POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DO MINISTÉRIO PÚBLICO DO TOCANTINS

(versão 2.1)

NOVEMBRO DE 2016

Sumário

O Comitê Estratégico de Tecnologia da Informação (CETI) e o Departamento de Modernização e Tecnologia da Informação (DMTI), departamento responsável pela normatização e padronização de procedimentos referentes à área de informática, define as políticas de segurança da informação do MPTO, estabelecendo os critérios relativos ao acesso, uso, armazenamento, procedimento, segurança e responsabilidade na utilização da tecnologia da informação do Ministério Público do Estado do Tocantins, aplicando-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.

1. INTRODUÇÃO

Considerando: a necessidade de disciplinar, padronizar e implementar procedimentos básicos quanto ao uso apropriado dos recursos de computação e redes, bem como a proteção, privacidade e segurança dos bancos de dados; 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; a imprescindível necessidade de garantir a segurança das informações e dados que trafegam nos recursos computacionais e tecnológicos deste Ministério Público; que são características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade, autenticidade e muitas vezes, sigilosidade; a premente demanda para racionalizar e operacionalizar de forma adequada o uso dos recursos e serviços relativos à tecnologia da informação disponibilizada nesta Instituição; que a utilização inadequada dos recursos e serviços da tecnologia da informação acarreta prejuízo e sobrecarrega a infraestrutura; que a utilização da rede de informática do MPE/TO deve ser voltada,

exclusivamente, para fins de natureza institucional e norteada pelo interesse público; a necessidade de se estabelecer os critérios para utilização e gerência da rede de informática sem fio no Ministério Público; o incremento das possibilidades de propagação de vírus de computadores em mensagens de correio eletrônico por meio de seus anexos, tais como arquivos executáveis, arquivos de apresentações, fotografias, arquivos de músicas, animações, entre outros, prejudiciais ao bom funcionamento da rede de informática do MPE/TO, inclusive acarretando queda de performance e a possível perda de dados e informações; a necessidade de segurança da informação trafegada e/ou armazenada na rede de informática uma vez que esta mantém documentos de elevada importância e informações processuais, muitas vezes sigilosas; que o login e senha de acesso são a identificação individual e intransferível dos usuários da rede de informática e sistemas institucionais; a necessidade de utilização de computadores, tablets, notebooks e smartphones particulares de membros e servidores na rede de informática do Ministério Público, bem como equipamentos de empresas que prestam serviços nas dependências da Instituição; a existência permanente de ameças ao bom funcionamento da rede e sistemas institucionais, tais como o ataque de hackers, vírus, spywares, acesso indevido a arquivos e pastas, perda de documentos, indisponibilidade de sistemas, dentre outras; a necessidade de padronização e de constante atualização de todas as estações de trabalho conectadas a rede, a fim de que estão não se tornem causadoras de tais ameaças; a necessidade de diminuir custos, melhorar a segurança contra ameaças virtuais, e regulamentar os softwares utilizados no Ministério Público do Estado do Tocantins; 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.

Fica estabelecida a Política de Segurança da Informação.

2. CONCEITOS

1. Tecnologia da Informação: serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação;
2. 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;
3. Comitê Estratégico de Tecnologia da Informação – CETI: formado por representante da Administração Superior, Corregedoria e representantes do Departamento de Modernização e Tecnologia da Informação para atender as demandas originárias da Política de Segurança da Informação;
4. Departamento de Modernização e Tecnologia da Informação – DMTI: Unidade Executiva do Ministério Público do Estado do Tocantins responsável pelo planejamento, coordenação, organização, controle e supervisão dos recursos computacionais da Instituição;
5. Recursos Computacionais: são todos os equipamentos, instalações, programas de computador e banco de dados (computadores, tablets, notebooks, netbook, ultrabooks, smartphones e terminais de qualquer espécie, incluídos acessórios; impressoras, leitores de código de barras e escâneres de qualquer espécie; servidores de arquivos, de impressão, de correio eletrônico, WEB e qualquer outro servidor de rede; modens, roteadores, firewall, switches, hub e redes; sistemas operacionais e aplicativos; 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 de armazenamento; salas de computadores, laboratórios, escritórios mobiliários específicos; sítio ou homepage do MPETO; manuais técnicos.), direta ou indiretamente administrados e operados pelo DTI para armazenar, processar, transmitir e

disseminar informações de interesse institucional;

