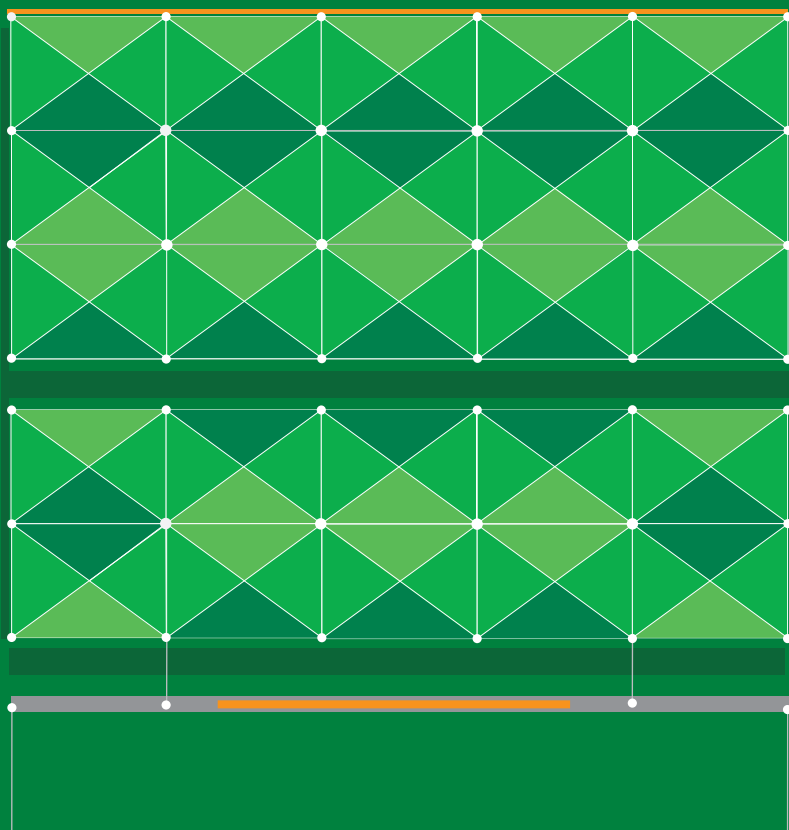


Segurança Institucional

Política e Plano



Procurador-Geral da República

Rodrigo Janot Monteiro de Barros

Vice-Procuradora-Geral da República

Ela Wiecko Volkmer de Castilho

Vice-Procurador-Geral Eleitoral

Eugênio Aragão

Ouvidor-Geral do Ministério Público Federal

Augusto Aras

Secretário-Geral

Lauro Pinto Cardoso Neto

SEGURANÇA INSTITUCIONAL

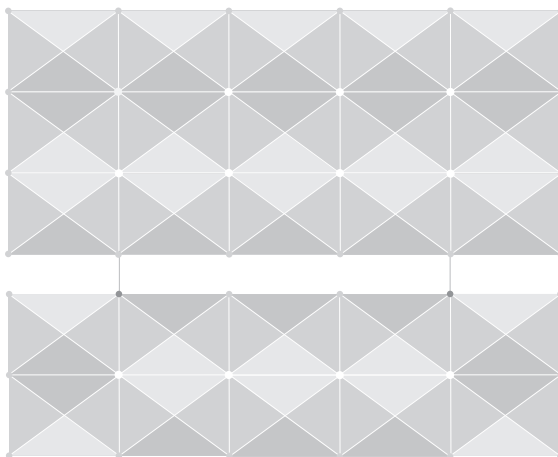
Política e Plano



MINISTÉRIO PÚBLICO FEDERAL

Segurança Institucional

Política e Plano



Brasília - DF
2014

Copyright © 2014 – Ministério Público Federal

Todos os direitos desta edição reservados ao Ministério Público Federal

Tiragem: 2000 exemplares

Impresso no Brasil

Elaboração, redação e organização: Unidade de Segurança Internacional

Editoração e projeto gráfico: Secretaria de Comunicação Social

NORMALIZAÇÃO BIBLIOGRÁFICA

Coordenadoria de Biblioteca e Pesquisa

Dados Internacionais de Catalogação na Publicação (CIP)

B823c

Brasil. Procuradoria-Geral da República. Unidade de Segurança
Institucional.

