Art. 1º. Instituir a equipe de planejamento para a contratação da Ação de Capacitação na área de Facilitação Visual aplicada ao redesenho de serviços públicos, no intuito de auxiliar na melhoria da relação do Estado com a sociedade, bem como suas estruturas de comunicação internas.
Art. 2º. Designar para compor a equipe de planejamento os servidores:
I - Juliana Avelar Lucena de Oliveira (área técnica);
II - Vick Mature Aglantzakis (área requisitante);
III - Julhierme Markus Emílio Peres da Cunha - ASPLAN/SADOR (área administrativa).
Art. 3º Cabe à equipe elaborar os estudos técnicos preliminares, o mapa de risco e o termo de referência.
Art. 4º Esta Portaria entra em vigor na data da publicação.
Palmas, 22 de junho de 2023.
José Machado dos Santos
Diretor-Geral

ATOS DA PRESIDÊNCIA

PORTARIA Nº 550/2023 PRES/DG/SGP/COPES

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO TOCANTINS, no uso de suas atribuições legais e regimentais, ex vi do inciso XXIV, do artigo 20, do Regimento Interno deste Tribunal e de acordo com a Resolução TSE nº 21.832, de 22/6/2004, alterada pela Resolução TSE nº 23.411, de 6/5/2014, e o teor do SEI nº 0028514-85.2023.6.27.8023, RESOLVE:
Art. 1º Designar o servidor requisitado VILMAR LUIZ WOICIK, para exercer, em caráter excepcional, a função de Chefe de Cartório Substituto, Nível FC-6, do Cartório Eleitoral da 23ª Zona, com sede no município de Pedro Afonso/TO, nos dias 19/06 a 23/06/2023, tendo em vista que, nessas datas, o titular Ravel de Sousa Alves e sua substituta automática, Rosangela Ferreira Pires, encontrar-se afastados por motivo de viagem a serviço e férias, respectivamente.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
Palmas, 22 de junho de 2023.
Desembargador Helvécio de Brito Maia Neto
Presidente

PORTARIA Nº 547/2023 PRES/DG/SGP/COPES

Aprova os Protocolos de Segurança Cibernética do Tribunal Regional Eleitoral do Tocantins.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO TOCANTINS no uso de suas atribuições legais e regimentais,
CONSIDERANDO o disposto na Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
CONSIDERANDO o disposto na Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO o disposto na Portaria CNJ nº 162/2021, que a prova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;
RESOLVE:
Art. 1º Aprovar os Protocolos de Segurança Cibernética do Tribunal Regional Eleitoral do Tocantins, constantes dos seguintes anexos:
I - protocolo de prevenção a incidentes cibernéticos (Anexo I);
II - protocolo de gerenciamento de crises cibernéticas (Anexo II); e
III - protocolo para investigação de ilícitos cibernéticos (Anexo III).

Art. 2º Os Protocolos deverão ser disponibilizados no portal eletrônico do Tribunal Regional Eleitoral do Tocantins.

Art. 3° Esta Portaria entra em vigor na data de sua publicação.

Palmas, 21 de junho de 2023.

Desembargador Helvécio de Brito Maia Neto

Presidente

ANEXO I

ANEXO I - PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para a prevenção de incidentes cibernéticos.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

1.3. Promover ações pró-ativas que contribuam para a prevenção de incidentes cibernéticos e também para a resiliência do ambiente tecnológico do Tribunal.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Gerenciamento de Crises Cibernéticas e o Protocolo para Investigação de Ilícitos Cibernéticos.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRE-TO.

2.3. Os atores atuantes ativamente na gestão de segurança cibernética no âmbito do TRE-TO, cujas instituições e atribuições estão definidas na Política de Segurança do TRE-TO (Resolução nº 496/2020), Regimento Interno e demais resoluções relacionadas, são os seguintes:

2.3.1. Comissão Permanente de Segurança da Informação;

2.3.2. Secretaria de Tecnologia da Informação;

2.3.3. Assessoria de Segurança Cibernética;

2.3.4. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR-TO).

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. FUNÇÕES DO PROTOCOLO

4.1. Com base na ENSEC-PJ, as funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar.

4.1.1. A função identificar consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade. No âmbito do TRE-TO, a função deve ser implementada pela seguinte atividade.

