TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
GABINETE DA PRESIDÊNCIA

PORTARIA N.° 233/2023 – GP

Estabelece a Política de Uso Aceitável dos Recursos de Tecnologia da Informação na Justiça Eleitoral.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO o § 6º do artigo 37 da Constituição Federal, que dispõe sobre a responsabilidade civil objetiva atribuída aos entes estatais;

CONSIDERANDO a necessidade de adequação à Lei Geral de Proteção de Dados (Lei nº 13.709/2018);

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 Resolução nº 23.644/2021 do TSE, que dispõe sobre a Política de Segurança da Informação (PSI), no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

CONSIDERANDO o disposto na Resolução TSE nº 23.387/2012, que dispõe sobre o uso da rede corporativa de comunicação de dados na Justiça Eleitoral;

CONSIDERANDO o disposto na Portaria TSE nº 456/2021, que dispõe sobre o uso aceitável de ativos de TI;

CONSIDERANDO as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO/IEC 27001:2013 e 27002:2013 que estabelecem, respectivamente, o sistema de gestão e o código de boas práticas em segurança da informação que recomendam o estabelecimento de regras para o uso aceitável dos ativos de informação;

CONSIDERANDO que as informações são armazenadas e veiculadas por diferentes formas, incluindo os recursos de Tecnologia da Informação, e são essenciais ao desempenho das atribuições no âmbito da Justiça Eleitoral;

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 Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

Art. 1º As diretrizes para o controle de acesso e uso aceitável dos recursos de Tecnologia da Informação, no âmbito do Tribunal, bem como os direitos e as responsabilidades dos usuários desses recursos, observarão as disposições contidas nesta portaria.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta norma, entende-se por:

I - acesso remoto: toda conexão estabelecida com a rede do TSE ou Tribunais Eleitorais originada de um ponto externo, fora das dependências do Tribunal ou de suas unidades administrativas;

II - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a instituição;

III - *antimalware*: programas informáticos desenvolvidos para prevenir, detectar e eliminar *malware* de computador;

IV - *antispam*: serviço de detecção e análise que tem como objetivo bloquear o recebimento de spam;

V - ativos de informação e comunicação: são os meios de armazenamento, de transmissão e de processamento, bem como os sistemas de informação, as instalações e as pessoas que a elas têm acesso;

VI - autenticidade: garantia de veracidade da fonte de informações, por meio da qual é possível confirmar a identidade das pessoas ou entidades que prestam a informação;

VII - *backup*: é uma cópia de segurança de dados;

VIII - código malicioso (*malware*): termo comumente utilizado para, genericamente, se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel, cujos tipos específicos são vírus, *worm, bot, spyware, backdoor*, cavalo de troia e *rootkit*;

IX - confidencialidade: garantia de que a informação esteja acessível somente a pessoas autorizadas;

X - conta de usuário: também conhecido como credenciais de acesso, é o conjunto de atributos (lógicos ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação. Ex: *login* e senha, certificado digital e senha, características biométricas etc;

XI - credenciais de acesso: permissões concedidas por autoridade competente, que habilita determinada pessoa, sistema ou organização ao acesso à informação ou recurso. A credencial pode ser física ou lógica para identificação de usuários;

XII - diretório compartilhado ou área compartilhada: espaço de armazenamento e compartilhamento de informações de um grupo de usuários específico na rede do Tribunal;

XIII - diretório pessoal ou área privativa: área reservada para armazenamento e compartilhamento de informações de um usuário interno, incluindo seu e-mail;

XIV - disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a utilizá-las;

XV - estação de trabalho: conjunto de hardware e software fornecido ao usuário para que este possa executar suas atribuições;

XVI - firewall: é um dispositivo, podendo existir na forma de software ou hardware, que possui a função de filtrar o tráfego nocivo recebido e impedir que esses dados sejam propagados;

XVII - geolocalização: o recurso tecnológico que permite localizar qualquer objeto ou pessoa, por meio da sua posição geográfica, detectada automaticamente por um sistema de coordenadas.

