MINISTÉRIO PÚBLICO
ESTADO DO TOCANTINS

ATO Nº 107/2020

Institui a Política da Segurança da Informação e estabelece critérios relativos ao acesso, uso, armazenamento, procedimento, segurança e responsabilidade na utilização da tecnologia da informação do Ministério Público do Estado do Tocantins – MPTO.

A PROCURADORA-GERAL DE JUSTIÇA, no uso de suas atribuições legais e conforme disposto no artigo 17, inciso X, alíneas "a", "e" e "g", da Lei Complementar Estadual nº 51/2008; e,

Considerando que a efetividade da tecnologia da informação no âmbito do Ministério Público é condição essencial para o pleno exercício das atividades institucionais dos integrantes e unidades administrativas;

Considerando imprescindível garantir a segurança das informações e dados que trafegam nos recursos computacionais e tecnológicos deste Órgão, assegurando os atributos de confidencialidade, integridade, disponibilidade, autenticidade e sigilosidade, quando autorizada;

Considerando premente racionalizar e operacionalizar adequadamente o uso dos recursos e serviços relativos à tecnologia da informação disponibilizada nesta Instituição;

Considerando a necessidade de definir padrões técnicos e procedimentos para uso dos recursos e serviços disponíveis, bem como alinhar as ações de Tecnologia da Informação no âmbito interno aos objetivos estratégicos da Instituição;

Considerando as diretrizes definidas pelo Conselho Nacional do Ministério Público, por meio da Recomendação nº 13/2009 e Resoluções nºs 70/2011, 77/2011, 156/2016 e 171/2017, bem como o Plano de Segurança Institucional do MPTO, instituído pela Resolução CPJ nº 011/2014;

Considerando as práticas descritas nos manuais de boas práticas de governança da Tecnologia da Informação, especialmente o COBIT 4.1, PO 4.2 - Comitê Estratégico de Tecnologia da Informação CETI;

Considerando os arts. 1º e 2º da Lei nº 11.419/2006, que tratam sobrea informatização do Processo Judicial, e, art. 4º da Lei nº 12.682/12 que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos;

Considerando a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2018 e a instituição da Comissão Permanente de Documentos Sigilosos do Ministério Público do Estado do Tocantins – CPDS, pela Resolução CPJ nº 007/2017;

Considerando a celeridade processual proporcionada pelo uso das ferramentas de tecnologia da informação, bem como a economicidade pela diminuição do fluxo de correspondências físicas e demais documentos oficiais, deslocamentos desnecessários de servidores, além do melhor controle dos atos e ações institucionais e a prestação de serviços à sociedade;

RESOLVE:

Art. 1º Instituir a Política da Segurança da Informação e estabelecer critérios relativos ao acesso, uso, armazenamento, procedimento, segurança e responsabilidade na utilização da tecnologia da informação do Ministério Público do Estado do Tocantins – MPTO.

Art. 2º Este regulamento, conforme disposto no Anexo Único, aplica-se a todos os órgãos - Administração Superior, Administração, Execução, Auxiliares e Ouvidoria, bem como as unidades administrativas e usuários autorizados que utilizam a tecnologia da informação disponibilizada pelo MPTO, na realização das atividades de interesse exclusivamente institucional.

Art. 3º Este ato entra em vigor a partir da data da publicação, revogando-se as disposições contrárias, em especial os Atos PGJ nºs. 80/2007, 189/2007,17/2008, 27/2009, 72/2011 e 71/2012.

PUBLIQUE-SE E CUMPRA-SE.

PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO TOCANTINS, em Palmas, 16 de setembro de 2020.

MARIA COTINHA BEZERRA PEREIRA
Procuradora-Geral de Justiça

MINISTÉRIO PÚBLICO
ESTADO DO TOCANTINS

ANEXO ÚNICO

Índice

CAPÍTULO I
SEGURANÇA DA INFORMAÇÃO

Seção I
Política da Segurança da Informação

Art. 1º Instituir a Política da Segurança da Informação no âmbito do Ministério Público do Estado do Tocantins - MPTO que tem como pressupostos básicos:

I – preservação da credibilidade e do prestígio da Instituição;

II – proteção das informações e/ou dados judiciais e extrajudiciais que circulam no âmbito do MPTO;

III – efetivação de medidas de conscientização dos recursos humanos das unidades administrativas sobre a importância das informações processadas e sobre o risco da vulnerabilidade e integridade;

IV – armazenamento e proteção de acesso ao uso adequado das informações.

Art. 2º Para efeitos da Política da Segurança da Informação ficam estabelecidas as seguintes conceituações:

I – Confiabilidade: princípio de Segurança da Informação pelo qual se garante que o acesso à informação seja obtido somente por pessoas autorizadas;

II – Criticidade: grau de importância da informação para a continuidade das atividades do MPTO;

III – Disponibilidade: princípio de Segurança da Informação pelo qual se estabelece que as informações e os recursos estarão disponíveis sempre que necessário;

IV – Integridade: princípio de Segurança da Informação por meio do qual é garantida que a informação não será alterada sem a devida autorização;

V – Recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

~~VI – Usuário: é toda pessoa física ou jurídica que utiliza quaisquer recursos computacionais do MPTO de forma autorizada pelo DMTI;~~

~~VII – Tecnologia da Informação: conjunto de recursos tecnológicos e computacionais para geração e uso da informação;~~

~~VIII – Política da Segurança da Informação: normas que visam estabelecer procedimentos de proteção das informações e dados que circulam no âmbito do MPTO, com adoção de medidas para dar efetividade ao uso racional e adequado da tecnologia da informação disponibilizada;~~

~~IX – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como a intrusão, a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;~~