Segurança institucional: política e plano / Unidade de Segurança
Institucional. Brasília : MPF/PGR, 2014.

96p.

1. Política de segurança – Ministério Público Federal. 2.
Segurança institucional – Ministério Público Federal. I. Título.

CDD 341.26

Procuradoria-Geral da República

SAF Sul Quadra 4 Conj. C

CEP 70050-900 Brasília – DF

Telefone: (61) 3105-5100

Apresentação

A inserção do Ministério Público Federal no efetivo combate à corrupção e ao crime organizado demanda a adoção de adequadas medidas de proteção aos seus membros e servidores, bem como a melhoria no controle de acesso e guarda de suas instalações, materiais, dados e informações. Para tanto, elaboramos a Política e o Plano de Segurança Institucional que orientarão a consolidação dos processos e procedimentos de salvaguarda de nossas ações finalísticas e administrativas.

A segurança institucional será permanente e deverá envolver todos os integrantes da instituição em atuação responsável e integrada. Definidas as diretrizes e as normas gerais, as unidades administrativas descentralizadas poderão elaborar seus planos de segurança orgânica, específicos às características e necessidades locais, contendo ações de prevenção de danos e ameaças, gerenciamento de crises, prospecção de cenários e saneamento de eventuais vulnerabilidades. O planejamento dessas atividades deverá considerar o necessário equilíbrio entre a funcionalidade de nossos órgãos e as restrições impostas pelas normas de segurança.

O Ministério Público Federal, nesta oportunidade, agradece o especial empenho dos servidores da Secretaria de Segurança Institucional, chefiada por Delfim Loureiro de Queiroz, e o indispensável auxílio do Procurador da República Wilson Rocha de Almeida Neto, que coordenou a comissão instituída para validação dos estudos e apresentação de proposta do presente plano de segurança. Merece também destaque a colaboração dos Procuradores da República Eduardo Santos de Oliveira, Guilherme Guedes Raposo, Sílvio Pereira Amorim e Sílvio Roberto Oliveira de Amorim Junior, e dos servidores Henrique Antônio Oliveira dos Santos e Luís Carlos Galvão.

Rodrigo Janot Monteiro de Barros
Procurador-Geral da República



Apresentação

PARTE I

Política de Segurança Institucional

1 Introdução	11
2 Objetivos	13
3 Amplitude	13
4 Fatores críticos de sucesso	13
5 Segurança de recursos humanos	14
6 Segurança de material	15
7 Segurança de áreas e instalações	15
8 Segurança da informação	16
9 Outros aspectos de segurança	18
10 Gestão de riscos	18
11 Planejamento de contingência e controle de danos	19
12 Atribuições	19
13 Disposições finais	21



PARTE II

Plano de Segurança Institucional

1 Apresentação	25
2 Estrutura Organizacional e Atribuições	26
3 Gestão Estratégica	33
4 Segurança Institucional	37
5 Disposições Finais	87

PARTE III

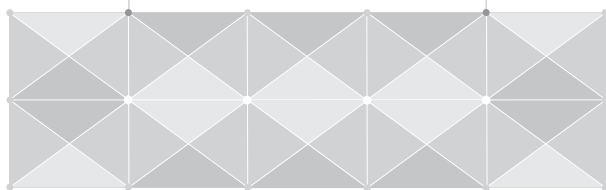
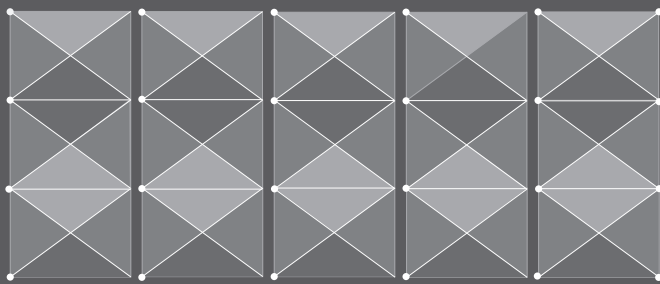
Anexos