XVIII - HTTP (*Hypertext Transfer Protocol*) é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. E e é a base para a comunicação de dados da *World Wide Web*. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

XIX - HTTPS: é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

XX - integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais;

XXI - IPTV: é um método de transmissão de sinais televisivos por meio de redes IP;

XXII - *phishing*: técnica de fraude utilizada por criminosos para roubar senhas de banco e demais informações pessoais, usando-as posteriormente de maneira fraudulenta;

XXIII - princípio do menor privilégio: premissa de fornecer as permissões necessárias e suficientes para que um usuário possa realizar suas atividades, por um tempo limitado e com os direitos mínimos necessários para as suas tarefas;

XXIV - PAM (*Privileged Access Management*): O Gerenciamento de Acesso Privilegiado é formado por um conjunto de estratégias e tecnologias de segurança cibernética para exercer controle sobre o acesso privilegiado e permissões para usuários, contas, processos e sistemas em um ambiente tecnológico;

XXV - *proxy* externo: são servidores não administrados pelo TSE ou pelo Tribunal Eleitoral, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que os *proxies* administrados pelo TSE ou Tribunais Eleitorais;

XXVI - *proxy*: servidor responsável por intermediar o acesso à internet, aplicando as regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede;

XXVII - Rede Corporativa de Comunicação de Dados da Justiça Eleitoral (RCJE): o conjunto formado pelos segmentos da Rede Nacional, da Rede Regional do Tribunal Superior Eleitoral, dos Tribunais Regionais Eleitorais, dos Cartórios Eleitorais e de suas Redes Locais;

XXVIII - rede de computadores: também conhecida por rede corporativa, é o conjunto de computadores, funcionalidades e outros dispositivos, de

propriedade do Tribunal, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

XXIX - risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

XXX - servidor de arquivos: equipamento disponibilizado para acesso dos usuários da rede com o intuito de armazenar todos os documentos e mídias de cunho institucional;

XXXI - site (ou sítio): conjunto de páginas web organizadas e acessíveis a partir de um URL da rede interna (Intranet) ou da Internet;

XXXII - softwares de mensagens instantâneas: são programas e os serviços de comunicações on-line que possibilitem a troca de mensagens textuais ou audiovisuais de forma imediata entre duas ou mais pessoas;

XXXIII - *spam*: prática de envio em massa de e-mails não solicitados;

XXXIV - teletrabalho: modalidade de trabalho realizado, em parte ou em sua totalidade, fora das dependências deste Tribunal, com a utilização de infraestrutura e recursos tecnológicos do usuário ou da instituição;

XXXV - URL: sigla correspondente às palavras inglesas "*Uniform Resource Locator*", traduzidas para o português como "Localizador Uniforme de Recursos". Trata-se da indicação do endereço de um recurso de informática disponível em uma rede, seja ela a Internet ou a Intranet de uma organização;

XXXVI - usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador da Justiça Eleitoral que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal;

XXXVII - usuário externo: servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas no âmbito da Justiça Eleitoral e que não se enquadre nas definições contidas nos incisos XXXVI e XXXVIII deste artigo;

XXXVIII - usuário interno: autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo órgão;

XXXIX - verificação em duas etapas: também conhecido como autenticação de dois fatores ou duplo fator de autenticação (2FA), é um recurso de segurança disponível que fornece uma camada extra de autenticação de usuário exigindo que os usuários forneçam informação extra para confirmar sua identificação;

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

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º Esta norma tem como princípio norteador a garantia da segurança, integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação e comunicação.

CAPÍTULO III
DO ESCOPO

Art. 4º O objetivo deste normativo é estabelecer diretrizes para o uso dos recursos de tecnologia da informação e comunicação, visando à preservação dos recursos sob a responsabilidade do Tribunal, respeitando os princípios norteadores definidos no art. 3º desta norma.

