TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Portaria Presidência Nº 440/2021 TRE/PRESI/DG/STI, de 12 de julho de 2021

Estabelece a Política de Controle de Acessos e Uso Aceitável dos Recursos de Tecnologia da Informação do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO PIAUÍ, no uso de suas atribuições e

CONSIDERANDO o disposto na Resolução nº 356/2017 que instituiu a Política de Segurança da Informação do Tribunal Regional Eleitoral do Piauí;

CONSIDERANDO o disposto na Resolução nº 258/2013 que instituiu o Código de Ética dos Servidores do Tribunal Regional Eleitoral do Piauí;

CONSIDERANDO o disposto na Resolução CNJ nº 227/2016, alterada pela Resolução CNJ nº 298/2019, que regulamenta o teletrabalho no âmbito do Poder Judiciário;

CONSIDERANDO o disposto na Resolução CNJ nº 370/2021 que estabelece as diretrizes da Estratégia Nacional de Tecnologia da Informação e Comunicação para o Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o disposto na Resolução CNJ nº 396/2021 que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

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 do Tribunal Regional Eleitoral do Piauí (TRE-PI);

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

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.

RESOLVE:

Art. 1º Instituir, por esta norma, as diretrizes para o controle de acesso e uso aceitável dos recursos de Tecnologia da Informação e Comunicação no âmbito do TRE-PI, bem como os direitos e as responsabilidades dos usuários desses recursos.

Parágrafo único. Consideram-se recursos de Tecnologia da Informação do TRE-PI o conjunto de ativos de TI mantidos ou operados pelo TRE-PI, tais como equipamentos de rede, telecomunicações, computadores, dispositivos móveis, dispositivos de armazenamento, programas, banco de dados, sistemas e serviços de TI.

SEÇÃO I

DOS CONCEITOS E DEFINIÇÕES

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

I - acesso remoto: toda conexão estabelecida com a rede do TRE-PI 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 - *antispam*: serviço de detecção e análise que tem como objetivo bloquear o recebimento de spam;

IV - 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;

V - 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;

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

VII - 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;

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

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

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

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

XII - dispositivo de comunicação: equipamento, como roteador e switch, utilizado para prover serviços de TI e comunicação entre estações de trabalho e dispositivos portáteis por meio da rede do TRE-PI, com ou sem fio;

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

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

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

XVI - *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;

XVII - *proxy* externo: são servidores não administrados pelo TRE-PI, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o proxy administrado pelo TRE-PI;

XVIII - rede de computadores do TRE-PI (rede TRE-PI): também conhecida por rede corporativa, é o conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do TRE-PI ou por ele providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

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

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

XXI - 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;

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

XXIII - 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;

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

XXV - usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TRE-PI;

XXVI - usuário externo: servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo tribunal e que não se enquadre nas definições contidas nos incisos XXIV e XXV deste artigo;

XXVII - usuário visitante: pessoa física, que não se enquadre na definição disposta nos incisos XXIV, XXV e XXVI deste artigo, com acesso temporário, somente à Internet ou a recurso específico da rede, autorizado a partir da rede do TRE-PI;

XXVIII - 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;

XXIX - *Virtual Private Network* (VPN): rede de comunicação privada, construída sobre a infraestrutura de uma rede pública ou compartilhada, usando tecnologias que possam manter seguros os dados trafegados, destinada a estabelecer comunicação entre os dispositivos remotos e a rede TRE-PI;

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

SEÇÃO II

DAS DISPOSIÇÕES GERAIS

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

Art. 4º O uso dos recursos de TI de propriedade do TRE-PI pelos usuários internos e colaboradores, destina-se às atividades relacionadas com suas atribuições funcionais e sua utilização será monitorada, podendo ser objeto de auditoria.

Art. 5º 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 TRE-PI os programas desenvolvidos para o Tribunal por usuários internos.

Art. 6º O TRE-PI se reserva ao direito de inspecionar, sem a necessidade de aviso prévio, os computadores e arquivo armazenado, que estejam no disco local dos computadores, nas áreas privativas ou nas áreas compartilhadas da rede, visando assegurar o cumprimento desta norma.

