ATO PGJ Nº 860/2018

Aprova o Plano de Segurança Institucional do Ministério Público do Estado do Piauí.

O **PROCURADOR-GERAL DE JUSTIÇA**, no exercício de suas atribuições legais, especialmente as definidas no art. 12, V da Lei Complementar Estadual nº 12/93 e no art. 10, V da Lei Federal nº 8.625/1993;

CONSIDERANDO a relevância da segurança institucional para o exercício livre e independente das funções constitucionais do Ministério Público;

CONSIDERANDO a aprovação da política de segurança institucional por meio do Ato PGJ nº 821/2018;

RESOLVE:

Art. 1º Aprovar o Plano de Segurança Institucional do Ministério Público do Estado do Piauí.

Art. 2º Este Ato entra em vigor na data de sua publicação.

Teresina, 06 de dezembro de 2018.

CLEANDRO ALVES DE MOURA
Procurador-Geral de Justiça

PLANO DE SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO DO ESTADO DO PIAUÍ

TERESINA-PI
2018

ÍNDICE GERAL

CAPÍTULO I

Disposições Gerais

Art. 1º A Segurança Institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação.

§ 1º As medidas a que se reporta o *caput* compreendem a segurança orgânica e a segurança ativa.

§ 2º A segurança orgânica é composta pelos seguintes grupos de medidas:

I – segurança de pessoas;

II –segurança do material;

III – segurança das áreas e instalações; e

IV – segurança da informação.

§ 3º A segurança ativa compreende ações de caráter proativo e imediato relativas a:

I –contrassabotagem;

II – contraespionagem;

III - contra crime organizado;

IV - contrapropaganda.

CAPÍTULO II

Estrutura Organizacional e Atribuições

Art. 2º As funções de gestão de segurança institucional no MPPI serão desempenhadas pelos seguintes órgãos:

I - Procuradoria-Geral de Justiça;

II - Gabinete de Segurança Institucional;

III - Assessoria Militar;

IV - Comitê Gestor de Segurança Institucional;

V - Comitê Gestor de Segurança Aproximada; e

VI - Coordenadores no âmbito das respectivas unidades administrativas.

Paragrafo único. A coordenação técnica e operacional da atividade de segurança institucional será de responsabilidade do Gabinete de Segurança Institucional.

Seção I

Das atribuições do Gabinete de Segurança Institucional (GSI)

Art. 3º Ao Gabinete de Segurança Institucional compete:

I – planejar, coordenar e acompanhar as atividades relacionadas à segurança institucional no âmbito do Ministério Público do Estado do Piauí;

II – promover a articulação com as demais áreas do Ministério Público para garantir um tratamento integrado, multidisciplinar e sistêmico da segurança institucional, estimulando a cooperação entre elas;

III - sugerir a implementação de medidas que visem ao aprimoramento da segurança institucional, dentre elas, a realização de convênios com outras instituições;

IV - propor mecanismos de fiscalização do cumprimento das normas de segurança institucional;

V – fiscalizar a observância das normas de segurança institucional e a realização dos programas e projetos a ela relacionados;

VI – desenvolver projetos para a construção e difusão da cultura de segurança institucional;

VII - propor a edição de normas, instruções, planos, procedimentos e mecanismos

de proteção no âmbito da segurança institucional;

VIII - propor a revisão e o aprimoramento da política de segurança institucional;

IX – implementar medidas visando a garantir a observância, por cada área do Ministério Público, das normas de segurança institucional;

X - apreciar os relatórios emitidos mensalmente pelo chefe da Assessoria Militar do MPPI, adotando as providências que se mostrarem cabíveis.

Seção II

Das atribuições da Assessoria Militar

Art. 4º Compete à Assessoria Militar do MPPI:

I – executar as atividades de segurança ostensiva e velada do Procurador-Geral de Justiça;

II - colaborar no planejamento e elaboração dos programas e planos de viagens e visitas do Procurador-Geral de Justiça, procedendo-se ao levantamento de dados e informações e supervisionando a operação sob o aspecto de sua segurança;

III – auxiliar o Gabinete de Segurança Institucional nos procedimentos de segurança institucional;

IV – cumprir as medidas de segurança aproximada quando devidamente autorizadas;

V - participar do Comitê Gestor de Segurança Institucional;

VI - auxiliar na promoção de cursos, palestras e treinamentos na área de segurança, visando à capacitação técnica dos policiais militares, membros, servidores e colaboradores do Ministério Público;

VII - operar os sistemas internos de videomonitoramento da Procuradoria-Geral de Justiça;

VIII - fiscalizar o pleno funcionamento do sistema de proteção contra incêndios, elevadores, escadarias e saídas de emergência dos edifícios da Procuradoria-Geral de Justiça;

IX - controlar, mantendo sob sua guarda, o claviculário geral dos edifícios da Procuradoria Geral de Justiça.

X - supervisionar os meios de transporte que servem diretamente ao Procurador-Geral de Justiça, acompanhando inclusive o cronograma de manutenção preventiva e recuperativa dos veículos;

XI - supervisionar os processos seletivos e de treinamento dos motoristas da Procuradoria-Geral de Justiça, especialmente aos que servem ao Gabinete do Procurador-Geral de Justiça, promovendo, periodicamente, treinamentos e cursos de direção defensiva e ofensiva;

XII – apoiar as operações e demandas dos Grupos Especiais de Atuação Funcional, observando as disposições legais e atos normativos internos;

XIII – exercer outras atividades correlatas à área de atuação.

Seção III

Das atribuições do Comitê Gestor de Segurança Institucional

Art. 5º Compete ao Comitê Gestor de Segurança Institucional:

I – propor atos normativos, recomendações, diretrizes, protocolos, rotinas, ações e medidas de seguranças institucionais de interesse do Ministério Público do Estado do Piauí;

II – promover a articulação de diversos setores e/ou órgãos da instituição para a concretização das ações relativas à área, tudo dentro de uma concepção sistêmica de proteção e salvaguarda da instituição.

III - desenvolver outras atribuições previstas em normas específicas.

Seção IV

Das atribuições do Comitê Gestor de Segurança Aproximada

Art. 6º Compete ao Comitê Gestor de Segurança Aproximada:

I – decidir sobre a concessão ou a suspensão de segurança aproximada em situação especial, submetendo essa decisão ao Procurador-Geral de Justiça;

II – deliberar sobre situações que impliquem risco ou ameaça à integridade física de membros e seus familiares, diante da situação de risco decorrente do exercício da função;

III – representar pelas providências do artigo 5º da Resolução nº 116/14 do Conselho Nacional do Ministério Público;

IV – elaborar plano de proteção e assistência aos Membros em situação de risco;

V– monitorar a edição de normas sobre proteção pessoal no âmbito do Conselho Nacional do Ministério Público, diligenciando junto ao Procurador-Geral de Justiça para a adequação das medidas de segurança de pessoas, estrutura e capacidade para gerir situações de risco a Membros;

VI – aprovar planejamento operacional para segurança aproximada de Membros;

VII- elaborar e aprovar regimento interno próprio;

VIII - exercer outras atividades correlatas que lhe forem delegadas.

Seção V

Das atribuições dos órgãos e unidades administrativas do Ministério Público

Art. 7º Compete aos respectivos órgãos e unidades administrativas do Ministério

Público, sob a supervisão do Gabinete de Segurança Institucional, a aplicação das normas de segurança institucional, assim como pela propositura e implementação de outras medidas de segurança em sua esfera de atribuição.

CAPÍTULO III

DAS MEDIDAS DE SEGURANÇA INSTITUCIONAL

Seção I

Segurança de pessoas e segurança da informação de pessoas

Art. 8º A segurança de pessoas compreende um conjunto de medidas destinadas a proteger a integridade física e moral de membros, ativos e inativos, de servidores, assim como de seus respectivos familiares, quando comprometida em face do desempenho das funções institucionais.

Art. 9º A segurança da informação de pessoas compreende um conjunto de medidas voltadas a estabelecer comportamentos adequados dos integrantes do MPPI que proporcionem a proteção da informação, englobando medidas de segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição.

Subseção I

Segurança da integridade física

Art. 10. No tocante à segurança da integridade física serão observados:

I – as orientações expedidas pelo Gabinete de Segurança Institucional a respeito da

conduta a ser observada pela pessoa que estiver submetida ao sistema de proteção;

II - os atos normativos específicos para otimizar as ações de proteção pessoal e padronizar procedimentos;

III – o controle de acesso a que estarão submetidos os membros, servidores, terceirizados, estagiários e demais usuários, atendidas as particularidades de cada caso e às normas operacionais de segurança física;

IV - os projetos de engenharia, de construção e reforma, bem como definição quanto ao local de imóveis e terrenos para novas aquisições ou locação, devem ser analisados em conjunto com o GSI, para fins de análise de risco e orientações de segurança, as quais devem ser observadas nos respectivos projetos.