Art. 5º Este normativo se aplica a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizam os ativos de informação e comunicação da Justiça Eleitoral.

Parágrafo único. Todos são corresponsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir esta Portaria.

CAPÍTULO IV
DAS DISPOSIÇÕES GERAIS

Art. 6º Respeitado o disposto na Lei Federal nº 9.609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade do Tribunal os programas desenvolvidos, para os fins institucionais, pelos usuários elencados no art. 5º.

Art. 7º O acesso aos recursos de tecnologia da informação e comunicação podem ser restringidos a horários definidos pela STIE para garantir a segurança cibernética do órgão.

Art. 8º A STIE poderá restringir, para garantir a segurança cibernética:

I – os horários de acesso;

II – a geolocalização, por determinação do TSE; e

III – os dias específicos ou feriados.

Art. 9º Os recursos de TI disponibilizados aos usuários destinam-se à execução de atividades da Justiça Eleitoral ou a elas diretamente correlatas.

§ 1º A utilização dos recursos de TI será monitorada, podendo ser objeto de auditoria.

§ 2º O uso indevido dos recursos de TI é passível de sanção disciplinar, na forma da lei.

Art. 10. Os recursos de TI não deverão ser utilizados para acessar, criar, transmitir, distribuir ou armazenar conteúdo em desrespeito às leis e regulamentações, especialmente aqueles referentes aos crimes cibernéticos, contra a pessoa, contra os costumes, à ética e à decência.

CAPÍTULO V
DAS ESTAÇÕES DE TRABALHO

Art. 11. Todo servidor da Justiça Eleitoral terá, em seu posto de trabalho, acesso a uma estação de trabalho destinada à execução de atividades da Justiça Eleitoral ou a elas diretamente correlatas.

Parágrafo único. Aos estagiários e aos terceirizados será disponibilizado, quando possível e pertinente, acesso a uma estação de trabalho.

Art. 12. As estações de trabalho possuirão configurações de hardware e software padronizadas pela STIE, de acordo com a necessidade de utilização dos usuários e deverão atender, no mínimo, aos seguintes requisitos de segurança:

I - O sistema operacional deve possuir suporte ativo para recebimento, automático, de atualizações de segurança, devidamente configurados pela STIE;

II - Deverão possuir software antimalware instalado, ativado, permanentemente atualizado e configurado para realizar verificação automática das mídias removíveis;

III - Todos os softwares instalados deverão ser configurados pela STIE para receber atualização de forma automática, exceto quando a atualização for tecnicamente inviável;

IV - A reprodução automática de mídias removíveis, nas estações de trabalho, deve estar desativada pela STIE.

V - As configurações de segurança das estações de trabalho dos usuários serão definidas pela STIE.

Art. 13. As estações de trabalho receberão softwares homologados e licenciados pela STIE conforme a necessidade de cada usuário e a disponibilidade de licenças.

Art. 14. A critério da STIE, poderão ser desabilitados dispositivos de hardware e software nativos dos equipamentos, a fim de preservar a segurança e a integridade da rede de comunicação de dados.

Art. 15. Não é permitido o compartilhamento de pastas de arquivos locais na rede sem a anuência da STIE.

Art. 16. É dever do usuário bloquear a sua estação de trabalho sempre que se ausentar do seu posto de trabalho.

Parágrafo único. As estações de trabalho devem ser configuradas pela STIE para ter bloqueio automático de tela em casos de período de inatividade e, para restaurar a sessão, o usuário deverá ser obrigado a fornecer novamente suas credenciais de acesso.

Art. 17. Compete ao usuário zelar pela integridade e conservação dos ativos de TI, responsabilizando-se por eventuais danos causados aos equipamentos em seu poder.

§ 1º É vedada a abertura das estações de trabalho por pessoal não autorizado pela STIE.

§ 2º O usuário deve informar à STIE quando identificar violação da integridade física do equipamento por ele utilizado.

