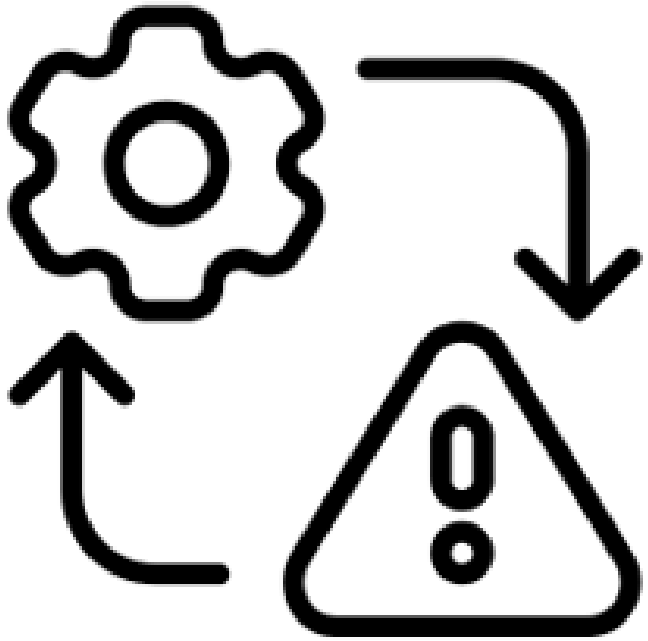
MATRIZ DE RISCOS DE TIC



TRE-GO

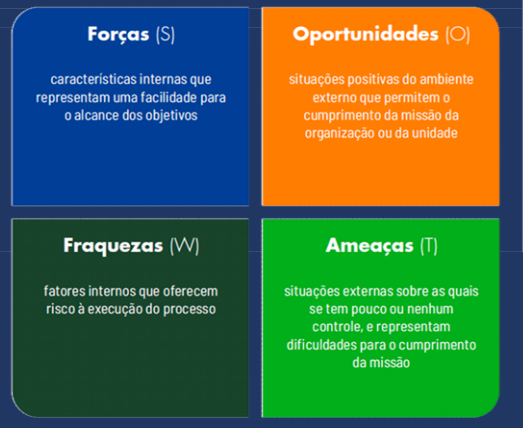
ESCOPO DA GESTÃO DE RISCOS

GRUPO

Equipe	Gestor de Risco (representante do grupo)
	1. Augusto César de Castro Ovelar
	2. Dory Gonzaga Rodrigues
	3. Frank Wendell Ribeiro
	4. Marcilio Zaccarelli Bersaneti
	5. Paulo Sérgio Taira
Serviços essenciais de TIC	Cadastro de eleitores (ELO)
	PJE
	DJE
	SEI
	Links/Redes de comunicação de dados
	Bancos de Dados
	Sistemas Eleitorais
	Sítio de Internet
	Correio eletrônico
	Manutenção e distribuição das urnas eletrônicas
Objetivos	Em um ambiente onde a dependência da tecnologia é cada vez maior, os serviços essenciais de TIC visam atender com eficiência e celeridade, aos processos finalísticos do TRE-GO definidos na sua cadeia de valor: Cadastro Eleitoral, Prestação Jurisdicional e Eleições.
Descrição dos Serviços	O Cadastro de Eleitores (ELO) gerencia o registro e atualização dos dados dos eleitores. O Processo Judicial Eletrônico (PJE) digitaliza a tramitação de processos judiciais, enquanto o Diário da Justiça Eletrônico (DJE) publica oficialmente atos judiciais e administrativos, garantindo transparência. O Sistema Eletrônico de Informações (SEI) facilita a gestão documental e a tramitação de processos administrativos. Links e Redes de Comunicação interconectam sistemas e unidades, permitindo a troca segura de informações. Bancos de Dados armazenam e gerenciam informações críticas para suporte às operações e decisões. Os Sistemas Eleitorais suportam o processo eleitoral, desde a votação até a apuração de resultados. O Sítio de Internet serve como um portal de comunicação pública e serviços online. O Correio Eletrônico é fundamental para a comunicação interna e externa. A manutenção e distribuição das urnas eletrônicas asseguram que estejam prontas e funcionais para as eleições, garantindo a integridade do processo de votação.