~~X – Comitê Estratégico de Tecnologia da Informação - CETI: formado por representantes da Administração Superior e do DMTI para atender às demandas originárias da Política da Segurança da Informação;~~

~~XI – Comissão Permanente de Documentos Sigilosos – CPDS: instituída com a finalidade de decidir sobre o tratamento e classificação de informações e arquivos sigilosos, dentre outras competências;~~

~~XII – Departamento de Modernização e Tecnologia da Informação – DMTI: órgão da estrutura administrativa da Diretoria-Geral do MPTO responsável pelo planejamento, coordenação, organização, controle e supervisão dos recursos computacionais da Instituição;~~

~~XIII – Recursos Computacionais: são todos os equipamentos, instalações, programas de computador e bancos de dados, direta ou indiretamente administrados e operados pelo DMTI para armazenar, processar, transmitir e disseminar informações de interesse institucional, dentre eles:~~

~~a) computadores, *tablets, notebooks, ultrabooks, smartphones* e terminais de qualquer espécie, incluídos acessórios;~~

b) impressoras, multifuncionais, leitores de código de barras e *escaneres* de qualquer espécie;

c) servidores de arquivos, de impressão, de correio eletrônico, *WEB,* aplicação e outros tipos de servidores de redes;

d) *modens*, roteadores, *switches*, *hubs,* redes de dados, soluções de segurança e demais equipamentos de conexão e comunicação de dados;

e) sistemas operacionais e aplicativos;

f) intranet, internet e correio eletrônico;

g) *softwares* adquiridos ou desenvolvidos pelo DMTI;

h) banco de dados ou documentos residentes em servidor de rede, disco, fita e outros meios;

i) salas de computadores, laboratórios, escritórios mobiliários específicos;

j) *site* ou *homepage* do MPTO;

k) manuais técnicos.

XIV – Material de Consumo de Informática: utilizados, direta ou indiretamente, para armazenar, processar, transmitir e disseminar informações na área de informática, consistindo em HD externos, *pendrives*, toner para impressora, CD, DVD, fita magnética e outros;

XV – Conta de Acesso Pessoal: pertence ao usuário e lhe permite acessar à rede, o correio eletrônico, a intranet e os *softwares* do MPTO;

XVI – Serviço de Correio Eletrônico Institucional: serviço de envio e recebimento de mensagens eletrônicas (e-mails) do MPTO, implementado e gerenciado pelo DMTI;

XVII – Serviço Externo de Correio Eletrônico: qualquer serviço de correio eletrônico disponibilizado por terceiros;

XVIII – Webmail: serviço de correio eletrônico disponível por meio de um sítio;

XIX – Login: processo de identificação e autenticação de usuários em programas computacionais e serviços de e-mail;

XX – Spam: mensagem geralmente destinada à realização de propaganda e marketing de produtos e serviços disponíveis no mercado, bem como veicular outros tipos de conteúdos indevidos;

XXI – Corrente: mensagem enviada com o objetivo de propagar um boato ou determinado assunto sem relação com as atividades da Instituição;

XXII – Scam: mensagem enviada com o objetivo de obter informações sensíveis, tais como senhas e números de cartão de crédito para utilização em fraudes;

XXIII – Código Malicioso: termo genérico que se refere a todos os tipos de software que executam ações maliciosas em um computador, como: vírus, worms, bots, cavalos de troia e rootkits;

XXIV – Software: qualquer programa, aplicativo ou sistema desenvolvido para utilização em computadores ou em outros dispositivos eletroeletrônicos;

XXV – Cliente de Correio Eletrônico: software no qual o usuário pode receber e enviar e-mails;

XXVI – Grupo ou Lista de e-mails: é um grupo de endereços eletrônicos organizados para fins de recebimento conjunto de mensagens.

Art. 3º São objetivos da Política da Segurança da Informação:

I – dotar o MPTO de instrumentos jurídicos, normativos e organizacionais que o capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, integridade e a disponibilidade dos dados e/ou informações tratadas, classificadas e sensíveis;

II – eliminar a dependência extrema em relação a sistemas, equipamentos, dispositivos e atividades vinculadas a segurança dos sistemas de informação;

III – promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

~~IV – estabelecer normas jurídicas necessárias para a efetiva implementação da segurança da informação;~~

~~V – promover as ações necessárias à implementação e manutenção da segurança da informação;~~

~~VI – promover o intercâmbio científico e tecnológico com outros órgãos estaduais ou federais sobre as atividades de segurança da informação;~~

~~VII – assegurar a operatividade dos sistemas de segurança da informação.~~

~~Seção II~~
~~Comitê Estratégico de Tecnologia da Informação~~

~~**Art. 4º** Para atender às demandas originárias da Política da Segurança da Informação fica instituído o Comitê Estratégico de Tecnologia da Informação – CETI que será composto, no mínimo, conforme o art. 2º da Res. CNMP nº 70/2011, pelos seguintes integrantes:~~

~~I – um Membro indicado pelo Procurador-Geral de Justiça;~~

~~II – um Membro indicado pelo Conselho Superior do Ministério Público;~~

~~III – um Membro indicado pela Corregedoria-Geral;~~

~~IV – Diretor-Geral da Procuradoria-Geral de Justiça;~~

~~V – Chefe do Departamento de Modernização e Tecnologia da Informação.~~

~~§ 1º O CETI terá como Presidente o Membro indicado pelo Procurador-Geral de Justiça e como Secretário o Chefe do Departamento de Modernização e Tecnologia da Informação.~~

~~§ 2º Em caso de ausência, afastamento ou impedimento, os integrantes do Comitê, se necessário, indicarão seus substitutos.~~

~~§ 3º O CETI reunir-se-á, ordinariamente, uma vez a cada trimestre e, extraordinariamente, por convocação de seu Presidente.~~

§ 4º Por deliberação do Comitê ou de seu Presidente poderão ser convidados a participar de reuniões pessoas físicas ou jurídicas que possam contribuir para o esclarecimento das matérias a serem apreciadas.

