

Presidente

## **PORTARIA Nº 010/2023**

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, no uso das atribuições que lhe são conferidas pelo artigo 23, inciso XV, do Regimento Interno deste Tribunal e considerando o contido no Processo Administrativo Digital nº 566/2023-TRE, RESOLVE

Art. 1º DISPENSAR, a pedido, a Doutora DENISE HAMMERSCHMIDT, Juíza de Direito da Turma Recursal dos Juizados Especiais do Estado do Paraná, do Foro Central da Comarca da Região Metropolitana de CURITIBA, do Juízo da 175ª Zona Eleitoral de CURITIBA, a partir de 09 de janeiro de 2023.

Art. 2º DESIGNAR, em conformidade com o disposto na Resolução TRE nº 467/2005, de 04/04/2005, a Doutora GIANI MARIA MORESCHI, Juíza de Direito da 1ª Vara Descentralizada do Boqueirão, do Foro Central da Comarca da Região Metropolitana de CURITIBA, para responder pelos serviços da 175ª Zona Eleitoral de CURITIBA, a partir de 09 de janeiro de 2023.

Art. 3º Esta Portaria entra em vigor na data de sua publicação, com efeitos a partir de 09 de janeiro de 2023.

Curitiba, 12 de janeiro de 2023.

Des. COIMBRA DE MOURA

Presidente

## **DIRETORIA-GERAL**

### **INSTRUÇÃO NORMATIVA**

#### **INSTRUÇÃO NORMATIVA Nº 04/2022**

Regulamenta a utilização dos recursos computacionais no âmbito da Justiça Eleitoral do Paraná.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, no uso de suas atribuições que lhe são conferidas pelo art. 43, inc. VII da Resolução TRE/PR nº 903, de 31 de agosto de 2022;

CONSIDERANDO a necessidade de implantação de práticas que favoreçam a governança e a gestão da Tecnologia da Informação - TI no TRE/PR;

CONSIDERANDO a importância de definição e padronização dos processos, a fim de prover e manter serviços e soluções de TI que viabilizem e priorizem o cumprimento da missão institucional do TRE/PR; e

CONSIDERANDO o contido no PAD nº 28370/2022,

RESOLVE

#### **CAPÍTULO I**

##### **DAS DISPOSIÇÕES PRELIMINARES**

Art. 1º A utilização dos recursos computacionais no âmbito da Justiça Eleitoral do Paraná observará os termos desta Instrução Normativa.

#### **CAPÍTULO II**

##### **DOS CONCEITOS**

Art. 2º Para os efeitos desta instrução normativa aplicam-se os seguintes conceitos:

I - acesso remoto: acesso remoto de usuário em um computador, por meio da Internet, permitindo o seu controle direto, independentemente da distância física que separa ambos;

II - antivírus: programa ou software especificamente desenvolvido para detectar, anular e eliminar vírus de computador;

- III - armazenamento em nuvem: estratégia de armazenamento de arquivos onde não há necessidade de estar na rede local para acesso aos dados;
- IV - ativo de TI: todo e qualquer componente de hardware, software e rede de dados em uso no Tribunal, nos Cartórios Eleitorais e pelos servidores do quadro funcional da Justiça Eleitoral do Paraná, quando no exercício de suas funções;
- V - backbone: espinha dorsal de uma rede, geralmente uma infraestrutura de alta velocidade que interliga várias redes;
- VI - backup ou cópia de segurança: cópia de dados de um dispositivo para outro com o objetivo de eventual recuperação, caso haja algum problema;
- VII - Central de Serviços de TI: unidade funcional cujo objetivo principal é fornecer um ponto único de contato entre os usuários e os serviços oferecidos, sendo formada por um número dedicado de pessoas, responsáveis por lidar com atividades variadas, via telefone ou interface web, ou eventos da infraestrutura automaticamente reportados por meio de ferramentas de monitoração;
- VIII - CGSI: Comitê Gestor de Segurança da Informação;
- IX - CGTI: Comitê Gestor da Tecnologia da Informação;
- X - criptografia: a ciência e a arte de escrever mensagens em forma cifrada ou em código, sendo um dos principais mecanismos de segurança utilizados para proteção contra os riscos associados ao uso de redes compartilhadas;
- XI - criptografado: informação/dado codificado ou cifrado;
- XII - correio eletrônico (e-mail): sistema que permite compor, enviar e receber mensagens por meio de sistemas eletrônicos de comunicação;
- XIII - DNS (Domain Name System): serviço onde são armazenadas ligações entre endereços IPs e domínios;
- XIV - e-GOV: sigla que representa o Programa de Governo Eletrônico brasileiro, que visa orientar as relações do Governo com os cidadãos, empresas e também entre os órgãos do próprio governo, de forma a aprimorar a qualidade dos serviços prestados, promover a interação com empresas e indústrias e fortalecer a participação cidadã por meio do acesso à informação e a uma administração mais eficiente;
- XV - exfiltração: transferência não autorizada de dados de um sistema de informação;
- XVI - firewall: dispositivo de rede que regula o tráfego de rede entre redes distintas;
- XVII - forense computacional: conjunto de técnicas utilizadas para identificar e coletar evidências digitais, essenciais para o caso de uma eventual averiguação;
- XVIII - hardware: parte física dos equipamentos de Informática;
- XIX - Interlocutor de Tecnologia da Informação: analista, técnico ou assistente de TI alocado nas unidades da Secretaria de Tecnologia da Informação com a função de dar suporte às atividades e recursos de Tecnologia da Informação;
- XX - internet: rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum, unindo usuários particulares, entidades de pesquisa, órgãos culturais, institutos militares, bibliotecas e empresas;
- XXI - telefonia IP: utilização de conversação humana usando a Internet ou qualquer outra rede de computadores, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados;
- XXII - IP: Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação;

