

ATO Nº 072/2011

Institui a Política de Segurança da Informação no âmbito do Ministério Público do Estado do Tocantins e regulamenta os critérios básicos de uso, serviços, segurança e responsabilidades relativos à utilização da Tecnologia da Informação do Ministério Público do Estado do Tocantins.

O PROCURADOR GERAL DE JUSTIÇA, no uso de suas atribuições legais e conforme disposto no artigo 17, Incisos X, letras "a", "e" e "g", da Lei Complementar Estadual nº 51/2008; e,

Considerando que o regular funcionamento da tecnologia da informação no âmbito do Ministério Público é condição para o pleno exercício das atividades institucionais dos membros, dos servidores, das unidades administrativas, beneficiando, sobremaneira, a sociedade;

Considerando a imprescindível necessidade de garantir a segurança das informações e dados que trafegam nos recursos computacionais e tecnológicos deste Ministério Público;

Considerando que são características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade, autenticidade e, muitas vezes, sigilosidade;

Considerando a premente demanda para racionalizar e operacionalizar de forma adequada o uso dos recursos e serviços relativos à tecnologia da informação disponibilizada nesta Instituição;

Considerando a necessidade de definir padrões técnicos e procedimentos para utilização desses recursos e serviços, bem como alinhar as ações de Tecnologia da Informação no âmbito do Ministério Público do Estado do Tocantins aos objetivos estratégicos da Instituição;

Considerando que a utilização inadequada dos recursos e serviços da tecnologia da informação acarreta prejuízo e sobrecarga a infraestrutura;

Considerando a Recomendação nº 13, de 16.06.2009, do Conselho Nacional do Ministério Público, que dispõe sobre a implantação do Plano de Segurança Institucional nas áreas da Segurança da Informação, Segurança de Recursos Humanos, Segurança de Materiais e Segurança de Áreas e Instalações;

Considerando as práticas descritas nos manuais de boas práticas de governança da Tecnologia da Informação, especialmente o COBIT 4.1¹, PO 4.2 - Comitê Estratégico de TI;

Considerando as recomendações constantes no Acórdão nº 436/2007 do Tribunal de Contas da União;

Considerando os seguintes conceitos:

Tecnologia da Informação: serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação.

Política da Segurança da Informação: conjunto de normas que visam estabelecer procedimentos de proteção das informações e dados que circulam no âmbito do Ministério Público, bem como implementar medidas para dar efetividade ao uso racional e adequado da tecnologia da informação disponibilizada;

Comitê Estratégico de Tecnologia da Informação - CETI: formado por representante da Administração Superior e representantes do Departamento de Tecnologia da Informação para atender as demandas originárias da Política da Segurança da Informação.

Departamento de Tecnologia da Informação - DTI: Unidade Executiva do Ministério Público do Estado do Tocantins responsável pelo planejamento, coordenação, organização, controle e supervisão dos recursos computacionais da Instituição;

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

- computadores, *tablets*, *notebooks* e terminais de qualquer espécie, incluídos acessórios;
- impressoras, leitores de código de barras e *scanners* de qualquer espécie;
- servidores de arquivos, de impressão, de correio eletrônico, *WEB*;
- *modems*, roteadores, *switches*, *hubs* e redes;
- sistemas operacionais e aplicativos;

¹ Trata-se de um guia internacional de boas práticas dirigido para a gestão de tecnologia de informação (TI). Traduzido para a língua portuguesa em 2010, na versão 4.1.

- intranet, internet e correio eletrônico;
- softwares adquiridos ou desenvolvidos pelo DTI;
- banco de dados ou documentos residentes em servidor de rede, disco, fita e outros meios;
- salas de computadores, laboratórios, escritórios mobiliários específicos;
- site ou homepage do MPE/TO;
- manuais técnicos.

Material de Consumo de Informática: materiais utilizados, direta ou indiretamente, para armazenar, processar, transmitir e disseminar informações na área de informática, tais como: formulários contínuos, discos, disquetes, HD externos, pen drives, toner para impressora, CD, DVD, fita magnética, tinta para impressora matricial e outros.

