

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO

PROCURADORIA GERAL DE JUSTIÇA

Retificar, em parte, o Cronograma de Correições Ordinárias nas Promotorias de Justiça - exercício de 2016, publicado no Diário Oficial do dia 11.12.2015, para considerar a seguinte alteração:

ONDE SE LÊ: "...OBS.: 1º - Os endereços das Promotorias de Justiça abaixo relacionadas encontram-se no site <http://www.mp.mt.gov.br/promotor.php> ..."

LEIA-SE: "...OBS.: 1º - Os endereços das Promotorias de Justiça abaixo relacionadas encontram-se no site <http://www.mpmt.mp.br/promotor.php> ..."

ATO ADMINISTRATIVO Nº 495/2015-PGJ

Institui a Política de Segurança da Informação e o uso de Internet e Correio Eletrônico no Ministério Público do Estado de Mato Grosso.

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DE MATO GROSSO, no uso de suas atribuições, nos termos da Lei Complementar Nº 11/1996,

CONSIDERANDO a informação como um ativo essencial que necessita de adequada proteção aos vários tipos de ameaças externas e internas que possam comprometer a integridade, confidencialidade e disponibilidade das informações do Ministério Público do Estado de Mato Grosso ou que estejam sob sua responsabilidade, visando a garantia da continuidade do negócio, a minimização de riscos e a maximização dos resultados;

CONSIDERANDO a necessidade de implantar um conjunto de controles, normas, procedimentos, padrões e sistemas que visem a análise e o melhoramento contínuo da segurança da informação;

CONSIDERANDO a crescente importância e reconhecimento da segurança da informação, que suscita a busca por um ambiente seguro, a melhoria dos processos de trabalho, a adoção de novas tecnologias e, sobretudo, a conscientização dos usuários da rede corporativa do Ministério Público de Mato Grosso;

CONSIDERANDO a importância da utilização de canais e ferramentas apropriadas no trâmite de informações, exclusivamente para a manutenção dos processos de trabalho e a geração do conhecimento no âmbito institucional;

CONSIDERANDO a necessidade de estabelecer mecanismos de controle que garantam o uso adequado dos serviços de correio eletrônico no âmbito institucional;

CONSIDERANDO a importância da utilização da internet como ferramenta de apoio para a manutenção dos processos de trabalho e a geração do conhecimento no âmbito institucional;

CONSIDERANDO a atribuição do Comitê Estratégico de Tecnologia da Informação para definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

CONSIDERANDO os seguintes conceitos:

Ameaça - agente ou ação, espontânea ou proposital, que afeta um sistema através de suas vulnerabilidades, causando prejuízos e/ou redução de disponibilidade.

Ativos de tecnologia da informação - estações de trabalho, Ativos de Rede e automação, servidores, software, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação, bem como conexões com a internet, hardware e software.

Backup - cópia de segurança gerada para possibilitar o acesso e recuperação futura das informações.

Caixa corporativa do correio eletrônico - identifica, de forma não pessoal, um único órgão, unidade administrativa, grupo de trabalho, projeto, evento ou serviço do Ministério Público do Estado de Mato Grosso, o mesmo que e-mail institucional.

Confidencialidade - proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação.

Conta individual do correio eletrônico - Caixa postal que identifica um único usuário, pessoa física, conforme padrão estabelecido pelo Ministério Público do Estado de Mato Grosso, o mesmo que e-mail individual.

Disponibilidade - garantir que o serviço esteja funcionando conforme especificado e os acessos às informações esteja disponível somente a usuários autorizados.

Firewall - sistema de segurança de computadores usado para restringir acesso de/para em uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas.

Gestão de risco - atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo, inclusive, análise e avaliação, tratamento, aceitação e comunicação dos riscos.

Incidente de segurança da informação - representado por um simples ou por uma série de eventos de segurança da informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação.

Integridade - toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada.

Listas de destinatários - grupos de usuários do correio eletrônico corporativo (restrito aos endereços do Ministério Público do Estado de Mato Grosso), criados mediante solicitação dos responsáveis por órgãos, projetos, eventos e serviços institucionais, para o envio de mensagens.

Segurança da informação - conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos.

Serviço de correio eletrônico - sistema utilizado para criar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, mostrar, ler ou imprimir informações, com o propósito de comunicação entre pessoas ou grupos, exclusivamente em concordância com os interesses da Instituição, vedado como meio de armazenamento de informações. O mesmo que e-mail corporativo ou correio institucional.

Spam - mensagens não solicitadas, geralmente destinadas a um grande número de pessoas, por meio do correio eletrônico.

Usuário - qualquer colaborador seja ele membro, servidor, estagiário, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa ou utiliza informações custodiadas ou de propriedade, do Ministério Público do Estado de Mato Grosso.

Usuário do correio eletrônico - pessoa física, seja membro ou servidor, e órgão, unidade administrativa, grupo de trabalho, projeto, evento ou serviço do Ministério Público do Estado de Mato Grosso reconhecido e habilitado pela administração do serviço de correio eletrônico para utilizá-lo.

Vulnerabilidade - fragilidade de um software, sistema operacional ou outro componente da infraestrutura de TI que pode ser explorada por uma ou mais ameaças.