§ 5º Ao Presidente do CETI compete instituir comissões para auxiliar a tomada de decisão sobre assuntos de natureza técnica, definindo, no ato de constituição, seus objetivos específicos, sua composição e prazo para a conclusão dos trabalhos.

Art. 5º Compete ao CETI:

I – elaborar e aprovar o seu regimento interno;

II – estabelecer políticas e diretrizes de tecnologia de informação, alinhadas aos objetivos estratégicos da Instituição;

III – aprovar o Plano Diretor de Tecnologia da Informação do MPTO;

IV – definir as prioridades dos investimentos em tecnologia da informação;

V – estabelecer as prioridades para execução de projetos de tecnologia da informação;

VI – definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

VII – administrar e gerenciar a implantação, manutenção e aperfeiçoamento das Tabelas Unificadas no âmbito do MPTO, conforme artigo 6º da Res. CNMP n.º 63/2010.

CAPÍTULO II
DAS NORMAS DE USO E SEGURANÇA DA INFORMAÇÃO

Seção I
Dos Direitos e Obrigações dos Usuários

Art. 6º São direitos dos usuários autorizados:

I – fazer uso dos recursos computacionais da Instituição para a realização de atividades profissionais relacionadas aos serviços de interesse do MPTO;

II – ter conta de acesso pessoal à rede de computadores e aplicativos mediante a liberação automática de senha pelo Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP após os devidos registros em seus sistemas, sendo disponibilizado o suporte do DMTI, caso tenha problema de acesso e permissões;

III – ter conta de acesso pessoal ao correio eletrônico mediante a liberação automática de senha pelo Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP, após os devidos registros em seus sistemas, sendo disponibilizado o suporte do DMTI, caso tenha problema de acesso e permissões;

IV – acessar Internet, pelo navegador (*browser)* indicado pelo DMTI, e a Intranet por meio da senha pessoal liberada pelo Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP, encaminhada para e-mail não institucional cadastrado em sistema próprio deste departamento, com auxílio e suporte do DMTI, caso necessário;

V – ter restrita e/ou limitada privacidade das informações na sua área de armazenamento;

VI – solicitar atendimento técnico do DMTI por meio do *link* "Atendimento Informática", constante na página da Intranet, podendo se valer do pedido via telefone para o número (63) 3216-8888 e e-mail para suporte.ti@mpto.mp.br;

VII – receber o adequado atendimento do suporte técnico;

VIII – acessar a rede da Instituição por meio de computadores e/ou notebook pessoais quando devidamente autorizado pela Administração através da Chefia de Gabinete ou Diretoria-Geral, sem nenhum ônus para a Administração;

IX – inserir e/ou executar *pen drive* ou outro dispositivo similar nos recursos computacionais do MPTO somente quando proceder prévia varredura do antivírus disponível na rede no respectivo dispositivo.

Art. 7º São obrigações dos usuários autorizados:

I – zelar pela integridade e segurança dos equipamentos e pelas informações processadas e armazenadas nos recursos computacionais sob sua responsabilidade de uso;

II – utilizar dos recursos computacionais exclusivamente para os serviços da Instituição;

III – zelar pelo sigilo e segurança da sua senha de acesso pessoal à rede e aplicativos, que é de uso individual e intransferível, não podendo ser compartilhada com terceiros;

VI – manter, nos locais onde não tiver disponível servidor de rede, em especial nas Promotorias de Justiça do Interior, cópia de segurança de seus dados e/ ou informações, evitando a interrupção do serviço;

V – manter sigilo, integridade e segurança de todos os dados e/ou informações que tiverem acesso;

VI – não autorizar que pessoas estranhas ao quadro da Instituição tenham acesso físico aos equipamentos sob sua responsabilidade;

VII – manter constante cuidado de proteção contra vírus, principalmente quando do recebimento de mensagens pelo correio eletrônico, acesso à internet, download de arquivos com extensão que apresentem perigo de inserção ou execução de dispositivos nos recursos computacionais desta Instituição;

VIII – fazer uso racional do material de consumo da Instituição, combatendo o desperdício em todas as formas;

VIX – manter o bom uso, a limpeza e a conservação dos equipamentos de informática colocados a sua disposição;

X – manter o DMTI informado sobre qualquer mudança efetuada nos recursos computacionais colocados a sua disposição;

XI – respeitar e seguir as normas e procedimentos definidos pelo Procurador-Geral de Justiça, pelo CETI e pelo DMTI.

Seção II

Das Proibições aos Usuários

Art. 8º Fica proibido aos usuários:

I – utilizar os recursos e materiais de informática para trabalhos particulares ou que não tenham ligação com a finalidade da Instituição;

II – remover, transferir, emprestar, modificar ou proceder qualquer alteração nas características físicas ou técnicas dos equipamentos, sem a prévia autorização do DMTI;

III – compartilhar com terceiros contas de acesso pessoal à rede, às aplicações e outras espécies de autorização de uso individual e intransferível;

IV – executar ou configurar os recursos computacionais ou tecnológicos com a intenção de facilitar o acesso a usuários não autorizados;

V – obter acesso não autorizado aos sistemas;

VI – copiar, transferir ou emprestar software para finalidade ou pessoa estranha aos serviços da Instituição;

VII – destruir, estragar ou desconfigurar intencionalmente os equipamentos, softwares ou dados pertencentes à Instituição;