4.1.1.1. Implantação do processo de Gestão de Riscos de Segurança da Informação.

4.1.2. A função proteger consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados (inclusive pessoais), além de contribuir para a eficiência e eficácia da prestação de serviços. No âmbito do TRE-TO, a função deve ser implementada pelas seguintes atividades:

4.1.2.1. Plano de Continuidade de TI dos serviços essenciais.

4.1.2.2. Gerenciamento da Disponibilidade e Capacidade de TI dos serviços essenciais.

4.1.2.3. Realização de cópias de segurança do ambiente tecnológico.

4.1.2.4. Implementação de boas práticas de gerenciamento e proteção do ambiente

tecnológico, observando normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002 e CIS Controls), tais como:

a. Gestão de vulnerabilidades dos ativos de TI;

b. Implementação de soluções de segurança do ambiente (firewall, IPS, filtro de conteúdo web, proteção de endpoint, detecção e resposta de endpoint, dentre outras);

c. Uso de antivírus de rede e redes privadas virtuais (VPN);

d. Hardening de serviços e de sistemas;

e. Gestão de identidades e rotacionamento de credenciais privilegiadas;

f. Integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento;

g. Promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;

h. Atualização tecnológica constante;

4.1.2.5. Adequação gradual aos seguintes Manuais de Referência, juntos com a ENSECPJ, observando a aplicabilidade de cada controle em relação ao porte e à maturidade do TRETO em segurança cibernética: Proteção de Infraestruturas Críticas de TIC e Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, Manual de Gestão de Identidade e de Controle de Acesso;

4.1.2.6. Implantação gradual de uma Política de Educação e Cultura em Segurança Cibernética, conforme o anexo VII da Portaria nº 162, de 10 de junho de 2021 do Conselho Nacional de Justiça;

4.1.3. A função detectar consiste no desenvolvimento e aplicação de medidas para identificação de eventos e/ou incidentes de segurança cibernética. A função responder consiste na definição e implementação de medidas para responder com eficiência e eficácia a incidentes de segurança cibernética. A função recuperar consiste no desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos quando da ocorrência de eventos e/ou incidentes de segurança cibernética. Essas três funções devem ser implementadas pelas seguintes atividades:

4.1.3.1. Implantação e aprimoramento da Gestão de Incidentes de Segurança da Informação.

4.1.3.2. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

4.1.3.3. Plano de Continuidade de TI dos serviços essenciais.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.

Palmas, 21 de junho de 2023.

Desembargador Helvécio de Brito Maia Neto

Presidente

ANEXO II

ANEXO II - PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos[1] e o Protocolo para Investigação de Ilícitos Cibernéticos.
2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRE-TO.
2.3. Este protocolo deve ser acionado nos casos em que as medidas estabelecidas no Protocolo de Prevenção de Incidentes Cibernéticos não forem suficientes para evitar a ocorrência de um incidente.
2.4. Para efeitos deste protocolo, são considerados críticos para o funcionamento do Tribunal os seguintes sistemas:
2.4.1. Kenta - Gravação de Áudio das Sessões Plenárias
2.4.2. Malote Digital - Correspondência Oficial do Judiciário
2.4.3. SEI! - Sistema Eletrônico de Informações
2.4.4. SGIE - Gestão Integrada de Eleições
2.4.5. Ata de Seções Eleitorais
2.4.6. Autorizador
2.4.7. Balcão Virtual
2.4.8. Diplomas de Eleitos e Suplentes
2.4.9. Eleitor Online - Atendimento do Eleitor Pela Internet
2.4.10. Titulonet - Atendimento ao Eleitor Pela Internet
2.4.11. Portal das Eleições
2.4.12. TRE-Saúde - Gestão do Plano de Saüde
2.4.13. Drive - Arquivo Corporativo - Workspace
2.4.14. SPCA - Prestação De Contas Anual
2.5. Uma crise cibernética se configura na ocorrência de evento ou série de eventos danosos, que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes, afetando diretamente ou indiretamente os sistemas críticos do Tribunal.
2.6. Os atores atuantes ativamente no gerenciamento de crises cibernéticas do TRE-TO, cujas instituições e atribuições estão definidas na Política de Segurança do TRE-TO (Resolução nº 496 /2020), Regimento Interno e demais portarias relacionadas, são os seguintes:
2.6.1. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR-TO).[2]
2.6.2. Grupo executivo estabelecido no Plano de Continuidade dos Serviços Essenciais de TI.[3]
3. GLOSSÁRIO
3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.
4. GERENCIAMENTO DE CRISES CIBERNÉTICAS
4.1. O gerenciamento de crise cibernética se inicia quando:
4.1.1. ficar caracterizado grave dano material ou de imagem;
4.1.2. restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
4.1.3. o incidente impactar gravemente os serviços de TI essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do plano de continuidade de TI do Tribunal[4] ;
4.1.4. atrair grande atenção da mídia e da população em geral; ou;
4.1.5. ocorrer incidente de segurança com dados pessoais;