6. Material de Consumo de Informática: materiais utilizados direto ou indiretamente, para armazenar, processar, transmitir e disseminar informações na área de informática, tais como: formulários contínuos, discos, disquetes, HD externos, pendrives, toner para impressoras, CD, DVD, fita magnética, tinta para impressoras e outros;
7. Usuário Autorizado: é toda pessoa física ou jurídica que se utilize de quaisquer recursos computacionais desta Instituição de forma autorizada pelo Departamento de Modernização e Tecnologia da Informação. São eles: membros, servidores (efetivo, comissionado ou à disposição), estagiários, prestadores de serviços e demais servidores de instituições conveniadas;
8. Conta de Acesso Pessoal: conta que pertence ao usuário e lhe permite acessar à rede de informática, correio eletrônico, a intranet e os softwares do Ministério Público do Estado do Tocantins;
9. Mensageiro Corporativo: sistema de acesso voluntário dos usuários da rede de informática, destinado à troca de mensagens instantâneas entre os usuários autorizados;

3. SEGURANÇA DA INFORMAÇÃO

3.1. POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

3.1.1. PRESSUPOSTOS BÁSICOS

1. Preservação da credibilidade e do prestígio da Instituição;
2. Proteção das informações e/ou dados judiciais e extrajudiciais que circulam no âmbito do Ministério Público;
3. Efetivação de medidas de conscientização dos recursos humanos das unidades administrativas sobre a importância das informações processadas e sobre o risco de vulnerabilidade e integridade;

4. Armazenamento e proteção de acesso ao uso adequado das informações.

3.1.2. CONCEITUAÇÕES

1. Confiabilidade: princípio da segurança da informação pelo qual se garante que o acesso à informação seja obtido somente por pessoas autorizadas;
2. Criticidade: grau de importância da informação para a continuidade das atividades do MP;
3. Disponibilidade: princípio de Segurança da Informação pelo qual se estabelece que as informações e os recursos estarão disponíveis sempre que necessário;
4. Integridade: princípio da Segurança da Informação por meio do qual é garantida que a informação não será alterada sem a devida autorização;
5. Recurso: além da própria informação, todo meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
6. Usuário: quem utiliza de forma autorizada recurso do MP;
7. Segurança da Informação: proteção dos sistemas de informação contra a negação de serviços 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.

3.1.3. OBJETIVOS

1. 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 informações tratadas, classificadas e sensíveis;
2. Eliminar a dependência extrema em relação a sistemas, equipamentos,

dispositivos e atividades vinculadas a segurança dos sistemas de informação;

3. Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
4. Estabelecer normas jurídicas necessárias para a efetiva implementação da segurança da informação;
5. Promover as ações necessárias à implementação e manutenção da segurança da informação;
6. Promover o intercâmbio científico e tecnológico com outros órgãos estaduais ou federais sobre as atividades de segurança da informação;
7. Assegurar a operatividade dos sistemas de segurança da informação.

4. DAS NORMAS DE USO E SEGURANÇA

4.1. DIREITOS E OBRIGAÇÕES DOS USUÁRIOS

4.1.1. DIREITOS DOS USUÁRIOS AUTORIZADOS

1. Fazer uso dos recursos computacionais da Instituição para a realização de atividades profissionais relacionadas aos serviços de interesse do MPE/TO;
2. Ter conta de acesso à rede de computadores e aplicativos mediante a liberação de senha pelo DTI;
3. Ter conta de acesso ao correio eletrônico mediante liberação de senha pelo DTI;
4. Acessar Internet, pelo navegador (browser) indicado pelo DTI, e a Intranet, esta por meio de senha pessoal liberada pelo DTI;
5. Ter restrita e/ou limitada privacidade das informações na sua área de armazenamento;
6. Solicitar atendimento técnico do DTI, por meio do sistema de abertura de chamado técnico on line, constante na página da intranet (ATHENAS), podendo se valer do pedido via telefone quando o defeito do computador

inviabilizar o chamado técnico eletrônico;

