Anexo

ANEXO I

PORTARIA PRESIDÊNCIA Nº 183/2024 TRE-DF/PR/DG/GDG

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 1º Submetem-se às disposições desta Portaria no que couber, sem prejuízo do contido em outras normas:

I - Membros(as) da Corte e Magistrados(as);

II - Membros(as) do Ministério Público;

III - Servidores(as) do quadro de pessoal, ocupante de cargo efetivo ou não;

IV - Servidores(as) requisitados(as), cedidos(as), removidos(as) ou em lotação provisória no TRE-DF;

V - Estagiários(as);

VI - Prestadores(as) de serviço, colaboradores(as) e fornecedores(as).

Art. 2° Aplicam-se, para os efeitos da Política de Segurança da Informação deste Tribunal, os termos e as definições a seguir elencados, utilizando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República:

I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

II - atividades críticas: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, dano à imagem institucional, prejuízo ao Erário, entre outros;

III - atividades precípuas: conjunto de procedimentos e de tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

IV - ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

V - ativo de processamento: patrimônio composto por todos os elementos de *hardware*, *software* e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;

VI - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

VII - 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;

VIII - confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

IX - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

X - credencial (ou conta de acesso): permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

XI - custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

XII - decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

XIII - diretriz estratégica de nivelamento: determinações, instruções ou indicações a serem observadas na execução da ENTIC-JUD tendo em vista o alcance dos objetivos estratégicos;

XIV - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XV - governança de TIC: conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam assegurar que as decisões e ações relativas à gestão e ao uso de TIC mantenham-se harmoniosas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais;

XVI - 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;

XVII - integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo(a) proprietário(a);

XVIII - irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

XIX - missão: definição de finalidade da área;

XX - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXI - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXII - 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;

XXIII - 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;

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, entre outras propriedades;

XXVI - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter,

processar, armazenar, fazer uso e disseminar informações;

XXVII - usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXVIII - vulnerabilidade: fragilidade de um ativo ou de um grupo de ativos, que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II
DAS DIRETRIZES DE ACESSO

Art. 3º O controle de acesso lógico deverá ser regido pelos seguintes princípios:

I - necessidade de saber: os(as) usuários(as) estabelecidos(as) no art. 1º deverão ter acesso somente às informações necessárias ao desempenho de suas atividades diárias;

II - necessidade de uso: os(as) usuários(as) estabelecidos(as) no art. 1º deverão ter acesso apenas aos ativos (equipamentos de TI, sistemas, aplicações, serviços, dispositivos e procedimentos) necessários ao desempenho de suas atividades e atribuições;

III - privilégio mínimo: deverão ser conferidos apenas os privilégios necessários para que os(as) usuários(as) realizem suas atividades e atribuições; e,

IV - segregação de funções: separação das funções desempenhadas no controle de acesso, como pedido, autorização e administração de acesso, deverão estar segregadas na equipe responsável por essas atribuições e atividades.

Art. 4º O acesso às informações produzidas ou custodiadas pelo TRE-DF, que não sejam de domínio público, deverá ser limitado às atribuições e funções do cargo exercido, necessárias ao desempenho das respectivas atividades dos(as) destinatários(as) desta política, listados no *caput* do art. 1º.

§ 1º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dependerá de prévia autorização formal da chefia imediata e do(a) chefe da(s) área(s) que se pretenda acessar a informação.

§ 2º O acesso às informações produzidas ou custodiadas pelo TRE-DF que não sejam de domínio público, quando autorizado, será condicionado ao aceite de termo de sigilo e de responsabilidade.

Art. 5º Todo(a) usuário(a) deverá possuir credenciais de acesso, pessoais e intransferíveis, qualificando-o(a), inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação, salvo se, comprovadamente, a atividade decorrer de subtração das credenciais.

Art. 6º O(a) usuário(a) deverá receber permissão de acesso aos serviços, respeitando-se o princípio do privilégio mínimo, mediante autorização expedida por superior hierárquico ou setor competente.

§ 1º O(a) usuário(a) será responsável pelos acessos realizados por meio de sua conta, devendo zelar pelo sigilo de sua senha, respondendo por eventuais danos decorrentes do seu uso indevido.

§ 2º As credenciais de acesso poderão ser suspensas, a qualquer momento, caso ocorram tentativas de acesso não autorizado a recursos de tecnologia, ou realização de atividades que apresentem risco à segurança da informação.

Art. 7º Os serviços de tecnologia da informação disponibilizados pelo TRE-DF não deverão ser utilizados para acessar, criar, transmitir, distribuir ou armazenar conteúdo em desrespeito às

leis e regulamentações, especialmente aquelas referentes à prática de crimes.

§ 1º A fim de garantir a segurança cibernética, a Secretaria de Tecnologia da Informação e Comunicação - STIC poderá restringir:

I - os horários de acesso;

II - a geolocalização, por determinação do TSE;

III - os dias específicos ou feriados;

§ 2º A STIC poderá restringir o acesso para garantir a segurança do ambiente, por determinação do CGOVTIC, do TSE ou de Órgão de Controle:

I - em determinados horários;

II - para determinadas geolocalizações;

III - em determinados dias.

CAPÍTULO III
DO ACESSO À REDE CORPORATIVA

Art. 8º O acesso aos serviços disponibilizados no ambiente da rede corporativa do TRE-DF deverá ser previamente autorizado pela chefia imediata dos destinatários desta Política, e serão permanentemente controlados.

Art. 9º A Central de Serviços de TIC (*Service Desk*) disponibilizado pela STIC, deverá ser utilizada em atendimento ao artigo anterior, para solicitação das credenciais de acesso à rede do TRE-DF.