Usuário Autorizado: é toda pessoa física ou jurídica que se utiliza de quaisquer recursos computacionais desta Instituição de forma autorizada pelo Departamento de Tecnologia da Informação. São eles: membros, servidores (efetivo, comissionado ou à disposição), estagiários, prestadores de serviço e demais servidores de instituições conveniadas.

Conta de Acesso Pessoal: conta que pertence ao usuário e lhe permite acessar à rede, o correio eletrônico, a intranet e os softwares do Ministério Público do Estado do Tocantins.

Mensageiro Corporativo: sistema de acesso voluntário dos usuários da rede, destinado à troca de mensagens instantâneas entre os usuários autorizados.

RESOLVE:

Artigo 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.

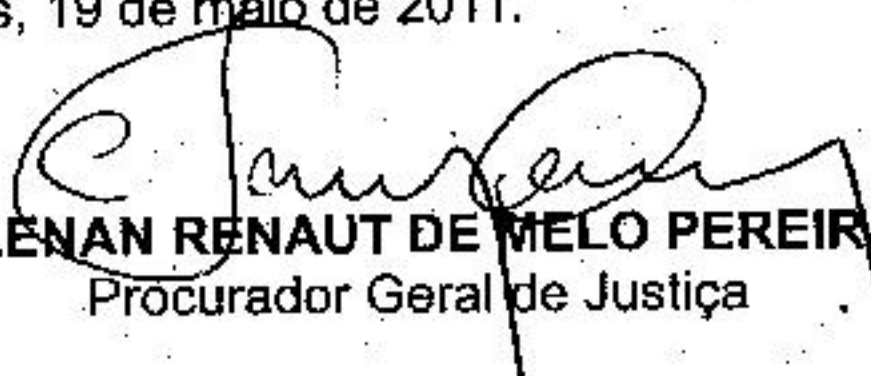
Artigo 2º - Este regulamento, conforme disposto no Anexo I, aplica-se a todos os órgãos (Administração Superior, Execução ou Auxiliares), unidades administrativas e usuários autorizados que utilizam a tecnologia da informação, disponibilizada pelo Ministério Público do Estado do Tocantins, na realização das atividades de interesse exclusivamente institucional.



Artigo 3º - Este ato entra em vigor a partir da data da publicação, revogando-se as disposições contrárias, em especial os Atos nºs. 80/2007, 17/2008, 27/2009.

PUBLIQUE-SE E CUMPRA-SE.

PROCURADORIA GERAL DE JUSTIÇA DO ESTADO DO TOCANTINS, em Palmas, 19 de maio de 2011.


CLEON RENAUT DE MELO PEREIRA
Procurador Geral de Justiça

ANEXO I

SUMÁRIO

CAPÍTULO I - SEGURANÇA DA INFORMAÇÃO	6
Seção I – Política da Segurança da Informação	6
Seção II – Comitê Estratégico de Tecnologia da Informação	7
CAPÍTULO II – DAS NORMAS DE USO E SEGURANÇA DA INFORMAÇÃO	9
Seção I – Dos Direitos e Obrigações dos Usuários	9
Seção II – Das Proibições dos Usuários	11
Seção III – Do Acesso à Internet	12
Seção IV – Do Uso da Intranet	14
Seção V – Do Uso do Correio Eletrônico	14
Seção VI – Da Utilização do Mensageiro Corporativo	15
CAPÍTULO III – DOS EQUIPAMENTOS DE INFORMÁTICA, MANUTENÇÃO E DESENVOLVIMENTO DE SOFTWARES	16
Seção I – Da Instalação e Manutenção dos Equipamentos	16
Seção II – Da Cópia de Segurança (BACKUP)	17
Seção III – Do Desenvolvimento de Softwares	18
CAPÍTULO IV – DAS DISPOSIÇÕES GERAIS	19

CAPÍTULO I

SEGURANÇA DA INFORMAÇÃO

Seção I

Política da Segurança da Informação

Artigo 1º - instituir a Política de Segurança da Informação no âmbito do Ministério Público do Estado do Tocantins 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 Ministério Público;
- 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.