SEÇÃO III

DA IDENTIFICAÇÃO DE USUÁRIOS E DO TRATAMENTO DE SENHAS

Art. 7º O usuário é responsável por garantir a confidencialidade de suas credenciais de acesso, sendo sua obrigação garantir o seu sigilo, jamais compartilhando com outros usuários ou com terceiros.

Art. 8º A utilização de nome de usuário identificador (*login*) e senha serão utilizadas como tipo de conta de usuário padrão para acesso aos sistemas e serviços de informação deste Tribunal.

Parágrafo único. Sempre que possível, todos os sistemas e serviços utilizarão a mesma base de dados para autenticar seus usuários.

Art. 9º O nome de usuário identificador da credencial de acesso à rede corporativa será formado pelo primeiro nome e pelo último sobrenome do usuário, separados pelo sinal gráfico de ponto (".").

Parágrafo único - Em situações justificadas, outro identificador do usuário poderá ser utilizado.

Art. 10. Cada usuário deve possuir uma única credencial de acesso à rede do TRE-PI, exceto nos casos excepcionais autorizados pela Secretaria de Tecnologia da Informação (STI).

§ 1º A Secretaria de Gestão de Pessoas (SGP) comunicará à STI, imediatamente, os novos cadastramentos, as alterações de lotação, as mudanças de função e os desligamentos dos usuários internos e estagiários.

§ 2º O gestor do contrato comunicará à STI, imediatamente, os novos cadastramentos e os desligamentos dos usuários colaboradores do respectivo contrato, à exceção dos estagiários.

§ 3º A STI realizará, sempre que identificado usuários com múltiplas credenciais, o contato com usuário para verificar a real necessidade de utilização das mesmas, bloqueando ou deletando as desnecessárias.

Art. 11. A conta de usuário para acesso à rede do TRE-PI é pessoal, intransferível e o sigilo da senha é de responsabilidade exclusiva do titular da conta.

§ 1º A utilização de conta de usuário para uso coletivo é permitida para usuários em treinamento.

§ 2º A criação de conta de usuário para uso coletivo para finalidade diferente de treinamento deve ser solicitada à Central de Serviços de TI e autorizada somente em casos devidamente justificados e avaliados pela STI, para os quais não seja possível trabalhar com a conta individual de usuário.

§ 3º O usuário poderá ser responsabilizado pelas operações realizadas com a utilização de suas credenciais de acesso.

Art. 12. A conta de usuário terá permissão de uso da rede do TRE-PI suspensa quando ocorrer uma das condições a seguir:

I - conta de usuário com 03 (três) tentativas sucessivas de autenticação com senha incorreta;

II - conta de usuário sem uso por período igual ou superior a 90 (noventa) dias;

III - quando o servidor ativo não estiver em efetivo exercício, por prazo igual ou superior a 30 (trinta) dias, em função das licenças e dos afastamentos previstos na Lei nº 8.112, de 1990;

IV - quando servidor ativo estiver em afastamento preventivo do exercício do cargo em decorrência do disposto no art. 147 da Lei nº 8.112, de 1990;

V - em casos de suspeita de infração das normas de segurança da informação.

Parágrafo único. A STI poderá modificar a quantidade de tentativas e os prazos estabelecidos nesta norma, com a finalidade de adequação às boas práticas de segurança, desde que a mudança seja precedida de ampla divulgação.

Art. 13. As senhas utilizadas pelas contas de usuários devem obedecer aos seguintes critérios:

I - a senha não deve conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos;

II - a senha não deve ser igual às três últimas senhas utilizadas;

III - a senha deve ter pelo menos 12 caracteres;

IV - a senha deve conter caracteres que atendam a, pelo menos, três das condições a seguir:

a) caracteres maiúsculos (**A** a **Z**);

b) caracteres minúsculos (**a** a **z**);

c) cumerais (0 a 9);

d) caracteres não alfabéticos (por exemplo, !, $, #, %, @).

§ 1º O suporte à alteração da senha poderá ser solicitado à Central de Serviços de Tecnologia da Informação (CSTI);

§ 2º As senhas devem ser alteradas periodicamente, no máximo, a cada seis meses;

§ 3º O titular da conta poderá fazer uso de caracteres especiais em sua senha;

§ 4º O usuário deve evitar utilizar a mesma senha de acesso à rede TRE-PI em outros serviços na internet.