4.2. Confirmada a crise cibernética, o grupo executivo estabelecido no plano de continuidade de serviços essenciais de TI do Tribunal, deverá se reunir imediatamente.
4.2.1. São atribuições do grupo executivo:
4.2.1.1. Gerenciar as ações necessárias para o tratamento de crises cibernéticas;
4.2.1.2. Respaldar as ações da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;
4.2.1.3. Atuar como ponto de contato com órgãos externos para comunicação referente ao tratamento de crises cibernéticas, centralizando a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;
4.2.1.4. O reporte da crise ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).
4.2.2. Caso a crise envolva dados pessoais, o Encarregado de Tratamento de Dados Pessoais do Tribunal deve informar as entidades externas nos termos da LGPD e das demais normativas relacionadas à proteção de dados pessoais vigentes no TRE-TO.
4.2.3. A reunião dar-se-á em local conhecido como "sala de situação", ambiente que permita ao grupo deliberar com tranquilidade e que possua equipe dedicada à execução de atividades administrativas para o período de crise.
4.3. Para o tratamento do incidente que ocasionou a crise, deverão ser utilizadas políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres[5] e procedimentos técnicos já elaborados e formalizados.
4.4. A crise encerra-se no momento em que for constatado o retorno à normalidade das operações.
4.4.1. Deve ser elaborado um relatório da crise com o intuito de registrar as ações que foram efetivas e as melhorias necessárias para corrigir as causas do incidente que originou a crise (lições aprendidas). O relatório deve conter as seguintes informações:
4.4.1.1. a identificação e análise da causa-raiz do incidente;
4.4.1.2. a linha do tempo das ações realizadas;
4.4.1.3. a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
4.4.1.4. os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
4.4.1.5. as ações realizadas para tratamento da crise e avaliação de sua eficácia.
5. CONSIDERAÇÕES FINAIS
5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.
5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.
Palmas, 21 de junho de 2023.
Desembargador Helvécio de Brito Maia Neto
Presidente
ANEXO III
ANEXO III - PROTOCOLO PARA INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS
1. OBJETIVOS
1.1. Estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.
1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

1.3. Definir requisitos para adequação dos ativos de tecnologia da informação no que tange à configuração e ao registro de informações de auditoria;

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo de Gerenciamento de Crises Cibernéticas.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRE-TO.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS EM RELAÇÃO AO REGISTRO DE INFORMAÇÕES

4.1. Os ativos tecnológicos do Tribunal (ex.: estações de trabalho, servidores, serviços, sistemas, dentre outros) devem:

4.1.1. Ser configurados de acordo com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

4.1.2. Ser configurados de forma a registrar eventos relevantes de segurança da informação, bem como de informações que possibilitem a depuração de incidentes e de problemas.

4.1.3. Registrar, sempre que possível, as seguintes informações:

4.1.3.1. identificação inequívoca do usuário que acessou o recurso;

4.1.3.2. natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;

4.1.3.3. data, hora e fuso horário, observando-se a HLB; e

4.1.3.4. endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação e demais informações que possibilitem identificar a origem do evento;

4.2. Os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

4.3. O armazenamento dos registros de auditoria deve ser realizado remotamente (e não apenas localmente), por meio do uso de tecnologia aplicável, para, ao menos, os ativos tecnológicos considerados críticos.

5. PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

5.1. Confirmada a ocorrência de um incidente, deve ser avaliada a necessidade de ativação do Protocolo de Gerenciamento de Crises Cibernéticas.[1]

5.2. A investigação do ilícito cibernético deve ser realizada de acordo com as normas estabelecidas na Política de Segurança da Informação vigente, especificamente no tocante ao assunto de gestão de incidentes de segurança da informação e à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

5.3. Os incidentes de segurança cibernética devem ser registrados em Relatório de Incidente de Segurança da Informação, que contém os dados de identificação de quem o preencheu, data e hora da ocorrência, informações sobre o incidente, como ele foi tratado, oportunidades de melhoria e lições aprendidas.

5.4. Caso seja necessária a coleta de evidências, ela deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.

5.5. Se o incidente de segurança envolver a suspeita de crime, os órgãos competentes devem ser acionados, nos termos da legislação vigente.
Palmas, 21 de junho de 2023.
Desembargador Helvécio de Brito Maia Neto
Presidente

ZONAS ELEITORAIS

1ª ZONA ELEITORAL - ARAGUAÍNA

PRESTAÇÃO DE CONTAS ANUAL(12377) Nº 0600028-51.2023.6.27.0001

PROCESSO	: 0600028-51.2023.6.27.0001 PRESTAÇÃO DE CONTAS ANUAL (ARAGUAÍNA - TO)
RELATOR	**: 001ª ZONA ELEITORAL DE ARAGUAÍNA TO**
FISCAL DA LEI	: PROMOTOR ELEITORAL DO ESTADO DO TOCANTINS
INTERESSADO	: CIDADANIA - ARAGUAINA - TOCANTINS - MUNICIPAL
INTERESSADO	: FABIO JUNIOR ALVES DE SOUSA
INTERESSADO	: FRANCISCO VILARINDO DA SILVA

JUSTIÇA ELEITORAL
001ª ZONA ELEITORAL DE ARAGUAÍNA TO
PRESTAÇÃO DE CONTAS ANUAL (12377) Nº 0600028-51.2023.6.27.0001 / 001ª ZONA ELEITORAL DE ARAGUAÍNA TO
INTERESSADO: CIDADANIA - ARAGUAINA - TOCANTINS - MUNICIPAL, FRANCISCO VILARINDO DA SILVA, FABIO JUNIOR ALVES DE SOUSA
EDITAL
Pelo presente, expedido nos autos em epígrafe, Amilton Brasileiro Pereira, Chefe de Cartório da 1ª Zona Eleitoral do Estado do Tocantins, com sede no município de Araguaína/TO, no uso de suas atribuições legais e regimentais, em cumprimento ao disposto no inciso I do Art. 44 da Resolução do Tribunal Superior Eleitoral (TSE) nº 23.604, de 17 de dezembro de 2019,
TORNA-SE PÚBLICO a todos que o presente edital virem ou dele conhecimento tiverem, em cumprimento ao disposto no inciso I do Art. 44 da Resolução/TSE 23.604/2019, a apresentação da prestação de contas anual de EXERCÍCIO FINANCEIRO 2022, na forma de Declaração de Ausência de Movimentação de Recursos pelo Partido CIDADANIA (CIDADANIA) e respectivos responsáveis, acima destacados, facultando a qualquer interessado, no prazo de três dias contados da publicação do edital, a apresentação de impugnação que deve ser apresentada em petição fundamentada e acompanhada das provas que demonstrem a existência de movimentação financeira ou de bens estimáveis no período.
E para que se dê ampla divulgação, determinou o Excelentíssimo Senhor Juiz Eleitoral, Dr. Deusamar Alves Bezerra, que fosse publicado o presente Edital no Diário da Justiça Eletrônico do Tribunal Regional Eleitoral do Estado do Tocantins DJE/TO.
Araguaína/TO, 22 de junho de 2023.
Amilton Brasileiro Pereira
Chefe de Cartório da 1ª Zona Eleitoral

CUMPRIMENTO DE SENTENÇA(156) Nº 0600800-19.2020.6.27.0001