§ 3º Será considerado uso indevido por parte dos usuários, permitir pessoas estranhas aos quadros da Justiça Eleitoral ter acesso aos equipamentos e/ou recursos de TI do Tribunal.

Art. 18. É vedado aos usuários:

I - Instalar, por conta própria, quaisquer tipos de software nas estações de trabalho, ficando facultada à STIE a verificação, de forma presencial ou remota, e a desinstalação, sem necessidade de comunicação prévia.

II - Alterar quaisquer configurações de hardware ou software nas estações de trabalho sem a autorização e orientação da STIE.

Art. 19. É vedado à STIE conceder aos usuários privilégios de administrador local nas estações de trabalho, salvo em casos excepcionais, mediante justificativa do titular da unidade.

Parágrafo único. Comprovada a necessidade prevista no caput, a STIE deverá criar uma outra conta de rede para o usuário, que deverá ser utilizada

apenas para a instalação ou desinstalação de sistemas, não sendo permitido o uso comum do usuário de forma a atender ao princípio do menor privilégio.

Art. 20. Sempre que for necessário um novo serviço ou software provido pela área de TI e não disponível na estação de trabalho, o usuário deverá, com a anuência do superior imediato solicitar a STIE, no canal de atendimento de requisições de serviços sua instalação ou acesso com a finalidade de uso e justificativa fundamentada, condicionado o atendimento do pedido à disponibilidade de licença.

Parágrafo único. Quando um software ou serviço não for mais útil para o desempenho das atividades institucionais, o usuário deverá solicitar à STIE a desinstalação do mesmo.

Art. 21 As unidades do Tribunal devem, obrigatoriamente, submeter à prévia análise da Secretaria de Tecnologia da Informação e Eleições a intenção em adquirir ou instalar software, equipamento ou serviço que não tenha sido provido pela área de TI e que faça uso ou requeira recursos de tecnologia da informação e comunicação.

Parágrafo único. A STIE poderá aprovar ou vetá-las por questões de segurança ou falta de compatibilidade ou de padronização com as soluções já adotadas.

Art. 22. Poderão ser disponibilizadas máquinas virtuais quando houver necessidade de acesso a mais do que um ambiente, ou em casos especiais a serem analisados pela STIE.

CAPÍTULO VI
DA REDE CORPORATIVA

Art. 23. A STIE poderá fazer uso de ferramentas, softwares e procedimentos que venham garantir a segurança da rede corporativa do Tribunal e dos dados que nela trafegam.

Parágrafo único. Equipamentos que forem identificados como potencialmente nocivos à rede de dados do tribunal, seja por contaminação por vírus ou por outro tipo de anomalia, poderão ser postos em quarentena sem aviso prévio ao usuário, somente saindo dessa condição após a devida análise da situação pela STIE.

Art. 24 Somente os servidores indicados pela STIE têm permissão de adicionar, configurar ou retirar dispositivos de comunicação da rede corporativa do tribunal.

Art. 25. Todos os pontos de rede sem uso serão desativados pela equipe técnica da STIE, sendo reativados quando necessários, por meio de solicitação a STIE, no canal de atendimento de requisições de serviços.

Art. 26. É proibida a conexão de qualquer dispositivo não fornecido pelo tribunal em qualquer ativo que compõe a infraestrutura de rede do Tribunal, salvo em redes preparadas pela STIE para essa finalidade mediante a orientação e anuência da STIE.

§ 1º A conexão de qualquer equipamento à rede corporativa do tribunal será feita pela STI, ou por terceiros por ela autorizados.

§ 2º Em situações excepcionais será admitido o uso de equipamentos particulares para acesso à rede corporativa de forma local ou remota, mediante permissão e orientação da STIE, ficando neste caso o acesso condicionado ao atendimento de requisitos de segurança estabelecidos em procedimentos definidos pela STIE.

Art. 27. Os pontos de acesso sem fio conectados à rede corporativa deverão ser registrados e aprovados pela STIE.

Parágrafo único. É vedado o uso de pontos de acesso particulares de comunicação de dados sem fio.