7. Receber o adequado atendimento do suporte técnico;
8. Acessar a rede da Instituição por meio de computadores, notebook, tablet, smartphones e outros equipamentos pessoais quando devidamente autorizado pelo DTI;
9. Inserir e/ou executar pendrive, HD externo ou outro dispositivo similar nos recursos computacionais do MPE/TO somente quando proceder prévia varredura do antivírus disponível na rede no respectivo dispositivo;
10. Acessar o mensageiro corporativo adotado pela Instituição para comunicação interna informal;
11. Acessar a rede sem fio quando disponível, desde que autorizado e regularmente habilitado e cadastrado na rede de informática do MPE/TO;
12. Ter uma cópia de seu e-mail Institucional, desde que solicitado formalmente em um prazo de 30 dias, quando o mesmo for desligado do quadro do MPETO, antes da exclusão definitiva de suas informações. Não sendo solicitado em um prazo de 30 dias após o desligamento o e-mail será excluído definitivamente.

4.1.2. OBRIGAÇÕES DOS USUÁRIOS AUTORIZADOS

1. Zelar pela integridade e segurança dos equipamentos e pelas informações processadas e armazenadas nos recursos computacionais sob sua responsabilidade e uso;
2. Utilizar dos recursos computacionais exclusivamente para os serviços da Instituição;
3. Zelar pelo sigilo e segurança de sua senha de acesso à rede e aplicativos, que é de uso individual e intransferível, dedado o seu compartilhamento com terceiros;
4. Alterar a senha pessoal gerada em caráter provisório, através de ferramenta do sistema disponibilizado pelo DTI, no prazo de 3 (três) dias úteis;

5. Compor sua senha definitiva de acesso de no mínimo 8 caracteres entre letras e números;
6. 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 interrupção do serviço;
7. Manter sigilo, integridade e segurança de todos os dados que tiverem acesso;
8. Não autorizar que pessoas estranhas ao quadro da Instituição tenham acesso físico aos equipamentos sob sua responsabilidade;
9. Manter constante cuidado de proteção contra vírus, principalmente quando do recebimento de mensagens pelo correio eletrônico, acesso à internet, downloads de arquivos com extensão que apresentem perigo de inserção ou execução de dispositivos nos recursos computacionais desta Instituição;
10. Fazer uso racional de material de consumo da Instituição, combatendo desperdício em todas as suas formas, optando, quando disponível, pela utilização do meio eletrônico ao papel e impressão;
11. Manter o bom uso, a limpeza e a conservação dos equipamentos de informática colocados à sua disposição;
12. Manter o DMTI informado sobre qualquer mudança efetuada nos recursos computacionais colocados à sua disposição;
13. Respeitar e seguir as normas e procedimentos definidos pelo Procurador-Geral de Justiça, pelo Comitê Estratégico de Tecnologia da Informação e Departamento de Modernização e Tecnologia da Informação.

4.2. PROIBIÇÕES AOS USUÁRIOS

Fica expressamente proibido aos usuários:

1. Utilizar os recursos e materiais de informática para trabalhos particulares ou que não tenham ligação com a finalidade da Instituição;
2. Remover, transferir, emprestar, modificar, ou proceder qualquer alteração nas características físicas ou técnicas dos equipamentos, sem a prévia

autorização do DTI;