RESOLVE:

Art. 1º - Instituir a PSI - Política de Segurança da Informação do Ministério Público do Estado de Mato Grosso, com a finalidade de estabelecer diretrizes de segurança da informação, visando à adoção de procedimentos e mecanismos relacionados à proteção das informações de sua propriedade e sob sua guarda.

## CAPÍTULO I

### DAS DIRETRIZES BÁSICAS

Art. 2º - São diretrizes relacionadas ao cadastro de novos usuários e autenticação em ambientes virtuais:

- I. Um novo usuário será cadastrado apenas após o comunicado e solicitação do Departamento de Gestão de Pessoas - DGP.
- II. Caberá ao DGP notificar à administração do serviço de correio eletrônico as alterações de dados cadastrais relacionadas aos servidores do Ministério Público do Estado de Mato Grosso.
- III. Os logins para autenticação nos ambientes virtuais e serviços serão criados apenas para servidores do Ministério Público do Estado de Mato Grosso.
- IV. Todo login será preferencialmente criado da seguinte forma: primeira letra do nome seguido do último sobrenome. Em caso de duplicidade será utilizada a segunda letra do nome, e assim sucessivamente.

Art. 3º - São diretrizes básicas da PSI do Ministério Público do Estado de Mato Grosso:

- I. Responsabilidade pela garantia da segurança, do controle e da administração das suas informações.
- II. A informação produzida ou recebida é de propriedade do Ministério Público do Estado de Mato Grosso, devendo ser armazenada e protegida quanto ao seu acesso.

III. O acesso às informações de propriedade do Ministério Público do Estado de Mato Grosso será direcionado ao desempenho das atividades ministeriais e plenamente adequado aos objetivos institucionais.

IV. Divulgação ampla e irrestrita da PSI.

V. Vedação do uso de informações de propriedade do Ministério Público do Estado de Mato Grosso para interesses que não estejam de acordo com os objetivos institucionais.

VI. Responsabilidade pela realização e acompanhamento das manutenções preventivas periódicas dos equipamentos e instalações, visando à preservação do patrimônio institucional.

VII. Ambiente tecnológico mantido, atualizado e supervisionado, de modo a atender os níveis e requisitos de segurança próprios e inerentes às funções institucionais.

Art. 4º - São diretrizes relativas ao ambiente e acesso físico:

I. Controle do acesso físico às dependências e instalações do Ministério Público do Estado de Mato Grosso, disciplinando a circulação de pessoas, materiais e equipamentos.

II. Recursos e instalações críticas ou sensíveis protegidos física e adequadamente aos riscos identificados, contra acessos não autorizados, danos ou interferências, por meio de barreiras de segurança e controles de acesso.

III. Acessos aos painéis de controle e cabeamentos de energia e de comunicações restritos aos técnicos e profissionais das áreas de segurança e de infraestrutura.

IV. Exigência de autorização formal para executar intervenções e manutenções no ambiente físico do Ministério Público do Estado de Mato Grosso que deverão estar submetidas a uma supervisão previamente responsabilizada.

V. Exigência de instalações apropriadas para guarda, utilização e lotação dos recursos tecnológicos e materiais.

Art. 5º - São diretrizes relativas à segurança dos usuários:

I. Compromisso de confidencialidade e de cumprimento da política, normas e procedimentos de segurança da informação do Ministério Público do Estado de Mato Grosso, com previsão de sanções e penalidades em caso de violação das regras.

II. Ampla divulgação entre membros, servidores e colaboradores do Ministério Público do Estado de Mato Grosso das medidas e procedimentos que eliminem riscos de acessos não autorizados, perdas, danos e violações de segurança.

III. Obrigatoriedade do porte e uso de identificação funcional durante a permanência de servidores e colaboradores nas dependências, instalações e unidades do Ministério Público do Estado de Mato Grosso.

IV. Identificação de membros, servidores e colaboradores imprescindível, pessoal e intransferível, responsabilizando-os pelas ações praticadas por meio dela.

V. Treinamento e atualização sistemática de membros, servidores e colaboradores do Ministério Público do Estado de Mato Grosso sobre políticas, normas e procedimentos de segurança da informação, visando o pleno exercício de suas funções.

VI. Responsabilidade pessoal e intransferível pelo sigilo, privacidade e uso de senhas de acesso aos recursos computacionais, não podendo ser compartilhadas, divulgadas, anotadas em papel ou em sistema visível ou de acesso não protegido.

VII. Troca imediata das senhas, nos casos de perda de sigilo, ou mesmo suspeita. É necessário também realizar trocas periódicas, conforme a mesma expira e a troca é solicitada ao usuário em sua estação de trabalho.

VIII. Bloqueio imediato dos acessos aos recursos tecnológicos com perfil de usuário, nos casos de exoneração, aposentadoria, desligamentos de qualquer natureza, rescisão ou término de contrato de terceirizados, demissão e descredenciamento ou cessão de servidores à outras instituições.

IX. Previsão formal e contratual de cuidados e responsabilização quanto à segurança dos ativos do Ministério Público do Estado de Mato Grosso nas contratações de prestação de serviços.