Parágrafo único. As unidades administrativas e os(as)gestores(as) autorizados a solicitar a criação de credenciais de acesso à rede corporativa, aos serviços, sistemas e aplicações serão:

I - Presidência e Corregedoria, para solicitação das credenciais de acesso de Membros(as) da Corte, Magistrados(as), Membros(as) do Ministério Público que estiverem exercendo atividades no TRE-DF;

II - gestores(as) titulares e respectivos(as) substitutos(as) de cada unidade, ou área administrativa responsável por sistema administrativo ou finalístico específico, responsáveis pelas credenciais de acesso a sistemas, aplicações ou serviços que são disponibilizados aos(às) usuários(as) por necessidade do serviço.

Art. 10. Caberá à Secretaria de Tecnologia da Informação e Comunicações - STIC, prover solução para consulta das unidades e gestores(as) especificados no art. 9º, com informações dos(as) usuários(as) do Tribunal, que permitam validar os dados estritamente necessários para autorizar a criação, cadastramento, liberação e definição dos acessos solicitados nos chamados abertos na Central de Serviços de TIC.

Parágrafo único. No repositório, que deverá ser sustentado pela infraestrutura tecnológica da STIC, e mantido e atualizado pela SGP, deverão constar informações necessárias e suficientes para validar que o(a) usuário(a) está vinculado ao TRE-DF, por vínculo funcional, caso se tratar de servidor(a) efetivo(a), cedido(o), requisitado(a), removido(a), como também o seu cargo, sua lotação e demais informações complementares que orientem a definição correta e precisa da credencial e acessos que estes precisarão obter para desenvolver suas atividades laborais.

Art. 11. Visando adequação, atualização e gestão das credenciais e perfis de acesso aos

sistemas, aplicativos, soluções, ferramentas e serviços disponibilizados aos(às) usuários(as) relacionados no art. 1º desta Portaria, as áreas administrativas abaixo relacionadas deverão manter, sob sua administração, as seguintes informações mínimas:

I - STIC:

a) perfil de acesso aos sistemas corporativos e base de dados do TRE-DF sob sua responsabilidade;

b) perfil de acesso remoto (VPN e demais);

c) perfil de acesso a rede *Wi-Fi*;

d) perfil de acesso às pastas compartilhadas internas e na nuvem;

e) credencial comum de acesso a rede (contas sem acesso privilegiado);

f) lista de distribuição de correio eletrônico e grupos de segurança;

g) perfil de acesso aos sistemas com autenticação própria que estejam sob sua gestão (administrativos, finalisticos, etc);

h) perfil de acesso ao Sistema Eletrônico de Informações - SEI;

i) credencial administrativa de acesso a rede (contas com acesso privilegiado);

j) demais informações sob responsabilidade da STIC, que tenham relação com o previsto nesta Portaria.

II - Gestor(a) titular ou substituto(a) de unidade ou macrounidade, ou área administrativa responsável por sistema administrativo ou finalístico específico que não esteja sob gestão das áreas já mencionadas:

a) relação de credenciais, perfis de acesso, níveis de permissão e quantidade de usuários(as) cadastrados(as) nos sistemas sob sua responsabilidade; e

b) demais informações relevantes para gestão das credenciais e perfis de acesso dos sistemas sob sua gestão, e que tenham relação com o previsto nesta Portaria.

Parágrafo único. Caberá às unidades mencionadas no *caput* deste artigo, de posse das informações constantes nos chamados abertos pelas unidades administrativas e gestores especificados no art. 9º, criar as credenciais de acesso solicitadas, com o perfil que assegure a aplicação do privilégio mínimo aos sistemas sob sua gestão, devendo administrar de forma eficiente estas credenciais, tomando como referência sempre o repositório tratado no art. 10.

Art. 12. Todas as credenciais de acesso serão configuradas para expirarem automaticamente, ao término do prazo de vigência do contrato, no retorno do(a) servidor(a) ao órgão de origem ou finalizado seu exercício no tribunal.

Art. 13. Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade justificada, e acompanhada de parecer técnico da STIC acerca da possibilidade de aceitação dos riscos associados.

Art. 14. As senhas vinculadas às credenciais de acesso à rede deverão atender obrigatoriamente aos critérios estabelecidos pelo Comitê de Segurança do TRE-DF.

§ 1º Caberá à STIC implementar autenticação multifator sempre que possível, especialmente nos sistemas, serviços e aplicações mais críticos disponibilizados pelo TRE-DF.

§ 2º A definição da criticidade dos sistemas, serviços e aplicações deverá ser realizada pelas áreas gestoras dos sistemas, com apoio da STIC.

Art. 15. A gestão das credenciais e nível de permissões aos serviços, sistemas e aplicações disponibilizadas na rede corporativa, deverá ser realizada e configurada obrigatoriamente pela área gestora do serviço, sistema ou aplicação, e sempre que necessário, a STIC apoiará e orientará as demais áreas gestoras, no uso das melhores práticas.

Parágrafo único. Todas as ações, operações e procedimentos realizados com as credenciais de acesso fornecidas aos(às) usuários(as) do TRE-DF poderão ser monitorados e armazenados por período determinado, conforme o interesse, prioridade e necessidade em preservar a segurança, integridade, disponibilidade e confidencialidade das informações do Tribunal.

CAPÍTULO IV
DO ACESSO INTERNO AOS COMPARTILHAMENTOS DE REDE

Art. 16. Somente serão criados novos diretórios de rede para atender à necessidade de sistema específico que dependa do mesmo, e estes deverão ser solicitados via Central de Serviços de TIC (*Service Desk*) pelo(a) titular da unidade administrativa, e/ou seu(ua) substituto(a), à STIC, devendo a solicitação conter os(as) usuários(as) que precisam ter acesso, e o nível de acesso que cada um(a) poderá ter aos documentos da unidade solicitante.

