Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

INSTRUÇÃO NORMATIVA DG TRE-RJ Nº 08, DE 03 DE AGOSTO DE 2023.

Estabelece a Norma de Uso Aceitável de Recursos de Tecnologia da Informação.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso de suas atribuições conferidas pelo **art. 9º, I, da Resolução TRE/RJ n.º 1.266 de 31 de janeiro de 2023 (Regulamento Administrativo do Tribunal Regional Eleitoral do Rio de Janeiro) (https://www.tre-rj.jus.br/legislacao/regulamento-administrativo-do-tribunal-regional-eleitoral-do-rio-de-janeiro)**,

CONSIDERANDO o disposto na **Resolução CNJ nº 396, de 7 de junho de 2021 (https://atos.cnj.jus.br/atos/detalhar/3975)**, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o disposto na **Resolução TSE nº 23.644, de 1º de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**, que instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO o disposto na **Resolução TSE nº 23.387, de 4 de outubro de 2012 (https://www.tse.jus.br/legislacao/compilada/res/2012/resolucao-no-23-387-de-4-de-outubro-de-2012)**, que dispõe sobre o uso da rede corporativa de comunicação de dados na Justiça Eleitoral;

CONSIDERANDO as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO IEC 27001:2022 e 27002:2022;

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 de Janeiro; e

CONSIDERANDO, ainda, o teor do processo SEI n.º 2023.0.000007641-1,

RESOLVE:

Art. 1° As regras para o uso aceitável dos recursos de Tecnologia da Informação no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro ficam instituídas por meio desta Instrução Normativa.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2° Para efeitos desta norma aplicam-se os termos e definições conceituados na **Portaria TSE n.º 444, de 8 de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-444-de-08-de-julho-de-2021)**, além dos seguintes:

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

II - ativos de Tecnologia da Informação: 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;

III - conta de usuário: 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.;

IV - pasta compartilhada: espaço de armazenamento e compartilhamento de informações de um grupo de usuários específico na rede do Tribunal;

V - área ou pasta pessoal: espaço de armazenamento e compartilhamento de informações de um usuário interno;

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

VII - firewall: é um dispositivo de segurança, podendo existir na forma de software ou hardware, que possui a função de monitorar o tráfego de rede de entrada e saída, podendo permitir tráfegos específicos e bloquear tráfego considerado nocivo, além de acessos indevidos de acordo com regras de segurança definidas;

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

IX - HTTP (Hypertext Transfer Protocol ou Protocolo de Transferência de Hipertexto em português) é um protocolo que especifica como será a comunicação entre um navegador e um servidor web. Hipertexto é o texto estruturado que utiliza ligações lógicas (links) entre nós contendo texto;

X - 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;

XI - malware (ou código malicioso): software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades como e-mail, sites ou mídias removíveis. Entre os exemplos de malware estão os vírus, worms, cavalos de Troia, spyware, adware e rootkits;

XII - phishing: técnica de fraude utilizada por criminosos para enganar usuários e roubar credenciais de acesso e demais informações pessoais;

XIII - princípio do privilégio mínimo: 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;

XIV - proxy: servidor responsável por intermediar o acesso à internet, aplicando as regras de controle para impedir acesso indevido a endereços IP e URLs fraudulentos, de baixa reputação ou não relacionados ao trabalho cotidiano, bem como implementar mecanismos de proteção contra códigos maliciosos, controlar a alocação de recursos de rede e armazenar conteúdo (cache), ajudando a melhorar significativamente o desempenho;

XV - 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;

XVI - rede corporativa: é o conjunto ativos de hardwares e softwares (sistemas, computadores, impressoras, switches, roteadores e outros dispositivos), de propriedade do Tribunal, que, ligados em uma rede de comunicação de dados, possibilitam a comunicação entre os dispositivos e o compartilhamento de recursos;

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

XVIII - 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 disponível em uma rede, seja ela a internet ou a intranet de uma organização;

XIX - site (ou sítio): conjunto de páginas organizadas e acessíveis a partir de um endereço (URL) da rede interna (intranet) ou da internet;

XX - 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;

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

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

XXIII - tunelamento: técnica que consiste em encapsular protocolos de comunicação, podendo também ser utilizada para burlar as restrições da rede no acesso a sites ou conteúdos não permitidos.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3° Esta norma tem como princípio norteador a garantia da confidencialidade, integridade e disponibilidade dos ativos de tecnologia da informação do Tribunal Regional Eleitoral do Rio de Janeiro.