X. Vedação do uso de credenciais de terceiros (que não sejam membros, servidores e colaboradores) para acessar sistemas, internet, intranet, correio eletrônico e a rede do Ministério Público do Estado de Mato Grosso, para o desempenho de qualquer tipo de atividade, mesmo que temporariamente.

XI. Na Procuradoria Geral de Justiça e na Sede das Promotorias o acesso de visitantes é feito pela rede wireless específica para visitantes. Nas promotorias do interior do Estado de Mato Grosso, a chave de acesso ao roteador wireless é fornecida na própria promotoria.

XII. Uso e aplicação da prática de bloqueio da tela do computador em períodos de ausência do local de trabalho.

XIII. Utilização de sistemas e aplicativos após treinamento operacional específico, seguindo definições e procedimentos registrados em manuais ou documentos similares.

XIV. Obrigatoriedade da ciência e conhecimento de todo material referente à segurança da informação, disponibilizado pelo Ministério Público do Estado de Mato Grosso.

XV. Tratamento de documentos adequados e compatíveis com seu grau de sigilo.

XVI. Capacitação e desenvolvimento da equipe de tecnologia da informação do Ministério Público do Estado de Mato Grosso em segurança da informação.

XVII. Conscientização dos membros, servidores e colaboradores do Ministério Público do Estado de Mato Grosso quanto às ameaças externas (vírus, interceptação de mensagens e informações, grampos e fraudes e tentativas que ensejam o roubo de senhas) que possam afetar ou ameaçar a segurança das informações da instituição.

XVIII. Vedação a membro, servidor ou colaborador do Ministério Público do Estado de Mato Grosso de:

a) Conectar na rede do Ministério Público do Estado de Mato Grosso equipamentos não autorizados, salvo autorização prévia do DTI para Membros.

b) Alterar nomes padronizados dos ativos.

c) Compartilhar conta de correio eletrônico institucional.

d) Acessar e divulgar informações que contenham material obsceno, apologia ao fanatismo, práticas religiosas, político-partidário, qualquer forma de discriminação ou material que, explícita ou implicitamente, se refira à conduta imoral.

e) Fazer cópias de materiais da Internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte.

f) Alimentar-se próximo aos servidores de rede e estações de trabalho.

g) Fazer cópia não autorizada de softwares adquiridos ou desenvolvidos pelo Ministério Público do Estado de Mato Grosso.

h) Trazer, para uso nas instalações do Ministério Público do Estado de Mato Grosso, equipamentos de tecnologia pessoais, sendo notebooks, e ativos de rede (switch, roteadores e repetidores wireless ou qualquer equipamento do gênero).

i) Armazenar arquivos pessoais nos computadores das instituições ou no espaço disponibilizado em rede, sendo que o mesmo tem como finalidade armazenar arquivos da instituição.

Art. 6º - São diretrizes relativas à operação e comunicação:

I. Garantia da tramitação segura de documentos, no âmbito do Ministério Público do Estado de Mato Grosso.

II. Uso de aplicações de comunicação remotas e transmissões de informações com recursos de tecnologia da informação homologados e precedidos de aprovação formal do Ministério Público do Estado de Mato Grosso.

III. Armazenamento de informações críticas e estratégicas nos servidores da rede corporativa e em áreas protegidas.

IV. Cada usuário é responsável pelo controle e armazenamento seguro de informações sigilosas.

V. Proibição de acesso à informação institucional que não seja explicitamente autorizado.

VI. Vedação ao transporte e armazenamento de informações do Ministério Público do Estado de Mato Grosso em qualquer meio, seja CD, DVD, servidores em nuvem, pendrive, papel etc, salvo os casos em que haja interesse do Ministério Público de Mato Grosso e autorização da chefia imediata.

VII. Proibição para abrir ou executar arquivos de origem desconhecida.

Art. 7º - São diretrizes relativas ao ambiente de redes:

I. Disponibilização de recursos e estruturas tecnológicos adequados aos padrões de segurança do Ministério Público do Estado de Mato Grosso.

II. Adoção de manutenções preventivas periódicas e sistemáticas nos equipamentos instalados.

III. Liberação dos ativos de tecnologia de informação para uso condicionada à efetiva homologação e documentação.

IV. Controle sistemático da utilização de equipamentos de terceiros na rede de tecnologia do Ministério Público do Estado de Mato Grosso.

V. Proteção contra ameaças externas e internas da rede e das informações trafegadas.

VI. Monitoramento e documentação do ambiente de rede, assegurando a confidencialidade, integridade e a disponibilidade das informações trafegam neste ambiente.

VII. Manter as mesmas regras de segurança e navegação para rede sem fio e conexão via cabo.

Art. 8º - São diretrizes relativas a firewall e antivírus:

I. Procedimento formal de atualização do software de firewall e antivírus em todos os ativos de tecnologia instalados no Ministério Público do Estado de Mato Grosso, conforme instruções e determinações do fabricante.

