Art. 32. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação - CSI deste Tribunal.
Art. 33. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessária ou conveniente para o TSE.
Art. 34. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 35. Esta portaria entrará em vigor na data de sua publicação e sua implementação se fará no prazo de 24 (vinte e quatro) meses a contar dessa data.
Art. 36. Fica revogada a Portaria TSE nº 454, de 13 de julho de 2021.
ROGÉRIO AUGUSTO VIANA GALLORO
Documento assinado eletronicamente em 16/05/2024, às 12:13, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2831708&crc=CBE80144, informando, caso não preenchido, o código verificador 2831708 e o código CRC CBE80144.
2023.00.000003679-0

PORTARIA TSE Nº 325 DE 03 DE MAIO DE 2024.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, com base no disposto no *caput* do art. 38 da Lei nº 8.112, de 11 de dezembro de 1990, no inciso XV do art. 116 do Regulamento Interno e na Portaria TSE nº 288, de 08 de maio de 2020,
RESOLVE:
Art. 1º Ficam designados para substituir a Chefe de Seção de Atenção Odontológica, Nível FC-6, da Coordenadoria de Atenção à Saúde, da Secretaria de Gestão de Pessoas, da Secretaria do Tribunal, nos seus afastamentos e impedimentos legais ou regulamentares:
I - Cezar Anders Aidar, Analista Judiciário, Área Apoio Especializado, Odontologia, como 1° substituto; e
II - Maurício Santos de Oliveira, Analista Judiciário, Área Apoio Especializado, Odontologia, como 2º substituto.
Art. 2º Revogar a Portaria TSE nº 129, de 16 de fevereiro de 2016, publicada no Diário da Justiça Eletrônico, no dia 22 subsequente, página 182.
Art. 3º Esta portaria entra em vigor na data de sua publicação.
Documento assinado eletronicamente em 16/05/2024, às 12:22, horário oficial de Brasílíia, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php? acao=documento_conferir&id_orgao_acesso_externo=0&cv=2862469&crc=093883FC, informando, caso não preenchido, o código verificador 2862469 e o código CRC 093883FC.

PORTARIA TSE Nº 263 DE 08 DE ABRIL DE 2024

Dispõe sobre a instituição da Norma de Desenvolvimento Seguro de Sistemas, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
O DIRETOR GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, considerando a Resolução CNJ nº 370 , de 2020, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD); a Resolução-CNJ nº 396 , de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396 de 2021; a Resolução nº TSE

23.644 , de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral; e a Portaria TSE nº 262 de 8 de abril de 2024, que dispõe sobre o Controle de Acesso Físico e Lógico Relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral,

RESOLVE:

Art. 1º Fica instituída a Norma de Desenvolvimento Seguro de Sistemas, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral - TSE.

Art. 2º Para os efeitos da Política de Segurança da Informação do TSE e das normas a ela subordinadas, aplicam-se os termos e definições conceituados na Portaria TSE nº 444 , de 8 de julho de 2021.

Capítulo I

DA ARQUITETURA E DOS PADRÕES DE DESENVOLVIMENTO DE SISTEMAS

Art. 3º Os sistemas devem ser desenvolvidos unicamente por meio de linguagens de codificação, bibliotecas, *frameworks*, ferramentas e demais soluções de desenvolvimento previamente aprovadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de *software* da STI.

Art. 4º Devem ser adotados repositórios padronizados de armazenamento de dados para o desenvolvimento de sistemas, que permitam minimamente:

I - o controle de versionamento de códigos-fonte e de toda a documentação associada, tais como casos de uso, *workflows*, casos de testes, diagramas e relatórios; e

II - o versionamento de artefatos de desenvolvimento, tais como arquivos compilados, bibliotecas, contêineres, *snapshots*, pacotes de instalação, executáveis e binários.