3. Compartilhar com terceiros conta de acesso pessoal à rede, às aplicações e outras espécies de autorização de uso individual e intransferível;
4. Executar ou configurar os recursos computacionais ou tecnológicos com a intenção de facilitar o acesso a usuários não-autorizados;
5. Obter acesso não autorizado aos sistemas;
6. Copiar, transferir ou emprestar software para finalidade ou pessoa estranha aos serviços da Instituição, sem autorização formal do Procurador-Geral de Justiça e Termo de Cooperação e/ou doação;
7. Destruir ou estragar ou desconfigurar intencionalmente os equipamentos, softwares ou dados pertencentes à Instituição;
8. Violar os sistemas de segurança dos recursos computacionais, por exemplo: identificação de usuários, senhas de acesso, fechaduras automáticas ou sistemas antivírus, dentre outros;
9. Usar, instalar, executar, copiar ou armazenar aplicativos, programas ou qualquer outro material que não esteja devidamente autorizado pela Instituição;
10. Proibição conforme artigo 25 da seção VII.
11. Remover, copiar, emprestar ou divulgar documento confidencial e sigiloso, bem como lista de endereços residenciais, endereços eletrônicos de usuários, de propriedade da Instituição;
12. Utilizar os recursos computacionais para constranger, assediar, ofender, caluniar ou ameaçar qualquer pessoa ou instituição ou que seja incompatível com o ambiente de trabalho;
13. Retirar qualquer recurso computacional do local sem prévia autorização do Departamento de Modernização e Tecnologia da Informação (DMTI).
14. Utilizar programas de rádio, videoconferência, filmes, vídeos ou outros, que trafeguem dados que não sejam textos, sem a cientificação, estudo de impacto e devida autorização do Departamento de Modernização e Tecnologia da Informação, Diretoria-Geral ou Chefia de Gabinete.

15. Utilizar e/ou Conectar qualquer equipamento particular à rede local do MPE/TO sem o conhecimento e anuência do DTI.
16. Instalar ou utilizar outros programas de mensagens instantâneas que não aquele indicado pela Instituição.

4.3. UTILIZAÇÃO DA REDE DE DADOS, COM E SEM FIO

Fica expressamente proibido a utilização da rede de informática do MPE/TO para:

1. Jogos on-line; e
2. Para utilização de qualquer ferramenta, software ou aplicativo que provoquem sobrecarga no sistema.

O acesso à rede sem fio é restrito aos usuários regularmente habilitados e cadastrados na rede do MPE/TO, e sendo necessário o acesso à rede sem fio por usuários externos ou eventuais, deverá ser precedido de autorização da Chefia Superior.

É vedada a instalação de dispositivo móvel ou Acess Point (É o equipamento que torna possível a comunicação entre os dispositivos móveis e a rede de informática) na rede sem fio sem o conhecimento do Departamento de Modernização e Tecnologia da Informação, e caso autorizado a sua utilização, os Acess Point deverão, para utilizar a rede sem fio, ser compatível com as tecnologias adotadas pelo MPE/TO.

Os eventuais incidentes de segurança identificados por qualquer usuário da rede de informática do MPE/TO deverão ser imediatamente comunicados à Chefia do Departamento de Modernização e Tecnologia da Informação, para as providências cabíveis.

4.4. SENHA DE ACESSO

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

4.4.1. OBRIGATORIEDADES

1. Alterar a senha pessoal gerada em caráter provisório, através de ferramenta do sistema disponibilizado pelo DTI, no prazo máximo de 3 (três) dias úteis;
2. Por medida de segurança, o usuário deverá alterar sua senha pelo menos a cada seis meses.
3. A senha deve possuir o tamanho mínimo de 08 (oito) caracteres e ser composta pelos seguintes tipos de caracteres:
    - letras maiúsculas e minúsculas: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z;
    - números: 0 1 2 3 4 5 6 7 8 9.
4. A senha deverá ser formada preferencialmente pela combinação dos tipos de caracteres citados no parágrafo anterior;
5. Não utilizar as seguintes sequências de caracteres:
    - I - nomes próprios;
    - II – datas;
    - III - sequências numéricas, alfabéticas ou ambas intercaladas;
    - IV - palavras que constem em dicionários;
    - V - siglas de entidades conhecidas;
    - VI - informações pessoais como RG, CPF, telefone, senhas bancárias etc.

4.4.2. PERDA DE SENHA

Em caso de perda da senha pessoal provisória cadastrada, será gerada uma nova senha pessoal provisória mediante requerimento formal ao

Departamento de Modernização e Tecnologia da Informação e deverá seguiras mesmas exigências descritas no Item 4.4.1.