Subseção II

Segurança no Processo Seletivo

Art. 11. A Comissão de Concurso para ingresso de membros e servidores e a Coordenadoria de Gestão de Pessoas devem observar as seguintes orientações quanto à Segurança no Processo Seletivo:

I – adotar medidas e procedimentos em seus respectivos editais que contemplem ações para evitar o ingresso de pessoas com maus antecedentes ou outro aspecto que possam comprometer a segurança da Instituição;

II – realizar, com auxilio do GSI, a sindicância de vida pregressa e investigação social, observando que em caso de dados contraditórios ou existência de registros em órgãos públicos que indiquem potencial vulnerabilidade ou contraindicação do candidato serão realizadas diligências para elucidar os fatos.

Subseção III

Segurança no desempenho das funções

Art. 12. Para a segurança no desempenho das funções, as unidades do MPPI devem seguir as seguintes orientações:

I – os novos integrantes do MPPI devem ser submetidos a um curso de ingresso, com conteúdo relativo às funções a serem exercidas e à segurança institucional;

II – independentemente do exercício de função que trate diretamente com assuntos sigilosos, todos os membros, servidores, estagiários e terceirizados do MPPI assinarão Termo de Compromisso de Manutenção do Sigilo – TCMS e nos casos de exercício de função que trate diretamente com assuntos sigilosos, também será exigida a credencial de segurança.

III – Os integrantes do MPPI que desempenham função com acesso a dados e informações sigilosas devem ser submetidos a avaliação periódica para renovação da credencial de segurança, sendo que a vulnerabilidade pessoal que possa comprometer o desempenho da função na Instituição deve ser observada e considerada para renovação da credencial.

IV – Os integrantes do MPPI que possuam credencial de segurança serão submetidos periodicamente a treinamento específico para o trato com assuntos sigilosos;

V – Na designação de servidor para as funções que envolvam o trato com assuntos sigilosos ou sensíveis, devem ser considerados, entre outros, os seguintes aspectos:

a) tarefas sensíveis pertinentes à função;
b) grau de acesso a assuntos sigilosos pelo servidor;
c) capacidade de iniciativa e decisão do servidor;
d) concessão de credencial de segurança e investigação social atualizada.

Subseção IV

Segurança no desligamento

Art. 13. As unidades do MPPI devem seguir as seguintes orientações quanto ao desligamento:

I – o afastamento de função que trata de assuntos sigilosos deve ser realizado gradativa e paulatinamente, de forma a ocorrer uma desmobilização controlada;

II – os Membros e servidores que tenham acesso, por força de sua função, a sistemas ou serviços que tratem de assuntos sigilosos, devem ser excluídos do acesso por ocasião de seu desligamento da função;

§1º Para efeito do item anterior, as chefias imediatas e a Coordenadoria de Recursos Humanos devem informar ao responsável de cada sistema ou serviço sobre o afastamento das funções por membros e servidores, devendo o responsável de cada sistema ou serviço que trate de assuntos sigilosos devem auditar periodicamente os seus respectivos sistemas ou serviços para identificar acessos indevidos;

§2º Em situações de desligamento de membro, servidor, estagiário ou prestadores de serviço da instituição, devem ser adotadas as seguintes medidas de segurança:

I - entrevista com o desligado, orientando-o sobre a necessidade de manter discrição sobre os assuntos institucionais;

II - verificação de entrega de material ou equipamento acautelado com o desligado;

III - verificação da existência de pendências de ordem individual na Coordenadoria de Recursos Humanos; e

IV - verificação da existência de pendências em projetos, serviços ou trabalhos realizados pelo desligado.

Subseção V

Credencial de Segurança

Art. 14. Para definição de diretrizes da credencial de segurança as unidades do MPPI devem seguir as seguintes orientações:

I – A credencial de segurança é um documento que habilita membros, servidores, estagiários e prestadores de serviços do MPPI ao acesso a dados e informações sigilosos. Sua concessão é essencialmente funcional e independe de grau hierárquico. Relaciona-se à necessidade (funcional) de conhecer e pode ser limitada no tempo. O acesso a dados e informações sigilosos no MPPI somente é permitido com a certificação da credencial de segurança, de acordo com o perfil de acesso específico e o respectivo grau de sigilo, e com a presença da necessidade (funcional) de conhecer;

II – A credencial de segurança será objeto de regulamentação em ato normativo específico do MPPI, nos termos previstos no presente Plano;

III – A concessão de credencial de segurança também estará condicionada à realização de investigação social, à avaliação de desempenho pessoal, à avaliação de desempenho profissional, à capacitação para o trato com assuntos sigilosos e à verificação de aptidão para o trato com assuntos sigilosos;

IV – O processo para seleção de pessoal para concessão do credenciamento de segurança será sigiloso e observará as seguintes fases: indicação, pesquisa, avaliação, capacitação, credenciamento e descredenciamento;

V – Para a expedição da credencial de segurança será realizada investigação social com o intuito de identificar vulnerabilidades que possam comprometer a segurança de dados e informações sigilosas de interesse do MPPI;

VI – Os servidores públicos externos à Instituição que necessitarem, em razão do serviço, ter acesso a assuntos sigilosos referentes ao MPPI somente podem acessar dados e informações sigilosas com credencial de segurança expedida por seu órgão

de origem com o grau de sigilo compatível. Em tais casos, a liberação ao acesso a assuntos sigilosos será condicionada ainda à autorização expressa de autoridade competente do MPPI e à assinatura do Termo de Compromisso de Manutenção do Sigilo.

Subseção VI

Termo de compromisso de manutenção de sigilo - TCMS

Art. 15. O Termo de Compromisso de Manutenção do Sigilo – TCMS é um documento no qual uma pessoa se compromete formalmente a guardar segredo a respeito de dados ou informação sigilosos.

I - O TCMS pode ser genérico, para assuntos sigilosos de modo geral, ou específico, quando o grau de sensibilidade do assunto sigiloso exigir a assinatura de um termo que aborde uma determinada situação ou circunstância.

II - Compete ao Gabinete de Segurança Institucional elaborar o(s) modelo(s) de TCMS, que serão disponibilizados a todas as unidades do MPPI.

III - O TCMS deve ser arquivado em local seguro e estar disponível para consulta e auditoria.

IV - As empresas ou órgãos contratados ou conveniados e seus respectivos empregados ou servidores devem assinar o TCMS quando, por necessidade do serviço junto ao MPPI, tiverem acesso a informações sigilosas.

Seção II

Segurança do material

Art. 16. A segurança do material é um conjunto de medidas de segurança voltadas

para proteger o material pertencente e/ou em uso no MPPI, englobando genericamente os equipamentos, componentes, acessórios, mobiliários, veículos, matérias-primas, armas de fogo, munições e demais itens empregados nas atividades da instituição.

Art. 17. Os incidentes de segurança envolvendo material devem ser sempre observados sob a ótica da intencionalidade do fato, devendo ser averiguada a situação e as circunstâncias em que o fato ocorreu, para esclarecimento de possível ocorrência de sabotagem ou má-fé.

Art. 18. Os registros de incidente de segurança devem ser controlados em cada unidade do MPPI para análise e avaliação periódica, com a finalidade de estabelecer medidas preventivas.