§1º Os repositórios devem ser mantidos de forma centralizada em ambiente controlado, de modo a garantir a confidencialidade, a integridade e a disponibilidade dos códigos e artefatos neles armazenados.

§2º Devem ser mantidos acordos de confidencialidade para desenvolvedores ou demais interessados que necessitem acessar os códigos desenvolvidos ou sob custódia do TSE, mesmo que de forma temporária.

Art. 5º APIs, *webservices* e soluções semelhantes devem ser publicadas e controladas por ferramentas de gerenciamento de APIs.

Parágrafo único. A ferramenta deverá possuir ao menos as seguintes funcionalidades:

I - publicação de instruções de uso das APIs;

II - acompanhamento gráfico do perfil de utilização das APIs (frequência de acesso, endereços IP de origem, usuários que realizam acesso); e

III - controles de utilização das APIs, tais como frequência de utilização, cota máxima de utilização por período, controles de acesso por usuário, endereço IP de origem e outros.

Art. 6º A criação e a aprovação dos modelos de dados para o desenvolvimento dos sistemas, sob incumbência da unidade responsável pela modelagem de dados da STI, deve contemplar controles efetivos com o intuito de conferir segurança na disponibilização e no processamento dos dados.

Art. 7º Devem ser utilizados recursos de criptografia no desenvolvimento e na implantação de sistemas de informação para assegurar, entre outros:

§1º A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas em bases de dados ou sistemas de arquivo ou que sejam objeto de transmissão eletrônica.

§2º O não repúdio, como forma de comprovar a ocorrência de um evento ou ação e sua associação à entidade originária.

Art. 8º A identificação da necessidade da utilização de recursos criptográficos deverá ser resultado da análise dos requisitos de segurança da aplicação associada à análise de ameaças.

Parágrafo único. A transmissão eletrônica de credenciais de acesso aos sistemas de informação deverá sempre ser realizada de forma criptografada.

Art. 9º O Tribunal publicará um procedimento de uso de recursos criptográficos indicando quais são os recursos de criptografia aprovados para utilização, contemplando, ao menos, algoritmos para criptografia simétrica, assimétrica e cálculo de resumos criptográficos (*hashes*).

§1º Os sistemas eleitorais podem adotar padrões de criptografia específicos, também previstos no procedimento a que se refere o *caput* deste artigo, de acordo com as peculiaridades necessárias ao seu processo de desenvolvimento ou por força de legislação eleitoral que assim o requeira.

§2º O procedimento será revisado anualmente ou quando houver modificação relevante nas tecnologias de criptografia.

Art. 10. Devem ser estabelecidas arquiteturas de referência para as diferentes linguagens de desenvolvimento de sistemas, que incluam os controles mínimos de segurança aplicáveis.

Capítulo II

DOS AMBIENTES DE EXECUÇÃO DOS SISTEMAS

Art. 11. Os sistemas do Tribunal devem contar com ambientes de execução diferenciados para desenvolvimento, testes, homologação e produção dos sistemas.

Parágrafo único. Sistemas fornecidos por terceiros, com ou sem ônus para o Tribunal, deverão contar obrigatoriamente com os ambientes de teste, homologação e produção.

Art. 12. Os ambientes de desenvolvimento, testes e homologação devem reproduzir o mais fielmente possível o ambiente de produção, para fins de redução de vulnerabilidades de segurança, com exceção das características de dimensionamento dos ambientes.

Art. 13. Cabe exclusivamente à unidade responsável pela infraestrutura de TI da STI o controle sobre o dimensionamento e o acesso aos ambientes de execução dos sistemas.

Art. 14. Os sistemas devem ser devidamente testados e homologados em seus ambientes de execução apropriados, antes da sua liberação para a produção, de acordo com o processo de liberação de sistemas definido pela STI.