1 Portaria nº 580, de 17 de novembro de 2010	89
2 Portaria nº 124, de 18 de março de 2013	90
3 Portaria nº 417, de 5 de julho de 2013	91
4 Portaria nº 427, de 5 de julho de 2013	92
5 Portaria nº 902, de 13 de dezembro de 2013	94



PARTE I

Política de Segurança Institucional



PARTE I

Política de Segurança Institucional

1 | Introdução

Objetiva-se neste documento estabelecer a POLÍTICA DE SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO FEDERAL (MPF), expedindo diretrizes gerais de segurança. A Política será orientadora para fundamentação de normas, processos e procedimentos de segurança a serem implementados em todo o MPF, por meio do Plano de Segurança Institucional e dos Planos de Segurança Orgânica das unidades do MPF.

Para efeito desta Política, entende-se como Sistema MPF a Procuradoria Geral da República, as Procuradorias Regionais da República, as Procuradorias da República nos Estados e no Distrito Federal, as Procuradorias da República nos Municípios, assim como os seus membros e servidores. Estão também sob alcance do conceito de Sistema MPF os estagiários e funcionários terceirizados, por manterem algum tipo de vínculo com o MPF.

As especificidades, particularidades e características das Funções Institucionais do MPF exigem adoção de medidas de segurança para garantir o pleno exercício dessas funções, indicando a necessidade de normatização de processos, práticas, procedimentos e técnicas referentes à segurança.

As transformações globais introduzidas pela chamada "sociedade do conhecimento", resultado de novos referenciais sociais, econômicos, tecnológicos e culturais, ensejam a produção de informação de toda espécie, em grande volume e de forma cada vez mais rápida, determinando às instituições a necessidade de equacionar o compartilhamento com a compartimentação da informação, de acordo com a necessidade de proteção.

A complexidade dos cenários atuais, associada à existência de atores hostis com os mais variados interesses, revela que os assuntos relativos à segurança devem ser abordados de maneira sistêmica, inseridos em um contexto de planejamento estratégico da Instituição, ou seja, deve-se pensar a proteção do Sistema MPF como um todo, de forma integrada na Instituição e fora dela, com o envolvimento de todos os seus integrantes.

No MPF, a Segurança Institucional deverá ter como concepção os seguintes princípios:

- orientar suas práticas pela ética profissional, cultuando os valores fundamentais do MPF;
- desenvolver suas atividades com o objetivo principal de antecipar-se às ações hostis das diversas ameaças de forma preventiva e proativa;
- possuir um caráter permanente, interligando-se a outras áreas para proteção do Sistema MPF;
- orientar-se por ameaças reais ou potenciais ao Sistema MPF, exploradas por atores hostis de qualquer natureza e com os mais variados interesses. Incluem-se aqui os efeitos de acidentes naturais;
- salvaguardar sempre a Instituição, evitando sua exposição e exploração midiática negativa.

Para cumprir as atribuições de proteção do Sistema MPF, a Segurança Institucional se segmentará nos seguintes grupos de medidas de segurança orgânica:

- segurança de recursos humanos;
- segurança do material;
- segurança das áreas e instalações;
- segurança da informação.

Pela importância do ativo denominado informação e a complexidade que envolve as ações para sua proteção, incluindo a utilização de modernas tecnologias, a segurança da informação se desdobra em:



- segurança da informação nos meios de tecnologia da informação;
- segurança da informação no pessoal;
- segurança da informação na documentação;
- segurança da informação nas áreas e instalações.

Além dos grupos de medidas de segurança orgânica citados, a Segurança Institucional deverá despender especial atenção para ações antagônicas de sabotagem e acessos intencionais não autorizados para que haja proteção efetiva de todos os bens tangíveis e intangíveis.