XXIII - LAN: significa Local Area Network (em português, Rede Local) e é um conjunto de computadores que pertencem a uma mesma organização, conectados entre eles por uma rede, numa pequena área geográfica, geralmente através de uma mesma tecnologia (a mais usada é a Ethernet);

XXIV - LOG: expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional;

XXV - malware: termo em inglês que designa toda forma de software construído com intenção maliciosa, com o objetivo de causar dano, alteração, uso pernicioso do equipamento ou roubo de informação;

XXVI - pendrive: dispositivo móvel de memória constituído por dispositivo que armazena dados digitais como documentos, fotos, entre outros;

XXVII - pProxy (plural: proxies): serviço que intermedeia o acesso entre um cliente e um servidor;

XXVIII - recursos computacionais: equipamentos de tecnologia da informação, softwares próprios ou de terceiros, arquivos digitais e banco de dados que são direta ou indiretamente administrados, mantidos ou operados pela Secretaria de Tecnologia da Informação (SECTI), por meio das suas unidades subordinadas, tais como: computadores pessoais, servidores de rede e terminais de qualquer espécie, incluídos seus equipamentos acessórios, impressoras, redes de computadores e equipamentos de transmissão de dados, bancos de dados ou documentos residentes em disco, fita ou outros meios digitais, scanners (equipamentos digitalizadores), sistemas ou softwares desenvolvidos internamente ou por terceiros, entre outros, que possuam similaridade e reconhecimento cabal com a área de TI;

XXIX - rede de dados: possui a função de interligar computadores e/ou conectá-los a outros dispositivos, permitindo que haja a circulação de informações, comandos e recursos entre eles;

XXX - roteadores: equipamentos usados para fazer a comunicação entre diferentes redes de computadores, provendo a comunicação entre computadores distantes um do outro;

XXXI - scanner: equipamento capaz de digitalizar imagens físicas, normalmente documentos ou fotos, em arquivos digitais usáveis por equipamentos informatizados;

XXXII - servidor: computador que fornece serviços a uma rede de computadores.

XXXIII - site (sítio eletrônico): conjunto de páginas web, isto é, de hipertextos acessíveis geralmente pelo protocolo HTTP ou pelo HTTPS na internet via navegadores de internet;

XXXIV - SNMP (Simple Network Management Protocol): protocolo de gestão de rede da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede;

XXXV - software: conjunto de instruções para realizar ações nos sistemas computacionais;

XXXVI - spam: mensagem eletrônica não-solicitada enviada em massa;

XXXVII - switch (plural: switches): equipamento que interliga computadores, possibilitando a formação de uma rede local a partir de cabos de rede que se estendem da placa de rede dos computadores até o próprio equipamento;

XXXVIII - usuário de TI: os servidores do quadro, os estagiários, os requisitados, os magistrados e os contratados que dependem dos recursos de TI para o desempenho das atividades a serem executadas;

XXXIX - vírus: programa ou trecho de código projetado para danificar seu computador através da corrupção de arquivos do sistema, utilização de recursos e/ou destruição de dados;

XL - VPN: rede privada virtual, permite realizar um acesso seguro a uma rede remota a partir de uma rede de terceiros;

XLI - WAN: rede de longa distância ou rede de área alargada é uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente;

XLII - web ou www: sistema hipertextual que opera através da internet;

XLIII - wiki: termo utilizado para identificar um tipo específico de coleção de documentos em hipertexto ou software colaborativo usado para criá-lo;

XLIV - wireless: caracteriza qualquer tipo de conexão para transmissão de dados sem a utilização de fios ou cabos;

XLV - SECGP: Secretaria de Gestão de Pessoas;

XLVI - Gestor do sistema: responsável pelas regras de negócio de um sistema de informação e que tem autonomia de decisão sobre os processos de trabalho abrangidos pelo sistema informatizado;

XLVII - mídias de armazenamento: dispositivos que somente guardam informação;

XLVIII - dispositivos de digitalização: dispositivos destinados a realizar a conversão de um documento para o formato digital;

XLIX - serviços externos: recursos de tecnologia da informação, incluindo sítios, aplicações, ferramentas, sistemas, dados, compartilhamentos, fluxos de mídia, mapas, redes sociais, protocolos de comunicação, telefonia, serviços de mensagens, correio eletrônico, nuvem, dentre outros, desde que não sejam fornecidos pelo TRE/PR.

### CAPÍTULO III

#### DA UTILIZAÇÃO GERAL DOS RECURSOS COMPUTACIONAIS

Art. 3º São regras gerais no uso dos recursos computacionais:

I - todo e qualquer uso dos recursos computacionais deve estar de acordo com obrigações contratuais quando houver, assim como leis e regulamentações vigentes, inclusive perante as delimitações definidas nos contratos de software e outras licenças;

II - deverá existir, ser mantido e operacional, serviço de registros para auditoria (log) para os serviços essenciais e/ou críticos, com guarda dos dados de acordo com a Lei nº 12.965, de 23/04/2014 (Marco Civil da Internet) e Lei nº 12.527 de 18/11/11 (Lei de Acesso à Informação);

III - as instruções de funcionamento, bem como as limitações de um serviço, devem ser fornecidas aos seus usuários;

IV - serviços cuja informação é classificada como privativa e/ou confidencial devem fornecer métodos seguros de autenticação e autorização daquela informação;

V - deverá ser disponibilizado telefone de contato, acesso à sistema específico para chamado e/ou endereço de e-mail com finalidade de fornecimento de suporte aos usuários dos serviços de TI;

VI - todo serviço deverá ter um responsável a ser acionado para os casos de incidentes de segurança ou de outros motivos relacionados ao serviço;

VII - todo usuário interno, que utiliza recurso computacional, deve possuir uma conta de autenticação a ser utilizada nos serviços;

VIII - a área de tecnologia da informação deve manter um catálogo de softwares homologados pelo TER, atualizado e de fácil acesso aos usuários.