Art. 15. A infraestrutura dos ambientes de execução dos sistemas deve conter mecanismos que garantam o acesso seguro, observando-se, no mínimo, os seguintes controles:

I - somente a unidade responsável pela infraestrutura dos ambientes de produção da STI deve possuir acesso direto aos ambientes de produção dos sistemas, exceto por determinação da STI, após análise e aprovação de justificativa fundamentada;

II - O acesso aos ambientes de desenvolvimento, testes e homologação é permitido somente à equipe de infraestrutura e à equipe de desenvolvimento do sistema que esteja sendo construído ou testado; e

III - A unidade responsável pela infraestrutura de TI da STI poderá, após análise, conceder o direito de acesso remoto aos ambientes de desenvolvimento, teste e homologação do sistema aos seus desenvolvedores ou interessados, desde que seja solicitado com as devidas justificativas.

Parágrafo único. Toda e qualquer concessão de permissões de acesso aos ambientes deve ser precedida de assinatura de acordos de confidencialidade.

Capítulo III

DO PROJETO DE SISTEMAS

Art. 16. Devem ser especificados os requisitos de segurança relativos ao sistema a ser desenvolvido, quanto a confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio e privacidade dos dados por ele tratados.

§1º Todos os requisitos e especificações devem ser analisados e revisados quanto ao aspecto da segurança da informação, antes e durante a codificação, de acordo com as definições de desenvolvimento seguro aprovadas para cada tecnologia de codificação empregada.
§2º A análise de segurança dos requisitos e especificações do sistema deve direcionar as ações de verificação e testes de segurança necessárias ao longo do processo de desenvolvimento do sistema.
Art. 17. Os sistemas sob responsabilidade do TSE classificados como de criticidade alta devem ser submetidos à análise de riscos, observado o disposto na Portaria TSE 784/2017, devendo também considerar:
a) O apetite ao risco do TSE;
b) O perfil de risco do TSE;
c) A realização de análise de ameaças; e
d) A avaliação e revisão periódica dos riscos das aplicações.
Art. 18. Os sistemas desenvolvidos por terceiros por meio de demanda formalizada pelo Tribunal, bem como sua documentação e artefatos, devem ser submetidos à verificação de segurança pelo TSE, de acordo com critérios de avaliação definidos pela unidade responsável pela gestão da segurança de TI do TSE.
Capítulo IV
DA CODIFICAÇÃO DOS SISTEMAS
Art. 19. O processo de desenvolvimento de sistemas do TSE deve considerar os procedimentos para desenvolvimento seguro definidos conjuntamente pela unidade responsável pela gestão de segurança de TI do TSE e pelas coordenadorias de desenvolvimento, de acordo com as tecnologias empregadas na codificação, com vistas à garantia da integridade, da confidencialidade e da disponibilidade dos sistemas e seus dados.
Parágrafo único. Os procedimentos para desenvolvimento seguro serão publicados por meio da unidade responsável pela gestão de segurança de TI do TSE, em guias especializados.
Art. 20. Os procedimentos de codificação segura dos sistemas devem considerar, no mínimo, os seguintes controles de segurança:
I - O desenvolvimento deve ser auxiliado por interfaces, ferramentas ou procedimentos que garantam a codificação segura do sistema;
II - O sistema deve utilizar camada de persistência segura para acesso ao banco de dados, de modo a evitar ataques contra a integridade, a confidencialidade e a disponibilidade dos dados;
III - Os dados de entrada do sistema devem ser submetidos a validação ou sanitização antes da sua inserção na base de dados;
IV - Os dados de saída do sistema devem ser codificados de forma a garantir a integridade e a confidencialidade das informações, quando seus requisitos assim o requererem;
V - A ocorrência de exceções e erros na execução dos sistemas em ambiente de produção deve ser tratada com a apresentação de mensagens de erro na tela dos usuários que não apresentem códigos ou textos que revelem detalhes técnicos sobre os erros. Tais detalhes devem ser apresentados exclusivamente no registro do evento no *log* do sistema; e
VI - Os sistemas não devem conter senhas, chaves de criptografia, credenciais ou informações pessoais como CPF, nome, *e-mail*, título de eleitor ou outros dados sensíveis diretamente escritos em seus códigos-fonte.
Capítulo V
DO AMBIENTE DE COMPILAÇÃO E IMPLANTAÇÃO DE *SOFTWARE*
Art. 21. Devem ser definidos e documentados procedimentos de compilação de *software* de acordo com as linguagens de programação utilizadas.