§ 1º Além dos procedimentos de controle patrimonial previstos em ato normativo específico da PGJ, devem ser adotadas as seguintes medidas:

I – a produção, o recebimento, a distribuição, o manuseio, o armazenamento e o acondicionamento de materiais devem seguir as normas técnicas próprias;

II – os materiais sensíveis ou de alto valor devem ser armazenados ou acondicionados em condições especiais de proteção, de acordo com a sua necessidade e o acesso às áreas ou locais de armazenamento ou acondicionamento de tais materiais deve ser restrito, com a devida sinalização;

III – os materiais em trânsito, conforme a necessidade e de acordo com suas características, devem receber medidas adicionais de segurança para sua proteção, entre elas: utilização de criptografia para proteção de seu conteúdo, recibo de entrega, entrega pessoal, com material acompanhado de um servidor, escolta de segurança e guarda;

IV – a saída de material das unidades do MPPI deve atender normas administrativas

e constar em registro, mantido pelas áreas de segurança das unidades, em conjunto com os demais setores;

V – os equipamentos e outros materiais portáteis, em viagens, devem ser conduzidos como bagagem de mão;

VI – a doação de material seguirá norma administrativa específica e o material a ser doado contendo dados e informações sigilosos deve ter o seu conteúdo descartado pela área competente antes da sua entrega;

VII – o incidente de segurança envolvendo material deve ser informado ao Gabinete de Segurança Institucional do MPPI;

VIII – o descarte de material que exige medidas especiais para recolhimento ou eliminação, quando inservível, deve ser feito de acordo com as normas do respectivo órgão regulador;

IX – o armazenamento ou o acondicionamento de materiais que exijam condições especiais deve seguir o constante em normas técnicas específicas;

X – os equipamentos e outros materiais do MPPI devem ser instalados de forma a reduzir riscos ambientais em caso de um incidente de segurança;

XI – os equipamentos ou outros materiais que exijam cuidados de manutenção devem ser incluídos em planejamentos de manutenção coordenados pelas respectivas áreas responsável;

XII – os equipamentos e outros materiais que exijam capacitação técnica para sua operação somente podem ser utilizados por pessoa capacitada;

XIII – as atividades de operação e manuseio de equipamentos e outros materiais nas unidades do MPPI devem estar em conformidade com as normas de segurança no trabalho;

XIV – as bibliotecas das unidades do MPPI devem possuir sistemas de controle do acervo;

XV – em caso excepcional de aquisição de material externo ou de recebimento de

bens em doação ou cessão, tais como equipamentos de informática e telefonia, as unidades do MPPI devem efetuar análise técnica com o intuito de verificar a existência de alguma anormalidade; em caso de identificação de conteúdo não utilizado ou autorizado pela instituição, a respectiva área técnica deve proceder à sua exclusão;

XVI – a unidade com atribuição específica deverá elaborar normas de controle e armazenamento de material.

Seção III

Segurança de áreas e instalações e segurança da informação nas áreas e instalações

Art. 19. A Segurança de áreas e instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade do MPPI ou onde se realizem atividades de interesse da instituição.

Art. 20. A segurança da informação nas áreas e instalações compreende um conjunto de medidas voltadas a proteger informações sensíveis armazenadas ou em trâmite no espaço físico sob a responsabilidade da instituição ou no espaço físico onde estejam sendo realizadas atividades de interesse institucional.

§ 1º As salvaguardas previstas em tais grupos de medidas têm destacada importância por prevenir ações adversas de qualquer natureza contra os demais ativos do MPPI ao proporcionar segurança aos locais onde se desenvolvem atividades de interesse institucional.

§ 2º As medidas de segurança de áreas e instalações interagem com os demais grupos de medidas, integrando a segurança como um todo e sua execução exige auditorias e fiscalização dos sistemas e serviços implementados para o cumprimento

das normas de segurança, sendo a validação de processos fundamental para a verificação constante da eficácia de um serviço ou sistema.

§ 3º Os sistemas de segurança devem ser integrados e complementares, aumentando o espectro de proteção.

Art. 21. A Segurança das áreas e instalações engloba:

I – Sistema Físico: composto por policiais militares ou vigilância privada;

II – Sistema Eletrônico: composto por equipamentos eletrônicos de segurança, como sensores, circuito fechado de televisão (CFTV), alarmes, fechaduras eletrônicas, sistemas de registro, catracas, cancelas, sistema de controle de acesso, entre outros mecanismos;

III – Sistema de Barreiras: envolve as diversas barreiras para segurança dos perímetros.

Art. 22. Quanto às barreiras e instalações físicas devem ser observado:

I – A instalação de barreiras para impedir o acesso físico de pessoas não autorizadas às instalações das Unidades do MPPI;

II – Os perímetros das unidades do MPPI devem possuir barreiras dispostas de acordo com avaliação de risco do local, que se estendem do perímetro externo e chegam até as salas e gabinetes, passando pelas portarias, constituindo-se em linhas de proteção;

III – Os perímetros externos devem ser cercados por muros ou cercas de metal, sendo que em áreas de alto risco de invasão, as cercas ou muros podem conter concertinas ou cercas elétricas nas suas extremidades e na existência de cercas eletrificadas, devem ser afixados avisos de advertência ao longo de todo o perímetro, alertando sobre sua existência;

IV – As guaritas de vigilância devem possuir um campo de visada que possibilite

vigiar as áreas externas e internas das unidades do MPPI;

V – Os prédios e instalações devem possuir serviço de portaria com computadores e sistema para cadastro de pessoal e *webcam* para captura de foto;

VI – Os locais de entrada nos perímetros externos e internos devem possuir portões ou portas de acesso com mecanismos que permitam o seu chaveamento;

VII – As áreas externas e os estacionamentos devem ser iluminados para garantir uma vigilância noturna adequada. Quando possível, podem ser instalados sensores de presença para acionamento da iluminação auxiliar para melhorar as condições de luminosidade no local;

VIII – Os muros e cercas dos perímetros devem estar livres de vegetação que impeça a observação por parte da segurança ou que facilite o acesso não autorizado às unidades do MPPI;

IX – O cabeamento da rede elétrica ou do sistema de CFTV deve ser protegido, em particular nas áreas externas. Nas áreas internas, os quadros de energia elétrica devem ser de fácil acesso, livre de obstáculos;

X – O cabeamento da rede lógica deve ser protegido, bem como os quadros e *racks* devem possuir sistemas de fechadura com chave ou sistema de controle de acesso, a fim de impedir o acesso indevido;

XI – O cabeamento de energia elétrica deve ser instalado separadamente do cabeamento da rede lógica;

XII – As salas em que são tratados assuntos sigilosos ou que, pela sua sensibilidade, mereçam maior grau de segurança, devem possuir isolamento acústico. Esses locais devem, de acordo com a necessidade, ser submetidos à varredura eletrônica e à inspeção de ambiente;

XIII – Os equipamentos de ar-condicionado instalados em paredes externas devem possuir grades de proteção que impeçam o acesso indevido;

XIV – As mesas de trabalho em que são tratados assuntos sigilosos devem ser

dispostas nas salas de forma a evitar a observação externa pelas janelas;

XV – As áreas destinadas à circulação do público externo devem ser dispostas em locais favoráveis ao controle do fluxo de visitantes;

XVI – As Unidades do MPPI que possuam postos de atendimento avançado de agências bancárias e caixas eletrônicos em suas dependências devem cumprir a legislação específica relacionada à segurança do local;

XVII – A Unidade do MPPI deve regular em seu respectivo Plano de Segurança Orgânica as rotinas e horários para abastecimento de valores nos caixas eletrônicos existentes em suas dependências;

XVIII – As salas onde se guardam materiais, sobretudo os de alto custo e/ou sensíveis, devem possuir teto com laje, grades em suas janelas, portas, sistema de alarme, além de controle específico de chaves, CFTV ou fechadura eletrônica.

Subseção I

Do Controle de Acesso

Art. 23. No Controle de Acesso aos órgãos e unidades do MPPI deverão ser observados:

I – As entradas dos prédios, preferencialmente, havendo disponibilidade de pessoal, devem possuir um posto de serviço de segurança 24 horas;

II – As portarias de acesso devem ter um serviço de recepcionistas, para realizar o registro de visitantes que entram no prédio, o qual deve conter dados pessoais de identificação (inclusive CPF), data e hora do acesso, locais a que se dirigem, órgão de origem (quando cabível) e telefones para contato, sendo que tal registro deve ser realizado, preferencialmente, por meio de sistemas informatizados que permitam fotografar os visitantes;

III- antes do acesso do visitante à área desejada, deve ser feito contato com uma pessoa do setor de destino para a devida autorização;

IV- a unidade deverá adotar as providências necessárias para o controle do

deslocamento do visitante nas dependências internas, inclusive, quando possível, com a utilização de sistemas informatizados e barreiras que permitam, tão somente, o acesso ao setor de destino;

V– As portarias das unidades devem possuir um sistema de catracas com leitores de cartão (ou similar) e biométrico, para registros de servidores, estagiários, prestadores de serviço, adolescentes aprendizes, terceirizados e visitantes;

VI – É obrigatório o uso de crachá de identificação para acesso às áreas e instalações das unidades do MPPI e permanência em seu interior, exceto pelos membros do MPPI, que poderão utilizar credencial específica;

VII – Em locais onde houver detectores de metais, os portadores de marca passo não serão a eles submetidos, mas devem apresentar documentação que identifique sua situação, submetendo-se a outros meios de vistoria;

VIII – As portas devem possuir dispositivos de fechadura com chave, as janelas devem possuir dispositivos de fechadura com trancamento interno e os locais que exigem maior controle de acesso devem possuir fechadura eletrônica controlada por equipamento de controle de acesso, com auditoria periódica dos relatórios de acesso;

IX – A entrada de servidores e estagiários em dias e horários sem expediente ou após o expediente deve ser regulada e controlada e os dados de acesso devem constar em registro específico.