Solicitação de alterações de senhas ao DMTI, só podem ser realizadas pelo proprietário da conta, enviando uma autorização de alteração através de ofício ou do e-mail INSTITUCIONAL, colocando informações que ajudam a identificar e ter certeza que trata-se do mesmo sendo elas a Data de nascimento, CPF, nome completo, nome da mãe e matrícula, uma vez que, e-mail não Institucionais podem ser criados em vários domínios, não sabendo se realmente trata-se de e-mail de membro ou servidor.

Após solicitado a alteração formalmente, deverá ligar ao DMTI, identificando-se, assim como o documento enviado, para comprovação dos dados enviados verbalmente e em consulta aos dados do sistema de RH.

Caso o Membro ou Servidor encontre-se em Palmas-TO, no prédio sede, a alteração poderá ser realizada fisicamente pelo mesmo, apenas apresentando a identidade funcional, na área de redes e segurança do DMTI.

4.4.3. CANCELAMENTO E/OU BLOQUEIO

O cancelamento e/ou bloqueio de usuário e senhas nos sistemas informáticos do Ministério Público do Estado do Tocantins será realizado pelo Departamento de Modernização e Tecnologia da informação nas seguintes hipóteses:

1. Desvinculação do usuário de suas respectivas unidades, departamento, setores e/ou funções, devendo ser comunicado pelo Departamento de Recursos Humanos através de documento oficial ao Departamento de Modernização e Tecnologia da Informação;
2. Mediante solicitação pessoal do integrante do Ministério Público do Estado do Tocantins, nos casos de suspeita de uso indevido de sua senha pessoal, até que seja realizada a perícia técnica designada para esse fim;

3. Em casos de investigação, quando solicitado por chefe da unidade administrativa que é vinculado o integrante, pelo Corregedor Geral quando se tratar de Membro de Ministério Público, por presidente de Comissão Sindicante Decisória ou pelo Presidente da Comissão Processante Permanente, com a determinação do Procurador-Geral de Justiça.

4.5. INTERNET

Todos os usuários autorizados terão direito ao acesso à Internet para a realização das atividades relacionadas ao serviço da Instituição, por meio do navegador de Internet indicado pelo DTI.

4.5.1. PROIBIÇÃO DE UTILIZAÇÃO PARA

1. Participar de salas de bate-papo, exceto aquelas de exclusivo interesse das atividades da Instituição;
2. Engajar-se em atividades comerciais ou político partidárias;
3. Copiar arquivos que ofereçam riscos potenciais à segurança do ambiente de rede do MPETO, tais como arquivos com as extensões exe, src, bat, pif, vbc, bin, app e outros de mesma natureza;
4. Copiar arquivos (download) que contenham som, vídeo ou animação, que não sejam de interesse das atividades do MPE/TO;
5. Acessar sites impróprios que contenham conteúdos pornográficos, ilegais ou antiéticos;
6. Participar de qualquer ação que comprometa a segurança do site e das informações e/ou dados que circulam na Instituição;
7. Para exibição, veiculação ou armazenamento voluntário de páginas com conteúdos pornográficos, eróticos, jogos de qualquer espécie, comercial, político partidário, ofensivo ao decoro pessoal e ao princípio de urbanidade e que provoquem sobrecarga no sistema.

4.5.2. MONITORAMENTO

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

4.5.3. BLOQUEIO

O bloqueio de sítios eletrônicos estranhos a atividade institucional, com base na Política de 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 de rede do MPE/TO, cabendo ao CETI verificar a necessidade de bloqueio de outras espécies de sítios eletrônicos;

Havendo imprescindível necessidade, em razão de serviço, de acessar sítio eletrônico ou documento previamente bloqueado pelo DTI, deverá o pedido de liberação ser autorizado pelo Diretor-Geral ou Chefe de Gabinete, de forma temporária, com prazo estabelecido, para que o servidor ou membro execute o trabalho.

4.5.4. PUBLICAÇÃO DE CONTEÚDO

Incumbe ao Chefe de Gabinete do Procurador-Geral de Justiça a análise prévia das matérias a serem publicadas no sítio eletrônico do MPE/TO, que após deferido encaminhará ao departamento competente para divulgação.

4.6. INTRANET

O acesso à Intranet desta Instituição é restrito aos usuários autorizados.

4.6.1. PUBLICAÇÃO

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, após a autorização da Chefia de Gabinete.

