meter todos que queiram ter acesso às áreas e instalações da Instituição, ainda que exerçam qualquer cargo ou função pública, ressalvados os integrantes de missão policial, a escolta de presos e os agentes ou inspetores de segurança próprios, nos termos do artigo 3º, inciso III, da Lei nº 12.694, de 24 de julho de 2012, além dos casos em que recomendações médicas o contraindiquem;
XI - instalação de câmeras de vigilância e sistemas CFTV;
XII - prevenção e conduta em emergência; e
XIII - outras técnicas e procedimentos de segurança.
§ 2º Os projetos de construção e reforma de áreas e instalações do Ministério Público devem ser planejados e executados pelo Departamento de Obras e Manutenção (DOM) com a observância de todos os demais aspectos de segurança e com a integração dos demais setores, de modo a reduzir as vulnerabilidades e otimizar os meios de proteção.
§ 3º As áreas e instalações que abriguem dados e informações sensíveis ou sigilosos e as consideradas vitais para o pleno funcionamento da Instituição serão objeto de especial proteção.
§ 4º O Procurador-Geral de Justiça expedirá ato para restringir o ingresso e a permanência de pessoas armadas em áreas e instalações do Ministério Público, observando nesses casos que as armas de fogo que tais pessoas estiverem legalmente portando deverão ser acauteladas e depositadas em cofre ou móvel adequado da Instituição que propicie a segurança necessária com registro de acautelamento da arma e entrega de recibo.

Seção IV

Da Segurança da Informação e da tecnologia da informação

Art. 12. A segurança da informação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosos, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza ao Ministério Público ou proporcionar vantagem a atores antagônicos.
§ 1º A segurança da informação visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, informação ou conhecimento.
§ 2º A segurança da informação, pela sua relevância e complexidade, desdobra-se nos seguintes subgrupos:
I - segurança da informação nos meios de tecnologia da informação;
II - segurança da informação nos recursos humanos;
III - segurança da informação na documentação; e
IV - segurança da informação nas áreas e instalações.
§ 3º Todo dado ou informação deve ser classificado de acordo com o grau de sigilo exigido por seu conteúdo, de forma a assegurar que receba nível adequado de proteção, nos termos da legislação pertinente.
§ 4º O MPPA deverá proporcionar ao Grupo de Atuação Especial de Inteligência e Segurança Institucional (GSI) o acesso aos bancos de dados e sistemas institucionais, ou de acesso à Instituição, para subsidiar as respectivas atividades de segurança institucional, inteligência e contrainteligência, observados os procedimentos de segurança e controle.
Art. 13. A segurança da informação nos recursos humanos compreende um conjunto de medidas voltadas a assegurar comportamentos adequados dos integrantes da Instituição que garantam a salvaguarda de dados e informações sensíveis ou sigilosos.
§ 1º A segurança da informação nos recursos humanos engloba medidas de segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição.
§ 2º As medidas de segurança a que se reporta o presente artigo, entre outras finalidades, devem detectar, prevenir, obstruir e neutralizar infiltrações, recrutamentos e outras ações adversas de obtenção indevida de dados e informações nos recursos humanos, sobretudo em razão de falhas no processo seletivo e no acompanhamento funcional dos integrantes da Instituição.
§ 3º Todos os integrantes da Instituição que, de algum modo, possam ter acesso a dados e informações sensíveis ou sigilosos deverão subscrever Termo de Compromisso de Manutenção de Sigilo (TCMS) a ser regulamentado por ato do Procurador-Geral de Justiça.
§ 4º Toda Instituição com a qual o Ministério Público compartilhe dados ou informações sensíveis ou sigilosos deverá possuir doutrina de confidencialidade e de não divulgação ou firmar acordos para preservar o seu conteúdo, sem prejuízo da subscrição de termos específicos para cada um dos respectivos integrantes que possam ter acesso àqueles.
Art. 14. A segurança da informação na documentação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosos contidos na documentação que é arquivada ou tramita na Instituição.
§ 1º As medidas a que se reporta o "caput" deverão ser adotadas em cada fase de produção, classificação, tramitação, difusão, arquivamento e destruição da documentação.
§ 2º Os documentos deverão ser classificados de acordo com o grau de sigilo exigido por seu conteúdo, de forma a assegurar que recebam nível adequado de proteção, nos termos da legislação pertinente.
§ 3º A Instituição deverá adotar as providências necessárias que garantam uma gestão documental adequada para documentos ostensivos e sigilosos, inclusive com o estabelecimento dos respectivos protocolos de segurança.
Art. 15. A segurança da informação nas áreas e instalações compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosos armazenados ou em trâmite no espaço físico sob a responsabilidade da Instituição ou no espaço físico onde estejam sendo realizadas atividades de interesse da Instituição.
Parágrafo único. As medidas a que se reporta o "caput" também englobam os procedimentos necessários para preservar as informações sobre áreas e instalações da Instituição ou sobre o espaço físico onde estejam sendo realizadas atividades de interesse da Instituição, tais como fluxo de pessoas nas dependências, distribuição interna de móveis, "layouts" das instalações, localização de áreas sensíveis, proteção contra observação externa, iluminação e paisagismo, entre outras.
Art. 16. A segurança da informação nos meios de tecnologia da informação compreende um conjunto de medidas voltado a salvaguardar dados e informações sensíveis ou sigilosos gerados, armazenados e processados por intermédio da informática, bem como a própria integridade dos sistemas utilizados pela Instituição, englobando as áreas de Informática e de Comunicações.
§ 1º Estas medidas deverão privilegiar a utilização de tecnologias modernas e o uso de sistemas criptográficos na transmissão de dados e informações sensíveis ou sigilosos, inclusive nos meios de comunicação por telefonia.
§ 2º A utilização de certificação digital, no trato de assuntos que necessitem de sigilo e validade jurídica, e o armazenamento de dados ("backup"), que promova a segurança e disponibilidade da informação, serão priorizados pela Instituição.
§ 3º Os sistemas informatizados utilizados pela Instituição deverão conter funcionalidades que permitam os "logs" de acesso e registro de ocorrências, com armazenamento em prazo razoável para fins de auditoria.
§ 4º Ser efetivada por cruzamento de verificação e com segregação de funções preferencialmente por estrutura não subordinada à área de Tecnologia da Informação e Comunicações.