X - Terceirizados não devem acessar as áreas e instalações das unidades do MPPI nos dias e horários sem expediente, exceto em situações de prestação de serviços devidamente autorizados e monitorados;

XI – O estacionamento das Unidades do MPPI deve ter o seu procedimento de controle de acesso regulado por norma específica, devendo a entrada e saída de veículos serem registradas em controle específico;

XII– O claviculário deve estar localizado em área segura e possuir registro, os

terceirizados não devem ter acesso direto ao claviculário, que ficará sob a responsabilidade da respectiva unidade de segurança ou assessoria militar;

XIII- Os relatórios de acesso a claviculários devem ser auditados periodicamente;

XIV – Os registros de retirada e entrega de chaves devem possuir itens de controle que permitam auditorias posteriores;

XV – As áreas que abriguem instalações sensíveis e que sejam de acesso restrito devem ser sinalizadas com placas indicativas desta situação;

XVI – Nos casos necessários, o acesso a determinadas áreas será condicionado à credencial de segurança compatível com o grau de sigilo do local;

XVII – Os locais onde se processam dados e informações sigilosas devem ser separados fisicamente de locais onde trabalham terceirizados;

XVIII – A presença de terceirizados de limpeza, serviço de copa, recepcionistas, mensageiros e outros serviços (incluindo manutenção de qualquer tipo) nas salas onde há dados ou informações sigilosas, deve ser supervisionada por servidor;

XIX – A presença de fornecedores nas unidades do MPPI deve ser sempre acompanhada de um servidor ou vigilante previamente designado;

XX – O material do patrimônio somente poderá sair de uma unidade com autorização da área competente, devendo ser registrado na portaria;

XXI – Não será permitido o ingresso de pessoas nas unidades do MPPI portando arma de qualquer natureza, ressalvados os casos especificados em ato próprio;

XXII – As portarias de acesso das unidades do MPPI devem possuir cofre ou, na sua ausência, artefato similar para guarda de armas, assim como uma caixa de areia de descarga para ações de desmuniciamento do armamento, que deve ser instalada em local reservado;

XXIII – É vedado o ingresso nas dependências das unidades do MPPI de pessoas para a prática de comércio e propagandas diversas ou angariação de donativos e congêneres, salvo as campanhas institucionais;

XXIV – Sempre que as condições técnicas permitirem, os sistemas de registro de pessoas nas portarias das unidades do MPPI devem ser integrados a sistemas de identificação de pessoas e pesquisa de antecedentes;

XXV – Em situações de solenidades e eventos organizados nas unidades do MPPI, os integrantes de serviços de segurança armada de autoridades devem ser previamente identificados para eventuais autorizações de entrada e permanência com armamento;

XXVI – Não é permitida a filmagem ou fotografia no interior das unidades do MPPI sem prévia autorização da autoridade competente, comunicada à respectiva área de segurança institucional;

XXVII – A cobertura jornalística, filmagem e fotografia realizadas nas dependências do MPPI serão feitas por profissionais de imprensa previamente credenciados pela Coordenadoria de Comunicação Social, que deverá informar o Gabinete de Segurança Institucional.

Subseção II

Do Sistema de Vigilância Eletrônica

Art. 24. As Unidades do MPPI, em regra, devem possuir um sistema de Circuito Fechado de Televisão – CFTV- com cobertura das áreas e locais sensíveis e, obrigatoriamente, este sistema deve monitorar o perímetro externo, estacionamentos, portarias, entradas de instalações sensíveis (almoxarifado, acesso aos gabinetes de Promotores, etc.), interior da sala de equipamentos de informática, Centro de Processamento de Dados, locais de circulação e locais de atendimento ao público.

I - Os sistemas de CFTV devem ser monitorados em tempo real e possuir capacidade de armazenar, no mínimo, trinta dias de gravação de imagens de forma ininterrupta.

II - O acesso aos itens de configurações do sistema de CFTV ou opções de edição de imagens é restrito ao responsável da unidade de segurança ou servidor autorizado. Os terceirizados, envolvidos em atividades de segurança, somente poderão ter acesso ao sistema CFTV para visualização das imagens em tempo real. As imagens do CFTV devem ser classificadas e armazenadas em locais com acesso restrito.

III - O acesso às imagens gravadas pelo CFTV é vinculado à necessidade do serviço e deve ser autorizado pela autoridade competente.

IV - O terceiro que demonstrar legítimo interesse poderá requerer informações e dados sigilosos à respectiva unidade de segurança, condicionado o acesso ao deferimento do pedido, em todos os casos, pelo Procurador-Geral de Justiça, mediante norma específica.

V - Os perímetros externos ou áreas sensíveis no interior das unidades do MPPI, sempre que necessário, devem ser monitoradas por sensores de presença ligados a central de alarme.

Subseção III

Do serviço de segurança privada

Art. 25. Os perímetros das Unidades do MPPI devem ser protegidos, preferencialmente, por um serviço de vigilância privada.

§1º Os Procedimentos Operacionais Padrão para cada posto de segurança devem conter a composição do posto, com especificação do número de vigilantes; finalidade do posto; atribuições dos vigilantes; procedimentos comportamentais, em que são discriminados os procedimentos em relação ao tratamento com pessoas, apresentação individual e outros.

§2º Todos os terceirizados que atuam na área de segurança e recepção devem assinar um Termo de Compromisso de Manutenção do Sigilo – TCMS, que deve ser

arquivado e mantido no Gabinete de Segurança Institucional;

§3º Os postos de vigilância devem ser dotados de equipamento de comunicação para uso dos vigilantes, ligado à área de segurança da Unidade do MPPI.

Subseção IV

Da Emergência, Prevenção a Pânico e Prevenção e Combate a Incêndio

Art. 26. Todas as Unidades do MPPI devem possuir um planejamento de prevenção e combate a incêndio em conformidade com a legislação e com as normas técnicas em vigor.

I **-** Os planos devem ser simples, exequíveis, viabilizar ações com pessoal e material existente e prever situações em dias e horários com e sem expediente.

II - A instalação dos equipamentos de combate a incêndio deve atender aos requisitos técnicos de utilização de cada dependência, considerando a quantidade de equipamentos existentes e de pessoal.

III - O sistema de detecção e combate a incêndio e o agente químico de combate ao fogo devem ser verificados periodicamente.

IV- Os relatórios de manutenções preventivas programadas ou corretivas devem ser arquivados, devendo ser realizados testes periódicos, simulando incêndio, previstos em cronogramas de manutenção preventiva.

V - As condições de manutenção e recarga dos extintores de incêndio devem ser verificadas periodicamente e especial atenção deve ser dada aos contratos de manutenção e aos seus prazos.

VI **-** A sinalização de segurança contra incêndio e pânico deve ser disposta nas instalações das unidades, para orientação do pessoal em situações de emergência.

VII - Cada unidade do MPPI deve possuir um serviço de Bombeiro Voluntário, com a

participação de servidores, garantindo-se treinamento específico.

VIII - As saídas de emergência não podem ser obstruídas com equipamentos, móveis ou outro tipo de material que impeça a livre movimentação de pessoas.

IX - Os locais com material ou equipamento de combate a incêndio não podem ser obstruídos com qualquer tipo de material e as suas adjacências devem estar livres para plena utilização dos equipamentos.

X - O Gabinete de Segurança Institucional deve prever planejamento de capacitação/treinamento continuado, para cada unidade do MPPI e para os integrantes da Brigada de Combate a Incêndio.

XI -Os equipamentos e a sinalização de prevenção e combate a incêndio devem ser instalados nas dependências das unidades do MPPI e verificados periodicamente, em particular o sistema de detecção com alarme de incêndio; rede de hidrantes e extintores e sinalização de segurança contra incêndio e pânico.

XII - Procedimentos para situações extraordinárias ou de emergência, tais como interrupção de energia elétrica, ameaças com bomba, ameaças a integridade das pessoas, pane nos sistemas de ar condicionado, gás e água, devem constar em planejamento específico e tais procedimentos devem ser executados e treinados sistematicamente pelos integrantes da área de segurança e Brigada de Combate a Incêndio.