Art. 14. Os sistemas e serviços de informação deste Tribunal que utilizam nome de usuário identificador (*login*) e senha passarão a exigir as condições deste normativo quando do procedimento de criação e/ou alteração de senhas.

§ 1º A senha inicial do usuário será gerada automaticamente, de forma aleatória, satisfazendo as condições previstas neste normativo, sendo vedado o uso de senha padrão, devendo a senha ser alterada no primeiro acesso;

§ 2º Aplicam-se ao procedimento de recuperação de senhas as exigências deste normativo;

§ 3º Apenas o titular da conta poderá solicitar sua reinicialização.

§ 4º A reinicialização de senhas de magistrados ou promotores poderá ser solicitada por seus auxiliares, devendo a nova senha ser encaminhada ao e-mail pessoal funcional do órgão de origem do magistrado ou promotor.

Art. 15. O gerenciamento de senhas utilizadas em sistemas e serviços de informação externos, como sítios eletrônicos, instituições financeiras e de outros órgãos, será de responsabilidade exclusiva dos usuários.

Art. 16. Os usuários devem observar as boas práticas e procedimentos relacionados à utilização segura de senhas divulgados pela STI.

SEÇÃO IV

DA REDE CORPORATIVA E DAS ESTAÇÕES DE TRABALHO

Art. 17. A STI poderá fazer uso de ferramentas, softwares e procedimentos que visem garantir a segurança da rede TRE-PI e dos dados que nela trafegam.

Art. 18. Somente os servidores autorizados pela STI têm permissão de adicionar, configurar ou retirar dispositivos de comunicação da rede TRE-PI.

§ 1º A cada ponto de acesso à rede de dados do TRE-PI poderá ser conectado apenas um equipamento.

§ 2º É vedado a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da STI.

Art. 19. Todos os pontos de rede sem uso serão desativados pela equipe técnica da STI, sendo reativados quando necessários, através de chamados abertos junto à Central de Serviços de TI.

Art. 20. É de responsabilidade do usuário todo e qualquer recurso de TI disponibilizado para o desempenho de suas atividades.

Art. 21. É proibida a conexão de qualquer dispositivo não fornecido pelo TRE-PI nas redes de computadores das unidades, sem a prévia anuência da STI.

Parágrafo único. A conexão de qualquer equipamento à rede cabeada do TRE-PI será feita pela STI ou por pessoas por ela autorizadas.

Art. 22. As estações de trabalho possuirão configurações de *hardware* e *software* padronizadas pela STI, de acordo com a necessidade de utilização dos usuários.

Art. 23. As estações de trabalho receberão *softwares* homologados e licenciados pela STI, conforme a necessidade de cada usuário e a disponibilidade de licenças.

Art. 24. É vedado a concessão aos usuários privilégios de administrador local nas estações de trabalho, salvo em casos excepcionais autorizados pela STI, mediante justificativa do titular da unidade.

Art. 25. É vedado aos usuários:

I - instalar ou remover *softwares* de suas estações de trabalho;

II - alterar a configuração de *hardware* e de *software* da estação de trabalho sem autorização da STI;

III - desativar ou impedir o funcionamento de qualquer software instalado pela STI.

Parágrafo único. A STI poderá designar pessoas com permissão para realização dos procedimentos definidos no caput.

Art. 26. Poderão ser bloqueados os acessos à rede, temporariamente ou por tempo indeterminado, de equipamentos identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

Art. 27. O usuário deverá bloquear o acesso à sua estação de trabalho sempre que se ausentar do equipamento.

Art. 28. O uso de software antivírus nas estações de trabalho disponibilizadas aos usuários é obrigatório e deverá ser mantido sempre ativado e atualizado.

§ 1º O software antivírus deve ser configurado para executar a varredura completa na estação de trabalho disponibilizada pelo Tribunal com periodicidade máxima semanal;

§ 2º É proibida a inativação do antivírus ou a interrupção da execução da varredura pelo usuário da rede.

SEÇÃO V

DO ARMAZENAMENTO DE ARQUIVOS NA REDE DO TRE-PI

Art. 29. Cada unidade do TRE-PI terá disponível área de armazenamento em rede (diretório compartilhado) para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

§ 1º Esses arquivos serão acessíveis apenas internamente, a partir da rede TRE-PI;

§ 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. 30. A definição das permissões de acesso aos diretórios de cada unidade é de responsabilidade do respectivo titular.