Art. 4º São regras gerais aplicáveis aos usuários dos recursos computacionais:

I - o usuário utilizador de recursos computacionais deve conhecer as instruções, regras e penalidades de funcionamento do serviço que esteja utilizando, devendo ainda:

a) não se passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;

b) responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros;

c) se titular da conta, responder pelo mau uso dos recursos computacionais em qualquer circunstância;

d) responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos e também, se for o caso, às penalidades impostas por outras instâncias;

e) o usuário deve manter seus computadores pessoais com softwares autorizados pelo TRE/PR e antivírus atualizados, não podendo impedir tais correções de segurança;

f) se necessário, os usuários devem procurar a Central de Serviços de TI para esclarecimentos.

Art. 5º São deveres dos analistas e técnicos de TI, lotados na Secretaria de Tecnologia da Informação:

I - preservar a integridade e a segurança dos sistemas;

II - manter os registros (logs) de utilização dos serviços entregues, conforme regulamento interno vigente, no que diz respeito ao tempo e requisitos técnicos;

III - fornecer registros de sistema e utilização sempre que solicitado formalmente ou conforme regulamento interno, quando houver;

IV - acessar dados dos usuários somente quando for indispensável para manutenção do sistema ou em casos de falhas de segurança, sempre observando os regulamentos vigentes sobre privacidade conforme regimento interno do Tribunal;

V - utilizar o sincronismo de tempo (ntp) nos servidores de rede responsáveis por fornecimento de serviço de tecnologia da informação;

VI - manter atualizados os sistemas e serviços de tecnologia da informação;

VII - manter atualizada tecnologicamente a infraestrutura de tecnologia da informação;

VIII - informar aos usuários sobre os mecanismos recomendados para correção de vulnerabilidades, quando cabível;

IX - utilizar sempre que possível as melhores práticas de segurança da informação, especialmente as definidas para a administração pública nos sistemas e serviços de tecnologia da informação entregues ao TRE/PR;

X - garantir a disponibilidade na entrega de serviços aos usuários do TRE/PR e ao público em geral, conforme acordo de níveis de serviço definidos pelos gestores de negócio do Tribunal;

XII - garantir que o armazenamento dos registros de eventos (logs) gerados pelos ativos de informação relevantes sejam centralizados sempre que houver viabilidade técnica. Nos casos em que existir limitação técnica o armazenamento dos registros de eventos (logs) deve ser mantido nos sistemas de origem;

XIII - garantir que os registros de eventos (logs) estejam sempre sincronizados cronologicamente;

XIV - garantir que os registros de eventos (logs) sejam protegidos e armazenados adequadamente, de acordo com a sua classificação;

XV - garantir a proteção das informações dos registros (logs), de forma que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado;

XVI - garantir que os registros (log) das atividades dos administradores e operadores em sistemas sejam devidamente armazenados;

XVII - garantir que os registros (logs) das falhas ocorridas sejam armazenados e analisados para correção dos problemas encontrados.

Art. 6º São regras gerais de acesso a serviços externos:

I - compete à SECTI bloquear acessos externos que sejam classificados como risco à disponibilidade dos serviços providos pelo Tribunal, assim como serviços que representem riscos à segurança da tecnologia da informação e que sejam classificados como vetores de disseminação de vírus, malwares e pragas digitais;

II - compete ao CGSI definir o bloqueio de serviços que sejam classificados como risco à segurança da informação, como, por exemplo, serviços que permitam a exfiltração de dados classificados como sigilosos ou confidenciais.

Art. 7º Consideram-se violações das regras desta norma:

I - mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;

II - efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais do TRE /PR;

III - utilizar os recursos computacionais do TRE/PR para acesso não autorizado a terceiros;

IV - violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;

V - interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto quando autorizado explicitamente pela SECTI;

VI - provocar interferência ou bloqueio em serviços de outros usuários, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais;

VII - desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;

VIII - utilizar os recursos computacionais do Tribunal para ganho indevido.

Art. 8º Sobre a distribuição de informação imprópria:

I - O usuário ou administrador não pode transmitir, difundir ou disponibilizar a terceiros, informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos e som e/ou imagem, fotografias, gravações, software ou qualquer classe de material que de qualquer forma:

a) contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades públicas reconhecidas constitucionalmente, nos tratados internacionais e no ordenamento jurídico como um todo;

b) induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

c) induzam, incitem ou promovam atos, atitudes ou ideias discriminatórias por causa de sexo, raça, religião, crenças, idade ou condição;

d) incorporem, ponham à disposição ou permitam acessar produtos, elementos, mensagens e/ou serviços ilegais, violentos, pornográficos, degradantes ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

f) sejam contrários ao direito de honra, à intimidade pessoal e familiar ou à própria imagem das pessoas;

g) infringjam as normas sobre segredo das comunicações;

h) constituam publicidade ilícita e enganosa, em geral, que constituam concorrência desleal.