Artigo 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 MP;
- 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: quem utiliza de forma autorizada recursos do MP;
- VII - 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.

Artigo 3º - São objetivos da Política de Segurança da Informação :

I - dotar o Ministério Público de instrumentos jurídicos, normativos e organizacionais que o capacite científica, tecnológica e administrativamente a assegurar a confidencialidade, integridade e a disponibilidade dos dados e/ou informação 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

Artigo 4º - Para atender as demandas originárias da Política da Segurança da Informação fica instituído o Comitê Estratégico de Tecnologia da Informação que será composto, no mínimo, pelos seguintes integrantes:

I - Chefe de Gabinete do Procurador Geral de Justiça ;

II - representante da Corregedoria Geral do MPE/TO;

III - Dois membros (Procuradores ou Promotores de Justiça) indicados pelo Procurador Geral de Justiça;

IV - Assessor Jurídico do Procurador Geral de Justiça;

V - Diretor Geral da Procuradoria Geral de Justiça;

VI - Chefe de Planejamento e Gestão;

VII - Chefe do Departamento de Tecnologia da Informação.

§ 1º - O Comitê Estratégico de Tecnologia da Informação terá como Presidente o Chefe de Gabinete do Procurador Geral de Justiça e como Secretário o Chefe do Departamento de Tecnologia da Informação.

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

§ 3º - O Comitê Estratégico de Tecnologia da Informação reunir-se-á, ordinariamente, uma vez a cada bimestre 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 Comitê Estratégico de Tecnologia da Informação compete instituir comissões para auxiliar a tomada de decisão sobre assuntos de natureza técnica.

Parágrafo único - O ato de constituição da comissão definirá seus objetivos específicos, sua composição e prazo para a conclusão dos trabalhos.

Artigo 5º - Compete ao Comitê Estratégico de Tecnologia da Informação:

I - Estabelecer políticas e diretrizes de tecnologia de informação, alinhadas aos objetivos estratégicos da Instituição;

II - Aprovar o Plano Diretor de Tecnologia da Informação do MPE/TO;

III - Definir as prioridades dos investimentos em tecnologia da informação;

IV - Estabelecer as prioridades para execução de projetos de tecnologia da informação;

V - Definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação; e

VI - Administrar e gerenciar a implantação, manutenção e aperfeiçoamento das Tabelas Unificadas no âmbito do MPE/TO, conforme artigo 6º da Resolução n.º 63/2010 do CNMP.

CAPÍTULO II

DAS NORMAS DE USO E SEGURANÇA DA INFORMAÇÃO

Seção I

Dos direitos e Obrigações dos usuários

Artigo 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 MPE/TO;
- II - ter conta de acesso pessoal à rede de computadores e aplicativos mediante liberação de senha pelo DTI;
- III - ter conta de acesso pessoal ao correio eletrônico mediante liberação de senha pelo DTI;
- IV - acessar Internet, pelo navegador (*browser*) indicado pelo DTI, e a Intranet, esta por meio da senha pessoal liberada pelo DTI;
- V - ter restrita e/ou limitada privacidade das informações na sua área de armazenamento;
- VI - solicitar atendimento técnico do DTI por meio do *link* "Atendimento Informática", constante na página da Intranet, podendo se valer do pedido via telefone quando o defeito do computador inviabilizar o chamado técnico eletrônico;
- 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 pelo DTI;
- IX - inserir e/ou executar *pen drive* ou outro dispositivo similar nos recursos computacionais do MPE/TO somente quando proceder prévia varredura do antivírus disponível na rede no respectivo dispositivo;
- X - acessar o mensageiro corporativo adotado pela Instituição para comunicação interna informal.

