



**MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR**

Portaria nº 256 /PGJM, de 19 de dezembro de 2022.

Institui a Política de Utilização dos Recursos de Tecnologia da Informação no âmbito do Ministério Público Militar.

O **PROCURADOR-GERAL DE JUSTIÇA MILITAR**, no uso de suas atribuições legais, tendo em vista o disposto no artigo 124, inciso XX e XXII da Lei Complementar nº 75, de 20 de maio de 1993,

CONSIDERANDO a deliberação do Comitê Estratégico de Tecnologia da Informação (1214185) que, no uso das atribuições que lhe são conferidas pelo artigo 3º do seu Regimento Interno, aprovou os procedimentos de controles de acesso aos recursos de Tecnologia da Informação no âmbito do Ministério Público Militar,

RESOLVE:

Art. 1º Instituir a Política de Utilização dos Recursos de Tecnologia da Informação, no âmbito do Ministério Público Militar (MPM), nos termos do disposto no Anexo I (1212342) desta Portaria.

Art. 2º Revoga-se a Portaria nº 23, de 1º de fevereiro de 2013.

Art. 3º Revoga-se a Portaria nº 24, de 1º de fevereiro de 2013, que aprova o Regulamento para a Utilização da Rede Wireless da PGJM para Acesso à Internet.

Art.4º Esta Portaria entrará em vigor na data de sua publicação.



Documento assinado eletronicamente por **ANTÔNIO PEREIRA DUARTE**, **Procurador-Geral de Justiça Militar**, em 21/12/2022, às 18:45, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1233578** e o código CRC **61635FD5**.



MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO
POLÍTICA DE UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Estabelecer a Política de Utilização dos Recursos de Tecnologia da Informação no âmbito do Ministério Público Militar.

O **COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO**, no uso das atribuições que lhe são conferidas pelo artigo 3º, incisos I e V, do Ato nº 03/CETI-MPM, de 19 de abril de 2022, que aprovou seu Novo Regimento Interno;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, a Lei 12.965, de 23 de abril de 2014, a Lei Nº 13.709, de 14 de agosto de 2018, com o objetivo de estabelecer um sistema de gestão de segurança e de uso de tecnologia da informação alinhados às melhores práticas de mercado e à missão da instituição,

RESOLVE:

Art. 1º Estabelecer a Política de Utilização dos Recursos de Tecnologia da Informação (TI) no âmbito do Ministério Público Militar (MPM), estabelecendo-a como um componente fundamental para a realização da missão Institucional, fixando direitos e responsabilidades de seus usuários e de suas unidades executivas.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º O uso dos recursos de Tecnologia da Informação deve ter sua aplicação restrita à realização de atividades funcionais relacionadas à Instituição, sendo proibida a sua utilização para fins particulares ou alheios às atividades do órgão.

Art. 3º Para fins desta Política, considerar-se-ão Recursos de Tecnologia da Informação, os sistemas e equipamentos cuja finalidade é coletar, manter, armazenar, processar e disseminar informações eletronicamente, bem como as definições estabelecidas na Política de Segurança da Informação nos meios de tecnologia da informação do Ministério Público Militar (PSITI).

CAPÍTULO II
DAS NORMAS DE USO E SEGURANÇA

Seção I
Dos Direitos e Obrigações do Usuário

Art. 4º São direitos do usuário:

I - fazer uso de recursos de Tecnologia da Informação para a realização de atividades funcionais, relacionadas aos serviços de interesse do MPM;

II - possuir login e senha, de acordo com os critérios definidos pelo DTI, para acesso à rede de computadores, sistemas e correio eletrônico, mediante cadastro junto ao DTI;

III - acessar a Intranet e a Internet para a realização de atividades funcionais, salvo nas hipóteses de restrição de acesso;

IV - solicitar e receber suporte técnico de TI, quando necessário, para a realização de atividades funcionais.