#### CAPÍTULO IV

##### DOS DISPOSITIVOS COMPUTACIONAIS

Art. 9º A gestão dos ativos de TI em todo o seu ciclo de vida, incluindo aquisição e desfazimento, é de responsabilidade da SECTI.

Art. 10. O uso dos ativos de TI da rede corporativa está restrito aos usuários de TI autorizados, conforme os acordos de segurança por eles assinados, e deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades.

Art. 11. É vedado à SECTI fazer manutenção ou suporte em equipamentos particulares ou não pertencentes ao patrimônio da Justiça Eleitoral do Paraná, salvo os utilizados para acesso aos sistemas e aplicativos vinculados às competências da Justiça Eleitoral.

Parágrafo único. O suporte técnico a sistemas e aplicativos, instalados em equipamentos particulares, será prestado apenas nas dependências deste Tribunal e desde que esses serviços estejam vinculados às competências da Justiça Eleitoral.

Art. 12. Todas as aquisições de equipamentos computacionais deverão ser encaminhadas, na fase de elaboração do Estudo Técnico Preliminar (ETP), para análise técnica da SECTI, que deverá emitir laudo certificando que o equipamento a ser adquirido é compatível com a infraestrutura ou com os padrões existentes no Tribunal.

Parágrafo único. A inobservância do *caput* deste artigo poderá ensejar a impossibilidade de uso do equipamento.

Art. 13. Todo usuário terá direito a 1 (uma) estação de trabalho.

I - a estação de trabalho é fornecida ao usuário como um conjunto de hardware e software, sendo atribuição da SECTI definir a sua especificação.

II - é dever da SECTI manter atualizadas as estações de trabalho do Tribunal, sejam elas fixas ou móveis, com as atualizações de segurança e correções de software, de forma gerenciada e, preferencialmente, automatizada.

III - em relação ao equipamento ou conjunto deles:

a) o usuário de TI é responsável e deverá zelar pelo bom uso de sua estação de trabalho, seguindo os princípios éticos e morais na sua utilização;

b) no caso de necessidade de mudança de local físico da estação de trabalho, a SECTI deverá ser informada através da Central de Serviços de TI;

c) terceiros deverão ser autorizados pelo fiscal da correspondente contratação.

IV - no caso de estação de trabalho móvel (notebook, smartphones e tablets), acrescenta-se:

a. que deve ser considerada a utilização de criptografia no disco de armazenamento interno, conforme seja definido pela SECTI;

b) deverá o computador móvel ser entregue para manutenção sempre que solicitado pela SECTI.

V - em relação aos dados armazenados no equipamento:

a) os documentos de interesse do Tribunal devem ser exclusivamente armazenados em serviço de armazenamento fornecido pela SECTI. Os arquivos contidos apenas na sua própria estação de trabalho correm risco de serem perdidos por falha aleatória do equipamento, por atualização do sistema operacional ou em caso de contaminação cibernética.

VI - em relação às licenças de uso de softwares instalados nas estações de trabalho:

a) apenas é autorizado o uso de softwares que possuam licenças legais para utilização no TRE /PR, credenciadas e homologadas pela SECTI;

b) é facultado à SECTI, desinstalar softwares sem a devida licença em nome do Tribunal ou que estejam em desacordo com o item anterior;

c) o nome de identificação das estações de trabalho, os softwares previamente instalados, as configurações de hardware e de sistema operacional, não devem ser alterados, exceto pela SECTI;

d) a utilização de privilégios de administrador de máquina deve ser prioritariamente vedada, exceto nos casos expressamente autorizados pela SECTI;

e) as estações de trabalho conectadas à rede de dados do Tribunal deverão ser apenas as de propriedade do próprio Tribunal, exceto nos casos expressamente autorizados pela Direção-Geral;

f) é obrigação do usuário de TI comunicar à SECTI qualquer comportamento que fuja ao padrão normal de funcionamento do equipamento, por exemplo sintomas de vírus;

g) o usuário de TI não deverá desabilitar, nem mesmo temporariamente, os serviços administrativos de sua estação de trabalho, como antivírus, serviços de inventário, de acesso remoto e de atualização de sistema operacional.

VII - Estações de trabalho que não autenticarem na rede do Tribunal por mais de 20 (vinte) dias poderão ser desativadas sem prévia comunicação.

Art. 14. Quanto ao uso de impressoras ou dispositivos de digitalização:

I - os usuários deverão realizar impressões somente quando estritamente necessário;

II - as impressões serão realizadas preferencialmente no modo frente e verso, salvo situações em que isso não for possível;

III - os usuários que possuem necessidade de impressão policromática e não tiverem acesso a equipamentos com essa capacidade, deverão solicitar essa impressão à área responsável por serviços gráficos;

IV - é vedada a movimentação dos equipamentos de impressão e digitalização pelo usuário.

Art. 15. A política de desfazimento dos dispositivos computacionais, incorporados ao patrimônio do Tribunal Regional Eleitoral do Paraná, observará as diretrizes estabelecidas em normativo próprio.

## CAPÍTULO V

### DA AUTENTICAÇÃO E CREDENCIAIS

Art. 16. O gerenciamento de contas e suas respectivas senhas, constituem o mecanismo básico para a autenticação de usuários dos sistemas computacionais do TRE/PR.