§ 1º Cabe, ainda, ao(à) titular das unidades administrativas internas, e/ou seu(ua) substituto(a), informar à STIC, alterações de usuários(as) e as permissões de acesso ao compartilhamento criado, para que a STIC faça os ajustes necessários e mantenha os controles atualizados.

§ 2º Os dados e informações contidos nesses diretórios de redes somente poderão ser acessados a partir da rede interna do Tribunal, e, nesses somente, poderão conter informações corporativas de interesse da instituição.

§ 3º Dados pessoais armazenados nesses diretórios de rede serão excluídos pela equipe da STIC em até 24 (vinte e quatro) horas após a detecção, sem prévia comunicação ao(à) usuário(a) proprietário(a), podendo, ainda, a chefia imediata ser notificada a respeito.

§ 4º Os dados de interesse do Tribunal, e aqueles pessoais relativos ao vínculo do(a) servidor(a) com o TRE, que estejam nesses diretórios de rede, não serão alvo de exclusão, e estarão sujeitos ao procedimento de *backup*, conforme condições, frequência e prazos de retenção estabelecidos na Política de *Backup* do TRE-DF.

CAPÍTULO V
DO ACESSO À REDE SEM FIO

Art. 17. A STIC disponibilizará aos(às) usuários(as) internos(as) e externos(as), redes sem fio, apartadas da rede corporativa do Tribunal, para acesso exclusivo à Internet.

Art. 18. Usuários(as) internos(as) do Tribunal deverão utilizar as mesmas credenciais de acesso à rede corporativa.

Art. 19. Visitantes deverão solicitar credencial para acesso a rede sem fio, via sistema, que, primeiramente, deverá ser autorizada pelo(a) titular e/ou substituto(a) da área administrativa com quem estejam tratando, para que a STIC possa então criar o *voucher* para acesso a rede sem fio.

§ 1º Caberá à unidade promotora do evento solicitar à STIC, via sistema, a criação de credencial de acesso à rede sem fio aos(às) participantes de eventos realizados na sede do TRE-DF.

§ 2º Todas as solicitações de credencial de acesso para visitantes deverão ter validade específica, não podendo ultrapassar 24 (vinte e quatro) horas de validade.

Art. 20. O acesso às redes sem fio poderá ser monitorado eletronicamente e registrado em log pela STIC.

Art. 21. Os meios de acesso à rede sem fio deverão ser, obrigatoriamente, providos e configurados pela equipe responsável da STIC.

Parágrafo único. É vedado o uso de redes *WiFi* desconhecidas (não providas pelo TRE-DF) ou geradas a partir do roteamento de celular próprio ou de terceiros, para conexão das estações de trabalho, salvo se expressamente autorizado pela STIC.

CAPÍTULO VI
DO ACESSO AO SISTEMA DE MENSAGERIA

Art. 22. A STIC disponibilizará os serviços de correio eletrônico, destinados ao uso corporativo, sendo o(a) usuário(a) responsável por todas as mensagens enviadas a partir de sua credencial.

Art. 23. O serviço de mensageria (*e-mail*) de uso corporativo será monitorado pela equipe da STIC do TRE-DF, que poderá acessar conteúdos do(a) usuário(a), mediante autorização prévia da Diretoria-Geral, quando identificado que existe risco à segurança da informação ou à imagem institucional do Tribunal.

§ 1º O acesso autorizado às informações dos(as) usuários(as) deverá ser registrado formalmente, permitindo a realização de auditoria posterior ao procedimento.

§ 2º A autorização a que alude o *caput* deste artigo, deverá ser precedida de manifestação fundamentada do(a) Secretário(a) da STIC, explicitando os motivos, os riscos envolvidos, a imprescindibilidade da medida, bem como a delimitação do escopo e o prazo da ação.

Art. 24. O acesso aos serviços de mensageria (e-mail) e demais ferramentas do pacote de escritório disponível aos(às) usuários(as) do Tribunal será concedido mediante abertura de chamado via Central de Serviços de TIC (Service Desk), aplicando-se a estes a mesma condição estabelecida no art. 23.

CAPÍTULO VII
DO ACESSO AOS SISTEMAS DE INFORMAÇÃO

Art. 25. As credenciais de acesso aos sistemas de informação do TRE-DF serão concedidas e gerenciadas pelos(as) gestores(as) dos respectivos sistemas de informação observada a segregação de funções em todo o fluxo de gestão destes acessos.

§ 1º Para cada sistema, deverá ser fornecido o perfil de acesso que o(a) usuário(a) deverá possuir.

§ 2º A área administrativa gestora da solução será responsável pela criação da credencial, quando for o caso, e pela definição do perfil de acesso que o(a) usuário(a) solicitante deverá ter, observando sempre o princípio do privilégio mínimo, ou seja, a menor permissão possível para que ele realize suas atividades laborais diárias.

Art. 26. A gestão e o inventário das credenciais de acesso e senhas dos(as) usuários(as) deverá ser realizada, mensalmente, pela unidade administrativa gestora de solução, sistema, aplicativo ou

serviço sob sua responsabilidade.

§ 1º Caberá a todas unidades administrativas gestoras de solução, sistemas, aplicativos ou serviços, após consulta ao repositório de informações previsto no art. 10, validar se as credenciais de acesso e perfis em uso pelos(as) usuários(as) estão condizentes com suas lotações e atribuições funcionais.