II. Manutenção sempre ativa do firewall e de programas antivírus.

Art. 9º - São diretrizes relativas ao desenvolvimento e manutenção de sistemas de informação:

I. Definição dos requisitos de controle de segurança para novos sistemas ou melhorias em sistemas existentes.

II. Monitoramento de todos os arquivos de logs (ocorrências) previamente configurados, visando a identificação de falhas, violações de segurança e a recuperação de informações.

III. Definição de procedimentos para supervisão e monitoramento do desenvolvimento de sistemas por empresas terceirizadas.

IV. Os sistemas que armazenam informações estratégicas da instituição deverão ser disponibilizados para acesso apenas na rede interna do MPMT até que o DTI comprovadamente garanta os quesitos de segurança adequados para acesso externo.

Art. 10 - São diretrizes relativas ao armazenamento e backup:

I. Adoção de procedimentos formais de backup (cópia de segurança) e restore (recuperação) para todo o acervo de software e informações sob a responsabilidade do Ministério Público do Estado de Mato Grosso, de acordo com o perfil e especificidades de utilização.

II. Armazenamento dos backups em local e ambiente adequado, seguro e distinto em relação ao local das informações originais ou em produção.

Art. 11 - São diretrizes relativas ao controle de hardware e software adquiridos:

I. Manutenção das licenças dos softwares sempre compatíveis com o número de instalações efetuadas.

II. Adoção de procedimentos para controle de softwares e hardwares.

III. Instalação de softwares, formalmente aprovados, no ambiente de tecnologia da informação.

IV. Adoção de mecanismos e medidas de segurança que evitem a subtração de componentes de equipamentos de tecnologia.

V. Toda movimentação física de bens de tecnologia entre departamentos, promotorias, procuradorias, deverá ser autorizada pelo Departamento de Apoio Administrativo e pelo Departamento de Tecnologia da Informação, para que sejam realizadas todas as atualizações no sistema de controle patrimonial e as devidas orientações quanto ao remanejamento correto e seguro do equipamento.

Art. 12 - São diretrizes relativas à manutenção de equipamentos:

I. Adoção de procedimentos para remoção de informações, consideradas relevantes, dos equipamentos liberados para manutenção, descarte, cessão de uso ou reutilização.

II. Registro, controle e inspeção sistemáticos dos equipamentos de tecnologia da informação e seus componentes.

III. Adoção nos contratos de prestação de serviços de Termo de Responsabilidade e Sigilo sobre cuidados e responsabilização quanto à segurança de equipamentos de tecnologia da informação que saem para manutenção.

Art. 13 - São diretrizes relativas ao service desk:

I. Adoção de service desk (suporte técnico) centralizado no Departamento de Tecnologia da Informação para atendimento a todas as unidades do Ministério Público do Estado de Mato Grosso.

II. Composição e qualificação da equipe de service desk do Ministério Público do Estado de Mato Grosso de especialistas nas ferramentas de tecnologia da informação, sistemas e aplicativos utilizados.

III. Adoção de software integrado de service desk para gestão das solicitações de serviços e atendimentos, com a criação da base de conhecimento.

IV. Instalação nas estações de trabalho de programas e softwares homologados pelo Ministério Público do Estado de Mato Grosso e realizada por profissionais e equipes de serviço indicados pelo órgão.

V. A equipe de analistas do service desk poderá realizar suporte remoto, via software específico homologado pelo DTI, mediante prévia aprovação do usuário.

VI. As ligações efetuadas e recebidas pelo service desk poderão ser gravadas visando garantir a segurança dos atendentes e dos usuários, bem como servir de método de aferição da qualidade do serviço prestado.

Art. 14 - São diretrizes relativas à gestão de risco e continuidade de negócio:

I. Realização sistemática de análise e avaliação dos riscos relacionados à segurança da informação do Ministério Público do Estado de Mato Grosso.

II. Priorização das ações voltadas à mitigação dos riscos identificados, com a implantação de novos controles que se façam necessários, como a criação de novas regras e procedimentos, a reformulação de sistemas, dentre outros.

Art. 15 - São responsabilidades do Comitê Estratégico de Tecnologia da Informação - CETI do Ministério Público do Estado de Mato Grosso:

I. Discutir e aprovar a proposta de política de segurança da informação e as suas revisões periódicas.

II. Deliberar administrativamente acerca de descumprimentos da política e normas de segurança da informação.

III. Aprovar planos de ação para implementação da PSI.

IV. Aprovar planos de auditoria.

V. Aprovar planos de divulgação das ações de segurança da informação implementadas.

VI. Acompanhar e avaliar a implementação e o desenvolvimento das ações de segurança da informação, no âmbito do Ministério Público do Estado de Mato Grosso.

Art. 16 - São responsabilidades dos membros, servidores e colaboradores do Ministério Público do Estado de Mato Grosso:

I. Cumprir a política, normas e procedimentos de segurança da informação do Ministério Público do Estado de Mato Grosso.

II. Buscar orientação do superior hierárquico em caso de dúvidas relacionadas à segurança da informação.

III. Responsabilizar-se pelo cumprimento da política e das normas de segurança da informação, assinando o Termo de Responsabilidade e Sigilo.

IV. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Ministério Público do Estado de Mato Grosso.

V. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Ministério Público do Estado de Mato Grosso.