SWOT

FORÇAS	OPORTUNIDADES
Alta qualificação técnica dos servidores	Adoção de novas tecnologias para melhorar a eficiência e a segurança dos serviços disponibilizados
Compromisso da gestão com a Missão do TRE-GO	Parcerias com outras instituições para compartilhar conhecimentos e recursos.
	Capacitação e Treinamento: Oportunidades para aprimorar as habilidades técnicas dos servidores.
FRAQUEZAS	**AMEAÇAS**
Falta de pessoal	Ameaças crescentes de ataques cibernéticos visando sistemas críticos e dados sensíveis.
Gestão de processos com necessidade de melhoria	Novas leis ou regulamentos que possam exigir grandes mudanças nos sistemas atuais.
Dificuldade em executar o orçamento	Limitações financeiras que podem restringir investimentos em novas tecnologias.
	Dificuldade em manter profissionais qualificados devido à competição com o setor privado.



GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de Informação	**Cadastro eleitoral (ELO)**	Data da Avalilação:	19/04/2024
Responsável pela avaliação:	**CTGTI**	Versão:	1.0
Objetivo do Processo, Projeto ou Ativo:	**Gerenciar a base de dados de eleitores do TRE-GO**	Data da Revisão:	26/06/2024
		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Externo	Indisponibilidade do sistema ELO	- Bugs ou vulnerabilidades no sistema; - Falhas nos servidores ou no banco de dados; - Data Center indisponível (TSE e TRE); - Falha no funcionamento dos equipametos da rede local (TRE e ZEs); - Falha no link de comunicação de dados com o TSE; - Falha no link de comunicação de dados com as ZEs; - Queda de energia elétrica.	- Interrupção no atendimento ao eleitor; - Perda de dados; - Atrasos na atualização dos dados dos eleitores.	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações contínuas de software e hardware - Monitoramento dos links de comunicação de dados das Zonas Eleitorais - Monitoramento do data center - Reportar os bugs para o TSE	Forte	4,8 - Baixo	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema; - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética; - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados sensíveis dos eleitores, comprometendo sua privacidade; - Interrupção no atendimento ao eleitor; - Alteração ou exclusão de registros eleitorais, impactando na integridade do cadastro eleitoral; - Prejuízo à imagem da Justiça Eleitoral.	INTEGRIDADE:	Média - 6	Extremo - 10	60 - Extremo	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas. - Desenvolvimento de planos de contingência e recuperação. - Monitoramento de vulnerabilidade - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	36 - Alto	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilzação e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de Informação	**Processo Judicial Eletrônico (PJE)**	Data da Avalilação:	19/04/2024
Responsável pela avaliação:	**CTGTI**	Versão:	1.0
Objetivo do Processo, Projeto ou Ativo:	**Permite que magistrados, servidores e advogados pratiquem atos processuais diretamente no sistema**	Data da Revisão:	26/06/2024
		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Externo	Indisponibilidade do sistema PJE	- Bugs ou vulnerabilidades no sistema; - Falhas nos servidores ou no banco de dados do TSE; - Data Center do TSE indisponível; - Falha no funcionamento dos equipametos da rede local (TRE e ZEs) - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Interrupção na tramitação eletrônica de processos judiciais; - Prorrogação de prazos e atrasos nas decisões judiciais; - Dificuldades das partes interessadas para acessar as informações sobre seus processos; - Prejuízos à transparência e a publicidade dos atos judiciais; - Perda de informações dos processos judiciais; - Comprometimento da imagem do poder judiciário perante à sociedade; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações contínuas de software e hardware - Monitoramento dos links de comunicação de dados das Zonas Eleitorais - Monitoramento do data center - Monitoramento da disponibilidade do sistema - Reportar os bugs para o TSE	Satisfatório	9,6 - Médio	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema. - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados pessoais dos usuários, comprometendo sua privacidade; - Alteração indevida nas informações contidas das peças processuais; - Interrupção na tramitação eletrônica de processos judiciais; - Prorrogação de prazos e atrasos nas decisões judiciais; - Dificuldades das partes interessadas para acessar as informações sobre seus processos; - Prejuízos à transparência e a publicidade dos atos judiciais; - Perda de informações dos processos judiciais; - Prejuízo à imagem da Justiça Eleitoral.	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas; - Desenvolvimento de planos de contingência e recuperação; - Monitoramento de vulnerabilidades; - Antivírus atualizado; - Controle de permissões de usuários; - Troca de senhas periódicas, conforme requisitos estabelecidos.	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilzação e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de Informação	**Diário da Justiça Eletrônico (PJE)**	Data da Avalilação:	19/04/2022