§ 2º Periodicamente, todas as unidades administrativas gestoras de solução, sistemas, aplicativos ou serviços, após consulta ao repositório de informações previsto no art. 10, farão o bloqueio das credenciais relacionadas sob sua gestão, que não realizarem acesso (*login*) por mais de 90 (noventa) dias consecutivos, incluindo servidores(as) ativos(as) e licenciados(as).

§ 3º Com o intuito de atender ao princípio do privilégio mínimo, os direitos de acesso dos(as) usuários(as) deverão ser revisados, periodicamente, por todas unidades administrativas gestoras de solução, sistemas, aplicativos ou serviços, após consulta ao repositório de informações previsto no art. 10.

CAPÍTULO VIII
DO ACESSO À INTRANET E À INTERNET

Art. 27. O acesso de administração do portal de internet e dos serviços da intranet do TRE-DF serão efetuados, preferencialmente, a partir da rede da Justiça Eleitoral - JE, ou com uso de conexão segura criptografada.

Art. 28. Os acessos a sítios e serviços disponíveis na internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nas soluções de segurança da informação em uso no TRE-DF.

Parágrafo único. A STIC implementará mecanismos para gerenciar o tráfego no acesso a serviços críticos e de maior consumo de dados, visando preservar a disponibilidade da rede, podendo esse tráfego ser monitorado para garantir a segurança dos dados, informações e serviços do Tribunal.

Art. 29. A equipe da STIC fiscalizará o bom uso dos acessos à internet pelos usuários do TRE-DF e fazer os ajustes e restrições de acesso, que se apliquem em caso de mau uso deste recurso, ou, quando for necessário, em casos de período eleitoral, ou em situações de contingência que se apliquem em função da atividade finalística e do serviço jurisdicional prestado.

Parágrafo único. O titular e/ou substituto (a) das unidades administrativas do Tribunal, sempre que observarem o mau uso, deverão reportar à STIC, para que tome a ação devida pelas soluções sob seu controle.

Art. 30. Todos os acessos realizados pelos(as) usuários(as) à intranet ou internet serão monitorados e deverão ser registrados em arquivos, para fins de auditoria em caso de necessidade.

§ 1º O acesso do(a) usuário(a) poderá ser bloqueado, imediatamente, em caso de uso indevido dos recursos, consumo excessivo de tráfego, acesso a conteúdo proibido ou sempre que colocar em risco os dados e as informações da Justiça Eleitoral.

§ 2º Quando o acesso indevido resultar em indícios de prática de crime ou de conduta incompatível com a moralidade pública, a STIC ficará obrigada a reportar o fato, formalmente, em processo sigiloso, à Diretoria Geral.

Art. 31. Não será admitida, em nenhuma hipótese, a tentativa de burla aos filtros de conteúdo e às restrições de acesso impostas, cabendo à STIC reportar ao(à) gestor(a) da área o ocorrido.

§ 1º Não será permitida a utilização de outros meios de conexão à internet ou de outro tipo de rede, a partir de estações de trabalho do Tribunal, seja através de modems 3G ou 4G, de qualquer

outro tipo ou geração de rede móvel existente ou que venha a ser criado, salvo mediante expressa autorização da STIC.

§ 2º A tentativa de burlar os filtros de conteúdo e as restrições de acesso impostas pode configurar descumprimento de dever funcional, cuja apuração, caso determinada, dar-se-á na forma da lei.

CAPÍTULO IX

DOS PRIVILÉGIOS DE ADMINISTRADOR(A)

Art. 32. Será concedida credencial de administrador(a) aos(às) servidores(as) e colaboradores(as) lotados(as) nas unidades da STIC, que realizarem atividades de gestão de sistemas, softwares e aplicativos, observando sempre a aplicação do princípio do privilégio mínimo, ou seja, acesso e permissões restritos absolutamente às atividades necessárias que estes(as) usuários(as) precisarem para desempenhar suas responsabilidades e atividades.

§ 1º O modelo de controle de acesso será preferencialmente fundamentado e baseado em papéis, seguindo o padrão Role-Based Access Control – RBAC.

§ 2º Poderá ser concedida credencial de administrador(a) para servidor(a) ou colaborador(a) lotado(a) em unidade distinta da STIC, desde que seja plenamente justificável e seja autorizada pelo(a) Secretário(a) de TIC.

§ 3º O uso das credenciais com privilégio deverá ser realizado, obrigatoriamente, por meio de solução de PAM (Privileged Access Management), para fazer a gestão segura do uso destas credenciais, salvo impossibilidade devidamente comprovada.

Art. 33. Os privilégios concedidos serão exclusivamente voltados às demandas do TRE-DF, sendo vedada a utilização em desacordo com esta Política ou com o interesse público.

§ 1º O acesso privilegiado aos(às) administradores(as) deverá ser concedido usando credenciais de acesso exclusivas, distintas das credenciais de acesso utilizadas para realização de atividades que não exijam elevação de privilégio.

§ 2º Sempre que possível, as credenciais de acesso privilegiado, de administrador(a), deverão estar dissociadas da ferramenta de gestão de credenciais do serviço de diretórios – AD (*Active Directory Microsoft*), ou outra que vier a lhe substituir.

§ 3º Contas de administrador(a) genéricas devem ser renomeadas e ter sua função apagada, e não deverão ser utilizadas para acesso à internet, iniciar serviços de rede ou acessar arquivos externos.

§ 4º Todas as credenciais de administrador(a) deverão ser monitoradas e as atividades e ações realizadas armazenadas por, pelo menos, 180 (cento e oitenta) dias, para auditoria em caso de necessidade.