I - a SECTI é a responsável pela segurança e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle, bem como manter o sigilo das senhas de acesso a esse ambiente;

II - o usuário de TI é responsável por garantir a confidencialidade de suas credenciais por meio da assinatura de Termo de Sigilo e Responsabilidade conforme ([Anexo I](#)) deste regulamento, sendo sua obrigação garantir o seu sigilo, jamais compartilhando com outros empregados do Tribunal ou com terceiros;

III - as contas atribuídas a cada usuário de TI serão individuais, não devendo ser compartilhadas;

IV - cada usuário será identificado unicamente e todas as contas necessárias para acesso aos serviços oferecidos pela SECTI serão vinculadas a esta identidade;

V - uma conta recém-criada receberá uma senha gerada automaticamente, sendo esta considerada temporária até que o usuário faça seu primeiro acesso;

VI - a troca de senha temporária é obrigatória na primeira autenticação;

VII - as regras de formação e temporalidade das senhas serão definidas pelo CGSI em norma específica;

VIII - em atendimento ao Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) todas as contas criadas devem ser nominais, ou seja, vinculada diretamente a um usuário;

IX. é vedada a criação de contas de acesso a setores ou demais usos gerais que não permitam a individualização do usuário que efetuou a ação;

a) este inciso é aplicável também para contas de acesso de administrador;

b) excetuam-se dessa obrigatoriedade as contas criadas para integrações entre sistemas, que devem ser mantidas sob rígida guarda da SECTI e somente com as permissões necessárias para sua função de origem.

X - é obrigatória a adoção de múltiplo fator de autenticação para acesso a todos os sistemas disponibilizados pelo tribunal que possuam viabilidade técnica;

XI - é de responsabilidade do usuário manter o dispositivo ou serviço onde se encontram os demais fatores de autenticação protegidos contra ameaças;

Art. 17. Cada usuário de TI possuirá uma conta que lhe dará acesso aos recursos básicos da rede do TRE/PR, além de, quando necessário, uma conta de correio eletrônico vinculada.

I - diferentes contas podem possuir níveis de acesso distintos a sistemas e serviços, sendo o credenciamento e a definição de tais níveis de responsabilidade dos respectivos gestores;

II - a concessão de credenciais ao usuário com nível administrativo para serviços, recursos e aplicações deve ser solicitada pelos gestores dos respectivos serviços;

III - o gestor do sistema deve conduzir em intervalos regulares de tempo a análise crítica dos direitos de acesso dos usuários.

Art. 18. A criação de contas de acesso de agentes externos, como terceirizados, servidores de órgãos de controle e outros prestadores de serviço, deverá ser solicitada mediante formulário específico a ser disponibilizado na intranet e supervisionada pelo responsável pelo projeto ou unidade orgânica demandante, a quem compete levar ao conhecimento do agente externo as Políticas de Segurança da Informação do Tribunal, além desta Norma de Recursos Computacionais, garantindo tal ciência por meio da assinatura de "TERMO DE SIGILO E RESPONSABILIDADE", [Anexo I](#) desta Norma, pelos respectivos agentes externos.

I - cabe ao Gestor do Contrato o cadastramento do agente externo, incluindo os terceirizados, indicando o caráter temporário da conta, quando for o caso;

II - é obrigação do fiscal do contrato informar, no respectivo formulário, o desligamento de agentes externos sob sua gestão contratual;

## CAPÍTULO VI

### DO SERVIÇOS DE COMUNICAÇÃO

Art. 19. Para fins desta norma, serviços de comunicação englobam correio eletrônico, mensagens instantâneas, serviços de vídeo-chamada e a infraestrutura de telefonia IP fornecidos pela SECTI ou contratados pelo Tribunal.

I - os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo;

II - é permitida a utilização dos serviços de comunicação aos usuários de TI do TRE/PR nas seguintes condições:

a) os Juízes Membros deste Tribunal e os Juízes Eleitorais do Paraná podem utilizar dos serviços de comunicação mediante solicitação dos respectivos gabinetes e cartórios eleitorais;

b) os funcionários que prestam serviços terceirizados podem utilizar os serviços de comunicação, desde que solicitado pelo gestor do contrato que rege o serviço por eles prestado;

c) os estagiários podem utilizar os serviços de comunicação mediante solicitação do respectivo supervisor de estágio.

III - no momento da criação da conta, a escolha da identificação do usuário, que compõe o endereço eletrônico, obedecerá a uma lista de opções padronizada, gerada automaticamente com base no nome completo do servidor, evitando, dessa forma, a ocorrência de duplicidades e a inclusão de escolhas pessoais fora de padrão;

IV - a identificação de usuário no endereço do e-mail somente será modificada quando ocorrer alteração do nome do servidor e mediante manifestação expressa do interessado;

V - é vedada a criação de contas para unidades organizacionais do TRE/PR ou de uso compartilhado;

VI - define-se como regras para uso dos serviços de comunicação:

a) a utilização do serviço deve se dar de forma profissional, ética e legal, sendo vedado o uso para fins particulares;

b) é vedado, para fins particulares, o cadastro do e-mail corporativo em serviços de redes sociais ou comércio eletrônico e ferramentas de marketing;

c) é vedado o uso do serviço para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, bem como para veicular opinião político-partidária;

d) o envio de mensagens em massa somente será permitido com autorização do CGSI.