Parágrafo único. O titular da unidade poderá solicitar à STI relatório contendo os usuários que possuem acesso e respectivas permissões do diretório compartilhado.

Art. 31. 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.

Art. 32. Deve-se 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. 33. O compartilhamento de arquivos com usuários externos ou com terceiros se dará através do serviço de armazenamento de arquivos em nuvem privada, acessível pela internet.

Art. 34. Os usuários internos e colaboradores poderão solicitar diretório pessoal para o serviço de armazenamento de arquivos em nuvem privada, para autorização pela STI.

Parágrafo único. O serviço de armazenamento de arquivos em nuvem privada só poderá ser utilizado para armazenamento de dados de estrito interesse do Tribunal.

SEÇÃO VI

DOS SERVIÇOS DE COMUNICAÇÃO

Art. 35. 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. 36. Os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo.

Art. 37. É vedada a utilização de e-mail institucional em lojas virtuais, listas de discussões, fóruns, como credencial de acesso a sites externos ou qualquer outra finalidade que não seja de interesse da instituição.

Art. 38. 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. 39. A STI poderá implementar mecanismos para a coibir o uso indevido dos serviços de comunicação.

Art. 40. O uso dos serviços de comunicação pelos usuários colaboradores dependerá de solicitação do titular da unidade à qual esteja vinculado.

SEÇÃO VII

DO ACESSO À INTERNET

Art. 41. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela STI.

Parágrafo único. É expressamente proibido o uso de *proxies* externos ou similares, sendo sua utilização informada à STI para adoção das providências pertinentes.

Art. 42. Os usuários internos e colaboradores poderão ter acesso à internet, identificados pela sua conta de usuário, para uso de atividades exclusivamente relacionadas ao trabalho.

Parágrafo único. É vedado o uso da conta de e-mail institucional em serviços e sistemas na internet para fins particulares.

Art. 43. Constitui acesso indevido à internet as seguintes ações:

I - acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a Política de Segurança da Informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de *software*;

II - utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto os programas definidos como ferramentas de trabalho e homologados pela STI;

III - utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto aqueles definidos como ferramenta de trabalho;

IV - acessar sítios eletrônicos que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRE-PI;

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

VI - acessar a internet utilizando conta de usuário de terceiros.

§ 1º O acesso aos conteúdos relacionados neste artigo será bloqueado pela STI, tanto quanto possível, não isentando, porém, o usuário da responsabilidade em acessá-los, quando não houver bloqueio previsto ou possível.

§ 2º Fica a STI autorizada a atualizar a lista de acesso indevido a que se referem os incisos deste artigo, dando conhecimento geral através dos meios de comunicação disponíveis.

Art. 44. O acesso à internet será controlado, de forma automática, pela ferramenta de *proxy*, configurada de acordo com os termos desta norma.

Paragrafo único. A liberação de acesso a sítios eletrônicos e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, do titular da unidade à STI, que a submeterá, quando necessário, à Comissão de Segurança da Informação para deliberação.

Art. 45. 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 TRE-PI, seja através de modems 3G ou 4G ou de qualquer outro tipo existente ou que venha a ser criado, salvo mediante expressa autorização da STI.

Art. 46. A critério da STI, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, tais como:

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

II - limitação de banda de tráfego de dados;

III – bloqueio da conta de usuário.

SEÇÃO VIII

DA UTILIZAÇÃO DA REDE PRIVADA VIRTUAL

Art. 47. O acesso remoto à rede TRE-PI via VPN (*Virtual Private Network*), aqui tratada por rede VPN, pelos usuários internos e colaboradores far-se-á mediante adesão expressa ao Termo de Compromisso - Trabalho Remoto.

Parágrafo único. O acesso à rede VPN fica condicionado à compatibilidade, às permissões do usuário e autorização da STI.

Art. 48. O acesso à rede VPN por usuários internos e colaboradores não deverá ser realizado a partir de computadores de uso público.

Art. 49. Os certificados digitais para uso do acesso à rede VPN serão válidos por, no máximo, 90 (noventa) dias.