VI. Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual.

VII. Comunicar imediatamente ao seu superior hierárquico qualquer descumprimento ou violação da política, normas e procedimentos de segurança da informação do Ministério Público do Estado de Mato Grosso.

## CAPÍTULO II

### DO USO DO CORREIO ELETRÔNICO

Art. 17 - Disciplinar os procedimentos a serem observados pelos Órgãos e Unidades do Ministério Público do Estado de Mato Grosso para a utilização do serviço de correio eletrônico, na comunicação, interlocução e intercâmbio de informações, em conformidade com os interesses institucionais.

Parágrafo Único. A administração e a gestão do serviço de correio eletrônico são de responsabilidade do Departamento de Tecnologia da Informação.

Art. 18 - O acesso ao correio eletrônico dar-se-á por meio da Identificação do Usuário, cuja Senha é de natureza pessoal ou exclusiva e intransferível.

§ 1º - A identificação de e-mail individual e institucional será acrescida da extensão "mpmt.mp.br", observando os critérios definidos neste Ato Administrativo.

§ 2º - Todas as contas do correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização,

que deverá ser exclusivamente para fins profissionais.

§ 3º - Não são permitidas configurações em outros ambientes de e-mail para acessar a conta corporativa para recebimento ou envio de mensagens, como configurações permitidas em Gmail, Live Mail, dentre outros serviços.

Art. 19 - A criação de novas caixas postais corporativas será efetuada pela administração do serviço de correio eletrônico, mediante solicitação do DGP, com os dados cadastrais.

Art. 20 - Poderão ser emitidos comunicados, por meio do serviço de correio eletrônico, exclusivamente para o envio de mensagens de interesse institucional, para listas extensas de destinatários.

§ 1º - As listas extensas de destinatários são aquelas compostas de 30 (trinta) ou mais destinatários.

§ 2º - A emissão de Comunicados deverá ser feita preferencialmente por contas corporativas de correio eletrônico.

§ 3º - Os avisos de cunho solidário e de utilidade pública de interesse institucional serão de emissão preferencial do Departamento de Gestão de Pessoas, mediante solicitação da parte interessada.

Art. 21 - A criação e atualização de listas de destinatários deverão ser solicitadas diretamente ao Departamento de Tecnologia da Informação, de acordo com as necessidades do usuário do serviço de correio eletrônico.

§ 1º As listas extensas de destinatários serão identificadas pelas letras MPE\_, seguida de expressão que caracterize o referido grupo de destinatários.

Art. 22 - É proibida qualquer tentativa de acesso não autorizado às caixas postais de terceiros, salvo em casos de manutenção com autorização do Procurador-Geral de Justiça ou do usuário proprietário da caixa postal.

Art. 23 - O tratamento e linguagem utilizados na comunicação eletrônica devem ser compatíveis com o destinatário e o assunto, devendo ser evitadas expressões de circulação restrita, como gíria, regionalismos ou outras que têm sua compreensão dificultada.

Art. 24 - Não serão permitidos o envio e o armazenamento de mensagens contendo:

- I. Material obsceno, ilegal ou antiético.
- II. Matérias publicitárias, compra e venda de produtos, pois para isso, existe espaço próprio de classificados na INTRANET.
- III. Qualquer programa de computador danoso ao ambiente de tecnologia da Instituição.
- IV. Material preconceituoso ou discriminatório.
- V. Material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos ou trate de interesses particulares.
- VI. Assuntos ofensivos ao princípio da urbanidade, ao decoro pessoal, à honra e à dignidade de pessoas, instituições e autoridades.
- VII. Música, vídeo, animações ou fotografias que não sejam de interesse da instituição.
- VIII. Correntes ou similares.
- IX. Material que possa sobrecarregar as caixas postais dos usuários, com conteúdo muito extenso.

Parágrafo único - Os anexos de mensagem devem limitar-se a 15 MB (quinze megabytes) e devem reservar-se a documentos de interesse institucional.

Art. 25 - A utilização dos serviços de correio eletrônico implica nas seguintes responsabilidades:

- I. Do Departamento de Tecnologia da Informação:
  - a) Administrar o serviço e recursos do correio eletrônico, assegurando sua adequação às necessidades de trabalho.
  - b) Gerenciar e manter ativo o servidor de correio eletrônico do Ministério Público do Estado de Mato Grosso, acompanhando e avaliando seu uso e eventuais ocorrências e irregularidades.
  - c) Promover a garantia da segurança, proteção e privacidade no armazenamento e na transmissão das mensagens do correio eletrônico do Ministério Público do Estado de Mato Grosso.
  - d) Criar, configurar e excluir contas individuais, caixas corporativas e listas de destinatários do correio eletrônico.
  - e) Orientar os usuários quanto ao armazenamento e eliminação de mensagens da caixa postal.

- f) Manter registros para verificação do uso adequado do serviço de correio eletrônico.
- g) Executar o bloqueio de mensagens e anexos enviados, que contrariem este Ato Administrativo.
- h) Atualizar as listas de destinatários, quando solicitado.
- i) Estabelecimento de limite máximo para o tamanho de caixa de entrada e anexos.