Art. 28. As conexões a rede sem fio poderão ser avaliadas pela STIE em relação aos requisitos de segurança e deverão atender ao princípio do menor privilégio.

Art. 29. Os dispositivos conectados à rede corporativa por meio de conexão sem fio deverão utilizar as configurações estabelecidas pela STIE.

CAPÍTULO VII
DO ARMAZENAMENTO DE ARQUIVOS

Art. 30. Cada unidade do Tribunal poderá ter disponível área de armazenamento em rede (diretório compartilhado), de tamanho limitado, para salvaguardar os arquivos relacionados ao trabalho desenvolvido que será disponibilizado em estrutura interna ou por meio de solução de nuvem disponibilizada pelo TRE/RN.

§ 1º Esses arquivos serão acessíveis apenas internamente, a partir da rede do Tribunal.

§ 2º As informações corporativas de interesse do Tribunal serão armazenadas nesses diretórios.

§ 3º Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas no caput, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

Art. 31. O usuário deverá garantir que em sua estação de trabalho não permaneçam armazenados dados pessoais.

Parágrafo único. As informações de dados pessoais deverão ser apagadas das estações de trabalho e dispositivos de armazenamento após efetiva apresentação ao Tribunal a fim de garantir os requisitos de privacidade previstos na LGPD.

Art. 32. O Tribunal se reserva ao direito de inspecionar, sem a necessidade de aviso prévio, os computadores e arquivos armazenados, que estejam no disco local dos computadores, nas áreas privativas ou nas áreas compartilhadas da rede visando assegurar o cumprimento desta norma.

Art. 33. É vedado armazenar arquivos não relacionados com as atividades institucionais nas unidades de rede.

§ 1º Os arquivos de uso pessoal, armazenados no drive de rede corporativo, poderão ser excluídos pela STIE, sem prévia comunicação ao usuário proprietário.

§ 2º Consideram-se arquivos de uso pessoal músicas, filmes, fotografias,

entre outros, de propriedade particular do usuário.

§ 3º Os arquivos previstos no parágrafo anterior, se armazenados em disco local, não estarão sujeitos ao procedimento de backup pela STIE e poderão não estar mais disponíveis quando o equipamento for encaminhado para manutenção ou na realização de procedimento de segurança ou de clonagem com imagem padrão quando das atualizações das estações.

Art. 34. A STIE deve definir parâmetros para armazenamento de arquivos nos servidores de arquivo, incluindo requisitos como tamanho máximo e tipos de arquivos permitidos, com vistas a não comprometer o desempenho e a segurança dos serviços de TI.

Art. 35. A STIE pode estabelecer uma política de arquivamento de forma que apenas arquivos em uso ou recentes estejam armazenados nos servidores, sendo o material de necessidade histórica ou de uso para auditoria armazenado em meio óptico ou magnético.

Art. 36. É vedada a utilização de serviços em nuvem de caráter particular para o processamento ou armazenamento de informações de propriedade da Justiça Eleitoral.

§ 1º Constatada a ocorrência descrita no caput, a responsabilidade quanto à confidencialidade, integridade, disponibilidade e autenticidade de tais informações recairá, com exclusividade, sobre o usuário.

§ 2º O incidente de segurança da informação no Tribunal resultante da violação ao disposto neste artigo sujeitará o usuário responsável às penalidades cabíveis.

CAPÍTULO VIII
DO ACESSO REMOTO

Seção
Do Acesso Remoto para Suporte Técnico

Art. 37. O acesso remoto para suporte técnico aos equipamentos de informática do Tribunal tem por finalidade diminuir a necessidade do deslocamento do técnico do seu local de trabalho para onde estão instalados os equipamentos.

Art. 38. O acesso remoto às estações de trabalho somente será efetuado a partir de equipamentos de propriedade do Tribunal com o intuito de prestar suporte e promover a solução de problemas registrados formalmente pelo usuário.