CAPÍTULO III

DO OBJETIVO E DO ÂMBITO DE APLICAÇÃO

Art. 4° O objetivo deste normativo é estabelecer diretrizes para o uso dos recursos de tecnologia da informação, visando à preservação dos recursos sob a responsabilidade do Tribunal e respeitando o princípio norteador definido no art. 3°.

Art. 5° Este normativo se aplica a todas as magistradas e magistrados, servidoras e servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiárias e estagiários, prestadoras e prestadores de serviço, colaboradoras e colaboradores, bem como usuárias e usuários externos que utilizam os ativos de tecnologia da informação do TRE-RJ.

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

CAPÍTULO IV

DAS DISPOSIÇÕES GERAIS

Art. 6º Os ativos de TI da rede corporativa são para uso restrito de usuários autorizados.

Art. 7º O uso dos ativos de TI é de responsabilidade do usuário e deve manter afinidade exclusiva com a execução de atividades da Justiça Eleitoral ou a elas diretamente correlatas, desempenhadas nos limites dos princípios da ética, moralidade, razoabilidade e legalidade, inclusive em relação ao conteúdo de documentos, arquivos, trabalhos, mensagens, programas, imagens e sons, incumbindo-lhe:

I - proteger as informações e os ativos de TI que estejam sob sua responsabilidade ou custódia de atividades não autorizadas;

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

III - bloquear o acesso à seção dos ativos de TI sempre que se ausentar dela;

IV - efetuar fechamento (logoff) da conta de acesso ao final do uso;

V - desligar, sempre que possível, os ativos de TI ao final do expediente;

VI - colaborar na solução de problemas e no aprimoramento dos processos de segurança da informação.

Art. 8º Todos os usuários dos ativos de TI são responsáveis por:

I - criar senha segura para sua conta de acesso, segundo as orientações da Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico do TRE-RJ;

II - manter a confidencialidade das informações de sua conta de acesso e não compartilhá-las, em nenhuma hipótese, com outras pessoas;

III - não anotar senhas em papéis, arquivos ou dispositivos móveis;

IV - criar estratégia de memorização para as credenciais de acesso (usuário e senha) de contas mais críticas e não salvá-las em navegadores de internet;

V - alterar a senha de sua conta de acesso conforme periodicidade e nível de complexidade definidos ou sempre que suspeitar de falha ou risco que possa comprometer a confidencialidade das suas credenciais.

Art. 9º A conta de acesso aos sistemas ou serviços de informação e aos ativos de TI da rede corporativa é pessoal e intransferível, qualificando o usuário, inequivocamente, como responsável por quaisquer acessos e ações realizados com as suas credenciais, bem como pelos possíveis danos decorrentes de uso indevido.

Art. 10. O uso dos ativos de TI da rede corporativa está sujeito a monitoramento pelo Tribunal, sem necessidade de aviso prévio, com vistas a proteger a integridade da imagem e das informações institucionais, preservar a segurança de seus sistemas corporativos ou de seus usuários e, também, para fins de apuração de eventual prática indevida, ilegal ou não autorizada, podendo examinar, entre outros, os objetos e eventos abaixo relacionados:

I - informações recebidas e transmitidas, criptografadas ou não;

II - arquivos armazenados nos ativos de TI 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. 11. Salvo quando a execução das atividades funcionais justificarem a sua prática ou dela dependerem, são considerados usos indevidos dos ativos de TI da rede corporativa:

I - acessar, armazenar, realizar download, cópia, transferência ou compartilhamento de:

a) conteúdos não relacionados ao trabalho, como músicas, imagens, vídeos e programas de qualquer tipo;

b) arquivos que infrinjam a legislação referente à proteção da propriedade intelectual (direitos autorais, inclusive de software, e patentes);

c) arquivos que sejam considerados como possíveis portadores de códigos maliciosos ou que coloquem em risco as instalações e os ativos de TI da rede corporativa;

d) material obsceno, preconceituoso, discriminatório, difamatório ou que promova incitação à violência ou instrua à invasão da rede corporativa ou de redes externas, além de outros atos contrários à moralidade administrativa, à legislação e à regulamentação em vigor;