Art. 5º São deveres do usuário:

I - zelar pela integridade, segurança e uso adequado dos recursos de Tecnologia da Informação sob sua responsabilidade e daqueles aos quais possuir acesso;

II - zelar pelo sigilo e segurança de suas contas de acesso e senhas, as quais são de uso individual e intransferíveis, sendo vedado compartilhá-las com terceiros;

III - alterar imediatamente as senhas iniciais recebidas quando da efetivação de seu cadastro como usuário, de acordo com os critérios definidos pelo DTI, ficando responsável por qualquer atividade desenvolvida por meio do uso destas a partir do momento em que recebê-las;

IV - armazenar nos servidores de rede somente os dados que guardem relação com suas atividades funcionais;

V - preservar a confidencialidade, integridade e disponibilidade das informações e de todos os dados aos quais possuir acesso;

VI - controlar o acesso aos recursos de Tecnologia da Informação que estiverem sob sua responsabilidade e daqueles aos quais possuir acesso;

VII - bloquear o computador que estiver utilizando, ou efetuar logoff (encerrar sessão), quando se ausentar temporariamente

do seu local de trabalho ou ao final do expediente;

VIII - fazer uso racional dos recursos e materiais de consumo de TI, evitando-se o desperdício e utilizando-os apenas para finalidades que guardem relação com suas atividades funcionais;

IX - salvar os arquivos institucionais que necessitem de cópia de segurança (backup) nas unidades de armazenamento disponibilizadas pelo DTI;

X - informar imediatamente ao DTI sobre qualquer ocorrência de descumprimento desta Política da qual venha a ter conhecimento.

Seção II

Das Proibições ao Usuário

Art. 6º É proibido ao usuário:

I - utilizar os materiais de consumo de TI da Instituição para trabalhos particulares e outros que não guardem relação com a realização de suas atividades funcionais;

II - armazenar na infraestrutura de TI qualquer tipo de arquivo que não guarde relação com as suas atividades funcionais;

III - utilizar os recursos de Tecnologia da Informação para armazenar, copiar, emprestar, transferir, exibir, ou executar qualquer tipo de arquivo digital do qual não seja usuário autorizado, que não tenha adquirido legalmente ou que incorra em violação de direitos autorais ou propriedade intelectual;

IV - efetuar qualquer alteração nas características de hardware ou software, ou de local de instalação de recursos de TI, sem a prévia autorização do DTI;

V - compartilhar com terceiros suas contas de acesso, senhas e outros tipos de autorizações de uso individual e intransferível;

VI - apagar, alterar ou distribuir informações, arquivos, dados, softwares ou qualquer outro recurso de Tecnologia da Informação sem a devida autorização;

VII - criar ou propagar malwares;

VIII - obter acesso a sistemas ou outros recursos de TI, ou utilizá-los sem a devida autorização;

IX - conectar computadores pessoais ou qualquer tipo de dispositivo à rede cabeada sem autorização do DTI, que poderá concedê-la, excepcionalmente, desde que respeitados requisitos básicos de segurança a serem definidos pelo DTI em função do tipo e da finalidade de uso do equipamento;

X - remover, copiar, transferir, modificar ou emprestar software para finalidade diversa das atividades funcionais;

XI - usar, instalar, executar, copiar, armazenar aplicativos, programas ou qualquer outro material que não esteja devidamente licenciado e cuja utilização não seja autorizada pelo DTI;

XII - utilizar o acesso à Internet ou ao correio eletrônico para a exibição, veiculação ou armazenamento voluntário de jogos, correntes e mensagens indesejadas (spam); sites de encontros e bate-papo; conteúdo pornográfico, erótico, comercial e político-partidário; entretenimento; material ofensivo à honra e à dignidade de instituições e agentes públicos, ao decoro pessoal e ao princípio da urbanidade; ou material para a obtenção de qualquer tipo de vantagem pessoal;

XIII - utilizar o acesso à Internet para finalidade alheia aos interesses do órgão e de forma que degrade o seu desempenho, como download de músicas, vídeos, imagens, softwares, streamings de vídeo ou áudio, e outros;

XIV - utilizar o correio eletrônico para finalidade alheia aos interesses do órgão e de forma que degrade o seu desempenho, como envio ou recebimento de músicas, vídeos, imagens, softwares, apresentações e outros, e, especialmente, para o envio de mensagens com anexos para grande quantidade de destinatários;