§ 1º As estações de trabalho devem ser configuradas para permitir acesso remoto apenas para as pessoas que possuem o direito de prestar o suporte técnico remoto e se a solicitação for originada de endereço de rede permitido para fazer o acesso remoto.

§ 2º Em situações excepcionais será admitido o uso de equipamentos particulares para suporte técnico, com orientação e anuência da STIE, ficando neste caso o acesso remoto para suporte técnico condicionado ao atendimento dos requisitos de segurança estabelecidos pela STIE.

Art. 39 A liberação de acesso remoto às estações de trabalho se dará mediante ferramenta homologada pela STIE e de autorização expressa por

parte do usuário.

Parágrafo único. Sempre que possível o usuário deverá acompanhar as sessões de acesso remoto.

Art. 40 À pessoa que realizar o acesso remoto, para fins de suporte técnico, é vedado:

I - Acessar sem finalidade específica de prestar suporte, na forma regulamentada por esta norma;

II - Visualizar conteúdo contido no equipamento por curiosidade ou má fé;

III - Alterar ou adulterar conteúdo de equipamento do Tribunal sem autorização da STIE;

IV - Obter cópia de conteúdos, protegidos ou não, sem autorização;

V - Copiar softwares licenciados para o Tribunal ou licença de uso dos mesmos sem autorização da STIE;

VI - Sabotar ou interromper intencionalmente o funcionamento de serviço ou sistema dentro de equipamento do Tribunal;

VII - Qualquer ação que comprometa a segurança da rede de computadores da Justiça Eleitoral ou do equipamento acessado ou das informações nelas disponíveis.

Parágrafo único. O acesso remoto sem autorização expressa do usuário será realizado somente em regime de exceção, mediante autorização da STIE.

Seção II
Do Acesso Remoto a Recursos de TI publicados na Internet

Art. 41. A Secretaria de Tecnologia da Informação e Eleições STIE disponibilizará aplicações e serviços na internet e o acesso remoto à rede corporativa do Tribunal, conforme regras específicas e características técnicas de cada serviço.

Art. 42. As aplicações e serviços web do Tribunal que forem disponibilizados na internet poderão exigir autenticação de dois fatores.

Art. 43. O Tribunal não se responsabilizará pela infraestrutura tecnológica necessária para o acesso a recursos de TI publicados na internet, sendo responsabilidade de cada usuário propiciar esse meio de acesso.

Art. 44 Os usuários poderão fazer uso do acesso remoto, por meio de solução homologada pela STIE.

Parágrafo único. Por questão de segurança, o acesso remoto deverá exigir autenticação de dois fatores.

Art. 45. Equipamentos particulares não poderão fazer acesso remoto aos recursos de TI do Tribunal, salvo em casos excepcionais mediante a orientação e anuência da STIE, ficando neste caso o acesso remoto condicionado ao atendimento dos requisitos de segurança estabelecidos pela STIE.

Art. 46. O acesso remoto a rede do Tribunal não poderá ser realizado a partir de computadores de uso público.

Art. 47 A instalação e a configuração de certificados e aplicativos necessários para uso do acesso remoto serão realizadas por técnicos

autorizados pela STIE.

Art. 48. Os equipamentos fornecidos pelo Tribunal para acesso remoto à rede corporativa somente devem ser utilizados para atividades da Justiça Eleitoral ou a elas diretamente correlatas.

Art. 49. A STIE poderá solicitar aos servidores que receberam equipamentos para acesso remoto que realizem, em intervalos de tempo regulares, procedimentos de manutenção de segurança no equipamento ou que tragam o equipamento ao Tribunal para manutenção de segurança.

Art. 50. O suporte técnico para o acesso remoto pela internet aos recursos de TI do Tribunal estará disponível durante o horário de expediente.

Parágrafo único. Nos casos em que o acesso remoto seja autorizado a ser feito pelo equipamento pessoal do servidor, a STIE está desobrigada a prestar suporte técnico para problemas de hardware ou softwares do equipamento pessoal do servidor.