Parágrafo único. Em casos excepcionais, a STI poderá autorizar a emissão de certificados digitais por período superior ao informado no caput.

Art. 50. Sempre que possível, o acesso à rede VPN utilizará duplo fator de autenticação.

Art. 51. O serviço de acesso à rede VPN estará disponível no horário de 6:00 h às 21:00 h em dias úteis.

§ 1º O funcionamento do serviço de acesso à rede VPN nos finais de semana, feriados e período eleitoral serão submetidos à Diretoria-Geral pela unidade interessada, para deliberação sobre sua autorização.

Art. 52. O usuário é responsável pela guarda do certificado digital, não lhe sendo permitida a transferência para outras pessoas.

Art. 53. Ao utilizar o acesso à rede VPN do Tribunal, o usuário deverá permanecer conectado apenas enquanto estiver efetivamente utilizando os serviços disponibilizados, tomando o cuidado de desconectar-se nas interrupções e no término do trabalho.

Art. 54. 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. 55. O extravio do equipamento ou certificado digital utilizados para acesso remoto deverá ser imediatamente comunicado à STI pelo usuário.

Art. 56. A utilização do serviço de acesso à rede VPN por estagiários ficará condicionada à anuência do titular da unidade onde o mesmo encontra-se lotado.

Art. 57. O acesso à rede VPN do Tribunal será permitido às equipes técnicas da STI, em qualquer dia ou horário, para fins de manutenção da infraestrutura de TIC.

SEÇÃO IX

DOS SERVIÇOS ACESSÍVEIS PELA INTERNET

Art. 58. A STI poderá disponibilizar serviços acessíveis pela internet aos usuários a partir do sítio do Tribunal sem a utilização de rede VPN.

§ 1º Os serviços de que tratam o caput estarão disponíveis no horário de 6:00 h às 21:00 h em dias úteis;

§ 2º O funcionamento dos serviços acessíveis pela internet nos finais de semana, feriados e período eleitoral serão submetidos à Diretoria-Geral pela unidade interessada, para deliberação sobre sua autorização.

§ 3º Os serviços acessíveis pela internet incluem:

I - serviço de correio eletrônico (e-mail);

II - Sistema Eletrônico de Informações - SEI;

III - ambiente de videoconferência do Balcão Virtual;

IV - serviço de armazenamento de arquivos em nuvem privada;

V - Espaço do Servidor.

§ 4º Os serviços acessíveis pela internet estão disponíveis permanentemente para acesso pela na rede interna do TRE-PI.

SEÇÃO X

DOS MEIOS DE IMPRESSÃO

Art. 59. Os recursos de impressão pertencentes a este Tribunal, disponíveis para o usuário, serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

Art. 60. Sempre que possível, o compartilhamento de documentos deve ser priorizado, evitando o uso desnecessário de insumos.

Art. 61. As impressoras disponibilizadas aos usuários que possibilitarem impressão frente e verso da folha de papel deverão ter esta opção habilitada como modalidade de impressão padrão.

Art. 62. A opção de impressão em um só lado da folha ou de impressões em cores devem ser utilizadas apenas em hipótese de extrema necessidade, de forma a evitar o uso desnecessário de recursos.

Parágrafo único. Os papéis cujos versos não tenham sido utilizados devem ser reaproveitados para impressão de recibos ou para rascunhos ou devem ser encaminhados ao serviço de reprografia do Tribunal para a confecção de blocos de rascunhos.

SEÇÃO XI

DISPOSIÇÕES FINAIS

Art. 63. Cabe à Comissão de Segurança da Informação (CSI) monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste regulamento, e propor os ajustes que considerar necessários.

Art. 64. Os horários de funcionamento dos serviços poderão ser alterados pela Diretoria Geral, de modo a adequá-los à necessidade do Tribunal, mediante ampla divulgação dos novos horários.

Art. 65. Os casos omissos serão resolvidos pela Diretoria Geral.

Art. 66. Esta portaria entra em vigor na data de sua publicação.

Doutor AGLIBERTO GOMES MACHADO

Presidente do TRE-PI, em exercício

Documento assinado eletronicamente por **Agliberto Gomes Machado**, **Presidente, em exercício**, em 13/07/2021, às 14:32, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1288715** e o código CRC **16E9D5AF**.