Artigo 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;

IV – 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;

IX - manter o bom uso, a limpeza e a conservação dos equipamentos de informática colocados à sua disposição;

X - manter o DTI informado sobre qualquer mudança efetuada nos recursos computacionais colocados à sua disposição;

XI - respeitar e seguir as normas e procedimentos definidos pelo Procurador Geral de Justiça, pelo Comitê Estratégico de Tecnologia da Informação e pelo DTI;

Seção II

Das proibições aos usuários

Artigo 8º - Fica expressamente 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 DTI;

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 ou que sejam incompatível com o ambiente de trabalho;

XII - retirar qualquer recurso computacional do local destinado sem prévia autorização do Departamento de Tecnologia da Informação;

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

XIV - conectar qualquer equipamento particular à rede local do MPE/TO sem o conhecimento e anuência do DTI.

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

Seção III

Do acesso à Internet

Artigo 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 DTI;

Artigo 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 MPE/TO, 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 MPE/TO;

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 - para exibição, veiculação ou armazenamento de 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.

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

Artigo 12 - O bloqueio de sítios eletrônicos estranhos à atividade institucional, com base na Política da Segurança da Informação, ficará a cargo do DTI, 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 MPE/TO.

§ 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 o DTI, deverá o pedido de liberação ser autorizado pelo Diretor Geral, de forma temporária, para que o servidor execute o trabalho.

Artigo 13 – Incumbe ao Chefe de Gabinete do Procurador Geral a análise prévia das matérias a serem publicadas no site eletrônico do MPE/TO, que após deferimento encaminhará ao departamento competente para divulgação.

Seção IV

Do uso da Intranet

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

Artigo 15 - Os órgãos de execução, os órgãos auxiliares e os departamentos do Ministério Público do Estado do Tocantins poderão divulgar na Intranet as respectivas ações desenvolvidas.

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

Seção V

Do uso do Correio Eletrônico

Artigo 17 - O correio eletrônico será o meio preferencial para comunicação e troca de documentos internos, evitando-se, tanto quanto possível, a impressão do conteúdo de mensagens.

Artigo 18 - Compete ao usuário quando acessar o correio eletrônico:

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;

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

IV – responsabilizar-se pelas mensagens e anexos enviados e/ou recebidos.

Artigo 19 - É proibido fazer uso do correio eletrônico para envio de mensagens para divulgação de propaganda comercial, correntes de amizade, disseminação de SPAM (mensagem comercial não solicitada), material protegido por leis de propriedade intelectual, vírus, mensagens ofensiva à moral e aos bons costumes, lista de endereço eletrônico de usuários desta Instituição.

Artigo 20 - É vedado o envio de mensagens de natureza estritamente pessoal a listas ou grupos oficiais de endereços.

Artigo 21 - A caixa postal de correio eletrônico terá o valor inicial de 100MB.

Seção VI

Da Utilização do Mensageiro Corporativo

Artigo 22 - O mensageiro corporativo é um sistema de acesso voluntário dos usuários da rede, destinado à troca de mensagens instantâneas entre seus usuários.

I - O acesso ao mensageiro corporativo do MPE/TO é restrito aos usuários cadastrados na rede de informática da Instituição;

II - O DTI é o departamento responsável pela instalação, manutenção e armazenamento das informações que circulam no mensageiro corporativo;

III - 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

Artigo 23 - A instalação e desinstalação de equipamentos de informática nas dependências do Ministério Público do Estado do Tocantins, incluindo Promotorias de Justiça do interior é de responsabilidade do DTI, 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 de e-mail, ao DTI, 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 chefe do DTI informar ao Departamento de Patrimônio Público sobre a alteração.

Artigo 24 - A manutenção preventiva e corretiva dos equipamentos de informática do Ministério Público é de responsabilidade exclusiva do DTI, por meio do laboratório de informática LABIN, e será realizada por técnicos de informática.

I - Havendo necessidade de manutenção em equipamentos de informática, deverá o usuário comunicar o DTI por meio do link "Atendimento Informática" que se encontra na página da Intranet.