§1º A definição do processo de compilação deve ser disponibilizada em um local centralizado e acessível às ferramentas e profissionais envolvidos com o processo de desenvolvimento.
§2º As ferramentas utilizadas no processo de compilação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança por eles recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança disponibilizadas, como *patches*, *hotfixes*, entre outros métodos.
§3º As ferramentas utilizadas no processo de compilação devem prover mecanismos de verificação de integridade dos artefatos gerados (tais como *hashes* ou assinaturas).
§4º Verificações de segurança automatizadas devem ser integradas ao processo de implantação de *software*, tais como a Análise Estática de Código-Fonte (SAST).
§5º Os resultados das verificações de segurança automatizadas deverão compor os critérios de aceitação para a implantação dos sistemas em ambiente de produção.
Art. 22. Todos os componentes e bibliotecas de terceiros utilizados no desenvolvimento de sistemas do TSE devem ser mantidos em repositório centralizado.
§1º Os componentes e bibliotecas de terceiros devem ser submetidos à verificação de vulnerabilidade periodicamente ou sempre que necessária sua avaliação, de preferência de forma automatizada.
§2º Nos casos em que o componente a ser verificado integra sistema classificado como de alta criticidade, a verificação deve incluir uma análise manual detalhada, para a garantia de uma maior eficácia na realização dos testes.
§3º O processo de desenvolvimento de sistemas deve considerar preferencialmente o uso de bibliotecas já existentes e disponíveis no repositório, com o intuito de se reduzir a ocorrência de possíveis riscos no uso de bibliotecas de terceiros que estejam vulneráveis a ataques.
Art. 23. Devem ser definidos e documentados procedimentos de implantação de *software* nos ambientes de desenvolvimento, homologação e produção.
§1º A definição do processo de implantação deve ser disponibilizada em um local centralizado e acessível a ferramentas e profissionais envolvidos com o processo de desenvolvimento.
§2º As ferramentas utilizadas no processo de implantação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança para ela disponibilizadas como *patches*, *hotfixes*, entre outros métodos.
§3º Os procedimentos de implantação devem ser automatizados em todos os estágios, de forma a eliminar a possibilidade de erros em função de sua execução manual.
Art. 24. A realização de testes dinâmicos em aplicações e de testes de intrusão deverá ser feita observando-se a classificação dos sistemas, de acordo com procedimento definido pela unidade responsável pela gestão da segurança de TI do TSE, observando-se também os critérios de grau de sigilo, de criticidade das informações tratadas e o processo de modelagem de ameaças adotado pelo TSE, contando com o apoio de ferramentas especializadas, e deve considerar os seguintes controles:
I - todas as falhas encontradas, bem como as correções e evidências do teste devem ser registradas de forma centralizada e reportadas às equipes responsáveis pelo projeto de desenvolvimento e correção;
II - preferencialmente, deve ser realizada análise de riscos sobre as falhas encontradas e não corrigidas;

III - adicionalmente, na realização de verificação de segurança em aplicações críticas, devem ser realizados testes complementares envolvendo técnicas exploratórias sobre os controles de segurança da aplicação, como metodologia de autenticação, criptografia utilizada, controle de acessos e outros controles de segurança.