XV - utilizar as contas de e-mail institucionais para efetuar cadastros em sites ou serviços de terceiros que não guardem relação com as atividades funcionais;

XVI - divulgar informações sobre configurações de rede, softwares, sistemas, senhas ou quaisquer outras que possam representar ameaça à Segurança da Informação;

XVII - acessar sites da Internet enviados por fontes desconhecidas ou não confiáveis, salvo nos casos necessários para a execução de serviços de interesse da Instituição;

XVIII - averiguar ou testar fragilidades de Segurança da Informação - condutas que serão interpretadas como ameaças à Segurança da Informação.

Seção III

Dos Direitos e Obrigações do Departamento de Tecnologia da Informação

Art. 7º São direitos do DTI:

I - monitorar e armazenar o registro de acessos (logs), aplicar regras de controle de tráfego (traffic shaping), filtrar e/ou impedir o acesso a sites da Internet, por meio de ferramentas automatizadas, conforme critérios definidos pelo DTI e, nos casos excepcionais, pela Direção-Geral;

II - adotar, conforme a necessidade, diferentes perfis de acesso à Internet, tornando acessível aos usuários apenas os sites necessários para o cumprimento de suas atividades funcionais, considerando as atribuições de cada cargo ou unidade;

III - monitorar, armazenar, filtrar e/ou impedir o tráfego de mensagens de correio eletrônico, por meio de ferramentas automatizadas, conforme critérios definidos pelo DTI;

IV - monitorar a utilização dos recursos de TI por meio de auditorias ordinárias periódicas, ou extraordinárias, para detectar divergências entre as normas vigentes e os registros de eventos monitorados, ou apurar eventos prejudiciais à segurança e às boas práticas, fornecendo evidências nos casos de incidentes em segurança.

V - promover auditorias no tráfego de mensagens de correio eletrônico, de ofício ou por solicitação da Direção-Geral;

VI - promover inspeções em computadores e em recursos de Tecnologia da Informação do MPM com o objetivo de verificar a existência de malwares, softwares não licenciados, conteúdo que viole direitos autorais ou propriedade intelectual e para apurar a conformidade com as regras estabelecidas nesta Política;

VII - suspender serviços de rede, desligar equipamentos, bloquear acessos, apagar arquivos ou mensagens de correio eletrônico, quando tal procedimento se fizer necessário para proteger recursos de TI ou informações, devendo ser restabelecida a operação normal assim que cessar a ameaça identificada;

VIII - limitar os espaços em discos destinados ao armazenamento de arquivos ou mensagens de correio eletrônico, de acordo com a disponibilidade de recursos de Tecnologia da Informação;

IX - definir tipos e tamanhos de arquivos que poderão ser anexados às mensagens de correio eletrônico;

X - excluir arquivos armazenados nos servidores de rede que não guardem relação com as atividades institucionais;

XI - bloquear temporariamente contas de rede, contas de correio eletrônico e outras contas de acesso quando for essencial para garantir o cumprimento desta Política ou para preservar a Segurança da Informação.

Art. 8º São deveres do DTI:

I - planejar, coordenar, organizar, manter, controlar e supervisionar os recursos de TI do MPM;

II - zelar pela Segurança da Informação relativas aos recursos de TI utilizados no âmbito do MPM;

III - adotar as medidas cabíveis para garantir aos usuários os direitos previstos nesta Política;

IV - informar previamente aos usuários sobre paralisações programadas nos serviços e recursos de TI e ações referentes ao art. 7º incisos VII e X;

V - manter registro, em sistema informatizado, das solicitações de suporte técnico recebidas de usuários e das providências adotadas para o seu atendimento;

VI - realizar cópias de Segurança (backup) periódicas dos dados armazenados na infraestrutura de TI, de forma a possibilitar a recuperação no caso de falhas ou defeitos em equipamentos;

VII - preservar a confidencialidade, a integridade e a disponibilidade de todos os dados aos quais tiver acesso em função de suas atribuições;