VIII – violar o sistema de segurança dos recursos computacionais, por exemplo: identificação de usuários, senhas de acesso, fechaduras automáticas, catracas, sistemas antivírus ou outros;

IX – usar, instalar, executar, copiar ou armazenar aplicativos, programas ou qualquer outro material que não esteja devidamente autorizado pela Instituição;

X – remover, copiar, emprestar ou divulgar documento confidencial e sigiloso, bem como endereços residenciais e eletrônicos de usuários, de propriedade da Instituição;

XI – utilizar a tecnologia da informação desta Instituição para constranger, assediar, ofender, caluniar ou ameaçar qualquer pessoa ou instituição que sejam incompatível com o ambiente de trabalho;

XII – retirar qualquer recurso computacional do local destinado sem prévia autorização do Procurador-Geral de Justiça ou Departamento autorizado por ele;

XIII – utilizar programas de rádio, videoconferência, filmes, vídeos ou outros, que trafegam dados que não sejam textos, sem a cientificação e devida autorização do DMTI;

XIV – conectar qualquer equipamento particular à rede local do MPTO sem o conhecimento e anuência da Administração através da Chefia de Gabinete ou Diretoria-Geral, e sem que o DMTI, através da Área de Redes, Telecomunicações e Segurança da Informação - RTSI, retire o serviço DHCP para esse equipamento e libere o acesso à rede Institucional por meio do registro do endereço MAC;

XV – instalar ou utilizar outros programas de mensagens instantâneas que não aquele indicado pela Instituição.

Seção III

Do Acesso à Internet

Art. 9º Todos os usuários autorizados terão direito ao acesso à Internet para realização das atividades relacionadas ao serviço da Instituição, por meio do *browser* indicado pelo DMTI.

Art. 10. É proibida a utilização da internet para:

I – participar de salas de bate-papo, exceto aquelas de exclusivo interesse das atividades da Instituição;

II – engajar-se em atividades comerciais ou político partidárias;

III – copiar arquivos que ofereçam risco potenciais à segurança do ambiente de rede do MPTO, tais como os arquivos com as extensões exe, src, bat, pif, vbc e outros de mesma natureza;

IV – copiar arquivos (*download*) que contenham som, vídeo ou animação, que não sejam de interesse das atividades do MPTO;

V – acessar sites impróprios que contenham conteúdos pornográficos, ilegais ou antiéticos;

VI – participar de qualquer ação que comprometa a segurança do site e das informações e/ou dados que circulam na Instituição;

VII – exibição, veiculação ou armazenamento voluntário de páginas com conteúdo pornográfico, erótico, jogos de qualquer espécie, comercial, político partidário, ofensivo ao decoro pessoal e ao princípio de urbanidade e que provoquem sobrecarga no sistema.

Art. 11. O uso da internet será monitorado pelo DMTI mediante emprego de ferramentas específicas, com a possibilidade de geração de relatórios e estatísticas dos sites visitados, serviços utilizados e usuários com maior acesso.

Art. 12. O bloqueio de sítios eletrônicos estranhos à atividade institucional, com base na Política da Segurança da Informação, ficará a cargo do DMTI, principalmente quando se tratar de arquivos de vídeos, áudios, executáveis, *batches*, *scripts*, macros e qualquer outro que porventura possam comprometer a segurança e estrutura da rede do MPTO.

§ 1º Cabe ao CETI verificar a necessidade de bloqueio de outras espécies de sítios eletrônicos.

§ 2º Se houver imprescindível necessidade, em razão de serviço, de acessar sítio eletrônico ou documento previamente bloqueado pelo DMTI, deverá o pedido de liberação ser autorizado pelo CETI ou seu Presidente, de forma temporária ou definitiva, para que o servidor execute o trabalho.

Art. 13. Incumbe ao Chefe de Gabinete do Procurador-Geral de Justiça a análise prévia das matérias a serem publicadas no site eletrônico do MPTO, que após deferimento encaminhará ao departamento competente para divulgação.

Seção IV

Do Uso da Intranet

Art. 14. O acesso à intranet desta Instituição é restrito aos usuários autorizados.

Art. 15. Os órgãos de execução, os órgãos auxiliares e os departamentos do MPTO poderão divulgar na Intranet as respectivas ações desenvolvidas.

Art. 16. O acesso à intranet é monitorada e auditada por meio de *login* e senha pessoal.

Seção V
Do Uso do Correio Eletrônico

Art. 17. O correio eletrônico institucional deve ser utilizado somente em atividades estritamente relacionadas às funções institucionais e será para comunicação e troca de documentos internos, evitando-se, tanto quanto possível, a impressão do conteúdo de mensagens.

Art. 18. É garantido a cada integrante do MPTO o uso de uma conta de correio eletrônico da Instituição, criada pelo DMTI, desde que possua identificação de acesso para utilização do serviço.

§ 1°. Servidores cedidos, prestadores de serviços terceirizados, consultores e estagiários poderão ter acesso ao correio eletrônico institucional durante o período de cessão, de prestação dos serviços, consultoria ou estágio, observando as normas aqui enumeradas, mediante cadastro realizado pelo Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP.

§ 2º. Solicitações para criação ou exclusão serão realizadas de forma automática após os devidos cadastros ou bloqueios pelo Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP no sistema de Recursos Humanos.

§ 3°. As unidades administrativas poderão ter endereço de correio eletrônico, devendo ser encaminhado o pedido formal ao DMTI, com a justificativa do chefe ou responsável da unidade.

§ 4°. A caixa postal de uma unidade administrativa poderá ser acessada pelo gestor da unidade e pelos servidores por ele designados.