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

III - manter, divulgar ou utilizar mensagens eletrônicas que possam afetar negativamente a rede corporativa, 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 que possam conter códigos maliciosos;

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

V - expor a risco, atacar ou, sem autorização, monitorar ou acessar os ativos de TI da rede corporativa ou de redes externas, utilizando quaisquer meios;

VI - utilizar processo criptográfico não autorizado pela STI em arquivos residentes nos ativos de TI da rede corporativa, para evitar que arquivos de uso corporativo fiquem inacessíveis;

VII - realizar todo e qualquer procedimento no uso dos ativos de TI da rede corporativa não previsto nesta norma que possa afetar de forma negativa o Tribunal ou seus usuários.

Parágrafo único. Os arquivos e materiais de que tratam o inciso I deste artigo poderão ser apagados sem prévia comunicação ao usuário.

Art. 12. Respeitado o disposto na **Lei Federal n° 9.609/1998 (https://www.planalto.gov.br/ccivil_03/leis/l9609.htm)**, 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 internos e prestadores de serviço externo, assim como as obras intelectuais, artísticas ou científicas produzidas em razão de vínculo contratual ou laboral.

CAPÍTULO V

DAS ESTAÇÕES DE TRABALHO

Art. 13. As estações de trabalho serão padronizadas pela STI (hardware e software) de acordo com a necessidade de utilização dos usuários e deverão atender, no mínimo, aos seguintes requisitos de segurança:

I - o sistema operacional deve permitir suporte ativo para recebimento automático de atualizações de segurança, devidamente configurado pela STI;

II. deverão contar com software antimalware instalado, ativado, permanentemente atualizado e configurado para realizar verificação automática das mídias removíveis;

III. os softwares instalados deverão ser configurados pela STI para receber atualização de forma automática, sempre que possível;

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

Art. 14. As estações de trabalho receberão softwares homologados e licenciados pela STI, conforme a necessidade de cada usuário e a disponibilidade de licenças.

Parágrafo único. A STI deverá manter listagem de softwares homologados que podem ser utilizados nas estações de trabalho, sendo vedada a utilização de quaisquer outros.

Art. 15. Não é permitido criar novos compartilhamentos de pastas de arquivos locais na sua própria estação de trabalho, além daqueles padronizados já existentes, criados pela STI.

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 STI 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, em caso de dolo ou culpa.

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

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

§ 3° Será considerado uso indevido por parte dos usuários permitir a pessoas não autorizadas o acesso aos equipamentos ou outros recursos de TI do Tribunal.

Art. 18. É vedado aos usuários:

I - instalar, por conta própria, quaisquer tipos de software ou hardware nas estações de trabalho, ficando facultada à STI 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 STI;

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

IV - remanejar ativos de TI da rede corporativa, tais como desktops e impressoras, sem autorização da STI.

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

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, encaminhando a anuência do superior imediato, solicitar à STI, na Central de Serviços de TI, sua instalação ou acesso com a finalidade de uso e justificativa fundamentada, condicionado o atendimento do pedido ao uso do software para execução das atividades da unidade e à disponibilidade de licença.

Art. 21. Quando um software ou serviço não for mais útil para o desempenho das atividades institucionais, o usuário deverá solicitar à STI a desinstalação.

CAPÍTULO VI

DA REDE CORPORATIVA

Art. 22. A STI 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 malware 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 STI.

Art. 23. Somente pessoas indicadas pela STI têm permissão de adicionar, configurar ou retirar dispositivos de comunicação da rede corporativa do Tribunal.

Art. 24. Todos os pontos de rede sem uso poderão ser desativados pela equipe técnica da STI, sendo reativados quando necessário, por solicitação dirigida à Central de Serviços de TI.

Art. 25. É proibida a conexão de qualquer dispositivo não fornecido pelo Tribunal em qualquer ativo que componha a infraestrutura de rede do Tribunal, salvo em redes preparadas pela STI para essa finalidade mediante a orientação e anuência da STI.