Responsável pela avaliação:	**CTGTI**	Versão:	1.0
Objetivo do Processo, Projeto ou Ativo:	**Publica oficialmente, em meio eletrônico, atos judiciais e administrativos**	Data da Revisão:	26/06/2024
		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	**EVENTOS**	**CAUSAS**	**CONSEQUÊNCIAS**	**PILARES DE S.I**	Probabilidade	Impacto	Nível do Risco	**Descrição do Controle**	Eficácia	**Risco Residual**	Resposta ao Risco	**Controle em Implementação**	**Responsável**	**Data início**	**Data Final**	**Periodicidade**	**Status da Ação Proposta**	**Expectativa de Nível de Risco após os controles**	**Quem deve ser comunicado**
Externo	Indisponibilidade do sistema DJE	- Bugs ou vulnerabilidades no sistema. - Falhas nos servidores ou no banco de dados do TSE; - Data Center do TSE indisponível; - Falha no funcionamento dos equipametos da rede local (TRE e ZEs) - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Atrasos na comunicação de atos judiciais; - Dificuldades das partes interessadas para acessar as informações sobre seus processos; - Prejuízos à transparência e a publicidade dos atos judiciais; - Comprometimento da imagem do poder judiciário perante à sociedade; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações contínuas de software e hardware - Monitoramento da disponibilidade do sistema - Reportar os bugs para o TSE	Satisfatório	9,6 - Médio	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema. - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados sensíveis dos usuários, comprometendo sua privacidade; - Interrupção na publicação dos atos judiciais; - Prorrogação de prazos e atrasos nas decisões judiciais; - Dificuldades das partes interessadas para acessar as informações sobre seus processos; - Prejuízos à transparência e a publicidade dos atos judiciais; - Perda de informações dos processos judiciais; - Prejuízo à imagem da Justiça Eleitoral; - Prejuízos financeiros em razão das horas de trabalho perdidas e devido a eventual necessidade de recursos adicionais para o restabelecimento do sistema.	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas. - Desenvolvimento de planos de contingência e recuperação. - Monitoramento de vulnerabilidades - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilzação e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de	Sistema Eletrônico de Informações (SEI)	Data da	19/04/2022
Responsável pela avaliação:	CTGTI	Versão:	1.0
Objetivo do Processo, Projeto ou	Promover a eficiência administrativa por meio da produção, edição, assinatura e trâmitação de processos e documentos eletrônicos	Data da	26/06/2024
Ativo:		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Interno	Indisponibilidade do sistema SEI	- Bugs ou vulnerabilidades no sistema. - Falhas nos servidores ou no banco de dados - Data Center indisponível - Falha no funcionamento dos equipametos da rede local (TRE e ZEs) - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Interrupção na tramitação de processos administrativos; - Dificuldade no Acesso à Informação e na Tomada de Decisões por parte dos servidores e gestores; - Prejuízos à transparência e a publicidade dos atos administrativos; Comprometimento da eficiência Operacional; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações contínuas de software e hardware; - Monitoramento da disponibilidade do sistema; - Implementação de mecanismos de redundância da infraestrutura de TIC; - Implementação de links de comunicação redundantes; - Utilização de nobreaks e geradores de energia; - Implementar política de backup.	Satisfatório	9,6 - Médio	Aceitar									