Art. 34. Deverá ser realizado e mantido inventário de todas as contas gerenciadas, de usuário(a), de administrador(a), de serviço ou de departamento, devendo conter, no mínimo, informações sobre:

I - data de início e de término;

II - nome do usuário(a);

III - unidade de lotação;

IV - unidade gestora, para contas de serviço;

V - data de revisão realizada no inventário.

§ 1º As contas com privilégio deverão ser revisadas, mensalmente, pelo(a) gestor(a) da unidade que a utiliza, com o objetivo de averiguar se as contas ativas permanecem autorizadas e se as inativas poderão ser desabilitadas.

§ 2º A STIC deverá manter inventário dos sistemas de autenticação internos e daqueles que, porventura, estejam hospedados em provedores em nuvem, remotos.

CAPÍTULO X
DO USO DE EQUIPAMENTO COMPUTACIONAL

Art. 35. O TRE-DF fornecerá para seus(suas) usuários(as) equipamentos de TIC para o desempenho, exclusivamente, de suas atividades laborais.

Art. 36. O uso dos ativos e dos equipamentos de TIC de propriedade do TRE-DF é de responsabilidade do(a) usuário(a), que, como Custodiante, deverá mantê-lo em plena condição de uso, para atender, exclusivamente, ao cumprimento das atribuições de seu cargo/estágio, função pública, contrato de trabalho ou de prestação de serviços, sendo expressamente proibido o uso para fins particulares, inclusive em relação ao conteúdo de documentos, arquivos, trabalhos, mensagens, programas, imagens e sons, incumbindo-lhe:

I - proteger as informações e os ativos de TIC que estejam sob sua responsabilidade ou custódia, de atividades, ações ou procedimentos não autorizados;

II - aplicar às informações e aos ativos de TIC sob sua custódia a proteção e o tratamento adequado, conforme sua classificação de segurança;

III - utilizar os ativos de TIC exclusivamente para realização das atividades vinculadas ao exercício do cargo, estágio ou função exercidos no âmbito do TRE-DF, sendo vedado o uso para fins particulares e/ou estranhos ao interesse público;

IV - utilizar somente os meios de comunicação disponibilizados oficialmente para a troca de informações com outras instituições, observando a classificação que lhes for atribuída;

V - utilizar os equipamentos de TIC com o cuidado que cada aparelho requer visando garantir sua preservação e seu funcionamento adequado;

VI - efetuar a desconexão (logoff) da rede nos casos em que o(a) usuário(a) não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

VII - computadores de mesa (desktops) ou dispositivos móveis (tipo notebooks ou tablets) devem ser desligados ou deixados em modo suspenso sempre que o(a) usuário(a) estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

VIII - desligar, sempre que possível, os ativos de TIC de uso individual ou compartilhado, como computador(es), monitor(es) e impressora(s) ao final do expediente, excetuando-se os equipamentos utilizados para armazenamento, transmissão e comunicação de dados (Firewall, Roteador, Switch);

IX - colaborar na solução de problemas e no aprimoramento dos processos de segurança da informação;

X - bloquear o computador sempre que se ausentar do seu posto de trabalho;

XI - zelar pela integridade e conservação dos ativos de TIC, responsabilizando-se por eventuais danos causados por culpa ou dolo aos equipamentos em seu poder;

XII - informar à chefia imediata e também à STIC, quando identificar violação da integridade física do equipamento utilizado.

Art. 37. A alteração e/ou a manutenção na configuração de qualquer equipamento de propriedade do TRE-DF é uma atribuição exclusiva da STIC.

Art. 38. O bloqueio de tela protegido por senha será ativado, automaticamente, após 10 (dez) minutos de inatividade do computador de mesa ou móvel que estiver sendo utilizado.

Art. 39. Ao final do contrato de trabalho ou desligamento dos(as) usuários(as) definidas no art. 1°, os equipamentos disponibilizados para a execução de atividades profissionais deverão ser devolvidos em funcionamento e estado de conservação adequado.

Art. 40. Qualquer dano aos equipamentos do TRE-DF será devidamente analisado pela STIC e apurado nos termos definidos no Manual de Patrimônio do TRE-DF.

Art. 41. O TRE-DF, quando formalmente solicitado, a seu critério e sem prejuízo do contido no Manual de Patrimônio do TRE-DF, poderá permitir a utilização de equipamento particular ou de terceiro para o desempenho de atividades laborais, nas dependências físicas do Tribunal, devendo este, obrigatoriamente, passar por inspeção da área técnica da STIC, para garantir a adequação necessária aos requisitos e controles de segurança adotados pelo Tribunal e ser identificado, pela unidade de patrimônio, como bem de terceiro.

§ 1º A utilização dos ativos de TIC de terceiros, ou sua conexão à rede corporativa cabeada ou sem fio (*WiFi*) é, terminantemente proibida, exceto se for previamente, analisada e aprovada pela equipe responsável da STIC.

§ 2º O uso dos ativos de TIC da rede corporativa está restrito aos(às) usuários(as) previamente autorizados(as), devendo seu uso ser limitado às atribuições necessárias ao desempenho de suas respectivas atividades.

§ 3º Em hipótese alguma, o TRE-DF se responsabilizará pela guarda, conservação ou por danos sofridos por bens de terceiros utilizados em suas dependências.

§ 4º A utilização de equipamentos de TI sem prévia autorização e vistoria constitui ilícito funcional e, em se tratando de colaboradores(as), de irregularidade contratual a ser comunicada para Contratada.

CAPÍTULO XI

DO ARMAZENAMENTO E COMPARTILHAMENTO REMOTO (NUVEM)

Art. 42. O TRE-DF disponibilizará para os(às) usuários(as) espaço para armazenamento e compartilhamento remoto de arquivos na nuvem, através de solução de comunicação e colaboração corporativa.