VII - o TRE/PR se reserva o direito de aplicar filtros automatizados, para o bloqueio de mensagens que possuam conteúdos incompatíveis com o interesse da Instituição. Tais filtros serão definidos pela SECTI, conforme as melhores práticas do mercado;

VIII - os usuários são responsáveis pela segurança das informações da Justiça Eleitoral, cabendo a eles excluir mensagens recebidas cujo conteúdo suscite dúvidas quanto à potencialidade de prejudicá-la em sua integridade, confiabilidade e disponibilidade, seja pela contaminação por

códigos maliciosos ou vírus de computador, seja por quaisquer outros meios, principalmente os que apresentem, entre outras, as seguintes características:

- a. remetente desconhecido;
- b. links desconhecidos no corpo da mensagem;
- c. anexos com extensões que possam conter códigos maliciosos.

IX - o envio ou recebimento de mensagens será limitado, quando necessário, pelo tamanho máximo definido pelo CGTI, considerando parecer da SECTI baseado na capacidade disponível no ambiente de TI;

X - no caso de desligamento do usuário, as mensagens armazenadas em sua caixa de correio eletrônico ficarão disponíveis por 15 (quinze) dias após a data do seu desligamento, podendo os conteúdos serem disponibilizados ao usuário ou a seu superior imediato mediante solicitação à SECTI;

XI - compete à SECTI monitorar os serviços de comunicação para garantir sua disponibilidade e segurança, mantendo registro de envios e recebimentos de mensagens, respeitando a privacidade legal;

XII - todas as mensagens armazenadas são de propriedade do TRE/PR, podendo o sistema ser auditado, inclusive quanto ao conteúdo das mensagens e anexos, em cumprimento a ordem judicial ou, por determinação do Presidente, em caso de sindicância ou processo administrativo disciplinar, observadas as devidas garantias constitucionais;

XIII - o usuário é responsável por gerir suas mensagens dentro dos limites definidos pela sua quota, visando garantir seu funcionamento contínuo;

XIV - o conteúdo das mensagens não pode incluir arquivos anexos com extensões que possibilitem ou facilitem a propagação de programas danosos, como vírus de computador;

XV - uma vez anonimizados, os registros de envio e recebimento de mensagens, assim como o conteúdo dos mesmos, podem ser utilizados para análises estatísticas e desenvolvimento de serviços;

XVI - sobre os grupos de e-mail:

- a) o acesso à configuração do grupo e principalmente a seus inscritos deve ser rigorosamente controlado e limitado apenas ao administrador (ou dono) do grupo;
- b) o administrador do grupo pode delegar a outras pessoas (usuários que pertençam ao TRE/PR) a administração de um determinado grupo. Essa pessoa ficará encarregada da sua manutenção (inclusão/remoção de usuários, moderação, entre outros);
- c) poderão ser criados grupos com todos os usuários lotados em determinada unidade, com as zonas eleitorais, com unidades da secretaria do Tribunal e comissões, além de agrupamentos dessas unidades;
- d) a critério da Presidência, poderão ser incluídas outras áreas, para acompanhamento das comunicações no Tribunal;
- e) o grupo da unidade do usuário será alterado quando a sua lotação for alterada, o que poderá ocorrer de forma automática;
- f) novos nomes de grupos que não correspondam à estrutura do Tribunal podem ser criados no interesse da Administração, conforme análise da SECTI ou por determinação superior;
- g) fica vedado o envio de mensagens cujo usuário remetente não possa ser identificado, excetuando-se somente o envio de mensagens automáticas geradas por sistema disponibilizado pelo TRE/PR;

Art. 20. Os usuários terão suas contas de e-mail excluídas assim que forem formalizados os seus desligamentos.

I - os gestores de contrato deverão informar, em formulário próprio a ser disponibilizado pela SECTI, o desligamento de seus respectivos contratados, no prazo de 02 (dois) dias úteis após o

encerramento do respectivo contrato ou término das atividades por eles desempenhadas no TRE /PR, para fins de exclusão das contas de e-mail;

II - os supervisores de estágio deverão informar o desligamento do estagiário, no prazo de 02 (dois) dias úteis, para fins de exclusão da conta de e-mail;

III - os responsáveis, elencados nos parágrafos anteriores, que não solicitarem a exclusão dentro dos prazos previstos serão considerados corresponsáveis no caso de uso indevido da respectiva conta de e-mail;

IV - contas de e-mail sem utilização por mais de 40 (quarenta) dias serão bloqueadas;

V - contas de e-mail que não forem acessadas em 30 (trinta) dias desde sua criação poderão ser excluídas, sendo necessária nova solicitação de abertura.

## CAPÍTULO VII

### DO SERVIÇO DE ACESSO À INTERNET

Art. 21. A navegação na internet é disponibilizada como um serviço com o objetivo de permitir ao corpo funcional a execução de suas atribuições funcionais.

I - todos os acessos de navegação na internet serão devidamente registrados para fins legais e de análise estatística, respeitando a privacidade legal;

II - o acesso à rede disponibilizado aos usuários do TRE/PR deverá ser realizado prioritariamente para os interesses de trabalho, não ficando excluído o uso para outros interesses, desde que:

- a. seja feito, preferencialmente, fora do período normal de expediente;
- b. não contenha, receba ou transmita informações institucionais sigilosas ou protegidas;
- c. não contrarie as leis, normas e procedimentos institucionais vigentes;
- d. não interfira, prejudique ou desperdice recursos e serviços de rede.