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema. - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados sensíveis dos usuários, comprometendo sua privacidade. - Interrupção na tramitação eletrônica de processos judiciais; - Prorrogação de prazos e atrasos nas decisões judiciais; - Dificuldades das partes interessadas para acessar as informações sobre seus processos; - Prejuízos à transparência e a publicidade dos atos judiciais; - Perda de informações dos processos judiciais; - Prejuízo à imagem da Justiça Eleitoral; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas. - Desenvolvimento de planos de contingência e recuperação. - Monitoramento de vulnerabilidades - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilização e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de	Links/Redes de comunicação de dados	Data da	19/04/2024
Responsável pela avaliação:	CTGTI	Versão:	1.0
Objetivo do Processo, Projeto ou	Interconectar sistemas informatizados e unidades, permitindo a troca segura de informações	Data da	26/06/2024
Ativo:		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Interno	Indisponibilidade dos links/redes de comunicação de dados	- Falhas físicas de hardware; - Configurações erradas ou falhas em sistemas operacionais e software de rede; - Ataques cibernéticos; - Falhas de fornecedores de serviços; - Sobrecarga da infraestrutura de rede por tráfego de dados maior que o projetado; - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Indisponibilidade dos sistemas essenciais de TIC; - Dificuldade no Acesso à Informação e na Tomada de Decisões por parte dos servidores e gestores; - Prejuízos à transparência e a publicidade dos atos administrativos e judiciais; - Comprometimento da eficiência Operacional; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	Desenvolver planos detalhados de recuperação de desastres e contingência, com testes regulares; - Monitoramento da disponibilidade dos links e redes de comunicação de dados; - Implementação de mecanismos de redundância da infraestrutura de TIC; - Implementação de links de comunicação redundantes; - Utilização de nobreaks e geradores de energia; - Implementar política de backup.	Satisfatório	9,6 - Médio	Aceitar									
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades dos ativos de rede; - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética; - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados sensíveis dos usuários, comprometendo sua privacidade. - Indisponibilidade dos sistemas essenciais de TIC; - Prejuízo à imagem da Justiça Eleitoral; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	-Treinamento adequado para os usuários. - Planos de contingência e recuperação. - Monitoramento de vulnerabilidades - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilização e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de	Bancos de dados	Data da	19/04/2022
Responsável pela avaliação:	CTGTI	Versão:	1.0
Objetivo do Processo, Projeto ou	Armazenar e gerenciar informações relevantes para suporte às operações e decisões	Data da	26/06/2024
Ativo:		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Interno	Indisponibilidade dos Bancos de dados	- Falhas físicas de hardware; - Falhas nas configurações dos Servidores Gerenciadores de Bancos de Dados (SGDB); - Ataques cibernéticos; - Sobrecarga do SGDB por tráfego de dados maior que o projetado; - Interrupção do SGDB pela insuficiência da capacidade de armazenamento; - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Indisponibilidade dos sistemas essenciais de TIC; - Dificuldade no Acesso à Informação e na Tomada de Decisões por parte dos servidores e gestores; - Prejuízos à transparência e a publicidade dos atos administrativos e judiciais; - Comprometimento da eficiência Operacional; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Planos de recuperação de desastres e contingência, com testes regulares; - Monitoramento da disponibilidade dos links e redes de comunicação de dados; - Implementação de mecanismos de redundância da infraestrutura de TIC; - Implementação de links de comunicação redundantes; - Utilização de nobreaks e geradores de energia; - Política de backup.	Satisfatório	9,6 - Médio	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades do SGDB - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados pessoais dos usuários, comprometendo sua privacidade. - Indisponibilidade dos sistemas essenciais de TIC; - Prejuízo à imagem da Justiça Eleitoral; - Prejuízos financeiros para o restabelecimento do serviço (horas de trabalho, recursos adicionais, etc).	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	-Treinamento adequado para os usuários; - Planos de contingência e recuperação; - Monitoramento de vulnerabilidades; - Antivírus atualizado - Utilização de VPN; - Controle de permissões de usuários; - Troca de senhas; periódicas, conforme requisitos estabelecidos.	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilização e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de	Sistemas eleitorais	Data da	19/04/2022