XIII -Em cada treinamento, devem ser avaliados para validações das ações: atribuições do pessoal da segurança e da brigada de combate a incêndio; atribuições de integrantes da unidade do MPPI; e os procedimentos para evacuação das instalações;

XIV - Devem ser realizados exercícios de evacuação das dependências, de acordo com as especificidades locais;

XV - As unidades do MPPI devem possuir iluminação auxiliar para situações de emergência, independente da rede de energia elétrica convencional;

XVI - Os sistemas essenciais que constem na infraestrutura crítica do MPPI devem possuir dispositivos de *nobreak* que evitem interrupção do serviço;

XVII - As Unidades do MPPI devem possuir um planejamento para situações extraordinárias e de emergência, que inclua evacuação de pessoal, documentos sigilosos e equipamentos sensíveis das instalações.

Subseção V

Da auditoria em Serviços e Planejamentos

Art. 27. A Auditoria em Serviços e Planejamentos será realizada periodicamente pelo GSI e pela Assessoria Militar, observando os seguintes serviços e sistemas de segurança em funcionamento nas unidades do MPPI:

I - controle de acesso nas portarias;

II - controle de acesso de veículos nas garagens ou estacionamento;

III - controle de acesso de servidores e estagiários em dias ou horários sem expediente;

IV - controle de acesso às áreas e instalações sensíveis;

V -controle de acesso aos claviculários;

VI - controle de saída de material do patrimônio;

VII - verificação do funcionamento dos equipamentos dos sistemas de detecção de intrusão;

VIII – verificação do funcionamento dos equipamentos do sistema de CFTV

IX - verificação do funcionamento dos equipamentos do sistema de prevenção e combate a incêndio;

Parágrafo único. Os planejamentos de contingência ou de emergência devem ser

revistos periodicamente, avaliando-se a pertinência de seu conteúdo e as reformas, obras ou mudanças de rotinas devem ser precedidas de avaliação da área de segurança para análise da necessidade de alteração do planejamento de emergência ou contingência.

Subseção VI

Das prescrições diversas

Art. 28. No tocante às prescrições diversas quanto à segurança de áreas e instalações deve ser observado:

I – As pessoas que trabalham em cantinas, restaurantes ou postos avançados de agência bancária nas dependências da unidade do MPPI devem ser registradas na respectiva área de segurança e possuir crachá de identificação;

II – Os projetos de construção e ocupação de áreas das unidades do MPPI devem seguir os seguintes requisitos de segurança:

a) iluminação: a iluminação deve ser adequada, em particular para o período noturno. Os campos de visão dos vigilantes e locais de passagem devem ser iluminados;

b) fluxo de pessoas: o fluxo de pessoas, em particular os visitantes, deve ser direcionado para locais que facilitem a fiscalização por parte dos vigilantes;

c) pontos cegos: devem ser evitados locais que não possam ser monitorados por sistemas de vigilância eletrônica ou física;

d) sinalização: saídas de emergência e locais sensíveis devem ser amplamente sinalizados;

e) paisagismo: o paisagismo, quando apropriado, deve ser projetado para constituir-se em uma barreira, mas sem impedir a observação dos vigilantes;

f) áreas de atendimento ao público: devem ser posicionadas em local que evite o fluxo de pessoas pelo interior da unidade do MPPI;

III – Os projetos de arquitetura para construções de Unidades do MPPI devem prever *layout* de ambientes internos que privilegiem os aspectos de segurança;

IV – O Gabinete de Segurança Institucional deve disponibilizar apoio técnico às áreas de engenharia e arquitetura das unidades com a finalidade de prever medidas de segurança nas áreas e instalações de futuras unidades do MPPI, com a devida coordenação de ações entre os dois setores para a execução de projetos de construção, desde a sua primeira etapa;

V – O MPPI deve assegurar que as medidas de segurança de áreas e instalações atendam à legislação trabalhista e ambiental, às normas municipais aplicáveis e às demais normas técnicas de prevenção e combate a incêndio e de edificações;

VI – As informações sobre o fluxo de circulação de pessoas nas dependências das unidades do MPPI, a distribuição interna de móveis, os *layouts* das instalações, a localização de áreas sensíveis, os projetos elétricos, a rede lógica, entre outras, devem ser protegidas pela área de segurança da respectiva unidade.

Seção IV

Segurança da informação nos meios de tecnologia da informação

Art. 29. A Segurança da informação nos meios de tecnologia da informação constitui um grupo de medidas para salvaguarda da informação, da integridade dos sistemas e dos meios de tecnologia da informação, da confidencialidade da informação nos meios de tecnologia da informação e da disponibilidade dos recursos de tecnologia da informação, englobando as áreas de informática e comunicações.

Art. 30. Os recursos de tecnologia da informação disponíveis no MPPI destinam-se

exclusivamente ao suporte das atividades desempenhadas pelos membros, servidores (efetivos e comissionados) e estagiários.

Art. 31. As Unidades do MPPI devem seguir as seguintes orientações no uso de recursos de tecnologia da informação:

I – Os recursos de informática e comunicações disponíveis para os usuários do MPPI somente poderão ser utilizados em atividades estritamente relacionadas às funções institucionais;

II – O usuário do recurso de Tecnologia da Informação é responsável pelo seu estado e funcionamento, devendo comunicar qualquer defeito ou comportamento anormal às áreas de tecnologia da informação das unidades do MPPI;

III – Os programas adquiridos pelo MPPI e os sistemas desenvolvidos no órgão somente poderão ser instalados de forma automática pelo sistema, por acesso remoto ou presencialmente por servidor qualificado da área de tecnologia da informação e comunicação de cada unidade do MPPI.

IV – É vedada a instalação e/ou execução de qualquer outro programa ou sistema que não tenha sido adquirido ou desenvolvido pelo MPPI, exceto em casos de comprovada necessidade do serviço, mediante anuência técnica da Coordenadoria de Tecnologia da Informação do MPPI;

V – As áreas de tecnologia da informação das unidades do MPPI deverão prever rotinas de *backup* para as unidades de armazenamento de rede;

VI – A realização de cópias de segurança dos dados armazenados no disco rígido da estação de trabalho será de responsabilidade do usuário da estação;

VII – Os procedimentos e as operações realizados por intermédio das estações de trabalho conectadas à rede serão da responsabilidade dos usuários que nelas estiverem autenticados;

VIII – Ao afastar-se temporariamente da estação de trabalho, o usuário deverá

desconectar-se da rede ou, alternativamente, ativar rotina de proteção de tela com senha;

IX – As estações de trabalho e seus periféricos somente poderão ser removidos dos locais de instalação, mesmo que provisoriamente, por servidores das áreas de suporte, ou excepcionalmente, pelos servidores autorizados pela Coordenadoria de Tecnologia da Informação.

Parágrafo único. Somente os programas e os sistemas homologados pela Coordenadoria de Tecnologia da Informação do MPPI podem ser instalados.

Subseção I

Da Segurança de rede e internet

Art. 32. No tocante à segurança de rede e internet serão observados:

I – As áreas de armazenamento de dados disponibilizadas aos usuários deverão ser compartimentadas e auditadas com a finalidade de identificar utilização irregular;

II – O armazenamento e a transmissão de dados e informações sensíveis ou sigilosas no MPPI nos meios de informática e telefonia serão realizados mediante a utilização de recursos (sobretudo criptografia), padronizados institucionalmente, que garantam a integridade e confidencialidade dos respectivos dados e informações.

III – A retirada de dados e informações sigilosas ou sensíveis da rede do MPPI e das redes locais das respectivas unidades só poderá ser realizada mediante permissão da autoridade classificadora e por usuário com credencial de segurança com grau de sigilo compatível;

IV – Identificação do usuário e utilização de senha são condições indispensáveis para utilização dos recursos de tecnologia da informação do MPPI;

V – Informações a respeito do monitoramento dos recursos de tecnologia da informação deverão ser disponibilizadas aos usuários por ocasião do *login;*

VI – A solicitação para uso dos recursos de tecnologia da informação deverá ser realizada formalmente por membro ou responsável pelo setor do usuário à

Coordenadoria de Tecnologia da informação do MPPI, informando o perfil de utilização;

VII – As senhas de acesso deverão ser individuais, sigilosas e intransferíveis, cabendo à Coordenadoria de Tecnologia da Informação definir as regras de formação, de suas reutilizações e período de validade;

VIII – O acesso às redes institucionais e à *Internet* dar-se-á por meio disponibilizado e configurado pela Coordenadoria de Tecnologia da Informação. Para os acessos a sítios da *Internet* realizados a partir das redes institucionais serão gerados registros nos equipamentos de acesso e segurança de rede. Estes registros fornecerão o endereço de rede da estação utilizada, bem como o nome do usuário que realizou o acesso;

IX – É vedado o acesso às páginas ou serviços que possuam características diversas das atividades institucionais do MPPI, salvo as previamente autorizadas;