III - é facultado à SECTI, o acesso aos registros de navegação na internet para verificações de incidentes de segurança como detecção de falhas e/ou vulnerabilidades, resguardada a privacidade legal;

IV - uma vez anonimizados, os registros de acesso à internet podem ser utilizados para análises estatísticas e desenvolvimento de serviços;

V - somente é permitida a navegação na internet utilizando a infraestrutura fornecida pelo Tribunal, sendo vedado o uso de serviços externos como proxies de terceiros, anonimizadores de tráfego, VPNs e afins;

VI - os acessos a serviços externos que utilizem protocolos encriptados poderão ocorrer de forma interceptada, desde que se garanta a privacidade das informações, sendo o mecanismo de interceptação utilizado apenas quando estritamente necessário;

VII - Quando houver necessidade de análise das informações interceptadas, e estas contiverem dados relativos à privacidade de pessoas naturais, mesmo que para alguma eventual resolução de problemas e diagnóstico de falhas, deve haver, neste caso, formalização e autorização do superior imediato e das pessoas naturais impactadas pela quebra do respectivo sigilo, conforme Lei n.º 13.709/2018;

VIII - deve ser utilizado mecanismo de bloqueio de acesso a endereços que forem considerados impróprios, contendo software malicioso, pornografia ou cujo uso possa comprometer outros serviços do TRE/PR;

IX - caso algum site seja incorretamente classificado como sendo impróprio, o usuário poderá solicitar a liberação do mesmo, via Central de Serviços de TI;

X - cabe ao CGSI definir os parâmetros utilizados para controle de acesso a sites no TRE/PR;

XI - é facultado à SECTI, criar grupos com diferentes níveis de acesso à internet, de acordo com necessidade definida pelo gestor da área e, também, baseando-se nos parâmetros definidos pelo CGSI.

## CAPÍTULO VIII

## DO USO DA REDE

Art. 22. O acesso à rede de dados pelos recursos computacionais dos usuários deve ser disponibilizado através de tecnologia que garanta controle de acesso.

I - É vedado aos usuários da rede do TRE/PR:

- a. acessar ou tentar acessar a rede por meio de usuário, dispositivo, equipamento ou software não autorizado;
- b. fazer uso indevido da rede;
- c. interferir na infraestrutura física da rede e seus elementos, exceto aos servidores, estagiários e contratados designados pela SECTI;
- d. interceptar ou tentar interceptar a transmissão de dados através da rede, exceto quando autorizado pela SECTI;
- e. acessar, configurar, instalar ou conectar em ativos de rede, como: hub, switches, scanners, modem, roteadores, entre outros, sem o conhecimento e autorização da SECTI;
- f. desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores do TRE/PR;
- g. conectar, instalar ou utilizar equipamentos de rede sem fio (wireless), sem o conhecimento e autorização da SECTI;
- h. prospectar, planejar ou contratar serviços de rede, sem o conhecimento, apoio técnico ou autorização da SECTI.

II - cabe ao usuário da rede de dados do Tribunal comunicar à SECTI qualquer evento alheio ou estranho ao funcionamento normal da rede, por meio da Central de Serviços de TI, fornecendo as informações necessárias ao registro da ocorrência;

III - cabe à SECTI, por meio de suas áreas:

- a. apoiar tecnicamente a prospecção, planejamento e contratação de serviços de rede;
- b. administrar a rede corporativa do TRE/PR, observando às melhores práticas, normas, leis e padrões recomendados;
- c. realizar o monitoramento e resolução de problemas da rede;
- d. proteger os serviços e ativos de rede utilizando ferramentas apropriadas, como firewall, proxy, sistemas de detecção de intrusão, entre outros.

## CAPÍTULO IX

### DO CONTROLE DE ACESSO REMOTO

Art. 23. O acesso remoto à Rede Corporativa do TRE/PR deve ser realizado somente para atender aos interesses do Tribunal.

I - o acesso remoto à rede corporativa deve ser feito através de diferentes perfis de acesso, onde o superior imediato definirá o perfil de cada subordinado ou, caso o acesso remoto seja realizado por agente externo, o perfil concedido deverá ser solicitado pela área que motivou o acesso;

II - o acesso remoto, via VPN, aos recursos do TRE/PR, deve ser concedido como último recurso, apenas disponibilizado caso não seja possível ao usuário realizar suas atividades sem o mesmo;

III - as ferramentas utilizadas no acesso remoto devem ser previamente homologadas pela SECTI, não sendo permitido o acesso remoto a recursos mantidos dentro da rede corporativa por serviços que dependam da infraestrutura de terceiros. De forma geral, tais ferramentas devem obedecer às seguintes recomendações:

- a. utilizar estrutura de credenciais e autenticação já em uso no Tribunal;
- b. gerar registros de atividades, permitindo identificar não apenas as credenciais que foram utilizadas no acesso, como também quais recursos foram acessados e que ações foram tomadas;
- c. utilizar protocolo de rede criptografado;
- d. utilizar estrutura de permissão de uso da base de credenciais do Tribunal;

IV - nos serviços onde é utilizada estrutura de certificados para acesso, o usuário é o responsável pela guarda do certificado, não lhe sendo permitida a transferência do mesmo;

V - caso um certificado de acesso remoto seja perdido, extraviado ou divulgado para terceiros, o responsável deve solicitar imediatamente a sua revogação junto à Central de Serviços de TI de modo a evitar uso indevido por terceiros;

VI - o acesso remoto a estações de trabalho é condicionado à liberação do usuário corrente de forma excepcional e justificada;

VII - é facultado à SECTI, sem devido aviso prévio, acesso remoto às estações de trabalho para execução de rotinas que sejam consideradas de emergência, como remoção de malware ou atualizações de segurança;

VIII - o acesso remoto aos equipamentos servidores, para suporte e administração, deve ser limitado aos técnicos (servidores ou contratados) da área de tecnologia da informação vinculados à SECTI. Todos estes acessos devem possuir o menor nível de privilégio possível para execução de suas atividades.