II - O usuário deverá especificar detalhadamente o defeito apresentado nos recursos computacionais ou tecnológicos na ocasião da solicitação do suporte técnico ao DTI;

III - A permanência dos equipamentos de informática para manutenção no DTI:

§ 1º - O LABIN tem o prazo de até 04 (quatro) horas para informar ao usuário sobre a situação do equipamento, o diagnóstico e a previsão para devolução.

§ 2º - No caso do equipamento estar na garantia, será aberto um chamado junto à autorizada para adoção das providências de acordo com prazo de garantia cada fabricante, que será repassado ao usuário do equipamento.

Artigo 25 - É vedada a manutenção de equipamentos de informática particulares, de associações e sindicatos, incluindo *hardware* e *software*, por técnicos do

Departamento de Tecnologia da Informação no âmbito do Ministério Público, exceto quando os tais equipamentos estão sendo utilizados em prol da Instituição.

Artigo 26 - Todo computador é entregue lacrado e cabe ao respectivo usuário responsável pelo equipamento mantê-lo íntegro, de forma a garantir a inviolabilidade e segurança.

Seção II

Da Cópia de Segurança (*Backup*)

Artigo 27 - Este Ministério Público 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.

Artigo 28 - O Departamento de Tecnologia da Informação do Ministério Público do Estado do Tocantins 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.

Artigo 29 - Este Ministério Público 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.

I - É vedado a gravação no servidor de rede de arquivos que não contenham relação com as atividades desenvolvidas pelo Ministério Público, tais como: músicas, fotos, vídeos e outros arquivos. Em, havendo imprescindível necessidade dessa espécie de informação, a gravação deverá ser solicitada ao DTI - Área de Rede e Segurança.

II - É de responsabilidade exclusiva dos servidores da Área de Redes e Segurança a realização de backups diários e, quando necessário, as respectivas restaurações.

Parágrafo Único - É de responsabilidade dos membros e servidores, principalmente aqueles que atuam no Interior do Estado, salvar os arquivos armazenados no disco rígido - HD (*winchester*) do computador em que trabalham.

Seção III

Do Desenvolvimento de *Softwares*

Artigo 30 - O DTI desenvolverá *softwares* quando formalmente solicitado pelo responsável do Departamento.

§ 1º - A solicitação deverá ser dirigida ao Chefe de TI, 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 DTI, para execução do projeto, formará equipe de trabalho, que será composta por analista e técnicos de informática juntamente 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 DTI 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. A variação temporal dependerá do número de funcionalidades requeridas, da colaboração do departamento e da complexidade do sistema.

§ 5º - 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 DTI pelo departamento responsável.

§ 6º - O Comitê Estratégico de Tecnologia da Informação definirá as prioridades nos projetos de desenvolvimentos de *softwares*.

§ 7º - O DTI divulgará na Intranet o andamento da solicitação de *softwares* (aguardando, em desenvolvimento e concluído).

Artigo 31 - Os direitos autorais dos *softwares* desenvolvidos pelo Departamento de Tecnologia da Informação são de propriedade do Ministério Público do Estado de Tocantins.

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

Artigo 32 - O Departamento de Tecnologia da Informação, por meio da Área de Desenvolvimento de Sistemas, é responsável pela criação do *software*, coordenação do desenvolvimento, quando o mesmo ocorrer por terceiros, e pelo suporte técnico, porém não é responsável pela alimentação do mesmo, ou seja, não é o DTI que efetua o cadastro das informações no sistema.

CAPÍTULO IV

DAS DISPOSIÇÕES GERAIS

Artigo 33 - A autorização para utilizar os recursos computacionais da instituição é facultada a membro, servidor (efetivo, comissionado ou à disposição), estagiário ou prestador de serviço e demais servidores de instituições conveniadas, mediante abertura de conta pessoal junto ao DTI.

Artigo 34 - Todos os usuários autorizados tem o dever de noticiar ao DTI qualquer 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.

Artigo 35 - A violação das normas descritas neste Ato implicará em responsabilização disciplinar, independentemente da responsabilidade civil e penal.