X – Nos casos em que houver necessidade, em razão do serviço, de acesso que, em princípio, seja obstado pelos sistemas do MPPI, deverá ser realizada solicitação específica para a respectiva liberação à Coordenadoria de Tecnologia da Informação;

XI – O serviço de correio eletrônico destina-se a agilizar a comunicação interna e externa, e deverá ser utilizado para o envio e o recebimento de mensagens eletrônicas com conteúdo relacionado às funções desempenhadas pelo usuário, sendo vedado o uso dos recursos do correio eletrônico para a veiculação de mensagens desvinculadas do exercício das funções institucionais;

XII – A Coordenadoria de Tecnologia da Informação do MPPI poderá prover acesso sem fio às suas redes locais. Somente equipamentos autorizados e previamente homologados pela Coordenadoria de Tecnologia da Informação nas unidades poderão atuar como pontos de acesso sem fio às redes locais;

XIII – Os pontos de acesso sem fio às redes locais do MPPI deverão prover

mecanismos de criptografia e autenticação das conexões de usuários;

XIV – Será de responsabilidade do usuário solicitante a verificação de conformidade dos equipamentos particulares com as características de conexão sem fio utilizadas nas unidades do MPPI;

XV – A configuração do dispositivo que realizará o acesso remoto será de responsabilidade do usuário solicitante, sob orientação da Coordenadoria de Tecnologia da Informação;

XVI – As salas onde se encontram instalados os servidores de informática deverão, em regra, ter o seu interior monitorado por câmeras do sistema de CFTV e outros dispositivos de sensoriamento pertencentes ao sistema de segurança das Unidades do MPPI.

Parágrafo único. Ato normativo específico regulamentará o uso dos recursos previstos no inciso II deste artigo, no âmbito do MPPI, cabendo à Coordenadoria de Tecnologia da Informação elaborar estudos e prover os meios necessários para viabilizar tais providências.

Subseção II

Da segurança de mídias, acesso remoto e auditoria

Art. 33. No tocante à segurança de mídias, acesso remoto e auditoria serão observados:

I – As mídias contendo dados e informações sigilosas devem ser protegidas durante o transporte externo às instalações das unidades do MPPI, mediante o uso de criptografia;

II – O acesso aos recursos de tecnologia da informação poderá ser realizado a partir de ambiente externo às dependências do MPPI. Os recursos de tecnologia da informação que serão homologados para acesso remoto, bem como os perfis de usuários autorizados, serão definidos pela Coordenadoria de Tecnologia da Informação. Para o acesso, a autenticação do usuário deverá utilizar identificação e

senha, preferencialmente acompanhadas de certificação digital, e os dados transmitidos durante todo o acesso deverão ser protegidos mediante uso de criptografia;

III – A liberação do acesso deverá ser solicitada à Coordenadoria de Tecnologia da Informação, sendo tal acesso de uso exclusivo do usuário solicitante. A configuração do dispositivo que realizará o acesso remoto será de responsabilidade do usuário solicitante, sob orientação da Coordenadoria de Tecnologia da Informação;

IV – O uso dos recursos de tecnologia da informação, sempre que possível, deverá gerar informações que possam ser coletadas e transformadas em trilhas de auditoria, de forma que pela análise ou visualização destas, sejam respondidas questões de autoria e temporalidade;

V – Para fins de verificação do cumprimento das normas de segurança ou por determinação de autoridade competente, a Coordenadoria de Tecnologia da Informação poderá realizar auditoria nas trilhas de uso dos recursos de tecnologia da informação sob sua responsabilidade. As informações provenientes dessas auditorias receberão tratamento sigiloso;

VI – As auditorias e verificações de conteúdo das áreas de armazenamento das redes e estações de trabalho locais deverão ser realizadas sob prévia autorização da autoridade competente e de modo a não comprometer o sigilo de dados e informações assim classificados em razão do serviço. Tais atividades devem ser realizadas por servidores especificamente designados e de maneira a permitir a rastreabilidade das ações da auditoria. As informações provenientes dessas auditorias receberão tratamento sigiloso.

Subseção III

Da segurança das comunicações

Art. 34. No tocante à segurança das comunicações serão observados:

I – O uso de aparelhos de telefones sem fio somente será utilizado

excepcionalmente, e desde que devidamente motivado, e quando o setor respectivo inexiste infraestrutura necessária;

II – As instalações físicas destinadas à sala da central telefônica deverão ser dedicadas exclusivamente a este uso. Na impossibilidade, a central telefônica deve ser instalada em local que permita restringir o acesso, inclusive ser fechado com chave ou sistema similar;

III – Não é autorizado acesso remoto à central telefônica, inclusive por empregados de empresa de manutenção, sem monitoramento da ação pela Coordenadoria de Apoio Administrativo;

IV – Os computadores utilizados por telefonistas devem possuir acesso somente ao sistema de telefonia, sendo bloqueados os demais sistemas e serviços;

V – A sala de telefonistas e a sala da central telefônica são áreas restritas e devem ter acesso controlado, com a devida sinalização, as quais devem ser monitoradas por câmeras do sistema de CFTV ou possuírem sensores de presença ligados a alarmes;

VI – Os quadros de telefonia devem ser protegidos por sistemas de fechadura com chave ou similar;

VII – As empresas contratadas para realizar a manutenção da central telefônica e seus empregados que prestam serviço nas unidades do MPPI devem assinar TCMS;

VIII – As pessoas contratadas para a função de telefonista e serviço de manutenção deverão ser capacitadas em treinamento para exercício da função que inclua aspectos de segurança da informação. Tais pessoas também deverão assinar TCMS, que deve ser arquivado e mantido no GSI;

IX – Os usuários de equipamentos de comunicações não deverão introduzir mensagens com conteúdo sigiloso ou sensível nas secretárias eletrônicas.

Subseção IV

Prescrições Diversas

Art. 35. As Unidades do MPPI devem seguir as seguintes orientações:

I – Os usuários que necessitarem, devido à natureza de suas funções, de acesso privilegiado a recursos da rede do MPPI deverão realizar solicitação formal, apresentando os argumentos que justifiquem tal acesso;

II – O acesso a dados e informações sigilosos nos recursos de tecnologia da informação será de acordo com o grau de sigilo da credencial de segurança e atenderá os requisitos de necessidade do serviço e necessidade (funcional) de conhecer;

III – Os equipamentos que forem destinados à doação, considerados inservíveis ou que tenham que sofrer manutenções corretivas em ambientes fora do MPPI, deverão ter seus dados eliminados de forma segura pelas áreas de tecnologia da informação;

IV – As mídias inservíveis contendo dados e informações sigilosos ou sensíveis que por qualquer motivo devam ser destruídas, serão eliminadas de forma segura. A Coordenadoria de Tecnologia da Informação deverá identificar os itens que requeiram descarte seguro. O descarte de itens desta natureza deverá ser registrado em controle com descrição de conteúdo, para permitir a realização de auditorias futuras;

V – O acesso aos recursos de tecnologia da informação por visitante exige o cadastramento do usuário na área de tecnologia da informação;

VI – O ingresso e o uso de equipamentos de informática e periféricos particulares nas unidades do MPPI devem ser controlados e o material deverá ser registrado nas portarias das unidades do MPPI pelo serviço de segurança, com comunicação à respectiva área de tecnologia da informação.

Seção V

Segurança da Informação na Documentação

Art. 36. A Segurança da Informação na documentação é um conjunto de medidas que visa à proteção da informação contida na documentação que é arquivada ou que tramita no MPPI, incluindo medidas de segurança no ato de produzir, classificar, tramitar, arquivar e destruir a documentação.

Parágrafo único. Deve ser realizada a gestão documental para documentos ostensivos e sigilosos de acordo com a legislação em vigor, implementando-se protocolos de documentos adequados a essa classificação.

Art. 37. Para implantação de medidas de segurança da informação na documentação é necessária a classificação de segurança pelas unidades do MPPI, que devem seguir as seguintes orientações:

I – A documentação produzida no MPPI deve ser classificada quando o seu conteúdo exigir grau de sigilo;

II – A classificação dos documentos ou informações sigilosos do MPPI e os seus respectivos trâmites e tratamentos observarão, no que couber, a Lei nº 12.527, de 18 de novembro de 2011, sem prejuízo das demais hipóteses legais de sigilo e de segredo de justiça;

III – O acesso aos documentos ou informações sigilosos é restrito e condicionado à credencial de segurança e à necessidade (funcional) de conhecer;

IV – O princípio da compartimentação deve ser adotado no desenvolvimento das atividades de segurança da informação na documentação.