§ 5°. É permitida a criação de listas de correio eletrônico, com o objetivo de atender necessidades específicas de determinados grupos de usuários, com gerenciamento pelo DMTI.

§ 6°. Serão mantidas as contas de e-mail dos membros, servidores e comissionados exonerados e aposentados, pelo prazo máximo de 180 (cento e oitenta) dias, a contar da publicação dos respectivos atos no Diário de Oficial do MPTO, para cópia e envio das informações necessárias, sem possibilidade de recebimento de novos e-mails.

§ 7º. Após o decurso do prazo de 180 (cento e oitenta) dias a conta de e-mail deverá ser bloqueada totalmente.

§ 8°. A conta de e-mail desativada terá seu conteúdo preservado pelo DMTI por um período de 05 (cinco) anos, com exclusão após o decurso desse prazo.

§ 9º Por se tratar de e-mail funcional e institucional, após o desligamento do membro ou servidor a Administração terá pleno direito a todas as informações da conta, podendo acessar o conteúdo para análise ou interesse do serviço público.

Art. 19. O endereço de correio eletrônico institucional será composto pelo sufixo "@mpto.mp.br".

Art. 20. Constitui uso indevido do serviço de correio eletrônico institucional:

I – enviar qualquer tipo de spam, scam ou "corrente";

II – enviar mensagens com vírus ou códigos maliciosos anexados;

III – enviar material protegido por leis de propriedade intelectual;

IV – enviar mensagens com conteúdo considerado ofensivo, obsceno, discriminatório, antiético, ilegal ou impróprio, como: pornografia, pedofilia, racismo, apologia ao crime, calúnia, difamação, injúria, entre outros;

V – enviar mensagens com conteúdos, arquivos, fotos, imagens, sons ou vídeos não relacionados às funções institucionais;

VI – enviar material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos políticos, clubes, associações e sindicatos;

VII – assuntos que provoquem assédio, constrangimento ou que prejudiquem a imagem da Instituição;

VIII – utilizar clientes de correio eletrônico não homologados pelo DMTI e pela Procuradoria-Geral de Justiça;

IX – participar de lista de e-mails cujo tema não esteja relacionado às atividades institucionais;

X – enviar mensagens que representem riscos de segurança, ou que afetem o desempenho dos recursos de tecnologia da informação, ou, ainda, que possam comprometer, de alguma forma, a integridade, a confidencialidade ou a disponibilidade das informações institucionais;

XI – o redirecionamento automático de mensagens para serviços externos de correio eletrônico;

XII – enviar listas contendo o endereço eletrônico institucional (e-mails) de membros e servidores do MPTO para fins não relacionados às funções institucionais.

Art. 21. Os anexos e/ou *hiperlinks* das mensagens do correio eletrônico institucional poderão ser bloqueados quando oferecerem riscos à segurança da informação e comunicação.

Parágrafo único. A abertura de mensagens de remetentes desconhecidos, externos ao MPTO, deve ser avaliada, especialmente no caso de dúvidas quanto à natureza do seu conteúdo, como arquivos inesperados ou *hiperlinks* para endereços externos não relacionados às atividades profissionais em curso.

Art. 22. O uso indevido do correio eletrônico das unidades administrativas é de responsabilidade do respectivo gestor e dos servidores por ele eventualmente designados para acessá-lo, na medida de suas culpabilidades.

Art. 23. Compete ao DMTI a gestão das funcionalidades e a segurança do serviço de correio eletrônico institucional do MPTO, para garantir o cumprimento deste Ato.

§ 1º. O DMTI é responsável pela implementação, configuração e gerenciamento dos recursos de tecnologia da informação relacionados aos serviços de correio eletrônico institucional.

§ 2º. O DMTI manterá os registros de envio e recebimento de mensagens, resguardado o sigilo das correspondências.

§ 3º. O DMTI estabelecerá os limites de tamanho das caixas postais e das mensagens enviadas e recebidas pelos usuários, de acordo com a capacidade técnica dos servidores de armazenamento de dados.

§ 4º. A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de spam, cabendo ao DMTI estabelecer tal limite, bem como acordar com as demais áreas as eventuais exceções, de acordo com os interesses do MPTO.

Art. 24. São deveres dos usuários:

I – utilizar o correio eletrônico institucional para os objetivos e funções próprias e inerentes às atribuições funcionais;

II – verificar diariamente o conteúdo da conta pessoal, eliminando periodicamente as mensagens contidas nas caixas postais;

III – manter em sigilo sua senha de acesso ao correio eletrônico, visto que esta é de uso pessoal e intransferível, substituindo-a em caso de suspeita de violação;

IV – não permitir acesso de terceiros ao correio eletrônico por meio da senha pessoal;

V – responsabilizar-se pelas mensagens e anexos enviados e/ou recebidos;

VI – sair do acesso do e-mail institucional toda vez que se ausentar da estação de trabalho, evitando o uso indevido por terceiros;

VII – comunicar o recebimento de mensagens com os conteúdos indevidos ao DMTI;

VIII – efetuar a exclusão de e-mails da pasta Lixeira e de e-mails desnecessários, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo;

IX – notificar ao DMTI a ocorrência de alterações que afetem o cadastro do usuário de e-mail;

X – incluir no recurso “assinatura de e-mail” a identificação, contendo pelo menos os seguintes dizeres referente ao remetente: nome do usuário, função que exerce na Instituição, setor a que pertence e nome da Instituição, além de um aviso legal, referenciando a confidencialidade da informação, quando for o caso;

XI – comunicar ao destinatário quando identificar no envio de mensagens.