2 | Objetivos

- Estabelecer as diretrizes gerais do Procurador-Geral da República, a respeito de Segurança Institucional;
- Orientar a execução da atividade de Segurança Institucional no MPF;
- Definir as atribuições de segurança para as unidades do MPF;
- Desenvolver uma mentalidade de segurança no MPF.

3 | Amplitude

O conteúdo desta Política de Segurança Institucional se aplica às unidades do Ministério Público Federal e aos seus integrantes, naquilo que se refere às práticas e aos procedimentos individuais nas suas respectivas esferas de atribuições.

4 | Fatores Críticos de Sucesso

São considerados como fatores determinantes para o sucesso da implementação da Política de Segurança Institucional no MPF:

- comprometimento e apoio explícito de todos os níveis de direção e

chefia do MPF, com atitudes favoráveis ao cumprimento de normas de segurança no âmbito da Instituição;

- obtenção de uma mentalidade de segurança por todos os integrantes do MPF, incorporando o conceito de que cada um é responsável pela manutenção do nível de segurança adequado;
- estabelecimento de um Plano de Segurança Institucional e Planos de Segurança Orgânica, normas e procedimentos consistentes com a cultura organizacional da Instituição e consubstanciados na realidade de cada unidade do MPF;
- estabelecimento de estruturas de gerência, auditoria e validação de processos sensíveis, que envolvam quesitos de segurança;
- entendimento das necessidades de segurança que respalde o desempenho das Funções Institucionais do MPF;
- elaboração de programas de divulgação, educação e informação de conteúdos de segurança;
- provisão de recursos financeiros para as atividades de segurança;
- criação de programas de formação de recursos humanos e de treinamento continuado específico para servidores e para terceirizados com encargos de segurança;
- realização de Assessorias Técnicas de Segurança (ATS) para orientar as unidades do MPF.

5 | Segurança de Recursos Humanos

É um conjunto de medidas destinado a proteger a integridade física de membros, servidores do MPF e familiares, quando comprometida em face do desempenho das funções institucionais.

Envolve a proteção realizada por servidores do MPF ou a solicitação de proteção disponibilizada por Órgãos de Segurança Pública (OSP) estaduais e federais e, em último caso, pelas forças singulares.

Pela especificidade e circunstâncias do desempenho das Funções Institucionais, é fundamental que os integrantes do MPF, em particular os membros, desenvolvam uma cultura de conscientização e sensibilização quanto às prováveis ameaças, estabelecendo procedimentos de proteção e preservação de sua integridade.

6 | Segurança de Material

Compreende um conjunto de medidas de segurança voltadas para proteger o material pertencente ou em uso no MPF. O material constitui-se em um ativo economicamente importante para o MPF, além de poder conter dados e informações sensíveis e sigilosos de interesse de atores antagônicos.

O material compreende o patrimônio físico do MPF, estabelecido em bens móveis e imóveis, que permite o adequado funcionamento de uma unidade. Nas medidas de guarda e proteção do material, devem ser incluídas as condições técnicas adequadas e os procedimentos de segurança e manutenção do material.

Incidentes de segurança envolvendo material devem ser sempre observados sob a ótica da intencionalidade do fato. Cumpre levantar a situação e as circunstâncias em que o fato ocorreu, para esclarecimento a respeito de ocorrência de sabotagem.

7 | Segurança de Áreas e Instalações

Segurança de áreas e instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade do MPF ou onde se realizam atividades de interesse do MPF, com a finalidade de salvaguardá-las.

As ações de segurança nas áreas e instalações estão intimamente ligadas a outros grupos de medidas, como a segurança de recursos humanos e a segurança da informação. Essa integração é que proporciona maior nível de segurança para o Sistema MPF.

Incluem-se, na segurança de áreas e instalações: a) demarcação de áreas; b) controle de acessos; c) detecção de intrusão e monitoração de alarme; d) implementação de barreiras; e) estabelecimento de linhas de proteção; f) sistema de vigilância humana; g) proteção de cabeamentos e quadros de toda espécie; h) proteção de sistemas de energia, água, gás e ar condicionado; i) outras técnicas e procedimentos de segurança.