Subseção I

Da Gestão de documentos sigilosos

Art. 38. Na Gestão de documentos sigilosos serão observados:

I – Os responsáveis pela guarda ou custódia de documentos sigilosos os transmitirão a seus substitutos, por meio de inventário devidamente conferido,

quando da passagem ou transferência de responsabilidade;

II – A classificação de um grupo de documentos que formem um conjunto deve ser a mesma atribuída ao documento classificado com o mais alto grau de sigilo;

III – Os mapas, planos-relevo, cartas e fotocartas baseados em fotografias aéreas ou em seus negativos serão classificados em razão dos detalhes que revelem e não da classificação atribuída às fotografias ou negativos que lhes deram origem ou das diretrizes baixadas para obtê-las.

Subseção II

Dos documentos controlados

Art. 39. Nos documentos controlados serão observados:

I – Os Documentos Controlados – DCs – são documentos sigilosos cujo conteúdo requer medidas extras de segurança, que incluem guarda e custódia;

II – A segurança do Documento Controlado requer medidas adicionais de controle, tais como: identificação dos destinatários em protocolo e recibos próprios, quando da difusão; lavratura de termo de custódia e registro em protocolo específico; lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e lavratura de termo de transferência de custódia ou guarda.

§ 1º O termo de inventário deverá conter, no mínimo, os seguintes elementos: numeração sequencial e data; órgãos produtor e custodiante do DC; rol de documentos controlados; e local e assinatura.

§ 2º O termo de transferência deverá conter, no mínimo, os seguintes elementos: numeração sequencial e data; agentes públicos substituto e substituído; identificação dos documentos ou termos de inventário a serem transferidos; e local e assinatura.

Subseção III

Segurança na autuação e processamento administrativo

Art. 40. Na Segurança na autuação e no processamento administrativo serão observados:

I – Os documentos sigilosos encaminhados para autuação, além das diretrizes estabelecidas para os documentos ostensivos, devem estar classificados, conforme a legislação em vigor e os atos normativos regulamentares do Ministério Público, em sistema oficial de controle de documentação do MPPI;

II – Quando a autuação for realizada pelo MPPI, não devem constar da capa do processo sigiloso os dados que possam acarretar qualquer risco à segurança das atividades ou comprometer o respectivo sigilo;

III – Quando da realização de juntada de documentos sigilosos deve ser considerada a mesma classificação atribuída ao documento classificado com o mais alto grau de sigilo;

IV – As páginas do processo sigiloso serão numeradas seguidamente, devendo cada uma conter, também, a indicação do total de páginas que compõem o documento.

Subseção IV

Da marcação de documentos sigilosos

Art. 41. Na marcação de documentos sigilosos serão observados:

I – As páginas, os parágrafos, as partes componentes ou os anexos e apensos de um documento sigiloso podem merecer diferentes classificações, mas ao documento, no seu todo, será atribuído o grau de sigilo mais elevado conferido a quaisquer de suas partes;

II – A marcação ou indicação do grau de sigilo em documentos registrados em papel deve ser feita, em fase de produção, em todas as páginas do documento e na capa, se houver, por meio de carimbo contendo o grau de sigilo;

III – As páginas serão numeradas em ordem sequencial, devendo cada uma conter, também, quando possível, a indicação do total de páginas que compõem o

documento;

IV – A indicação será centralizada, preferencialmente no alto ou no pé de cada página, em cor contrastante com a do documento;

V – O DC também expressará, nas capas, se houver, e em todas as suas páginas, a expressão “Documento Controlado”, o respectivo número de controle e o respectivo grau de sigilo;

VI – A marcação em extratos de documentos, rascunhos, esboços e desenhos sigilosos obedecerá às mesmas regras;

VII – Os meios de armazenamento de dados ou informações sigilosos serão marcados com a classificação devida no invólucro, contendo carimbo ou sinal indicativo de tais circunstâncias;

Subseção V

Da Segurança na Expedição, Tramitação e Reprodução

Art. 42. Na Segurança na Expedição, Tramitação e Reprodução serão observados:

I – Toda a documentação sigilosa deve tramitar em grau de urgência;

II – Os mesmos critérios de segurança aplicados no encaminhamento ao MPPI de documentação classificada como sigilosa devem ser observados em seu trâmite interno e em sua devolução ao órgão de origem;

III – A documentação classificada como sigilosa, em sua tramitação interna e na expedição, obedecerá, entre outros, os seguintes procedimentos: serão acondicionados em invólucros duplos para remessa; no invólucro externo, não constará qualquer indicação do grau de sigilo ou do teor do documento, constando apenas o nome, a função do destinatário e seu endereço; no invólucro interno, serão apostos, pela unidade remetente, o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o invólucro externo; sempre que o assunto for considerado de interesse exclusivo do destinatário, será inscrita a

palavra “pessoal” no invólucro interno contendo o documento sigiloso; e o invólucro interno será fechado, lacrado e expedido mediante recibo (ou registro eletrônico no sistema de comunicação oficial do MPPI), que indicará remetente, destinatário e número ou outro indicativo que identifique o documento;

IV – Na tramitação interna da documentação sigilosa, pode ser utilizado envelope ou sacola reutilizáveis, desde que ofereça as mesmas condições de segurança e permita a aplicação de lacres;

V – A expedição, condução e entrega de documento classificado no mais alto grau de sigilo será efetuada por pessoa autorizada, sendo vedada a sua postagem;

VI – A expedição de documento sigiloso pode ser feita mediante serviço postal, com opção de registro, serviço de malote, mensageiro oficialmente designado, sistema de encomendas ou, se for o caso, mala direta;

VII – É vedada a extração de cópia com a finalidade de colher recibo de entrega de documentação classificada segundo o grau de sigilo;

VIII – Ao receber documentação sigilosa deve-se verificar a integridade e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na documentação recebida, dando ciência do fato à sua chefia imediata e ao destinatário, o qual informará imediatamente ao remetente;

IX – O invólucro interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior;

X – O invólucro interno contendo a marca “pessoal” somente pode ser aberto pelo próprio destinatário;

XI – A movimentação e o recebimento eletrônico de documentação sigilosa ficam restritos aos servidores credenciados;

XII – Os documentos sigilosos serão mantidos ou guardados em condições especiais de segurança, devendo-se observar, conforme o grau de sigilo, as seguintes prescrições: guarda do documento em cofre ou estrutura que ofereça

segurança equivalente ou superior. Os responsáveis pela guarda ou custódia de documentos sigilosos os transmitirão a seus substitutos, devidamente conferidos, quando da passagem ou transferência de responsabilidade;

XIII – A reprodução do todo ou de parte de documentação sigilosa terá o mesmo grau de sigilo do original e os procedimentos que vierem a instruir também passarão a ter grau de sigilo idêntico;

XIV – A reprodução total ou parcial de documentos sigilosos controlados condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto;

XV – As eventuais cópias decorrentes de documentos sigilosos serão autenticadas pela autoridade devidamente constituída;

XVI – Nas cópias expedidas devem constar marcas ou carimbos de identificação. Junto aos documentos originais, devem constar as destinações das cópias expedidas;

XVII – O responsável pela reprodução de documentos sigilosos deve providenciar a eliminação de notas manuscritas, provas ou qualquer outro recurso que possa dar origem a cópia não autorizada do todo ou parte;

XVIII – Sempre que a preparação, impressão ou reprodução de documento sigiloso for efetuada em impressoras, oficinas gráficas ou similares, essa operação deve ser acompanhada por servidor oficialmente designado, que será responsável pela garantia do sigilo durante a confecção do documento.

Subseção VI

Segurança na Publicação, Arquivamento e Acesso

Art. 43. Na Segurança na Publicação, Arquivamento e Acesso serão observados:

I – A publicação dos atos sigilosos, quando necessário, limitar-se-á aos seus respectivos números, datas de expedição e ementas, redigidas de modo a não

comprometer o sigilo;

II – Poderão ser elaborados extratos de documentos sigilosos, para sua divulgação ou execução, mediante autorização da autoridade classificadora ou autoridade superior competente para dispor sobre o assunto;

III – Os documentos sigilosos que forem objetos de desclassificação passarão a ter segurança de acordo com o novo grau atribuído, assim como a preservação e o acesso;

IV – Os documentos, enquanto classificados como sigilosos, não podem ser desfigurados ou destruídos, sob pena de responsabilidade penal, civil e administrativa, nos termos da legislação em vigor;

V – Ao ser desclassificado, o documento obedecerá às diretrizes de temporalidade e destinação estabelecidas em regulamento próprio;

VI – Os autos originais de processos extraviados ou destruídos acidentalmente devem ser reconstituídos;

VII – O acesso à documentação sigilosa é condicionado à emissão de credencial de segurança pela autoridade competente no correspondente grau de sigilo e à necessidade (funcional) de conhecer;

VIII – A credencial será concedida pelas autoridades competentes, conforme definido em ato normativo específico;

IX – O acesso a documentos sigilosos é restrito, sendo admitido: ao agente público, no exercício de cargo, função, emprego ou atividade pública, que tenha direito e necessidade (funcional) de conhecê-los; e ao cidadão, naquilo que diga respeito à sua pessoa, ao seu interesse particular ou do interesse coletivo ou geral, mediante requerimento ao órgão ou entidade competente. Os demais casos serão solicitados e concedidos na forma da legislação vigente.