Responsável pela avaliação:	CTGTI	Versão:	1.0
Objetivo do Processo, Projeto ou	Suportar o processo eleitoral, desde a votação até a apuração de resultados	Data da	26/06/2024
Ativo:		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Externo	Indisponibilidade dos sistemas eleitorais	- Bugs ou vulnerabilidades nos sistemas eleitorais; - Falhas nos servidores ou no banco de dados do TSE; - Data Center do TSE indisponível; - Falha no funcionamento dos equipametos da rede local (TRE e ZEs); - Falha no link de comunicação de dados com o TSE. - Falha no link de comunicação de dados com as ZEs. - Queda de energia elétrica.	- Interrupção nos procedimentos relacionados ao processo eleitoral; - Perda de dados; - Atrasos nas etapas do processo eleitoral.	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações contínuas de software e hardware; - Monitoramento dos links de comunicação de dados das Zonas Eleitorais; - Monitoramento do data center; - Reportar os bugs para o TSE.	Forte	4,8 - Baixo	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema. - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados pessoais dos usuários, comprometendo sua privacidade; - Interrupção nos procedimentos relacionados ao processo eleitoral; - Perda de dados; - Atrasos nas etapas do processo eleitoral.- Prejuízo à imagem da Justiça Eleitoral.	INTEGRIDADE:	Média - 6	Extremo - 10	60 - Extremo	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas. - Desenvolvimento de planos de contingência e recuperação. - Monitoramento de vulnerabilidade - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	36 - Alto	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilização e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de	Sítio de internet	Data da	19/04/2024
Responsável pela avaliação:	CTGTI	Versão:	1.0
Objetivo do Processo, Projeto ou	Portal de comunicação pública e serviços online	Data da	26/06/2024
Ativo:		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os	Quem deve ser comunicado
Externo	Indisponibilidade do Portal de internet	- Bugs ou vulnerabilidades no Portal; - Falhas nos servidores ou no banco de dados do TSE; - Data Center do TSE indisponível.	- Interrupção do acesso ao portal, impedindo o funcionamento de serviços online; - Dificuldades na comunicação com o público externo; - Atrasos no fornecimento de informações atualizadas sobre às eleições; - Comprometimento da imagem do poder judiciário perante à sociedade.	DISPONIBILIDADE:	Baixa - 4	Relevante - 6	24 - Médio	- Acompanhamento das atualizações; contínuas de software e hardware; - Monitoramento da disponibilidade do sítio de Internet; - Reportar os bugs para o TSE.	Satisfatório	9,6 - Médio	Aceitar								
Externo	Ataques de Segurança Cibernética	- Exploração de vulnerabilidades não corrigidas no sistema. - Falta de treinamento adequado para servidores e colaboradores sobre práticas de segurança cibernética. - Insuficiência de medidas de proteção e monitoramento contra intrusões.	- Acesso não autorizado ou perda de dados sensíveis dos usuários, comprometendo sua privacidade. - Interrupção do acesso ao portal, impedindo o funcionamento de serviços online; - Dificuldades na comunicação com o público externo; - Atrasos no fornecimento de informações atualizadas sobre às eleições; - Comprometimento da imagem do poder judiciário perante à sociedade.	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	- Treinamento adequado para os usuários. - Implementação de medidas de segurança robustas. - Desenvolvimento de planos de contingência e recuperação. - Monitoramento de vulnerabilidades - Antivírus atualizado - Utilização de VPN - Controle de permissões de usuários - Troca de senhas periódicas, conforme requisitos estabelecidos	Mediano	24 - Médio	Mitigar riscos	Adotar as medidas definidas na Estratégia Nacional de Segurança Cibernética da Justiça Eleitoral, conforme arquitetura estabelecida: Pessoas e Unidades, Políticas e Normatizações, Ferramentas Automatizadas, Serviços Especializados e Sensibilização e Conscientização.	ACIBER	08/01/2024	18/12/2026	Mensal	Em Implementação	Médio	CTGTI/CGSI