## II. Dos Usuários:

- a) Cumprir as normas e procedimentos relacionados ao uso do serviço de correio eletrônico.
- b) Utilizar o serviço de correio eletrônico para o desempenho das suas atribuições.
- c) Armazenar e eliminar mensagens das caixas postais conforme orientações recebidas.
- d) Proceder à atualização dos seus dados cadastrais, utilizando os meios disponíveis.
- e) Comunicar ao Departamento de Tecnologia da Informação o recebimento de mensagens, imagens ou notas indevidas, para as providências cabíveis.
- f) Encaminhamento imediato ao Departamento de Tecnologia da Informação dos alertas de vírus recebidos pelo correio eletrônico.
- g) Adoção da prática de varredura pelo programa antivírus dos anexos recebidos pelo correio eletrônico.

Art. 26 - Ao ser excluída uma conta de e-mail, os dados contidos no ato da exclusão permanecerão disponíveis durante 30 (trinta) dias.

## CAPÍTULO III

### DO USO DA INTERNET

Art. 27 - Disciplinar os procedimentos a serem observados pelos Órgãos e Unidades do Ministério Público do Estado de Mato Grosso para a utilização do serviço de internet, na comunicação, interlocução e intercâmbio de informações, em conformidade com os interesses institucionais.

Art. 28 - São diretrizes gerais relacionadas ao uso do serviço de internet:

- I. Adoção de ferramentas e procedimentos de segurança para os ambientes de internet e intranet.
- II. Ativação e monitoramento de logs (relatórios de ocorrências e acessos dos usuários) de segurança.
- III. Desenvolvimento de planos específicos que englobem a plena conservação do ambiente físico do Ministério Público do Estado de Mato Grosso.
- IV. Toda informação obtida na internet, de forma livre e gratuita, deve ter a sua autenticidade e confiabilidade confirmada, antes de ser efetivamente utilizada.
- V. Toda a área de transferência de informações acessível pela internet e disponível publicamente para gravação deve ser limpa regularmente.
- VI. Os ativos de tecnologia da informação do Ministério Público do Estado de Mato Grosso, incluindo as conexões com a internet, hardware e software, devem ser empregados na consecução dos objetivos do órgão, sendo vedada a sua utilização para outros fins, exceto para os casos explicitamente permitidos por este Ato Administrativo.
- VII. Cada dispositivo computacional (estação de trabalho, notebook, tablet, smartphone, servidor) do Ministério Público do Estado de Mato Grosso, com acesso à internet, deve possuir um sistema de proteção instalado, ativado e atualizado contra vírus ou qualquer outro software malicioso.
- VIII. As conexões com a internet feitas através de computadores ou notebooks homologados pelo Ministério Público do Estado de Mato Grosso somente podem ser feitas através da rede deste Ministério Público, ficando vedada a interligação com dispositivos pessoais que permitam o compartilhamento da conexão com a internet sem que haja controle do MP, tais como smartphones e modems (conexão 3G e 4G ou superiores).
- IX. Fica vedado o uso de aplicativos ou conexões que permitam acesso externo a empresas ou residências, partindo da rede interna do Ministério Público do Estado de Mato Grosso ou de outras redes para a rede deste Ministério Público. Salvo para os casos em que haja interesse do Órgão, autorização da chefia imediata e homologação do DTI.

Art. 29 - São diretrizes de controle de acesso aos serviços de internet:

I. A permissão de acesso à internet deve ser seletiva em relação aos serviços disponibilizados, tais como sítios web e correio eletrônico, e deve ser concedida exclusivamente àqueles usuários que necessitem deste acesso para o seu trabalho, sendo removida quando não for mais necessária.

II. O acesso seletivo à internet deve ser disponibilizado e controlado por meio de equipamento de firewall, cabendo ao Departamento de Tecnologia da Informação gerenciar as regras de controle de acesso.

III. A permissão de acesso à internet deve ser concedida através de uma conta de usuário que possibilite identificar, individualmente, seu proprietário, podendo o histórico de acesso, inclusive o conteúdo, ser monitorado pelo órgão, sem necessidade de notificação prévia. O histórico de acesso, juntamente com o conteúdo acessado, deve ser armazenado por um período mínimo estipulado pelo Departamento de Tecnologia da Informação.

IV. Não é permitida a utilização de qualquer software ou dispositivo de hardware que possa suprimir, omitir ou mascarar a identificação da conta de usuário em qualquer serviço da internet.

V. O Procurador-Geral de Justiça poderá, sem aviso prévio, determinar a restrição do acesso a serviços da internet, tais como sítios web, redes peer-to-peer e download de arquivos.

VI. O superior hierárquico pode solicitar restrição de acesso para usuários a eles subordinados.

VII. A possibilidade de acessar qualquer serviço da internet não implica em autorização para acessá-lo, ficando o usuário responsável pelos atos que prejudiquem os interesses do órgão.

VIII. Não é permitido o uso de mecanismos de dissimulação do usuário, como re-mailers, IP Spoofing e tradutores de URL.

Art. 30 - São diretrizes de conexão de rede com a internet:

I. É vetada a conexão entre qualquer rede de informações do Ministério Público do Estado de Mato Grosso e a internet, através de serviços de telecomunicações não autorizados pelo DTI.