Art. 25. São deveres dos usuários dos grupos de e-mail:

I – utilizar a ferramenta de distribuição de mensagens exclusivamente para troca de mensagens que sejam de interesse institucional ou do grupo;

II – não permitir acesso de terceiros às listas de distribuição de e-mail;

III – guardar sigilo funcional das discussões travadas nos respectivos grupos;

IV – notificar ao DMTI quando do recebimento de mensagens que contrariem o disposto nesta regulamentação.

Art. 26. O DMTI comunicará à Procuradoria-Geral de Justiça as irregularidades constatadas, a fim de que sejam tomadas as providências cabíveis.

Art. 27. Quaisquer violações às normas de segurança da informação e comunicação do MPTO ensejarão sanções administrativas, cíveis e criminais, caso aplicáveis.

Art. 28. A caixa postal de correio eletrônico terá o valor inicial de 400MB, podendo ser ampliada conforme disponibilidade de espaço, ficando o controle sob responsabilidade do DMTI.

Seção VI
Da Utilização do Mensageiro Corporativo

Art. 29. O mensageiro corporativo é um sistema de acesso voluntário dos usuários da rede, destinado à troca de mensagens instantâneas entre seus usuários.

§ 1º O acesso ao mensageiro corporativo do MPTO é restrito aos usuários cadastrados na rede de informática da Instituição.

§ 2º O DMTI é responsável pela instalação, manutenção e armazenamento das informações que circulam no mensageiro corporativo.

§ 3º As reclamações pertinentes ao conteúdo de mensagens veiculadas no mensageiro corporativo deverão ser encaminhadas à Corregedoria-

Geral, em se tratando de membro, ou à Diretoria-Geral, nos demais casos, para eventual provocação da suspensão do acesso e/ou apuração de eventuais faltas funcionais.

CAPÍTULO III
DOS EQUIPAMENTOS DE INFORMÁTICA, MANUTENÇÃO E SOFTWARES

Seção I
Da Instalação e Manutenção dos Equipamentos

Art. 30. A instalação e desinstalação de equipamentos de informática nas dependências do MPTO, incluindo Promotorias de Justiça do interior é de responsabilidade do DMTI, mediante prévio agendamento pelo usuário de, no mínimo, 02 (dois) dias.

§ 1º Havendo necessidade de mudança do local dos recursos computacionais, o chefe do departamento fará solicitação, por meio dos canais de atendimentos disponibilizados pelo DMTI a Área Controle de Equipamentos, Manutenção e Atendimento - ACEMA, informando o motivo, o número do patrimônio, a nova localização e quem é o responsável pelo equipamento.

§ 2º No caso de efetiva mudança do equipamento, deverá o Assessor de TI da Área Controle de Equipamentos, Manutenção e Atendimento - ACEMA informar a Área de Patrimônio do Departamento Administrativo sobre a alteração.

Art. 31. A manutenção preventiva e corretiva dos equipamentos de informática do MPTO é de responsabilidade exclusiva do DMTI, por meio da Área Controle de Equipamentos, Manutenção e Atendimento - ACEMA, e será realizada por técnicos de informática.

§ 1º Havendo necessidade de manutenção em equipamentos de informática, deverá o usuário comunicar o DMTI por meio do *link* "Atendimento Informática" que se encontra na página da Intranet ou dos canais de comunicações disponibilizados.

§ 2º O usuário deverá especificar detalhadamente o defeito apresentado nos recursos computacionais ou tecnológicos na ocasião da solicitação do suporte técnico ao DMTI;

§ 3º A permanência dos equipamentos de informática para manutenção no DMTI deverá observar que:

I – a Área Controle de Equipamentos, Manutenção e Atendimento - ACEMA tem o prazo de até 04 (quatro) horas para informar ao usuário sobre a situação do equipamento, o diagnóstico e a previsão para devolução;

II – no caso do equipamento estar na garantia, será aberto um chamado junto à autorizada para adoção das providências de acordo com prazo de garantia de cada fabricante, que será repassado ao usuário do equipamento;

III – no caso das estações de trabalho e servidores de redes serem enviados para manutenção externa, recomenda-se a retenção das mídias de armazenamento, de modo a preservar os dados contidos.

Art. 32. É vedada a manutenção de equipamentos de informática particulares, de associações e sindicatos, incluindo *hardware* e *software*, por técnicos do DMTI no âmbito do MPTO.

Art. 33. Todo computador é entregue lacrado e cabe ao respectivo usuário responsável pelo equipamento mantê-lo íntegro, de forma a garantir a inviolabilidade e segurança.

Art. 34. O sistema operacional utilizado nos equipamentos do MPTO deverá ser preferencialmente o LINUX, quando possível, e a ferramenta para escritório deverá ser o LibreOffice ou similar para todos os sistemas operacionais.

Parágrafo único. A adoção de um sistema operacional diferente do LINUX deverá ser justificada e comprovada sua necessidade.

Seção II
Da Cópia de Segurança (*Backup*)

Art. 35. O MPTO possui sistema de *backup* que armazena cópia das informações e/ou dados que circulam na rede institucional em meio digital para assegurar recuperação, quando se fizer necessário.

Art. 36. O DMTI do MPTO é responsável pelo *backup* das informações que trafegam na rede da Instituição.

Parágrafo único. O *backup* é realizado diariamente no horário compreendido entre 20h e 06h.

Art. 37. O MPTO conta com um servidor de rede que atende a Procuradoria-Geral de Justiça e as Promotorias de Justiça da Capital, situadas no prédio sede, para armazenar as informações e/ou dados institucionais que trafegam na rede da Instituição.