§ 1º Cabe à(ao) titular de unidade administrativa e/ou seu(ua) substituto(a) solicitar à STIC a disponibilização de acesso para usuário(a) de sua unidade, à solução de comunicação e colaboração corporativa.

§ 2º É de responsabilidade de cada usuário(a) administrar seu armazenamento e compartilhamento de dados em nuvem, as informações nele armazenadas, além das permissões e dos usuários(as) que poderão ter acesso aos dados, à luz da legislação vigente relacionada.

§ 3º Cabe à(ao) titular das unidades administrativas internas e/ou seu(ua) substituto(a), criar os espaços de trabalho virtuais para compartilhamento de dados, informações e documentos de sua unidade, troca de mensagens via chat, bem como para realizar reuniões com a equipe na solução de

colaboração em nuvem.

§ 4º O(a) titular das unidades administrativas será responsável pela definição dos(das) integrantes que farão parte dos espaços de trabalho criados, das permissões e privilégios de acesso aos documentos criados e compartilhados nestes espaços.

§ 5º As permissões e privilégios de acesso mencionados no parágrafo anterior deverão ser sempre as estritamente necessárias para que os(as) usuários(as) possam realizar suas atividades laborais diárias.

§ 6º Cabe, ainda, à(ao) titular das unidades administrativas internas e/ou seu(a) substituto(a) manter atualizados os(as) usuários(as) e suas permissões de acesso ao armazenamento e compartilhamento de sua unidade administrativa, para preservar o acesso aos dados e às informações a somente quem realmente deva ter acesso.

§ 7º Não é permitido o uso de qualquer outra solução de armazenamento na nuvem para armazenamento de documentos e/ou informações relacionadas ao TRE-DF, que não seja oficialmente adotada e homologada pelo Tribunal.

§ 8º Não será permitido o compartilhamento do espaço corporativo para armazenamento remoto de arquivos na nuvem com usuários(as) externos(as) ou fora do domínio da Justiça Eleitoral.

§ 9º A STIC realizará inspeções periódicas nas configurações de acesso para validar, identificar e remover os arquivos que não tenham relação com as atividades desempenhadas pelas unidades organizacionais, podendo a chefia imediata ser notificada a respeito.

§ 10º Caberá à STIC apoiar as unidades administrativas internas, no que couber, quanto ao uso da solução de colaboração em nuvem, em cumprimento ao estabelecido na presente norma, e estas, por sua vez, poderão contar com o apoio das demais áreas administrativas do Tribunal quando necessário.

CAPÍTULO XII
DA IDENTIFICAÇÃO DIGITAL

Art. 43. O TRE-DF poderá, a seu critério exclusivo, fornecer certificados digitais para usuários(as) em execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes gerais:

I - cabe exclusivamente ao(à) usuário(a) a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao usuário;

II - o(a) usuário(a) deverá informar à STIC sobre qualquer evento ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital, abrindo uma requisição de serviço na Central de Serviços de TIC (*Service Desk*).

CAPÍTULO XIII
DOS EQUIPAMENTOS DE IMPRESSÃO

Art. 44. O uso de equipamentos de impressão deverá ser feito, exclusivamente, para a impressão/reprodução de documentos que sejam de interesse do TRE-DF.

Art. 45. Ao imprimir documento considerado confidencial ou restrito, o(a) usuário(a) deve adotar as cautelas devidas para que a impressão não seja fonte de publicidade indevida.

Art. 46. O uso dos equipamentos será monitorado, mensalmente, e um resumo da

utilização será encaminhado a todos(as) usuários(as) e aos(às) titulares de cada unidade.

CAPÍTULO XIV
DA SEGURANÇA FÍSICA EM TIC

Art. 47. As instalações de processamento das informações do TRE-DF serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

Art. 48. O(a) usuário(a) deverá observar as seguintes disposições específicas quanto à segurança física:

I - crachás de identificação, inclusive temporários, são pessoais e intransferíveis, não sendo, sob nenhuma circunstância, permitido o seu compartilhamento;

II - os(as) colaboradores(as) devem portar crachás de identificação que exibam claramente seu nome e fotografia, na forma dos normativos internos do Tribunal;

III - excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

IV - é proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizados a áreas sensíveis do TRE-DF;

V - é resguardado ao TRE-DF o direito de monitorar seus ambientes físicos, sendo utilizado, para tanto, sistema de circuito fechado de televisão em áreas comuns, com armazenamento das imagens obtidas por, pelo menos, 90 (noventa) dias, e protegidas contra qualquer tipo de manipulação indevida;

VI - os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, cabendo ao(à) usuário(a), ao se ausentar, o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados pelo órgão;

VII - não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.

CAPÍTULO XV
DA DEVOLUÇÃO DOS ATIVOS

Art. 49. Ao realizar a devolução dos ativos/dispositivos de TIC, o(a) usuário(a) deverá:

I - apagar todas as informações de cunho particular que, porventura, neles estejam armazenadas;

II - transferir para os servidores de compartilhamento de arquivos, dados e informações externas na nuvem, todas as informações de cunho profissional que neles estejam armazenadas;

III - restituir no mesmo estado de conservação recebido e em pleno funcionamento.

Art. 50. O Tribunal não se responsabilizará por quaisquer informações de cunho particular que o(a) usuário(a) tenha deixado nos ativos/dispositivos de TIC após sua devolução.

Parágrafo único. O(a) usuário(a) deverá utilizar os servidores de compartilhamento de arquivos, dados e informações externos, na nuvem, como repositório principal de informações e documentos relacionados com o trabalho desempenhado, não devendo, nenhum arquivo, dado ou informação de trabalho, ser armazenado localmente na máquina utilizada pelos(as) usuários(as).

