequências	Resposta(s)	Nível de Riscos (IxP)		Tipos de Resposta(s)	Proprietário do Risco
(21) Acompanhar todas as solicitações dos usuários	Risco Operacional	(1) Não acompanhar a situação de todos as solicitações dos usuários que se encontram pendentes (subchamados abertos)	(1) Possível desconhecimento dos chamados pendentes, reincidentes e graves	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um *checklist* que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 24 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.21. Acompanhar todas as solicitações dos usuários [Unidade Demandante] (Risco 21 e Risco 22)

Anexo III.5 – Equipe de Serviço – Incidente Grave

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

Responsável: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva	**Aprovação:** Comitê Gestor de Riscos, em xx/xx/2019.	**Vigência:** 02 (dois) anos, a partir da data de aprovação.	**Versão: 1.0**

Formulário Perfil de Riscos

Gestor de Risco Setorial: Chefe da Seção de Segurança da Informação - Denilson Bastos da Silva | **Área Funcional:** SSI | **Data:** 13/11/2019

Risco (Descrição)	Classe(s)	Causa(s)	Consequências	Resposta(s)	Nível de Riscos (IxP)		Tipos de Resposta(s)	Proprietário do Risco
(25) Incidente grave	Risco Operacional	(1) Não informar a evolução do atendimento para o usuário (2) Não atualizar o registro de incidente, mantendo histórico completo e atualizado de todas as etapas e ações efetuadas para a resolução e recuperação	(1) Possível demora na solução do chamado devido a não recuperação dos dados do incidente não resolvido. (2) Possível necessidade de encaminhamento do chamado ao nível presencial	(1) Necessidade de um treinamento da ferramenta GLPI; (2) Criar um checklist que acompanhe as fases do chamado.	Nível de Risco Inerente = 6 x 4 = 16 (Média)	Nível de Risco Residual = 4 x 2 = 8 (Baixo)	Mitigar o risco	Unidade Demandante / SSI

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

10. Macroprocesso: Suporte

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

10.1. Subprocesso: Gerenciamento de Serviços de TIC

10.1.8. Gerenciamento de Incidentes de TIC

10.1.8.25. Incidente grave [Unidade Demandante] (Risco 25)