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

§ 2° 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 STI, ficando neste caso o acesso condicionado ao atendimento de requisitos de segurança.

Art. 26. Os dispositivos conectados à rede corporativa através de conexão sem fio deverão utilizar as configurações estabelecidas pela STI.

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

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

Art. 28. As conexões à rede sem fio serão avaliadas pela STI em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

CAPÍTULO VII

DO ARMAZENAMENTO DE ARQUIVOS

Art. 29. Cada unidade do Tribunal poderá ter disponível área de armazenamento na rede interna (diretório compartilhado), de tamanho limitado, para salvaguardar os arquivos relacionados ao trabalho, com garantia de integridade, disponibilidade e cópia de segurança.

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

§ 2° Havendo disponibilidade, as informações corporativas de interesse do Tribunal serão armazenadas nos diretórios referidos no caput.

§ 3° Os dados armazenados nas estações de trabalho dos usuários (pastas locais) 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. 30. Arquivos que contenham informações corporativas devem ser armazenados dentro do ambiente computacional do Tribunal, evitando-se o armazenamento, por exemplo, em ambientes de internet não corporativos, em computadores particulares ou em dispositivos externos, como mídias removíveis, sobretudo quando se tratar de informações de caráter sigiloso ou de dados pessoais sensíveis.

Parágrafo único. Informações de caráter sigiloso, dados pessoais, dados pessoais financeiros ou bancários e dados de crianças e adolescentes inadvertidamente armazenados fora do ambiente corporativo devem ser prontamente removidos e, quando necessários, armazenados em pastas ou espaços de compartilhamento de arquivo oficiais do Tribunal.

Art. 31. Informações e documentos que comprovem atividades do Tribunal, ou seja, aqueles que possuam natureza arquivística, devem ser transferidos, com a devida certidão, para sistemas oficiais do Tribunal, como o SEI e o PJe.

Art. 32. Exceto quando expressamente autorizado pela Diretoria-Geral, após ouvida a Assessoria de Segurança da Informação, é vedada a utilização de serviços em nuvem de caráter particular para o processamento ou armazenamento de informações de propriedade da Justiça Eleitoral.

Art. 33. A STI 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.

CAPÍTULO VIII

DO ACESSO REMOTO

Art. 34. A Secretária de Tecnologia da Informação disponibilizará aplicações e serviços na internet e o acesso remoto à rede corporativa do Tribunal, conforme regras específicas e características técnicas de cada serviço.

§ 1º Os meios tecnológicos a serem utilizados para a realização do acesso remoto deverão ser aqueles homologados pela STI.

§ 2º A concessão dos direitos de acesso remoto deverá respeitar a disponibilidade de recursos, incluídas as licenças de uso das soluções homologadas e fornecidas pela STI, e a capacidade dos meios de comunicação de dados e de outros elementos de infraestrutura necessários ao provimento do acesso.

§ 3° As permissões concedidas aos usuários para acesso remoto deverão atender ao princípio do privilégio mínimo, de forma que sejam disponibilizados para o usuário apenas os serviços que forem estritamente necessários ao desenvolvimento de suas tarefas.

Art. 35. Os ativos de TI utilizados para fins institucionais, fora da rede corporativa do Tribunal, devem seguir o mesmo padrão de segurança empregado internamente.

Art. 36. O acesso remoto à rede do Tribunal não deverá ser realizado a partir de computadores de uso público ou por meio de redes sem fio públicas.

Art. 37. A STI poderá solicitar aos usuários que receberam equipamentos para acesso remoto que realizem, em intervalos regulares, procedimentos de manutenção de segurança no equipamento ou que tragam o equipamento ao Tribunal para manutenção de segurança.

Art. 38. 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. 39. 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. 40. O acesso remoto poderá ser recusado a qualquer momento, independente de comunicação ao usuário, na hipótese de ser identificada a conexão de dispositivo que não possua nível de segurança adequado para acesso à rede.

Art. 41. O extravio do equipamento ou certificado utilizados para acesso remoto deverá ser imediatamente comunicado à STI.

Art. 42. Fica vedada a utilização de outros aplicativos de acesso remoto sem o conhecimento e autorização expressa da STI.

CAPÍTULO IX

DOS SERVIÇOS DE COMUNICAÇÃO

Art. 43. 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. 44. Os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo.