4.6.2. MONITORAMENTO

O acesso à Intranet é monitorada e auditada por meio de login e senha pessoal, ficando registrado as ações do usuário.

4.7. CORREIOS ELETRÔNICOS

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

4.7.1. AUTORIZAÇÃO

Compete ao usuário quando acessar o correio eletrônico:

1. Utilizar o correio eletrônico institucional para os objetivos e funções próprias e inerentes às atribuições funcionais;
2. Verificar diariamente o conteúdo da conta pessoal, eliminando periodicamente as mensagens contidas nas caixas postais;
3. Não permitir acesso a terceiros ao correio eletrônico por meio da senha pessoal;
4. Responsabilizar-se pelas mensagens e anexos enviados e/ou recebidos.

4.7.2. PROIBIÇÕES

É proibido fazer uso do correio eletrônico para envio de mensagens para divulgação de propaganda comercial, correntes de amizades, disseminação de

SPAM (mensagem comercial não solicitada), material protegido por leis de propriedade intelectual, vírus, mensagens ofensivas a moral e aos bons costumes, lista de endereço eletrônico de usuários desta Instituição.

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

4.7.3. CAPACIDADE DAS CAIXAS DE CORREIOS ELETRÔNICOS

A caixa postal de correio eletrônico terá o valor limite de 200MB para usuários e 600MB para departamentos, devido às limitações de espaço de armazenamento, devendo o usuário fazer a sua gerência.

O valor limite poderá ser aumentado, desde que devidamente justificado e aprovado pelo CETI, e que exista espaço em disco suficiente para o atendimento.

4.7.4. DESLIGAMENTO DE MEMBROS E SERVIDORES

Após o desligamento do membro ou servidor da Instituição, o e-mail Institucional será bloqueado, e o mesmo terá 30 dias para solicitação de uma cópia dos dados ali contidos, e não havendo a solicitação de uma cópia do e-mail após o desligamento do membro ou servidor, dentro do prazo estabelecido, o mesmo será excluído definitivamente para liberação do espaço de armazenagem nos servidores de rede.

4.8. MENSAGEIRO CORPORATIVO

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

1. O acesso ao mensageiro corporativo do MPE/TO é restrito aos usuários cadastrados na rede de informática da Instituição;
2. O DTI é o departamento responsável pela instalação, manutenção e

armazenamento das informações que circulam no mensageiro corporativo;

3. Às reclamações pertinentes ao conteúdo de mensagens veiculadas no mensageiro corporativo deverão ser encaminhadas a 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.

5. DOCUMENTOS ELETRÔNICOS

5.1. ASSINATURA ELETRÔNICA E A VALIDADE JURÍDICA DOS ATOS E DOCUMENTOS

Fica reconhecida, para os fins de instrução processual no âmbito administrativo do Ministério Público do Estado do Tocantins, a Assinatura Eletrônica inserida nos documentos por meio dos Sistemas de Informações do Ministério Público do Estado do Tocantins e suas funcionalidades.

A assinatura eletrônica (login e senha) será constituída, no mínimo, de assinatura cadastrada pelo Departamento de Modernização e Tecnologia da Informação – DMTI com login permanente e senha pessoal inicial de caráter provisório, que serão fornecidos aos integrantes da instituição, aos Estagiários e Funcionários Terceirizados, cadastrados no Departamento de Recursos Humanos e Folha de Pagamento ou na Área de Manutenção de Tecnologia.

Em havendo avanços na Tecnologia disponível, poderá o Departamento de Modernização e Tecnologia da Informação adotar meios de Certificação Digital ou instrumentos semelhantes a esta, para que sejam utilizados nos sistemas deste Ministério Público.

A prática de atos assinados digitalmente importa na responsabilização administrativa, civil e criminal pelo uso indevido da Assinatura Eletrônica.

Para fins de instrução dos Processos Administrativos em meio físico, o requerente em meio digital poderá digitalizar documentos comprobatórios

necessários, sendo que os originais deverão permanecer sob a posse do requerente, o qual certificará sua autenticidade mediante o uso da assinatura eletrônica, considerando que todo o servidor possuí fé pública.