VIII - restringir e controlar o acesso de terceiros aos recursos de TI que estiverem sob sua responsabilidade, como servidores de rede, equipamentos de conexão, equipamentos de backup, laptops, ferramentas, mídias e outros;

IX - examinar todos os equipamentos que contenham mídias de armazenamento antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança;

X - quando aplicável, destruir fisicamente dispositivos que contenham informações sensíveis;

XI - quando aplicável, apagar ou sobregravar as informações sensíveis, por meio de técnicas que tornem essas informações irrecuperáveis, em vez de usar as funções padrão de apagar ou formatar;

XII - analisar e avaliar os riscos, no caso de dispositivos defeituosos que contenham informações sensíveis, para determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo;

XIII - emitir pareceres técnicos para subsidiar as decisões da Direção-Geral relacionadas ao conteúdo desta Política;

XIV - fiscalizar o cumprimento desta Política;

XV - informar imediatamente à Direção-Geral sobre qualquer ocorrência de descumprimento desta Política.

Seção IV

Das Proibições ao Departamento de Tecnologia da Informação

Art. 9º É proibido ao DTI:

I - utilizar os direitos especiais da unidade para acessar, remover, copiar ou transferir informações confidenciais, sigilosas ou cujo acesso seja restrito, salvo quando estritamente necessário para preservar a Segurança da Informação, ou quando autorizado pela Direção-Geral ou pelo proprietário da Informação;

II - utilizar os direitos especiais de acesso da unidade para modificar ou divulgar informações confidenciais, sigilosas ou cujo acesso seja restrito;

III - utilizar os direitos especiais de acesso da unidade para obter vantagem direta ou indireta, para si ou para outrem;

IV - divulgar informações sobre configurações de rede, softwares, sistemas, senhas ou quaisquer outras que possam representar uma ameaça à Segurança da Informação ou que sejam restritas aos servidores do DTI;

V - atender a solicitações de serviços ou de suporte técnico em equipamentos ou softwares que não pertençam ao MPM ou que não tenham como finalidade direta a realização de atividades funcionais relacionadas aos serviços de interesse do MPM.

CAPÍTULO III DAS DISPOSIÇÕES GERAIS

Art. 10 As solicitações de suporte técnico devem ser registradas por meio de sistema informatizado disponibilizado pelo DTI, na Intranet do MPM.

Parágrafo único. Em caso de impossibilidade de registro de solicitação de suporte técnico nos termos do caput deste artigo, o usuário poderá fazer a solicitação preferencialmente pelo e-mail dti.chamados@mpm.mp.br, e em último caso, por telefone ou pessoalmente, ficando o DTI responsável pelo registro da solicitação.

Art. 11 O acesso à sala de servidores ou a instalações que contenham equipamentos de uso exclusivo do DTI somente poderá ser feito mediante autorização ou supervisão de servidor do DTI, salvo no caso de emergências.

Art. 12 Os dispositivos particulares - computadores, laptops, tablets e celulares - só poderão ter acesso à rede de dados do MPM mediante solicitação, por meio de sistema automatizado ou por escrito ao DTI, que poderá concedê-la, excepcionalmente, desde que tenham como finalidade direta a realização de atividades funcionais relacionadas aos serviços de interesse do MPM e o dispositivo atenda aos requisitos básicos de segurança a serem definidos pelo DTI.

Art. 13 O acesso à Internet via rede Wireless no âmbito da Procuradoria-Geral da Justiça Militar, caso disponível, será regido conforme disposições contidas em Regulamento próprio.

Art. 14 Constituem parte integrante desta Política, os regulamentos abordados na forma estabelecida pelos seguintes anexos:

- Anexo I - Utilização dos meios de armazenamento e transmissão de dados;
- Anexo II - Utilização dos meios de impressão;
- Anexo III - Utilização das estações de trabalho;
- Anexo IV - Utilização de computação móvel.

Art. 15 As mensagens direcionadas a todos os membros e/ou servidores do MPM, deverão ser encaminhadas pela Assessoria de Comunicação Institucional (ASCOM).