Art. 45. É vedado o cadastramento do endereço de correio eletrônico institucional em sites externos para:

I - cadastramento em lojas virtuais, empresas prestadoras de serviço, listas de discussões, fóruns;

II - como credencial de acesso a sites externos; ou

III - qualquer outra finalidade que não seja de interesse da instituição.

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

Art. 46. Os usuários são corresponsáveis pela segurança das informações da Justiça Eleitoral, devendo encaminhar para a ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética) do TRE-RJ mensagens recebidas cujo conteúdo suscite dúvidas quanto à potencialidade de causar prejuízo à confidencialidade, integridade e disponibilidade dos ativos de TI, seja através de contaminação por códigos maliciosos ou vírus de computador, seja por quaisquer outros meios, principalmente as mensagens que apresentem, entre outras, as seguintes características:

I - remetente desconhecido ou suspeito;

II - links desconhecidos no corpo da mensagem;

III - anexos com extensões suspeitas.

Art. 47. A STI poderá implementar mecanismos para coibir o uso indevido dos serviços de comunicação.

CAPÍTULO X

DO ACESSO À INTERNET

Art. 48. 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, violência, jogos on-line, apostas, drogas ilícitas, 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 similares;

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;

VIII - outros serviços não incluídos nos incisos acima, mas com potencial para prejudicar o desempenho da rede ou ameaçar a segurança cibernética.

§ 1° 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.

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

Art. 49. 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 STI, na Central de Serviços de TI.

Art. 50. A critério da STI, poderão ser adotadas medidas visando à 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.

Art. 51. 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. 52. O acesso à internet a partir da rede local corporativa dar-se-á, exclusivamente, pelos meios configurados e disponibilizados pela STI.

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

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

§ 3° 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, 4G, 5G ou de qualquer outro tipo existente ou que venha a ser criado, salvo mediante expressa autorização da STI.

§ 4° 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 STI.

Art. 53. Dispositivos móveis pertencentes ao Tribunal não devem ser conectados à internet por intermédio de redes sem fio públicas, desconhecidas ou inseguras.

Art. 54. Constitui uso indevido o acesso à internet utilizando conta de outros usuários.

CAPÍTULO XI

DA DEVOLUÇÃO DOS ATIVOS

Art. 55. Sem prejuízo de disposições contidas em orientações específicas, ao realizar a devolução dos ativos de TI, o usuário deverá:

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

II - transferir para pastas ou espaço de compartilhamento de arquivos oficiais do Tribunal todas as informações de cunho profissional que neles estejam armazenadas;

III - restituí-los nas mesmas condições em que lhe foram cedidos.

Parágrafo único. O Tribunal não se responsabilizará por quaisquer informações de cunho particular que o usuário tenha deixado nos ativos de TI após sua devolução.

CAPÍTULO XII

DAS DISPOSIÇÕES FINAIS

Art. 56. A Diretoria-Geral, para garantir a segurança cibernética, poderá restringir:

I - os horários de acesso aos recursos, seja ele de modo presencial ou remoto;

II - o acesso por geolocalização; e

III - o acesso em dias específicos ou feriados.

Art. 57. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida previamente a Comissão de Segurança da Informação.

Art. 58. Esta norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação, com participação da Secretaria de Tecnologia da Informação, e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 59. Esta Instrução Normativa entra em vigor na data de sua publicação.

ELINE IRIS RABELLO GARCIA DA SILVA
Diretora-Gera

Este texto não substitui o publicado no **DJE TRE-RJ nº 194, de 07/08/2023, p. 6 (https://dje.tse.jus.br/dje/pdf/v1/edicao/105500#page=6)**

FICHA NORMATIVA

Data de Assinatura: Não consta.

Ementa: Estabelece a Norma de Uso Aceitável de Recursos de Tecnologia da Informação.

Situação: Não consta revogação.

Diretor(a)-Geral: ELINE IRIS RABELLO GARCIA DA SILVA

Data de publicação: DJE TRE-RJ nº 194, de 07/08/2023, p. 6 (https://dje.tse.jus.br/dje/pdf/v1/edicao/105500#page=6)

Alteração: Não consta alteração.