Para fins de instrução dos Processos Administrativos eletrônicos, o interessado poderá digitalizar documentos físicos necessários, permanecendo estes sob sua posse, certificada sua autenticidade mediante o uso da assinatura eletrônica.

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 legai referentes ao processo administrativo e as despesas públicas.

Para garantia de identificação, deverá o sistema construído pelo DTI 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.

Os documentos eletrônicos gerados pelos sistemas de informação do Ministério Público do Estado do Tocantins, deverão possuir carimbo digital ou similar que identifique o autor, data e hora da ação, e caso esteja dotado de certificado digital a possibilidade de identificação no documento. Deverá ainda possuir um código único de identificação que possibilite a verificação de sua autenticidade no sítio do Ministério Público do Estado do Tocantins.

5.2. RESPONSABILIDADES

É responsabilidade exclusiva dos integrantes do MPE/TO:

1. 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;
2. A preparação dos documentos no sistema e a juntada de anexos, observadas

as restrições colocadas pelo DTI, no que diz respeito a redação oficial, características da peça e formatação.

Será de responsabilidade do Departamento de Modernização e Tecnologia da Informação – DMTI do Ministério Público do Estado do Tocantins:

1. Construir os sistemas de forma a garantir a segurança necessária às informações, observadas as diretrizes da Política de Segurança da Informação instituída no âmbito do Ministério Público do Estado do Tocantins e da legislação pertinente;
2. Armazenar as informações geradas no sistema em meio que garanta a preservação e a integridade dos dados;
3. Utilizar de tecnologia que permita identificar possíveis fraudes nos sistemas.
4. 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 Ministério Público.

6. CONTROLE

6.1. SISTEMAS

Os sistemas de informação do Ministério Público do Estado do Tocantins 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.

6.2. EQUIPAMENTOS

Os equipamentos só poderão ser retirados de suas respectivas localidades para realização de manutenção por terceiros, após comunicado ao

DMTI, e receber a autorização formal para tal, ficando os terceiros, responsáveis pelas informações ali contidas, bem como quanto a sua permanência e sigilo, e sendo necessário troca de unidades de armazenamento (disco rígidos / HD / Hard disk), o equipamento substituído não poderá ser descartado, devendo obrigatoriamente ser enviado ao Departamento de Modernização e Tecnologia da Informação, para a realização do descarte correto, na forma estabelecida.

6.3. SALA DE SERVIDORES DE REDE (DATACENTER) E SALA DE RACKS

O DATACENTER do MPETO e as salas dos racks (redes e telefonia) em Palmas, é área de acesso exclusivo para os servidores da área de redes e segurança e chefia de TI, ou a outros servidores mediante autorização da Diretoria Geral ou Chefia de Gabinete, porém, com acompanhamento de um dos servidores da área de redes e segurança, devendo ter câmera de monitoramento com gravação em tempo integral.

O DATACENTER deverá ter controle de umidade e temperatura, e detector de fumaça com aviso de falhas através de e-mails e mensagem celular, para evitar parada de serviços e perda de informações. Em caso de detecção de falha é obrigatório que um dos servidores (pessoa) da área de redes e segurança compareça ao local no mesmo dia para resolução do problema, devendo reportar a Chefia de TI qualquer impedimento na resolução de problemas.

Os servidores (pessoas) da área de redes e segurança, bem como o Chefe de TI, terão permissão para entrar no prédio sede em Palmas, a qualquer horário do dia e da noite, quando detectado qualquer problema ou falha de segurança da informação nos servidores de rede, devendo informar imediatamente a Diretoria-Geral ou Chefia de Gabinete.

7. CÓPIA DE SEGURANÇA (BACKUP)

No que se refere a cópia de segurança, a mesma será tratada por uma política exclusiva, devendo a mesma ser devidamente divulgada.

8. DISPOSIÇÕES GERAIS

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 a abertura de conta junto ao DMTI.

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

A violação das normas descritas neste documento implicará em responsabilização disciplinar, independente da responsabilidade civil e penal.

Huan Carlos Borges Tavares
Chefe do Departamento de Modernização e Tecnologia da Informação