Art. 16 Casos não previstos nesta Política serão analisados e decididos pela Direção-Geral do MPM, em conjunto com o DTI.



Documento assinado eletronicamente por **JORGE AUGUSTO CAETANO DE FARIAS, Chefe do Gabinete do Procurador-Geral de Justiça Militar**, em 12/12/2022, às 10:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANGELA MONTENEGRO TAVEIRA, Secretária-Geral de Pesquisa e Apoio à Investigação**, em 14/12/2022, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **AILTON JOSE DA SILVA, Procurador de Justiça Militar**, em 15/12/2022, às 10:54, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SOLANGE AGUIAR COELHO, Diretora do Departamento de Tecnologia da Informação**, em 15/12/2022, às 17:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDER JORGE PIRES, Diretor-Geral**, em 19/12/2022, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1212342** e o código CRC **77E393BF**.

19.03.0000.0008013/2022-65

CETI1212342v5



MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

ANEXO I

UTILIZAÇÃO DOS MEIOS DE ARMAZENAMENTO E TRANSMISSÃO DE DADOS

1. OBJETIVO

- 1.1.** Este documento é parte da Política de Utilização de Recursos de TI do Ministério Público Militar e tem como finalidade definir as regras a serem seguidas no órgão relativas à utilização dos meios de armazenamento e transmissão de dados.

2. DISPOSIÇÕES GERAIS

- 2.1.** Todas as informações corporativas deverão ser armazenadas nos servidores de dados do MPM e/ou em nuvem contratada pelo Órgão, sendo que as de natureza pública poderão ser também armazenadas em mídias e serviços tecnológicos como correio eletrônico, videoconferência e redes sociais corporativas;
- 2.2.** As informações a serem armazenadas em ambiente de computação em nuvem devem passar por um processo de Gestão de Riscos de Segurança da Informação;
- 2.3.** É vedada a transmissão, processamento ou guarda de informações corporativas do MPM em contas pessoais de serviços de computação ou armazenamento em nuvem;
- 2.4.** O Departamento de Tecnologia da Informação - DTI proverá os mecanismos necessários para a proteção das informações armazenadas somente nos servidores de rede corporativos do MPM visando garantir a integridade, disponibilidade e a confidencialidade das informações e conceder os privilégios de acesso adequados aos perfis de usuários;
- 2.5.** O DTI deverá efetuar backup periódico dos sistemas e das informações armazenadas nos servidores corporativos do MPM, com ciclos de backup e tempos de retenção em conformidade com a Política de Backup do órgão;
- 2.6.** A salvaguarda das informações armazenadas nas estações de trabalho ficará a cargo do usuário do recurso, que deverá responsabilizar-se por esses dados e pela realização de backup antes das manutenções do equipamento;
- 2.7.** É vedado o compartilhamento permanente de pastas nas estações de trabalho dos usuários. Caso haja a necessidade de nova área de trabalho para armazenamento de dados corporativos, esta deverá ser requerida ao DTI pelo titular da unidade;
- 2.8.** O DTI deverá prover mecanismos para o descarte seguro de informação armazenada em meio digital, de forma a assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança, antes do descarte ou reutilização.

3. DISPOSIÇÕES FINAIS

- 3.1.** Em caso de necessidade de recuperação de informações, o usuário deverá registrar as solicitações por meio de sistema informatizado disponibilizado pelo DTI, na Intranet do MPM. O DTI tomará as providências para a sua recuperação, quando possível, e orientará o demandante quanto ao acesso aos arquivos.
- 3.2.** Não será admitido o uso de áreas de armazenamento ou estações de trabalho para a manutenção de arquivos de fotos, músicas e filmes protegidos por direitos autorais ou conteúdo ofensivo, exceto por autorização do autor ou quando for de propriedade do agente público ou por necessidade do serviço (mantida as condicionantes de autoria comentada anteriormente).
- 3.3.** Os atos praticados em desconformidade com esta norma serão de responsabilidade dos envolvidos, que ficarão sujeitos às sanções administrativas e penais cabíveis, tanto o autor do ato como aquele que acessar as informações indevidamente.