Seção V

Das Medidas de Segurança Ativa

Art. 17. A contrassabotagem compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações intencionais contra material, áreas ou instalações da Instituição que possam causar interrupção de suas atividades e/ou impacto físico direto e psicológico indireto sobre seus integrantes.
Art. 18. A contraespionagem compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações adversas e dissimuladas de busca de dados e informações sensíveis ou sigilosos.
Art. 19. O contra crime organizado compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações adversas de qualquer natureza contra a Instituição e seus integrantes oriundas de organizações criminosas.
Art. 20. A contrapropaganda compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar abusos, desinformações e publicidade enganosa de qualquer natureza contra a Instituição.
Parágrafo único. A adoção de medidas de contrapropaganda, de responsabilidade de todos os integrantes do MPPA, será pautada pelos princípios e diretrizes da Política Nacional de Comunicação Social do Ministério Público, nos termos das normas de âmbito nacional, editadas pelo Conselho Nacional do Ministério Público (CNMP).

CAPÍTULO VI

DOS ÓRGÃOS E DA GESTÃO DA SEGURANÇA INSTITUCIONAL

Art. 21. O Sistema de Segurança Institucional do MPPA é composto:
I - pela Procuradoria-Geral de Justiça;
II - pela Comissão de Segurança Institucional (CSI);
III - pelo Grupo de Atuação Especial de Inteligência e Segurança Institucional (GSI);
IV - pelo Gabinete Militar;
V - pelo Departamento de Informática (DEINF); e
VI - pelo Departamento de Recursos Humanos (DRH).
Parágrafo único. Além dos Departamentos acima elencados, cabe a chefia de cada unidade:
I - conhecer, divulgar, cumprir, fiscalizar e estimular o cumprimento desta Política de Segurança Institucional, Normas Complementares e Procedimentos correlatos pelos colaboradores que supervisiona;
II - executar as solicitações operacionais previstas nesta Política de Segurança Institucional, normas complementares e procedimentos correlatos, além de prestarem todo o suporte necessário ao esclarecimento de dúvidas dos colaboradores sob sua supervisão;
III - atribuir o perfil adequado para acesso a recursos, dados e informações conforme a necessidade com base nos princípios do conjunto mínimo de permissões que precisam ser atribuídos;
IV - informar no menor tempo possível ao DRH as mudanças de lotação, afastamentos, retornos, desligamentos ou outras movimentações funcionais ocorridos em suas equipes;
V - identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos à Instituição;
VI - garantir que os ativos de propriedade ou sob a responsabilidade do MPPA sejam utilizados com cuidado e de acordo com as orientações do fabricante e da Instituição; e
VII - identificar incidentes de segurança de informação ou qualquer ação duvidosa praticada pelos colaboradores sob sua responsabilidade e comunicar ao GSI.
Art. 22. Cabe ao Procurador-Geral de Justiça:
I - cumprir e fazer cumprir esta Política de Segurança Institucional e Normas Complementares por todos os colaboradores do MPPA;
II - decidir sobre os Procedimentos Operacionais Padronizados planejados pelo GSI visando a uniformização de atuação;
III - desenvolver e difundir mentalidade de segurança institucional, fazendo com que todos os integrantes da Instituição compreendam as necessidades das medidas adotadas e incorporem o conceito de que cada um é responsável pela manutenção do nível de segurança adequado;
IV - desenvolver atitudes favoráveis ao cumprimento de normas de segurança no âmbito da Instituição, estimulando o comprometimento e o apoio explícito de todos os níveis de direção e chefia; e
V - prover recursos financeiros suficientes para as atividades de segurança.
Art. 23. Cabe à CSI apreciar os pedidos de proteção pessoal nos termos de regulamento específico com apoio técnico do GSI e operacional-logístico do Gabinete Militar.