Art. 51. O usuário, quando utilizar o acesso remoto, deverá permanecer conectado apenas enquanto estiver efetivamente utilizando os serviços disponibilizados, devendo desconectar-se nas interrupções e no término do trabalho.

Art. 52. O acesso remoto poderá ser interrompido a qualquer momento, independente de comunicação ao usuário, na hipótese de ser identificada situação de grave ameaça ou alto risco à integridade da rede interna e dos serviços disponíveis.

Art. 53. O extravio do equipamento ou certificado utilizados para acesso remoto deverá ser imediatamente comunicado à STIE.

Art. 54. Fica vedada a utilização de outros aplicativos de acesso remoto sem o conhecimento e autorização expressa da STIE.

CAPÍTULO IX
DOS SERVIÇOS DE COMUNICAÇÃO

Art. 55. Para fins desta norma, serviços de comunicação englobam correio eletrônico, mensagens instantâneas, listas de e-mail, serviços de videochamada e a infraestrutura de telefonia.

Art. 56. Os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo.

Art. 57 É vedada o cadastramento de endereço de correio eletrônico institucional em sites para fazer login em:

I - Lojas virtuais, listas de discussões, fóruns;

II - Sites externos ao Poder Judiciário ;

III - qualquer outra finalidade que não seja do interesse público.

Parágrafo único. O disposto no caput não se aplica aos casos em que seja justificada a necessidade para o desempenho das atividades funcionais.

Art. 58. Os usuários são corresponsáveis pela segurança das informações da Justiça Eleitoral, devendo excluir mensagens recebidas cujo conteúdo suscite dúvidas quanto à potencialidade de prejudicá-la em sua integridade, confiabilidade e disponibilidade seja por meio de contaminação por códigos maliciosos ou vírus de computador, seja por quaisquer outros meios, principalmente os que apresentem as seguintes características, dentre outras:

I - remetente desconhecido ou suspeito;

II - links desconhecidos no corpo da mensagem; e

III - anexos com extensões suspeitas.

Parágrafo único. Nos casos previstos no caput, é recomendado o envio do *email* para a equipe da ETIR realizar bloqueio do remetente ou do domínio do *email*.

Art. 59. O correio eletrônico deve registrar os envios e recebimentos de mensagens, de modo a identificar minimamente os remetentes e destinatários.

Art. 60. O uso do correio eletrônico será monitorado por meio de ferramentas *antispam* com o intuito de impedir o recebimento de *spam*, *phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio.

Art. 61. A STIE poderá implementar mecanismos para coibir o uso indevido dos serviços de comunicação.

Art. 62. O uso dos serviços de comunicação pelos usuários colaboradores dependerá de solicitação do titular da unidade à qual esteja vinculado.

CAPÍTULO X
DO ACESSO À INTERNET

Art. 63. Serão liberados na rede corporativa, independentemente de solicitação, acesso aos conteúdos de sites governamentais (por exemplo: domínios .jus.br, .leg.br, .mp.br, .gov.br, .edu.br), além de outros sites necessários à execução de atividades de trabalho.

Art. 64. Serão bloqueados, para todos os usuários e em todos os meios de acesso, os sites ou serviços com conteúdo ilegal, ou que possam comprometer a segurança da informação ou degradar os links de Internet do tribunal, tais como:

I - *sites* de pornografia, pedofilia, pirataria de software, violência, jogos online, apostas, drogas, *phishing*, *spyware* e similares;

II - serviços de transmissão de sinais televisivos como *IPTV* e similares;

III - serviços de compartilhamento de arquivos como *Torrent*, *Emule* e similares;

IV - serviços de acesso remoto como *TeamViewer* e similiares;

V - *sites* de comunidades sociais como *Facebook*, *Twitter*, *Instagram* e similares;

VI - *sites* de compartilhamento de vídeos como o *Youtube*, *Vimeo* e similares;

VII - *softwares* para capturar informações trafegadas pela rede

corporativa.