§1º A reconstituição obedecerá aos princípios normatizados para a restauração de autos ostensivos extraviados ou destruídos acidentalmente.

§2º A documentação sigilosa reconstituída terá o mesmo grau de sigilo do original e os procedimentos que vierem a instruir também passarão a ter grau de sigilo idêntico.

Subseção VII

Da Segurança em contratos envolvendo sigilo

Art. 44. Na Segurança em contratos envolvendo sigilo serão observados:

I – A celebração de contrato cujo objeto implique realização de ações sigilosas, ou a guarda, ou tratamento de dados ou informações (incluídos mapas, desenhos, cartas, modelos, plantas, fotografias, documentos, equipamentos, software, hardware ou outro tipo de material), de natureza sigilosa, deve condicionar o conhecimento do dado protegido à assinatura de TCMS pelos interessados na contratação (pessoa jurídica e pessoa física);

II – De acordo com cada situação, devem ser estabelecidas cláusulas prevendo a:

a) possibilidade de alteração do contrato para inclusão de cláusula de segurança não estipulada por ocasião da sua assinatura;

b) obrigação de o contratado manter o sigilo relativo ao objeto contratado, bem como à sua execução;

c) obrigação de o contratado adotar as medidas de segurança adequadas, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto contratado;

d) identificação, para fins de concessão de credencial de segurança, das pessoas que, em nome do contratado, terão acesso a material, dados e informações sigilosos;

e) responsabilidade do contratado pela segurança do objeto subcontratado, quando previamente autorizado, no todo ou em parte, extensivo à pessoa jurídica do

contratado e à pessoa física do empregado do contratado;

f) obrigação de o contratado se submeter a inspeção técnica de segurança por parte do MPPI nas dependências daquele, com o objetivo precípuo de verificação do nível de segurança em que estão sendo tratados os dados e informações sigilosos;

g) definição de direito por parte do MPPI de realizar auditorias, fiscalização e monitoramento de atividades que envolvam os dados e informações sigilosos acessados pelo contratado, englobando o direito de monitorar ambientes físicos e virtuais, meios de tecnologia da informação, manipulação de documentos e meios de comunicação, verificando o nível de segurança da Internet, VOIP e e-mails institucionais ou corporativos;

h) As atividades de auditoria e monitoração devem ser amplamente divulgadas entre os participantes do projeto, inclusive constará de contratos de trabalho;

i) definição dos dados e informações a serem protegidas e determinação do período de manutenção do sigilo;

j) definição de ações e comportamentos de ambas as partes ao final do contrato, contemplando, inclusive, providências a serem adotadas em caso de violação do acordo;

l) critérios para registro do conhecimento e a regulamentação da propriedade intelectual, quando for o caso;

m) regulamentação da eliminação de dados e informações sigilosos ou qualquer material sigiloso que não se prestam mais ao objetivo do contrato;

n) medidas de gestão de incidentes de segurança da informação, estabelecendo procedimentos a serem adotados pelas partes para notificação e tratamento de incidentes de segurança;

o) proibição de repasse de dados e informações por parte da contratada a pessoas que não estiverem formalmente contratadas, salvo no caso de terceirização e contratação de consultores, se houver anuência do MPPI. Nesse caso, os

terceirizados e consultores devem submeter-se às normas de segurança previstas no contrato;

III – As Unidades do MPPI devem providenciar para que seus gestores, fiscais ou representantes adotem as medidas necessárias para a segurança dos documentos sigilosos em poder dos contratados;

IV – Os dados e informações sigilosos concernentes a sistemas e serviços em uso no MPPI somente devem ser de conhecimento de pessoas que por suas funções oficiais e contratuais necessitem conhecê-los, submetendo-se à assinatura do TCMS;

V – É vedado o acesso, em qualquer caso, da contratada a dados e informações sigilosos referentes à atividade institucional do MPPI. Em caso da exigência de realização de ensaios ou exercícios pilotos para operacionalização de sistemas ou serviços, devem ser utilizados dados ostensivos;

VI – A ação de alimentação de dados e informações sigilosos em bancos de dados deve ser feita por servidor com credencial de segurança compatível com o grau de sigilo. Excetuam-se os casos de traduções de documentos, quando a contratada deve assumir compromisso de manutenção o do sigilo.

Subseção VIII

Segurança de documentos em meio digital

Art. 45. No tocante à Segurança de documentos em meio digital, serão observados:

I – Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil;

II – Os equipamentos e sistemas utilizados para a produção de documentos no mais alto grau de sigilo só podem estar ligados a redes de computadores seguras, e que

sejam logicamente isoladas de qualquer outra;

III – Os equipamentos e sistemas utilizados para a produção de documentos sigilosos só podem integrar redes de computadores quando a respectiva conexão possua controles de segurança adequados, visando à garantia da confidencialidade, da integridade e da disponibilidade das informações;

IV – Os documentos sigilosos submetidos à digitalização serão mantidos ou guardados em condições especiais de segurança, não podendo ser manuseados por terceirizados;

V – Atos normativos da instituição regulamentarão a gestão, o trâmite e a classificação (competência, prazos de duração, critérios etc.) de documentos no MPPI, conforme as diretrizes constantes no presente plano e os regulamentos já existentes, tudo sem prejuízo das especificidades dos dados e informações afetos a cada área de atuação, finalística e administrativa.

CAPÍTULO IV

DA GESTÃO DE RISCO

Seção I

Planejamento de contingência e controle de danos

Art. 46. A gestão de riscos, que inclui a identificação, análise, avaliação e tratamento do risco, constitui-se em atividade fundamental para proteção do MPPI, por ser um processo dinâmico e proativo de defesa do sistema.

Art. 47. A gestão de riscos precede o planejamento estratégico e tático e o estabelecimento de processos e tomada de decisões que envolvam risco e a sua implementação orienta a operacionalização de controles de segurança e a realização do Planejamento de Contingência.

Art. 48. O Planejamento de Contingência é a previsão de técnicas e procedimentos

alternativos adotados para efetivar processos que venham a ser interrompidos ou a perder sua eficácia. Visa a minimizar o impacto e a restabelecer a continuidade desses processos, combinando ações preventivas e de recuperação.

Art. 49. O Controle de Danos é a determinação de uma série de medidas que visem a avaliar a profundidade de um dano, o comprometimento dos ativos e as demais consequências para o MPPI decorrentes de um incidente, inclusive no que se refere à imagem institucional. Constitui-se em eficaz ferramenta de suporte para tomada de decisões em situações de crise, possuindo concepção complementar ao Planejamento de Contingência.

Art. 50. O GSI coordenará a elaboração de processos sensíveis em cada unidade do MPPI visando estabelecer um planejamento de contingência, dentre eles, relativo a prevenção e combate a incêndio.

Art. 51. O Plano de Contingência consiste em uma série de ações a serem realizadas para diminuir ou neutralizar o impacto de um incidente de segurança, buscando manter os sistemas e serviços funcionando de forma integral ou buscando alternativas, de modo a reduzir os danos e prejuízos de toda ordem à instituição. Deve ser previsto para atender incidentes em serviços e sistemas essenciais da instituição ou para situações de emergência.

Art. 52. O plano de controle de danos visa a avaliar a amplitude do dano causado, o comprometimento dos ativos e mensurar o impacto do incidente de segurança na instituição. Constitui-se em uma série de ações que permitirão atuar para redução dos impactos do incidente e identificar alternativas para a continuidade da atividade interrompida ou ameaçada.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 53. Os atos cuja publicidade possa comprometer a efetividade das ações de segurança institucional deverão ser publicados em extrato.

Art. 54. As normas, procedimentos e técnicas de segurança devem ser exequíveis e a sua implementação precedida de um programa ou projeto de capacitação e treinamento dos integrantes do Ministério Público.

Art. 55. O presente Plano de Segurança Institucional entrará em vigor 45(quarenta e cinco) dias da sua publicação.

Teresina/PI, 06 de dezembro de 2018.

Cleandro Alves de Moura
Procurador-Geral de Justiça