Documento assinado eletronicamente por **JORGE AUGUSTO CAETANO DE FARIAS**, **Chefe do Gabinete do Procurador-Geral de Justiça Militar**, em 12/12/2022, às 10:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANGELA MONTENEGRO TAVEIRA**, **Secretária-Geral de Pesquisa e Apoio à Investigação**, em 14/12/2022, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **AILTON JOSE DA SILVA**, **Procurador de Justiça Militar**, em 15/12/2022, às 10:55, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SOLANGE AGUIAR COELHO**, Diretora do Departamento de Tecnologia da Informação, em 15/12/2022, às 17:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDER JORGE PIRES**, Diretor-Geral, em 19/12/2022, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1212344** e o código CRC **7E2133FB**.

19.03.0000.0008013/2022-65

CETI1212344v3



MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

ANEXO II

UTILIZAÇÃO DOS MEIOS DE IMPRESSÃO

1. OBJETIVO

- 1.1. Este documento é parte da Política de Utilização de Recursos de TI do Ministério Público Militar e tem como finalidade definir as regras a serem seguidas no órgão relativas à impressão de documentos e à manutenção dos meios de impressão.

2. DISPOSIÇÕES GERAIS

- 2.1. Os dispositivos de impressão disponibilizados pelo MPM são para uso exclusivo em serviço;
- 2.2. DTI implementará “ilhas de impressão” nas unidades do MPM, com o intuito de primar pela otimização dos dispositivos de impressão, priorizando ao máximo o compartilhamento destes pelas estações de trabalho da unidade, visando atender ao Plano de Logística Sustentável do MPM;
- 2.3. Sempre que possível, o compartilhamento de documentos (impressos ou digitais) deve ser priorizado, o que evitará o uso desnecessário de insumos ou de cota de impressão;
- 2.4. As impressoras disponibilizadas aos usuários para a impressão frente e verso terão esta opção habilitada como modalidade de impressão padrão;
- 2.5. As impressoras disponibilizadas aos usuários para a impressão colorida terão a opção monocromática habilitada como modalidade de impressão padrão;
- 2.6. A opção de impressão em um só lado da folha deve ser utilizada apenas na hipótese de extrema necessidade, de forma a evitar o uso desnecessário de recursos;
- 2.7. As impressões em cores devem ser utilizadas apenas em hipótese de extrema necessidade, de forma a evitar o uso desnecessário de recursos;
- 2.8. Em caso de problemas nos equipamentos de impressão, o usuário deverá registrar as solicitações por meio de sistema informatizado disponibilizado pelo DTI, na Intranet do MPM.

3. DISPOSIÇÕES FINAIS

- 3.1. A solicitação de instalação de novo dispositivo de impressão deverá ser formalmente requerida pelo titular da unidade, justificando a necessidade, inclusive informando a não possibilidade de utilizar outro equipamento de impressão que possa ser compartilhado na unidade;
- 3.2. Após a instalação do dispositivo solicitado, caso aprovado, o DTI deverá repassar ao solicitante as instruções para a utilização do recurso, bem como os procedimentos necessários ao seu bom funcionamento, inclusive nas situações comuns do dia a dia;
- 3.3. Em nenhuma hipótese o usuário deverá mover o equipamento de local;
- 3.4. Os atos praticados em desconformidade com esta norma serão de responsabilidade dos envolvidos, que ficarão sujeitos às sanções administrativas e penais cabíveis.



Documento assinado eletronicamente por **JORGE AUGUSTO CAETANO DE FARIAS, Chefe do Gabinete do Procurador-Geral de Justiça Militar**, em 12/12/2022, às 10:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANGELA MONTENEGRO TAVEIRA, Secretária-Geral de Pesquisa e Apoio à Investigação**, em 14/12/2022, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **AILTON JOSE DA SILVA, Procurador de Justiça Militar**, em 15/12/2022, às 10:56, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SOLANGE AGUIAR COELHO, Diretora do Departamento de Tecnologia da Informação**, em 15/12/2022, às 17:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDER JORGE PIRES, Diretor-Geral**, em 19/12/2022, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1212345** e o código CRC **9DBC9CEF**.

