Art. 5º Para a eleição de que trata este edital poderão votar e ser votadas(os) as(os) servidoras(es) efetivas(os) da Justiça Eleitoral em exercício no TRE-CE, assim abrangidos a Secretaria do Tribunal, os cartórios eleitorais, diretorias dos fóruns, centrais de atendimento ao eleitor e postos de atendimento.
Art. 6º As(os) servidoras(es) deverão formalizar seus votos por meio de link na intranet do Tribunal, a ser divulgado no edital a que se refere o art. 2º, em ambiente seguro, mediante utilização de senha pessoal.
§ 1º Na votação de que trata o caput deste artigo, considerar-se-ão eleitas(os) as(os) duas(dois) que obtiverem o maior número de votos válidos, não computados os em branco e os nulos, figurando como suplentes respectivas(os) a(o) terceira(o) e a(o) quarta(o) mais votadas(os).
§ 2º Havendo empate entre as(os) candidatas(os), será considerada(o) eleita(o) aquela(e) com maior tempo de exercício no TRE-CE e, na sequência, a(o) que tenha maior idade.
Art. 7º O resultado da votação será divulgado por meio de edital no dia 31 de maio de 2023, a ser publicado no Diário da Justiça Eletrônico.
Art. 8º Caso na lista de inscritas(os) não haja interessadas(os) suficientes para ocupação das vagas de titulares e suplentes, caberá à Presidência indicar as(os) titulares e suplentes para completar a sua composição.
Art. 9º O mandato da(o) titular e da(o) suplente será de dois anos, sendo possível uma recondução.
Art. 10. A lista de inscritas(os) prevista no art. 2º deste Edital será utilizada para escolha da(o) integrante do Comitê de Gestão de Pessoas a que se refere o art. 2º, inciso I, alínea "c", da Portaria TRE-CE nº 210/2023.
Art. 11. Os casos omissos serão resolvidos pela Presidência deste Tribunal.
REGISTRE-SE, PUBLIQUE-SE E CUMPRA-SE.
GABINETE DA PRESIDÊNCIA DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ, aos 9 dias do mês de maio de 2023.
DESEMBARGADOR INACIO DE ALENCAR CORTEZ NETO
PRESIDENTE

PORTARIAS

PORTARIA Nº 462/2023 - SEGURANÇA DA INFORMAÇÃO

Institui o uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Ceará
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ, no uso das atribuições que lhe confere o artigo 23, inciso LX, do Regimento Interno deste Tribunal,
CONSIDERANDO o que dispõe os artigos 7º e 9º da Res. TRE/CE n.º 920/2022;
CONSIDERANDO o disposto no Processo Administrativo Digital SEI n.º 2022.0.000002929-4;
CONSIDERANDO a Resolução TRE nº 793/2020, que dispõe sobre o Planejamento Estratégico da Justiça Eleitoral do Ceará;
CONSIDERANDO a Resolução TRE nº 618/2016, que regulamenta a aplicação, no âmbito do Tribunal Regional Eleitoral do Ceará, da Lei nº 12.527, de 18 de novembro de 2011, que versa sobre o acesso à informação;
CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8.;
CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);
CONSIDERANDO as diretivas da lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações;
CONSIDERANDO a Res. TRE-CE 920/2022, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral do Ceará.
CONSIDERANDO a lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Ceará;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída, por meio deste normativo, a regulamentação do uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Ceará.
Art. 2º Esta norma é uma diretriz obrigatória, conforme disposto no inciso XII, Art. 7º da Política de Segurança de Informação da Justiça Eleitoral do Ceará, estabelecida pela Resolução nº 920, de 24 de outubro de 2022.
CAPÍTULO II
AS DEFINIÇÕES
Art. 3º Para efeitos desta norma, consideram-se os termos e definições a seguir:
I - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
II - Assinatura digital: tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos, de criptografia assimétrica, para garantir segurança quanto à autenticidade das documentações. Para assinar digitalmente um documento, é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio e tempestividade;
III - Atividades críticas: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como por exemplo: perda de prazos administrativos e judiciais, danos à imagem institucional, prejuízo ao erário, dentre outros;
IV - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;
V - Ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;
VI - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;
VII - Autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade;
VIII - Ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;

IX - Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los;
X - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;
XI - Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
XII - Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XIII - Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XIV - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;
XV - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
XVI - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;
XVII - Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;
XVIII - Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;
XIX - Recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XX - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
XXI - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;
XXII - Registro de eventos (log): processo com a finalidade de registrar eventos durante o seu ciclo de vida, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado;
XXIII - Resumo criptográfico: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor - conhecida como resultado hash - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável, ou seja, utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou;
XXIV - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
XXV - Segurança da informação: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, dentre outras propriedades;