§ 1º A gravação no servidor de rede de arquivos que não contenham relação com as atividades desenvolvidas pelo MPTO, tais como, músicas, fotos, vídeos e outros, é vedada, exceto em caso de imprescindível necessidade, a qual deve ser realizada pelo DMTI ou à Área de Redes, Telecomunicações e Segurança da Informação - RTSI, após a devida solicitação.

§ 2º É de responsabilidade exclusiva dos servidores da Área de Redes, Telecomunicações e Segurança da Informação – RTSI a realização de backups diários e, quando necessário, as respectivas restaurações.

§ 3º É de responsabilidade dos membros e servidores, principalmente àqueles que atuam no Interior do Estado, quando não houver servidor de rede, salvar os arquivos armazenados no disco rígido - HD (*winchester)* do computador em que trabalham em outro meio, a fim de preservar a informação no caso de erro ou defeitos nos equipamentos.

Seção III
Do Desenvolvimento de *Softwares*

Art. 38. O DMTI desenvolverá *softwares* quando formalmente solicitado pelo responsável do Departamento.

§ 1º A solicitação deverá ser dirigida ao Chefe do DMTI, com o detalhamento da funcionalidade almejada pelo sistema, cabendo ao CETI verificar a viabilidade e a prioridade no atendimento quando existirem outros *softwares* em desenvolvimento.

§ 2º Quando autorizado o desenvolvimento do sistema, o DMTI para execução do projeto formará equipe de trabalho, que será composta por analista e técnicos de informática com membros e servidores dos departamentos que farão uso do sistema a ser desenvolvido.

§ 3º Previamente aos trabalhos de desenvolvimento do *software*, a equipe de trabalho se reunirá para ratificar as funcionalidades que abarcará o sistema, bem como suas abrangências.

§ 4º O DMTI terá o prazo mínimo de 30 (trinta) dias e máximo de 6 (seis) meses para realizar o levantamento das informações, planejamento do sistema e dar início ao processo de desenvolvimento.

§ 5º A variação temporal dependerá do número de funcionalidades requeridas, da colaboração do departamento e da complexidade do sistema.

§ 6º O prazo máximo de 6 (seis) meses poderá ser excedido, por igual período, quando a complexidade do sistema reclamar ou as informações das rotinas departamentais não forem devidamente repassadas ao DMTI pelo departamento responsável.

§ 7º O CETI definirá as prioridades nos projetos de desenvolvimentos de *softwares*.

§ 8º O DMTI divulgará o andamento da solicitação de *softwares* (aguardando, em desenvolvimento e concluído) em reuniões do CETI.

Art. 39. Os direitos autorais dos *softwares* desenvolvidos pelo DMTI são de propriedade do MPTO.

Parágrafo único. É vedada a cessão de *software* ou de documentação relativa a sua programação sem expressa autorização do Procurador-Geral de Justiça.

Art. 40. O DMTI, por meio da Área de Análise e Desenvolvimento de Sistemas – ADS é responsável pela criação do *software*, coordenação do desenvolvimento, quando o mesmo ocorrer por terceiros e pelo suporte técnico.

Parágrafo único. O cadastro das informações no sistema e sua alimentação não se incluem no rol de atribuições do DMTI.

~~CAPÍTULO IV~~
~~DAS SENHAS DE ACESSOS~~

~~**Art. 41.** A senha de acesso é pessoal e intransferível, cabendo ao detentor sua guarda, sigilo e responsabilidade pelo uso.~~

~~**Art. 42.** Preferencialmente a senha deverá possuir no mínimo 08 (oito) caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais, devendo ser alterada a cada 06 (seis) meses, evitando repetições.~~

~~CAPÍTULO V~~
~~DA ASSINATURA ELETRÔNICA E VALIDADE JURÍDICA DOS ATOS E DOCUMENTOS PRODUZIDOS POR MEIO DOS SISTEMAS DE INFORMAÇÃO~~

~~**Art. 43.** Fica reconhecida, para os fins de instrução processual no âmbito administrativo desta Instituição, a assinatura eletrônica inserida nos documentos por meio dos Sistemas de Informações do MPTO e suas funcionalidades.~~

~~**Art. 44.** A assinatura eletrônica (login e senha) será constituída, no mínimo, de assinatura cadastrada pelo DMTI com login permanente e senha pessoal, que serão fornecidos aos integrantes da Instituição, colaboradores, estagiários e funcionários terceirizados, cadastrados no Departamento de Gestão de Pessoas e Folha de Pagamento - DGPFP.~~

~~**Art. 45.** Em havendo avanços na tecnologia disponível, poderá o DMTI adotar meios de Certificação Digital ou instrumentos semelhantes a esta, para utilização nos sistemas desta Instituição.~~

~~**Art. 46.** A prática de atos assinados eletronicamente importa na responsabilização administrativa, civil e criminal pelo uso indevido da assinatura.~~

~~**Art. 47.** Para fins de instrução dos processos e procedimentos administrativos eletrônicos, o interessado poderá digitalizar documentos físicos necessários, permanecendo estes sob sua posse, certificadas sua autenticidade mediante o uso da assinatura eletrônica.~~

Art. 48. Para fins de instrução processual deverão ser observadas, tanto na formatação dos sistemas, como na transferência das informações do mesmo para o processo físico, quando for o caso, as diretrizes legais referentes ao processo administrativo e as despesas públicas.

Art. 49. Para garantir a identificação deverá o sistema construído pelo DMTI produzir numeração sequencial e única para cada requerimento gerado pelo sistema, devendo ainda ser possível a consulta às informações a qualquer tempo, mediante o número criado.

Art. 50. Para construção de novos sistemas e ou modernização dos existentes, dever-se-á observar as diretrizes estabelecidas pela Lei de Acesso à Informação, para possibilitar consulta virtual por interessado, defeso alteração dos atos existentes e ressalvados os classificados em grau de sigilo.