19.03.0000.0008013/2022-65

CETI1212345v3



MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

ANEXO III

UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

1. OBJETIVO

- 1.1.** Este documento é parte da Política de Utilização de Recursos de TI do Ministério Público Militar e tem como finalidade definir as regras a serem seguidas no órgão relativas à utilização e à manutenção das estações de trabalho.

2. DISPOSIÇÕES GERAIS

- 2.1.** As estações de trabalho fornecidas possuirão configurações de hardware e software padronizadas pelo DTI, de acordo com a necessidade de utilização dos usuários;
- 2.2.** Nas estações de trabalho, somente deverão ser instalados softwares homologados e licenciados pelo DTI e necessários à execução das atividades relacionadas às atividades funcionais;
- 2.3.** É vedado conceder aos usuários privilégios de administrador local nas estações de trabalho, salvo em casos excepcionais, mediante justificativa da unidade requisitante, parecer técnico e autorização do DTI. Caso seja identificada alguma contraposição à solicitação, esta será remetida à Direção-Geral para deliberação;
- 2.4.** Os titulares das unidades poderão solicitar a instalação, nas estações de trabalho, de softwares complementares que julguem necessários à execução das atividades da unidade, cabendo ao DTI analisar a possibilidade de atendimento considerando os riscos para a segurança do ambiente de TI, bem como a necessidade de licenciamento dos softwares;
- 2.5.** As atualizações e correções de segurança de sistemas operacionais e demais softwares deverão ser aplicadas quando disponibilizadas pelo fabricante, podendo sofrer validação prévia em ambiente de homologação;
- 2.6.** As estações de trabalho possuirão software para proteção contra malwares instalado, permanentemente atualizado e com proteção em tempo real habilitada;
- 2.7.** Semanalmente as estações de trabalho serão completamente escaneadas com o objetivo de identificar e eliminar vírus, worms, cavalos de tróia, spywares, dentre outros, que não podem ser identificados pela proteção em tempo real;
- 2.8.** Diariamente as estações de trabalho poderão ser inventariadas por agente de software específico com o objetivo de mapear e gerir os ativos de TI;
- 2.9.** Os usuários deverão bloquear a estação de trabalho sempre que se afastarem dela, sendo necessária a digitação da senha de acesso para a liberação da área de trabalho;
- 2.10.** As estações de trabalho terão bloqueio de tela automático, ativado por tempo de inatividade habilitado. O tempo de inatividade será determinado pelo DTI;
- 2.11.** Quando possível, os recursos de hibernação e de suspensão serão habilitados nas estações de trabalho, de forma a economizar energia elétrica. Caso não seja possível habilitar tais recursos na estação, ela deverá ser desligada ao final do expediente, salvo recomendação expressa do DTI a esse respeito;
- 2.12.** Não será permitida a utilização de outros meios de conexão à internet ou de outro tipo de rede a partir de estações de trabalho do MPM, seja por meio de modems 3G ou 4G ou de qualquer outro tipo existente ou que venha a ser criado, salvo mediante expressa autorização do DTI;
- 2.13.** As estações de trabalho, a fim de evitar modificações não autorizadas, serão fornecidas sempre lacradas;
- 2.14.** É vedada a abertura das estações de trabalho em garantia;
- 2.15.** É vedada a abertura das estações de trabalho por pessoal não autorizado pelo DTI;
- 2.16.** O usuário deverá informar ao DTI quando identificar violação da integridade física do equipamento por ele utilizado;
- 2.17.** O Suporte Técnico do DTI, quando identificar violação da integridade física do equipamento recolhido ou devolvido pelo usuário, dará imediatamente ciência do fato à diretoria do DTI, que deverá comunicar à Direção-Geral.