XXVI - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XXVII - Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;
XXVIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
Art. 4º O uso de recursos criptográficos visa proteger a confidencialidade, a integridade e a autenticidade dos dados trafegados pelas redes de computadores, assim como dos dados em repouso, armazenados em servidores, microcomputadores, dispositivos móveis e bancos de dados.
CAPÍTULO III
DA CRIPTOGRAFIA DOS DADOS EM TRÂNSITO
Art. 5º É obrigatório o uso de protocolo seguro, como HTTPS, em todos os sistemas e portais web, independentemente de serem acessados pela rede interna ou pela Internet.
Art. 6º Toda comunicação cliente/servidor, especialmente aquelas onde trafeguem dados pessoais ou logins e senhas, deve utilizar protocolos de comunicação segura.
CAPÍTULO IV
DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS
Art. 7º Os dados pessoais sensíveis, armazenados em servidores e bancos de dados, devem adotar técnicas de criptografia ou anonimização visando diminuir o risco em caso de vazamento de dados.
Art. 8º As cópias de segurança (backups) que contenham dados pessoais sensíveis devem adotar técnicas de criptografia visando diminuir o risco em caso de vazamento de dados.
Art. 9º Os computadores, notebooks e dispositivos móveis, de propriedade da Justiça Eleitoral, utilizados em trabalho remoto, devem ter suas unidades de armazenamento (sistemas de arquivos) protegidas por criptografia visando diminuir o risco de vazamento de dados em caso de furto.
CAPÍTULO V
DA ASSINATURA DIGITAL
Art. 10 Caberá à Secretaria de Tecnologia da Informação - STI, mas não exclusivamente, distribuir e gerenciar certificados para assinatura digital, sejam do tipo A1 (arquivo digital com senha) ou A3 (token), de acordo com as necessidades do usuário interno e adotando os procedimentos técnicos cabíveis.
Art. 11 Os certificados digitais poderão ser utilizados como segundo fator de autenticação (2FA) em computadores ou sistemas, de acordo com sua criticidade e disponibilidade da tecnologia.
CAPÍTULO VI
DA AUTORIDADE CERTIFICADORA
Art. 12 O TRE-CE poderá manter Infraestrutura de Chaves Públicas (ICP) própria para uso em sistemas e computadores de uso interno, sendo permitido o modelo de AC (autoridade certificadora) autoassinada.
Art. 13 Os certificados digitais instalados em servidores e sistemas Web com acesso pela Internet deverão utilizar certificados digitais fornecidos por AC (autoridade certificadora) comercial, visando a compatibilidade com os computadores e dispositivos móveis dos usuários externos.
CAPÍTULO VII
DAS RESPONSABILIDADES
Art. 14 Cabe à STI, por meio de suas áreas técnicas:
I - Implementar o nível adequado de criptografia nos sistemas e dispositivos;
II - Implementar e manter Infraestrutura de chaves públicas interna, caso seja uma Autoridade Certificadora - AC;

III - Adquirir e gerenciar os certificados digitais para servidores e aplicações;
IV - Informar à Comissão de Segurança da Informação eventuais não-conformidades;
V - Gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;
VI - Distribuir chaves para os usuários devidos, incluindo a forma como as chaves são ativadas, quando recebidas;
VII - Manter registro e auditoria das atividades relacionadas ao gerenciamento de chaves.
Art. 15 Cabe ao usuário:
I - Zelar pela guarda do certificado digital recebido, não compartilhando o seu uso e a sua senha com terceiros;
II - Assinar termo de compromisso no ato do recebimento de certificado digital;
III - Informar imediatamente à STI ou unidade responsável em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação;
IV - O usuário deve estar ciente de que a assinatura ou login feitos por meio de certificado digital são irretratáveis, não podendo este alegar que não efetuou a ação.
DAS DISPOSIÇÕES FINAIS
Art. 16. No caso de algum equipamento, aplicação, aplicativo, sistema ou banco de dados não permitir a adoção de protocolos seguros, a informação deverá constar em documento de análise de riscos de segurança da informação, sendo imediatamente submetido para apreciação da Comissão de Segurança da Informação.
Art. 17. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.
Art. 18. A STI elaborará, em até 180 dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.
Art. 19. Qualquer descumprimento desta norma deve ser imediatamente comunicado à Assessoria de Segurança da Informação - ASEGI, com consequente adoção das providências cabíveis.
Art. 21. A STI deverá informar à Comissão de Segurança da Informação - CSI, no prazo de 180 dias, quais ativos de informação que não puderam se adequar a esta norma.
Art. 22. Esta Portaria entra em vigor na data de sua publicação.
CIENTIFIQUE-SE, PUBLIQUE-SE E CUMPRA-SE.
Fortaleza, 10 de maio de 2023.
Desembargador INACIO DE ALENCAR CORTEZ NETO
PRESIDENTE

PORTARIA TRE/CE N.º 457/2023

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ, no uso das atribuições que lhe confere o Regimento Interno deste Tribunal, com base na Lei nº 8.112/90, Portaria TRE/CE nº 323, de 4/6/2003 e SEI nº 2023.0.000007158-4, RESOLVE:
Designar LIVIA MARIA NOGUEIRA CASTRO CHAVES, Analista Judiciária do Quadro Permanente do Tribunal de Justiça do Distrito Federal, para ocupar a função comissionada de Assistente IV, nível FC-4, da Assessoria do Juiz 4 (jurista). PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 9 de maio de 2023.
Desembargador INACIO DE ALENCAR CORTEZ NETO
PRESIDENTE

PORTARIA N.º 454/2023 - LOTAÇÃO FUNCIONAL

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ, no uso das atribuições que lhe confere o inciso XLVIII do artigo 23 do Regimento Interno deste Tribunal,
CONSIDERANDO a decisão proferida no Processo Sei n.º 2023.0.000007158-4,