CAPÍTULO XVI
DAS PROIBIÇÕES

Art. 51. São consideradas ações indevidas nos ativos de TIC da rede corporativa:

I - instalar software, de sua propriedade ou de terceiros, sem prévia aprovação da Seção de Apoio ao Usuário - SEAPU, o qual poderá ser removido sem prévia comunicação ao(à) usuário(a);

II - alterar configurações de hardware e software, sem prévia aprovação da SEAPU, os quais poderão ser reconfigurados de acordo com o padrão estabelecido, sem prévia comunicação ao(à) usuário(a);

III - remover lacres ou proteções similares, atribuição exclusiva da SEAPU;

IV - remanejar ativos de TIC da rede corporativa, tais como desktops e impressoras, sem autorização da SEAPU;

V - expor os ativos de TIC a fatores de risco, tais como choques, interferências elétricas ou magnéticas, líquidos (corrosivos ou não), ou a outras ações que possam provocar danos físicos.

Art. 52. Salvo quando a execução das atividades funcionais justificarem a sua prática ou dela dependerem, serão considerados usos indevidos dos ativos de TIC da rede corporativa:

I - armazenar arquivos particulares nos servidores de arquivos disponibilizados na rede corporativa, tais como músicas, fotos, vídeos e documentos;

II - realizar download, cópia, transferência ou compartilhamento de arquivos que infrinjam a legislação vigente referente à proteção da propriedade intelectual (direitos autorais, inclusive de software, e patentes);

III - realizar download, cópia, transferência ou compartilhamento de arquivos que sejam considerados como possíveis portadores de códigos maliciosos ou que coloquem em risco as instalações e os ativos de TIC da rede corporativa;

IV - realizar download, cópia, transferência ou compartilhamento de material obsceno, preconceituoso, discriminatório, difamatório, político ou ideológico, que promova incitação à violência ou instrua a invasão da rede corporativa ou de redes externas, além de outros contrários à legislação e à regulamentação em vigor;

V - realizar download, cópia, transferência ou compartilhamento de arquivos da rede corporativa ou de seus(suas) usuários(as), programas de computador ou procedimentos, instruções de operação ou de controle e listas de endereços de correio eletrônico, sem a devida autorização do(a) responsável ou que vise a fins particulares ou lucrativos;

VI - manter, divulgar ou utilizar mensagens eletrônicas que suscitem dúvidas quanto à potencialidade de afetar de forma negativa a rede corporativa, quer seja pela contaminação por códigos maliciosos, por vírus de computador ou por quaisquer outros meios, principalmente as que apresentem, entre outros, remetente ou links desconhecidos, no corpo da mensagem ou anexos, com extensões que possam conter códigos maliciosos;

VII - acessar sítios com conteúdos que não coadunem com conduta compatível com a moralidade administrativa, inclusive os de pornografia, de pedofilia, de incitação à violência ou ao preconceito, de venda de drogas, de pirataria ou que divulguem número de série para registro de software e outros contrários à legislação;

VIII - executar atividades relacionadas a jogos eletrônicos, conteúdo multimídia, mídias sociais ou ferramentas de relacionamento com fins lucrativos, ideológicos ou recreativos;

IX - atacar ou, sem autorização, monitorar ou acessar os ativos de TIC da rede corporativa ou de redes externas, utilizando quaisquer meios;

X - configurar o compartilhamento de pastas e arquivos armazenados em estações de trabalho e dispositivos móveis;

XI - utilizar processo criptográfico não autorizado pela STIC em arquivos residentes nos ativos de TIC da rede corporativa;

XII - realizar todo e qualquer procedimento no uso dos ativos de TIC da rede corporativa não previsto nesta norma que possa afetar de forma negativa o Tribunal ou seus(suas) colaboradores(as).

Art. 53. Os arquivos e materiais de que tratam os incisos I a IV do art. 52 desta Portaria poderão ser apagados sem prévia comunicação ao(à) usuário(a).

Art. 54. É vedada a solicitação de suporte técnico à STIC para orientação ou resolução de problemas referente à utilização de recursos de TIC para fins particulares.

CAPÍTULO XVII
DO MONITORAMENTO

Art. 55. O uso dos ativos de TIC da rede corporativa estará sujeito a monitoramento pelo Tribunal, com vistas a proteger a integridade da imagem e das informações institucionais, preservar a segurança de seus sistemas corporativos ou de seus(suas) usuários(as) e, também, para fins de apuração de eventual prática indevida, ilegal ou não autorizada, podendo auditar, dentre outros, os objetos e eventos abaixo relacionados:

I - informações recebidas e transmitidas, criptografadas ou não;

II - arquivos residentes nos ativos de TIC e afins;

III - programas de computador (softwares), inclusive em execução;

IV - bases específicas de registros de eventos (logs);

V - acessos realizados a sítios ou serviços na rede corporativa e na internet.

Art. 56. O monitoramento ostensivo ou eventual nos ativos de TIC da rede corporativa poderá ser usado para fins de segurança e controle disciplinar, quando for o caso, por determinação do(a) Diretor(a)-Geral e/ou da CSI.

CAPÍTULO XVIII
DO DESLIGAMENTO DOS(AS) USUÁRIOS(AS)

Art. 57. É obrigatório à STIC manter atualizada a solução de consulta de informações definida no art. 10, para que todas as áreas administrativas e gestores(as) de sistemas, aplicações e serviços façam o devido acompanhamento e gestão das credenciais dos(as) usuários(as) que tenham afastamentos e licenças superiores a 30 (trinta) dias, para que seja feita, se for o caso, a suspensão da credencial (login e senha) e/ou o ajuste de novo perfil de acesso ao(à) usuário(a) nos sistemas, aplicativos e serviços.