3. DISPOSIÇÕES FINAIS

- 3.1.** A solicitação de instalação ou substituição de estação de trabalho deverá ser feita por meio de sistema informatizado disponibilizado pelo DTI, na Intranet do MPM;
- 3.2.** Equipamentos que forem identificados como potencialmente nocivos à rede de dados do MPM, seja por contaminação por vírus ou por outro tipo de anomalia, poderão ser postos em quarentena sem aviso prévio ao usuário, somente saindo dessa condição

após a devida análise da situação pelo DTI;

- 3.3. Os atos praticados em desconformidade com esta norma serão de responsabilidade dos envolvidos, que ficarão sujeitos às sanções administrativas e penais cabíveis.



Documento assinado eletronicamente por **JORGE AUGUSTO CAETANO DE FARIAS, Chefe do Gabinete do Procurador-Geral de Justiça Militar**, em 12/12/2022, às 10:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANGELA MONTENEGRO TAVEIRA, Secretária-Geral de Pesquisa e Apoio à Investigação**, em 14/12/2022, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **AILTON JOSE DA SILVA, Procurador de Justiça Militar**, em 15/12/2022, às 10:58, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SOLANGE AGUIAR COELHO, Diretora do Departamento de Tecnologia da Informação**, em 15/12/2022, às 17:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDER JORGE PIRES, Diretor-Geral**, em 19/12/2022, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1212348** e o código CRC **CE030725**.

19.03.0000.0008013/2022-65

CETI1212348v3



MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

ANEXO IV

UTILIZAÇÃO DE COMPUTAÇÃO MÓVEL

1. OBJETIVO

- 1.1. Este documento é parte da Política de Utilização de Recursos de TI do Ministério Público Militar e tem como finalidade definir as regras a serem seguidas no órgão relativas à utilização de computação móvel.

2. DISPOSIÇÕES GERAIS

- 2.1. Dispositivos móveis como notebooks, HD Externo e pendrives, quando conectados à rede do MPM deverão ser utilizados em conformidade com esta política;
- 2.2. Aplicam-se, quando pertinentes, aos dispositivos móveis, as regras de utilização das estações de trabalho;
- 2.3. É vedada a utilização de equipamentos pessoais na rede corporativa do órgão, salvo os casos autorizados pelo DTI;
- 2.4. O DTI deverá prover mecanismos que efetuem o bloqueio da utilização de dispositivos móveis sem autorização na rede corporativa do órgão, a fim de evitar a fuga de informações corporativas;
- 2.5. Os equipamentos portáteis do MPM, quando não estiverem sendo utilizados, deverão ser guardados em local seguro;
- 2.6. Equipamentos portáteis que forem identificados como potencialmente nocivos à rede de dados do MPM, seja por contaminação por vírus ou por outro tipo de anomalia, poderão ser postos em quarentena sem aviso prévio ao usuário, somente saindo dessa condição após a devida análise da situação pelo DTI;
- 2.7. Na devolução do equipamento portátil, o usuário deverá retirar todos os arquivos gravados e manipulados durante a utilização, além de todos os objetos pessoais, como CDs.

3. DISPOSIÇÕES FINAIS

- 3.1. A configuração de dispositivos móveis do MPM deverá seguir as indicações disponibilizadas pelo DTI, em havendo necessidade poderá ser solicitado auxílio à equipe de suporte técnico;
- 3.2. Os atos praticados em desconformidade com esta norma serão de responsabilidade dos envolvidos, que ficarão sujeitos às sanções administrativas e penais cabíveis.



Documento assinado eletronicamente por **JORGE AUGUSTO CAETANO DE FARIAS, Chefe do Gabinete do Procurador-Geral de Justiça Militar**, em 12/12/2022, às 10:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANGELA MONTENEGRO TAVEIRA, Secretária-Geral de Pesquisa e Apoio à Investigação**, em 14/12/2022, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **AILTON JOSE DA SILVA, Procurador de Justiça Militar**, em 15/12/2022, às 10:59, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SOLANGE AGUIAR COELHO, Diretora do Departamento de Tecnologia da Informação**, em 15/12/2022, às 17:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDER JORGE PIRES, Diretor-Geral**, em 19/12/2022, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.mpm.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1212351** e o código CRC **D7DB1D0E**.