Capítulo VI

DA GESTÃO DE IDENTIDADES, AUTENTICAÇÃO E CERTIFICAÇÃO DIGITAL

Art. 25. A autenticação de usuários nos sistemas do Tribunal deve ser realizada por meio de soluções de gestão de identidades e de autenticação padronizadas para o acesso dos usuários aos sistemas, não sendo permitido o armazenamento de quaisquer credenciais advindas de soluções de autenticação distintas das homologadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de *software* da STI, e devem ser observadas, obrigatoriamente, as disposições sobre bases de identificação de usuários e níveis de autenticação contidas na versão mais atualizada da Portaria TSE 454 de 13 de julho de 2021.

§1º As soluções de gestão de identidades e de autenticação devem prever a implementação de controles efetivos de segurança, tais como:

I - uso de duplo fator de autenticação (2FA);

II - suporte à utilização de certificação digital e tokens;

III - funções de identificação de robôs, tais como captcha;

IV - gestão de políticas de senhas;

V - gestão de direitos de acesso; e

VI - registros das atividades (*logs*) de criação, modificação e exclusão de credenciais, bem como de autenticação.

§1º As funcionalidades de autorização de acesso dos usuários aos sistemas devem ser implementadas preferencialmente por meio de perfis de direitos de acesso, em oposição a direitos de acesso atribuídos de forma individual.

§2º Os sistemas que necessitem ser expostos para acesso externo ao TSE, devem possuir controles específicos de segurança no acesso que complementem o uso simples de credenciais baseadas em usuário e senha, tais como o uso obrigatório de duplo fator de autenticação ou o uso de certificação digital.

§3º O Tribunal publicará procedimento divulgando quais são as soluções de gestão de identidades e autenticação homologadas para utilização pelos sistemas e aplicações do Tribunal, indicando os cenários em que podem ser utilizadas.

§4º O procedimento de que trata o parágrafo anterior será revisado com periodicidade mínima anual ou quando houver fato novo que exija sua revisão.

§5º As credenciais de acesso aos bancos de dados e aos sistemas devem possuir direitos de acesso mínimos necessários para suas funções.

Art. 26. Os sistemas expostos externamente ao TSE devem ser disponibilizados por meio de mecanismos que garantam a identidade do sistema, assim como a criptografia do tráfego de informações entre o ambiente do Tribunal e os clientes desses sistemas.

Parágrafo único. Quando utilizados certificados digitais, suas informações devem ser mantidas em repositório seguro controlado, de preferência por meio do uso de solução de gerenciamento centralizada, para fim de gestão de seus ciclos de vida.

Capítulo VII

DOS REGISTROS DE *LOG* DOS SISTEMAS

Art. 27. Os registros de *log* dos sistemas deverão atender às diretrizes estabelecidas no normativo publicado pelo Tribunal (Portaria nº 459/2021).

Art. 28. Os projetos de desenvolvimento dos sistemas devem prever mecanismos para a geração e armazenamento dos *logs*, conforme definições da unidade responsável pela segurança de TI do TSE, sendo necessário que o sistema mantenha uma base de *logs* local, a qual deve prever a sua replicação em base centralizada.

Art. 29. Os sistemas desenvolvidos pelo TSE devem gerar registros sobre sua utilização, com especificação de data e hora da ocorrência em milissegundos, tais como:

I - autenticação de usuários, com sucesso ou falha;

II - alteração de perfil do usuário;

III - erros e exceções sem tratamento nos sistemas;

IV - acesso a dados sensíveis para alteração;

V - acesso a dados sensíveis para leitura;

VI - negação de acesso a páginas ou funções;

VII - usuário autenticado executando a ação;

VIII - nome do servidor do sistema (se aplicável);

IX - IP e número da porta de origem da máquina cliente do sistema (se aplicável);

X - tipo da ação; e

XI - tipo de erro.

Capítulo VIII

DO CICLO DE VIDA DOS SISTEMAS

Art. 30. Deve ser observado o procedimento para manutenção do ciclo de vida dos sistemas desenvolvidos ou de propriedade do TSE, envolvendo a inclusão de regras para o descarte, descontinuação e transição segura de sistemas e base de dados previstas na Política de Segurança da Informação.