Parágrafo único. A STIC e demais áreas administrativas e gestores(as) de sistemas, aplicações e serviços, adotarão os procedimentos definidos no Capitulo III desta Portaria, para dar prosseguimento às ações mencionadas no caput.

Art. 58. É proibida a utilização de credenciais do TRE-DF de qualquer usuário(a) de TIC após o seu desligamento.

Art. 59. Os equipamentos disponibilizados para a execução de atividades profissionais deverão ser devolvidos no mesmo estado de conservação quando do desligamento ou término da relação do(a) usuário(a) com o TRE-DF.

Art. 60. O(a) usuário(a) desligado(a) ou em processo de desligamento, terá o certificado digital expedido pelo TRE-DF imediatamente revogado.

CAPÍTULO XIX
DA POLÍTICA DE SENHAS

Art. 61. Os sistemas, aplicações ou serviços de informação passíveis de controle de acesso deverão ter seu acesso restrito e controlado através do uso de senhas, tokens ou mecanismo similar de autenticação, quando for o caso.

§ 1º Sempre que possível, o acesso remoto à rede, o acesso interno e o acesso às aplicações expostas externamente, na internet, deverão se dar por autenticação multifator (MFA).

§ 2º A implementação de autenticação multifator (MFA) é obrigatória para todos os sistemas, serviços e aplicações que tenham a funcionalidade habilitada, sendo prioritária para aqueles mais críticos.

Art. 62. As senhas de acesso, tokens e outros fatores de autenticação que sejam utilizados na rede do Tribunal, serão de uso pessoal e intransferível.

Art. 63. As senhas deverão ser secretas e definidas considerando as seguintes recomendações:

I - utilizar números, letras maiúsculas e minúsculas, e caracteres especiais, conter, no mínimo, 12 (doze) caracteres e, sempre que possível, utilizar autenticação multifator (MFA);

II - não utilizar frases ou palavras que possam facilmente ser adivinhadas por terceiros baseadas nas informações relativas ao próprio(a) usuário(a), como nome de parentes, datas de aniversário e números de telefones;

III - não utilizar as mesmas credenciais para fins pessoais, para acesso a contas de serviço pessoais.

Art. 64. Sempre que houver indicação de possível comprometimento de alguma senha, o(a) usuário(a) deverá realizar sua alteração e comunicar o ocorrido ou a suspeita de comprometimento à STIC pelo serviço de atendimento ao usuário.

Art. 65. O sistema que gerencia as senhas dos(as) usuários(as) deverá:

I - permitir que usuários(as) modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II - forçar a mudança das senhas em intervalos regulares de, no máximo, 3 (três) meses para contas comuns, e, mensalmente, para contas de administrador(a);

III - manter registro das últimas 5 (cinco) senhas anteriores utilizadas e bloquear a reutilização;

IV - empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

V - garantir a alteração das senhas temporárias no primeiro acesso ao sistema ou serviço de informação;

VI - manter, para fins de auditoria, registro dos acessos, das operações realizadas e dos respectivos períodos, por, pelo menos, 180 (cento e oitenta) dias;

VII - desabilitar todas as contas que não tenham usuários(as) associados(as) ou processos de negócio;

VIII - monitorar tentativas de acesso a todas as contas, inclusive às contas desativadas, quando viável.

CAPÍTULO XX
DO ACESSO AOS EQUIPAMENTOS À REDE E AOS SERVIÇOS DE REDE

Art. 66. O acesso de novo equipamento à rede deverá ser regulado por procedimento de autorização específico, através de abertura de chamado de requisição de serviço via Central de Serviços de TIC (Service Desk).

Art. 67. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do Tribunal, sem autorização prévia da STIC.

Art. 68. Havendo necessidade de inclusão de equipamento de terceiro na rede interna cabeada do Tribunal, este deverá estar em sub-rede segura, ou VLAN específica para este tipo de uso, distinta das demais redes e VLANs internas e por período definido.

Art. 69. Será exigido múltiplo fator de autenticação (MFA), nos acessos externos realizados pela VPN, ou outra forma de acesso externo a rede interna do TRE-DF.

Art. 70. Os serviços de rede e as portas dos equipamentos de rede que não estiverem em uso deverão ser removidos ou desativados logicamente.

CAPÍTULO XXI
DAS DISPOSIÇÕES FINAIS

Art. 71. Durante o período de realização de eleições, a STIC poderá restringir a utilização e os acessos a quaisquer recursos de TIC, visando assegurar proteção necessária para manter o ambiente, a rede, os sistemas, aplicações e serviços internos seguros objetivando garantir o pleno atendimento às eleições, com a comunicação prévia às unidades diretamente impactadas.

Art. 72. O descumprimento desta PARTIC será objeto de apuração pela unidade competente do Tribunal, podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos(às) envolvidos(às) contraditório e a ampla defesa.

Art. 73. É de responsabilidade dos(as) usuários(as) do TRE-DF e da STIC, cumprir e fazer cumprir todas as diretrizes previstas nesta política.

Art. 74. Caberá aos(às) gestores(as) de contratos continuados com alocação de mão de obra, e, no caso dos(as) estagiários(as), aos(às) supervisores(as) de estágio, dar conhecimento do inteiro teor dessa norma aos(às) respectivos(as) usuários(as).

Andrey Bernardes Pousa Correa

Secretário STIC

Documento assinado eletronicamente por **ANDREY BERNARDES POUSA CORREA**, **Secretário**, em 30/07/2024, às 17:03, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-df.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1655218** e o código CRC **B4748BC2**.