GERENCIAMENTO DE RISCOS DE TIC

1. IDENTIFICAÇÃO DO ESCOPO

Processo, Projeto ou Ativo de Informação	**Manutenção e distribuição das urnas eletrônicas**	Data da Avalilação:	19/04/2022
Responsável pela avaliação:	**CTGTI**	Versão:	1.0
Objetivo do Processo, Projeto ou Ativo:	**A manutenção e distribuição das urnas eletrônicas asseguram que estejam prontas e funcionais para as eleições, garantindo a integridade do processo de votação.**	Data da Revisão:	26/06/2024
		Revisor:	AGSTI

2. PRIORIZAÇÃO E RESPOSTAS AOS RISCOS DO PROCESSO

RISCOS IDENTIFICADOS				ASPECTOS DE S. I.	ANÁLISE DO RISCO			CONTROLES EXISTENTES			TRATAMENTO DO RISCO					MONITORAMENTO			COMUNICAÇÃO
CONTEXTO	EVENTOS	CAUSAS	CONSEQUÊNCIAS	PILARES DE S.I	Probabilidade	Impacto	Nível do Risco	Descrição do Controle	Eficácia	Risco Residual	Resposta ao Risco	Controle em Implementação	Responsável	Data início	Data Final	Periodicidade	Status da Ação Proposta	Expectativa de Nível de Risco após os controles	Quem deve ser comunicado
Interno	Urnas eletrônicas não manutenicas atempadamente	- Problemas nos contratos que suportam a manutenção preventiva das urnas eletrônicas; - Incidente na infraestrutura utilizada na manutenção das urnas eletrônicas; - Falta de pessoal nas atividades de manutenção das urnas eletrônicas.	- Atraso na distribuição das urnas eletrônicas às zonas eleitorais para realização da carga e lacre.	DISPONIBILIDADE:	Baixa - 4	Muito Relevante - 8	32 - Alto	- Acompanhamento da execução dos contratos de mão de obra e da empilhadeira; - Acompanhamento da execução das manutenções preventivas.	Forte	6,4 - Baixo	Aceitar	a realização da manutenção,	CSEL	08/01/2024	18/12/2026				
Interno	- Urnas não distribuídas tempestivamente para a carga e lacre	- Indisponibilidade de recursos humanos: motoristas e braçais; - Indisponibilidade ou ausência de local para recepcionar as urnas eletrônicas nas zonas eleitorais; - Indisponibilidade de veículos de carga.	- Atraso na realização da carga e lacre das urnas eletrônicas.	DISPONIBILIDADE:	Muito Baixa - 2	Pouco Relevante - 4	8 - Baixo	- Acompanhamento da disponibilidade da área de transporte;	Satisfatóric	3,2 - Baixo	Aceitar								
Externo	- Violação da integridade das urnas eletrônicas após às eleições	- Indisponibilidade ou precariedade do local de armazenamento das urnas eletrônicas, após as eleições nas zonas eleitorais	- Descrédito do processo eleitoral; - Prejuízo em processo de auditoria.	INTEGRIDADE:	Baixa - 4	Extremo - 10	40 - Alto	- Sistemas de automação que viabilizam a rastreabilidade das urnas eletrônicas; - Coleta das urnas eletrônicas das zonas eleitorais, após a autorização da administração, antes do decurso do prazo previsto em resolução, para armazena-las no depósito central; - Expedição de Ofício-Circular, pela Alta Administração do TRE-GO, com recomendação aos Juízes Eleitorais, para disponibilização de locais adequados de armazenamento durante a quarentena.	Mediano	24 - Médio	Mitigar riscos								