§1º Para fins de transparência e obediência à Política de Gestão da Informação do TSE, o descarte deverá estar previsto na Tabela de Temporalidade, seguindo os trâmites internos de gestão documental para o descarte seguro dos dados e documentos, com registro no Sistema Eletrônico de Informações - SEI e publicação de edital de descarte no portal do Tribunal.

§2º Qualquer informação orgânica/arquivística armazenada em sistemas, bancos e bases de dados deverá ser avaliada e autorizada pela Comissão Permanente de Avaliação Documental (CPAD) antes do descarte, conforme a Política de Gestão da Informação e de Documentos.

Art. 31. O procedimento para manutenção do ciclo de vida dos sistemas deve considerar, no mínimo, os seguintes controles:

I - os Sistemas e suas Bases de Dados que foram substituídos ou legados devem ser retirados do ambiente de produção e preservados por meio de procedimento de armazenamento, de acordo com as regras definidas na Portaria nº 457 de 13 de julho de 2021, que institui a Norma de Gerenciamento de *backup* e restauração de dados, salvo por motivação legal ou por determinação da Secretaria de Tecnologia da Informação;

II - as bases de dados de sistemas legados que não mais realizem transações, porém necessitem disponibilizar os seus dados para consulta, devem preferencialmente ser disponibilizadas por meio de soluções de descoberta e disponibilização de dados;

III - os ambientes de desenvolvimento, homologação e testes devem ser desativados quando não mais houver evolução no sistema, quando o sistema for retirado do ambiente de produção ou quando formalmente solicitado pelo gestor do sistema;

IV - as unidades gestoras dos sistemas devem ser consultadas periodicamente quanto à necessidade de manutenção dos sistemas em produção.

Capítulo IX

DO INVENTÁRIO DE SISTEMAS

Art. 32. Todos os sistemas desenvolvidos internamente ou de propriedade do TSE devem ser claramente identificados e inventariados, contendo informações relevantes para o gerenciamento e manutenção da segurança dos dados institucionais.
Art. 33. Todas as informações sobre os ativos de sistema devem ser reunidas de forma integrada, preferencialmente por meio de base de gerência de ativos centralizada.
Art. 34. O detalhamento de informações no inventário sobre cada ativo de sistema deve contemplar, no mínimo e quando aplicável, os seguintes conjuntos de dados:
I - nome do sistema;
II - classificação do sistema;
III - versão atual do sistema;
IV - abrangência de uso;
V - unidade gestora responsável;
VI - unidade técnica responsável;
VII - data inicial de entrada em produção;
VIII - data de desativação;
IX - endereço de acesso ao sistema nos diversos ambientes (desenvolvimento, testes, homologação e produção);
X - arquitetura de referência;
XI - linguagem de codificação utilizada;
XII - integrações com outros sistemas;
XIII - bases de dados utilizadas; e
XIV - servidores e instâncias hospedeiras.
Parágrafo único. O gerenciamento dos ativos de sistemas deve considerar o disposto no processo de gerenciamento de configuração instituído no TSE, em acordo com a Portaria TSE nº 458, de 13 de julho de 2021, que instituiu a Norma de Gestão de Ativos.
Capítulo X
DISPOSIÇÕES FINAIS
Art. 35. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação - CSI deste Tribunal.
Art. 36. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessária ou conveniente para o TSE.
Art. 37. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 38. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 24 (vinte e quatro) meses a contar dessa data.
Art. 39. Fica revogada a Portaria TSE nº 540, de 23 de agosto de 2021.
ROGÉRIO AUGUSTO VIANA GALLORO
Documento assinado eletronicamente em 16/05/2024, às 12:13, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2831710&crc=3B199BB1, informando, caso não preenchido, o código verificador 2831710 e o código CRC 3B199BB1.
2023.00.000003679-0

ÍNDICE DE ADVOGADOS