II. Toda comunicação entre computadores e as redes do Ministério Público do Estado de Mato Grosso, através da internet ou outra rede pública, deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pelo DTI.

III. Toda a comunicação entre as redes do Ministério Público do Estado de Mato Grosso e a internet, ou qualquer outra rede pública, deve necessariamente passar por firewall, que deve ser configurado com uma política restritiva, monitoramento dos fluxos de comunicação e proteção contra ataques como, por exemplo, ataques Denial-Of-Service e SYN Flood.

IV. A conexão de internet em todas as Promotorias deverá possuir reserva de banda para acesso prioritário ao Sistema Integrado do Ministério Público do Estado de Mato Grosso - SIMP.

Art. 31 - São diretrizes de uso aceitável da internet:

I. É permitido o acesso a sites que sejam fontes de informação necessárias à execução das atividades do Ministério Público do Estado de Mato Grosso.

II. É permitido o uso de serviços pessoais prestados através da internet, tais como banco on-line, reservas de passagem e webmails.

III. Recomenda-se não serem utilizados os recursos de "Salvar Senha" ou "Lembrar Senha", disponíveis na maioria das aplicações e navegadores (Outlook, Internet Explorer, Edge, Google Chrome e Firefox).

IV. Quando o usuário estiver usando a internet e verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site e notificar um incidente de segurança da informação ao DTI.

V. Não é permitido o uso de aplicações para distribuição de arquivos, tais como 4Shared, peer-to-peer, dentre outros.

VI. Não é permitido o uso de jogos on-line.

VII. Ressalvados os interesses do Ministério Público do Estado de Mato Grosso, não é permitido:

a) O acesso a conteúdos impróprios, que são aqueles relacionados com pornografia, pedofilia, racismo, violência, incitação ao ódio, apologia ao uso de drogas e armas, invasão de computadores e jogos.

b) O uso de serviços de mensagem instantânea diferente do NEOS (comunicador oficial da instituição) e salvo substituto homologado pelo DTI, restando proibidos ICQ, Messenger, Google Talk, MSN, Skype e similares, seja por software específico ou via Web.

c) O acesso a sites de bate papo e serviços de relacionamento, tais como Facebook, Instagram, Gazzag, MySpace, Twitter e correlatos.

d) O uso de serviços de áudio e vídeo em tempo real, tais como rádio on-line, TV on-line e telefonia IP.

e) A sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas do Ministério Público do Estado de Mato Grosso ou de qualquer outra organização, através da internet ou de outra rede pública.

f) O uso ou a posse de ferramentas de hardware e software para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de informações.

Art. 32 - São diretrizes referentes aos direitos autorais e conteúdos impróprios:

I. Sempre que informações obtidas através da internet forem usadas em documentos internos, a fonte deve ser citada.

II. A indicação de direitos reservados deve ser presumida para todo conteúdo disponível na internet, a menos que contenha informação contrária.

III. Os usuários dos serviços de internet do Ministério Público do Estado de Mato Grosso não devem obter, armazenar ou transmitir conteúdo ilegal, tais como software não licenciado ou não homologado pela instituição, pornografia infantil, senhas e informações bancárias extraviadas, dentre outros que afetem os interesses e a imagem da instituição.

Art. 33 - Ressalvado os interesses do Ministério Público do Estado de Mato Grosso, são diretrizes referentes ao download de arquivos:

I. Não é permitido o download de filmes, músicas, vídeos ou conteúdos semelhantes relacionados ao entretenimento.

II. O download de arquivos, com grande volume de informações, deve considerar as limitações da conexão com a internet.

III. Todo arquivo obtido em fontes externas ao Ministério Público do Estado de Mato Grosso deve ser submetido à verificação de software antivírus antes de ser utilizado.

IV. No caso de download de arquivos que sejam de interesse comum a várias áreas do Ministério Público do Estado de Mato Grosso, convém que este seja realizado pelo Departamento de Tecnologia da Informação para que posteriormente seja disponibilizado aos interessados, através de um repositório compartilhado.

Art. 34 - O DTI analisará periodicamente os registros de acesso à internet para verificação do atendimento à Política de Segurança da Informação. Tais registros podem, referirem-se a websites visitados, bookmarks, arquivos copiados da internet, configurações dos softwares, tempo gasto nos acessos e outras informações necessárias para a otimização dos recursos de acesso à internet e realização de auditoria.

#### CAPÍTULO IV

##### DAS DISPOSIÇÕES GERAIS

Art. 35 - A PSI, instituída neste Ato Administrativo, assim como as normas e procedimentos de segurança da informação serão divulgados e disponibilizados a todos os membros, servidores e colaboradores do Ministério Público do Estado de Mato Grosso.

Art. 36 - Os casos omissos ou não previstos nesta PSI serão analisados e definidos pelo CETI, com aprovação do Procurador-Geral de Justiça.

Art. 37 - A violação dos dispositivos previstos neste ato caracteriza infração ao disposto no art. 143, III da Lei Complementar n. 04/90 sujeita, dentre outros, às sanções previstas no art. 154 da LC n. 04/90 c/c o art. 3º da LC n. 207/2004.