## CAPÍTULO X

### DOS SERVIÇOS DE ARMAZENAMENTO DE DADOS

Art. 24. Entende-se por serviços de armazenamento de arquivos o armazenamento em nuvem, compartilhamentos em computadores servidores e outros serviços de armazenamento de arquivos disponibilizados pelo TRE/PR aos usuários.

I - o acesso a compartilhamentos institucionais deve ser concedido sob solicitação do gestor da área correspondente.

II - o acesso aos serviços de compartilhamento deve prioritariamente utilizar as credenciais de acesso a rede do Tribunal.

III - deve-se estabelecer uma política de conteúdo para os serviços de armazenamento corporativo, garantindo ao administrador permissão de veto nas seguintes condições:

- a. armazenamento de arquivos não relacionados com o trabalho;
- b. armazenamento de conteúdo pornográfico, malware, softwares piratas ou não licenciados pelo TRE/PR;

IV - a SECTI tem permissão de remoção imediata de arquivos que contrariem essa norma, sendo o usuário responsável passível de medidas administrativas por mau uso;

V - a SECTI deve possuir acesso aos arquivos em qualquer meio para fins de gerenciamento de espaço de armazenamento e auditoria relacionada a uso irregular dos serviços, respeitando a privacidade legal dos usuários do Tribunal;

VI - deve-se estabelecer registro de rastreamento dos serviços de armazenamento de forma a permitir a auditoria do uso dos recursos, prevenir a ação de malware e analisar acessos indevidos aos arquivos;

VII - deve-se dar preferência a serviços que utilizem protocolos criptografados no processo de autenticação e transmissão de arquivos;

VIII - os usuários de TI são corresponsáveis pelos arquivos que compartilham, respondendo por uso indevido.

## CAPÍTULO XI

### DA APURAÇÃO DE RESPONSABILIDADES

Art. 25. O descumprimento dos critérios de segurança e das normas de conduta estipuladas neste normativo poderá ensejar, conforme a gravidade da falta, a instauração de sindicância ou processo administrativo disciplinar, visando à apuração da infração praticada pelo usuário.

Parágrafo único. Cabe à SECTI comunicar ao CGSI e à chefia imediata do usuário, a ocorrência de descumprimento das normas dispostas nesta instrução normativa, relatando o ocorrido para a adoção das medidas cabíveis.

**CAPÍTULO XII****DAS DISPOSIÇÕES FINAIS**

Art. 26. Aplicar-se-ão aos casos omissos as disposições do PSI/TSE.

Art. 27. Esta norma será atualizada ~~no~~ ~~mínimo~~ a cada 02 (dois) anos ou quando houver necessidade.

Art. 28. Revogam-se as Instruções Normativas TRE/PR/DG nº 03/2018 (correio eletrônico/e-mail), nº 01/2018 (serviços de compartilhamento de arquivos), nº 08/2018 (política de contas e senhas de acesso), nº 09/2018 (acesso à internet), nº 12/2018 (acesso aos serviços internos de Tecnologia da Informação por meio da Internet) e demais disposições em contrário.

Art. 29. Esta Instrução Normativa entrará em vigor na data da sua publicação.

Curitiba, 27 de outubro de 2022.

VALCIR MOMBACH

Diretor-Geral do TRE/PR

**SECRETARIA DE GESTÃO DE PESSOAS****PORTARIAS****PORTARIA N. 17/2023**

A BACHARELA DANIELE CRISTINE FORNECK FRANZINI, DIRETORA-GERAL EM EXERCÍCIO DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ,

usando das atribuições que lhe são conferidas pelo artigo 43, inciso VIII, do Regulamento da Secretaria deste Tribunal e conforme PAD n.º 1781/2023, resolve,

LOTAR

FRANCISCO GONÇALVES SIMÕES, servidor ocupante do cargo de Analista Judiciário, Área Judiciária, do Quadro de Pessoal deste Tribunal, na Coordenadoria Executiva da Escola Judiciária Eleitoral - COEJE, a partir de 12/12/2022.

PUBLIQUE-SE, ANOTE-SE E CUMPRA-SE. SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, em 18 de janeiro de 2023.

DANIELE CRISTINE FORNECK FRANZINI

Diretora-Geral em exercício

**12ª ZONA ELEITORAL****ATOS JUDICIAIS****PRESTAÇÃO DE CONTAS ELEITORAIS(12193) Nº 0600107-37.2022.6.16.0012**

PROCESSO : 0600107-37.2022.6.16.0012 PRESTAÇÃO DE CONTAS ELEITORAIS (SÃO MATEUS DO SUL - PR)

RELATOR : 012ª ZONA ELEITORAL DE SÃO MATEUS DO SUL PR

REQUERENTE : FERNANDA GARCIA SARDANHA

ADVOGADO : MARIA CAROLINE DE CAMARGO (110613/PR)

REQUERENTE : PARTIDO SOCIAL DEMOCRÁTICO - SÃO MATEUS DO SUL - PR - MUNICIPAL

ADVOGADO : MARIA CAROLINE DE CAMARGO (110613/PR)

REQUERENTE : RODRIGO SARDANHA

ADVOGADO : MARIA CAROLINE DE CAMARGO (110613/PR)

FISCAL DA