Art. 51. Os documentos eletrônicos gerados pelos sistemas de informações do MPTO deverão conter:

I – carimbo digital ou similar que identifique o autor, data e hora da ação;

II – identificação no documento, caso esteja dotado de certificado digital;

III – código único de identificação que possibilite a verificação de sua autenticidade no sítio do MPTO.

Art. 52. São de responsabilidade exclusiva dos integrantes do MPTO:

I – o sigilo da assinatura eletrônica, não sendo oponível, em qualquer hipótese, a alegação de seu uso indevido, sendo de responsabilidade do usuário a sua guarda e sigilo;

II – a preparação dos documentos no sistema e a juntada de anexos, observadas as restrições colocadas pelo DMTI, no que diz respeito à redação oficial, características da peça e formatação.

Art. 53. Será de responsabilidade do DMTI:

I – construir os sistemas de forma a garantir a segurança necessária às informações, observadas as diretrizes da Política da Segurança da Informação instituída no âmbito do MPTO e da legislação pertinente;

II – armazenar as informações geradas no sistema em meio que garanta a preservação e a integridade dos dados;

III – utilizar de tecnologia que permita identificar possíveis fraudes nos sistemas;

IV – informar possível caso identificado como fraude nos sistemas de informações, à Diretoria-Geral quando se tratar de servidor ou a Corregedoria-Geral do Ministério Público quando se tratar de membro do MPTO.

Art. 54. Os sistemas de informações do MPTO possuirão ferramenta de avisos e controle de prazos que permitam a responsabilização do usuário que der causa a atraso injustificado no cumprimento de sua obrigação.

CAPÍTULO VI
DOS SERVIDORES DE PRODUÇÃO E BANCO DE DADOS

Art. 55. O acesso ao servidor (equipamento) de produção pela equipe do DMTI será realizado através de autenticação por usuário e chave pública.

Art. 56. Toda operação realizada no servidor de produção deverá ser registrada em *logs*.

Art. 57. Cada integrante da equipe técnica que desempenhe atividades no banco de dados deverá possuir seu usuário de acesso exclusivo, vedada a utilização de usuário padrão disponível para todos.

Art. 58. Os *logs* de conexões e operações deverão ser registrados no banco de dados, bem como as provenientes a partir de qualquer cliente web, aplicativos desktops e terminal/shell.

Art. 59. Cada membro da equipe da Área de Análise e Desenvolvimento de Sistemas – ADS e da Área de Redes, Telecomunicações e Segurança da Informação - RTSI definirá a estratégia de individualização das ações executadas, principalmente em relação ao acesso de informações sensíveis da base de dados do MPTO.

CAPÍTULO VII
DAS DISPOSIÇÕES GERAIS

Art. 60. A autorização para utilizar os recursos computacionais da Instituição é facultada a membro, servidor, seja efetivo, comissionado ou à disposição, estagiário, colaborador ou prestador de serviço e demais servidores de instituições conveniadas, mediante abertura de conta pessoal junto ao DMTI.

Art. 61. Todos os usuários autorizados têm o dever de noticiar ao DMTI tentativa de acesso não autorizado, uso indevido ou qualquer ocorrência que evidencie desrespeito a este Ato, devendo tomar imediatamente as providências necessárias que estiverem ao seu alcance para garantir a segurança, integridade e a conservação dos recursos computacionais da Instituição.

Art. 62. O DMTI através da Área de controle de Equipamentos, Manutenção e Atendimento - ACEMA e da Área de Redes, Telecomunicações e Segurança da Informação - RTSI deverá adotar uma política de limpeza de mídias de armazenamentos para estações de trabalho e servidores de rede, utilizando-se de ferramentas para sobrescrita de dados, de modo a reduzir a possibilidade de recuperação dos arquivos e, em caso de impossibilidade de realizar a ação, recomenda-se a retenção e posterior destruição da mídia de armazenamento.

Art. 63. É necessária a supervisão de um profissional do quadro ministerial aos colaboradores do DMTI com vínculo externo, no acesso a dados sensíveis e nos atendimentos *in loco*.

Art. 64. O DMTI em atuação conjunta com o CETI deverão criar políticas complementares a este ato, quando for necessário, não sobrepondo as diretrizes aqui estabelecidas, a fim de preservar os interesses Institucionais, acompanhando as atualizações tecnológicas e novas políticas de segurança e boas práticas.

Parágrafo único. As políticas do DMTI aprovadas pelo CETI deverão ser publicadas na intranet para conhecimento de todos.

Art. 65. A violação das normas descritas neste Ato implicará em responsabilização disciplinar, independentemente da responsabilidade civil e penal.

Art. 66. Serão alcançados por este Ato os estagiários do Ministério Público, funcionários terceirizados, colaboradores, prestador de serviço e voluntário que para o exercício de suas funções possuam credenciamento de acesso aos sistemas de informações.

Art. 67. Os casos omissos serão decididos pelo Procurador-Geral de Justiça.

PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO TOCANTINS, em Palmas, 16 de setembro de 2020.

MARIA COTINHA BEZERRA PEREIRA
Procuradora-Geral de Justiça

Documento assinado eletronicamente por **Maria Cotinha Bezerra Pereira**, **Procuradora Geral de Justiça** , em 16/09/2020, às 17:08, conforme art. 33, do Ato PGJ nº 120, de 06 de novembro de 2019.

A autenticidade do documento pode ser conferida no site https://sei.mpto.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0032650** e o código CRC **0E42CC04**.

Autos SEI nº 19.30.1500.0000132/2019-76