§ 1º Excetuam-se da proibição constante dos incisos III ao VI aquelas definidas como ferramentas de trabalho pelo Tribunal e devidamente homologadas pela Secretaria de Tecnologia da Informação.

§ 2º O acesso a *sites*, serviços e softwares constantes dos incisos III ao VI poderá ser concedido, mediante avaliação da STIE, às unidades que, devido à natureza peculiar do serviço, possuam a necessidade do acesso para o desempenho das atribuições funcionais da unidade.

Art. 65. O acesso à Internet será controlado, de forma automática, por ferramenta de filtro de conteúdo, configurada de acordo com os termos desta norma.

Parágrafo único. A liberação, por tempo determinado ou indeterminado, de acesso a sítios eletrônicos e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação à STIE, no canal de atendimento de requisições de serviços.

Art. 66. A critério da STIE, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à Internet, seja em situações normais de funcionamento, seja nos períodos críticos do calendário eleitoral ou em situações de contingência, tais como:

I - bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios eletrônicos e serviços; e

II - limitação de banda de tráfego de dados.

Art. 67. O acesso do usuário 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 a segurança da informação na rede de computadores da Justiça Eleitoral.

Art. 68. O acesso à Internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela STIE.

§ 1º É expressamente proibido o uso de proxies externos ou similares e tunelamento HTTP ou HTTPS.

§ 2º É proibido o uso de programas ou tecnologias que burlem as restrições administrativas dos sistemas de segurança ou que possibilitem navegar anonimamente na Internet.

§ 3º 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 por meio de modems 3G ou 4G ou de qualquer outro tipo existente ou que venha a ser criado, salvo mediante expressa autorização da STIE.

§ 4º É proibido o uso concomitante da rede cabeada com a rede sem fio, em estações de trabalho que contenham adaptadores, de forma a burlar os controles de acesso implementados pela STIE.

§ 5º Apenas será permitido o acesso a redes sem fio ofertadas pelo Tribunal, sendo vedado o uso de redes desconhecidas ou geradas a partir de roteamento do celular próprio ou de terceiros, salvo mediante expressa autorização da STIE.

§ 6º É proibido a contratação de serviços de internet diretamente por cartórios ou outras unidades organizacionais, salvo por consentimento expresso da STIE.

Art. 69. Constitui acesso indevido à Internet qualquer das seguintes

ações:

I - acesso à Internet utilizando conta de outros usuários;

II - o compartilhamento de informações sigilosas ou protegidas por lei;

III - acessar ou fazer download de arquivos não relacionados ao trabalho, em especial, músicas, imagens, vídeos, jogos e programas de qualquer tipo; e

IV - acessar sítios eletrônicos que representem ameaça de segurança ou que possam comprometer, de alguma forma, a integridade da rede de computadores do Tribunal.

CAPÍTULO XI
DOS MEIOS DE IMPRESSÃO

Art. 70. Os recursos de impressão pertencentes a este Tribunal, disponíveis para o usuário, serão utilizados em atividades estritamente relacionadas as suas funções institucionais.

Art. 71. Sempre que possível, o compartilhamento de documentos deve ser priorizado evitando o uso desnecessário de insumos.

Art. 72. Os meios de impressão sempre que possível, devem ser compartilhados por mais de uma unidade, visando a economicidade dos recursos e as recomendações de sustentabilidade.

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 73. Os casos omissos serão resolvidos pela Diretoria-Geral, subsidiada pela Comissão Permanente de Segurança da Informação deste Tribunal.

Art. 74. A revisão deste normativo de uso de recursos de tecnologia da informação e comunicação relativo à Segurança da Informação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

Art. 75 O descumprimento desta política será objeto de apuração pela unidade competente do Tribunal e consequente aplicação das penalidades cabíveis a caca caso.

Art. 76. Esta portaria entra em vigor na data de sua publicação.

Natal/RN, 12 de dezembro de 2023.

Desembargador **Cornélio Alves**
Presidente