Parágrafo Único - Eventuais infrações ao disposto neste ato serão comunicadas de imediato pelo Procurador de Justiça, Promotor de Justiça ou Chefe de Departamento ao Comitê Estratégico de Tecnologia da Informação para a adoção das providências cabíveis.

Art. 38 - Este ato administrativo entra em vigor na data de sua publicação, revogadas as disposições contrárias a ele, especialmente o Ato Administrativo 93/2005-PGJ, Ato Administrativo 93/2007-PGJ e a Portaria n.º 251/2005-PGJ e suas alterações.

Cuiabá-MT, 01 de dezembro de 2015.

PAULO ROBERTO JORGE DO PRADO

Procurador-Geral de Justiça

#### ANEXO I

##### TERMO DE RESPONSABILIDADE E SIGILO

O presente documento, firmado entre o MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO, doravante denominado MPMT, e

o Sr.(a) \_\_\_\_\_, inscrito(a) no CPF n.º \_\_\_\_\_, doravante denominado(a) RESPONSÁVEL, celebra o Termo de Responsabilidade e Sigilo, por meio do qual o RESPONSÁVEL atesta ciência à Política de Segurança da Informação do MPMT, comprometendo-se a cumprir todos os seus requisitos e a não divulgar ou utilizar indevidamente, sob nenhuma forma ou meio - físico e lógico, dados e informações de propriedade da Instituição, em conformidade com as seguintes cláusulas:

PRIMEIRA - O RESPONSÁVEL é ciente que, em razão de sua relação laboral com o MPMT, lida com dados e informações internos, restritos e/ou confidenciais, de propriedade da Instituição. Estes dados e informações devem ser tratados com absoluta reserva, sob qualquer hipótese e em qualquer circunstância.

SEGUNDA - Os dados e informações a serem tratados sigilosamente são aqueles assim considerados no âmbito do MPMT, cujo conteúdo não deva ser do conhecimento de terceiros, parcial ou em sua totalidade:

- 1- Execução e acompanhamento de processos judiciais.
- 2- Estatísticas sociológicas e criminológicas, e relatórios de atividades da Instituição, enquanto não disponibilizadas publicamente.
- 3- Documentos com a finalidade de comunicação interna, tais como normativos e resoluções circulares.
- 4- Políticas e programas Institucionais.
- 5- Projetos implementados ou em fase de desenvolvimento, incluindo fluxogramas, estatísticas, especificações, avaliações, resultados de testes, arquivos de dados, topologias, protótipos, relatórios, etc.
- 6- Bases de dados dos sistemas de informação do MPMT.
- 7- Metodologias e ferramentas de trabalho desenvolvidas internamente.

TERCEIRA - O RESPONSÁVEL reconhece ser a lista acima meramente exemplificativa e ilustrativa, não contemplando todas as situações nas quais o sigilo faz-se necessário. Em caso de dúvida acerca do sigilo de um dado ou informação, o RESPONSÁVEL não deve divulgá-lo a terceiros, exceto se for expressa e previamente autorizada por escrito pelo MPMT.

QUARTA - O RESPONSÁVEL se obriga a fazer bom uso dos dados, informações, sistemas de informação e demais recursos do MPMT que lhe forem confiados, não utilizando informações privilegiadas a fim de obter vantagem indevida para si ou para outrem ou para causar dano à Instituição.

QUINTA - O RESPONSÁVEL concorda que, após a cessação de vínculo com o MPMT, deverá entregar ao seu superior imediato todo e qualquer recurso, seja de hardware, software ou material impresso, de propriedade da Instituição ou contendo dados e informações de propriedade da Instituição.

SEXTA - O presente Termo passa a vigorar a partir da data de sua assinatura pelas partes envolvidas. As obrigações a que alude este Termo perdurarão, inclusive, após a cessação de vínculo entre o RESPONSÁVEL e o MPMT, e abrangem, além das informações de que o RESPONSÁVEL venha a tomar conhecimento, aquelas que já possui na presente data.

SÉTIMA - Este Termo será regido e interpretado de acordo com as leis da República Federativa do Brasil.

OITAVA - As partes elegem o Foro da Comarca de Cuiabá - MT, para dirimir quaisquer dúvidas acerca da aplicação do presente documento.

E, por estarem justas e contratadas, as partes firmam o presente Termo de Responsabilidade e Sigilo em 3 (três) vias de igual teor e forma, para um só efeito, diante das 2 (duas) testemunhas abaixo nomeadas.

Cuiabá-MT, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_.

Ministério Público do Estado de Mato Grosso Responsável

1ª Testemunha 2ª Testemunha

---

Superintendência da Imprensa Oficial do Estado de Mato Grosso  
Rua Júlio Domingos de Campos - Centro Político Administrativo | CEP 78050-970 | Cuiabá, MT

Código de autenticação: 93015548

Consulte a autenticidade do código acima em [https://homolog.iomat.mt.gov.br/legislacao/diario\\_oficial/consultar](https://homolog.iomat.mt.gov.br/legislacao/diario_oficial/consultar)