O Plano de Segurança Institucional e os Planos de Segurança Orgânica devem prever procedimentos que contemplem as regras de segurança e instrumentos de auditoria e validação de cada norma. Todos os processos devem ser avaliados e auditados periodicamente.

Os projetos de construção de áreas e instalações do MPF devem ser planejados, integrando o setor de engenharia com o setor de segurança, de maneira a reduzir deficiências originadas no projeto. Dessa maneira, devem-se levar em consideração aspectos de iluminação; locais de trânsito de pessoas e veículos (servidores, visitantes, prestadores de serviço, entregadores); campos de visada para agentes de segurança; ocupação física de espaços; manutenção de áreas e equipamentos; cabeamento e instalação de equipamentos de energia e tecnologia da informação e delimitação de perímetros de segurança.

Além disso, os equipamentos de segurança para áreas e instalações devem ser integrados à vigilância humana e a outros sistemas de segurança e de controles de acesso, a fim de estabelecer a segurança de forma sistêmica.

É de fundamental importância o planejamento para prevenção e combate a incêndio, o que exige meticulosa avaliação de ameaças desse tipo e treinamento de pessoal. O emprego de pessoal especializado e o treinamento de servidores voluntários - como apoio em situações de crise - devem ser sempre considerados no planejamento.

Da mesma forma que na segurança do material, os incidentes envolvendo áreas e instalações devem ser sempre observados sob a ótica da intencionalidade do fato, buscando-se identificar indícios de sabotagem ou acessos intencionais não autorizados.

8 | Segurança da Informação

A segurança da informação é um grupo de medidas de segurança que envolve a proteção de dados, informações e conhecimentos sensíveis ou sigilosos, cujo acesso ou divulgação não autorizados podem acarretar prejuízos de qualquer natureza ao MPF ou proporcionar vantagem a atores antagônicos.

A segurança da informação visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade da informação.

Os acordos de confidencialidade ou de não divulgação, para preservar a informação, devem ser celebrados entre o MPF e as instituições ou organizações com as quais o Ministério Público compartilhe dados. Esses acordos devem ser estendidos aos integrantes das instituições e organizações que tiverem acesso a tais dados.



Os acordos devem ser estabelecidos por meio de cláusulas contratuais ou por meio de Termos de Compromisso de Manutenção do Sigilo, os quais devem ser específicos para cada situação e circunstância. Os integrantes do MPF que têm acesso a dados e informações sigilosos devem assinar também esses termos.

Toda informação deve ser classificada de acordo com o grau de sigilo exigido por seu conteúdo, de forma a assegurar que receba nível adequado de proteção. A classificação indicará as necessidades, prioridades e níveis de proteção desejados no tratamento da informação. A classificação de documentos no MPF seguirá o constante no Decreto nº 4.553, de 27 de dezembro de 2002, naquilo que for aplicável ao MPF.

A Segurança da Informação nos Meios de Tecnologia da Informação constitui um grupo de medidas para salvaguardar a informação, a integridade dos sistemas e os Meios de Tecnologia da Informação do MPF. Engloba as áreas de Informática e Comunicações.

No que se refere à Segurança da Informação nos Meios de TI, a busca de proteção de dados e informações deve sempre privilegiar a utilização de tecnologias modernas e o uso de sistemas criptográficos na transmissão de dados e informações, inclusive nos meios de comunicação por telefonia. Especial atenção deve ser dada aos procedimentos de armazenamento de dados (*backup*), os quais devem promover a segurança e disponibilidade da informação.

A Certificação Digital deve ser considerada para o trato com assuntos que necessitem de sigilo e validade jurídica. Mesmo não sendo classificados como sigilosos – pela sua sensibilidade e necessidade de salvaguarda temporária –, os assuntos que exigem proteção também devem ser considerados.

A Segurança da Informação no Pessoal refere-se ao conjunto de medidas destinadas a garantir comportamento dos integrantes do Ministério Público Federal que assegure a proteção da informação. Engloba medidas de segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição.

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

É relevante que se proceda a gestão documental para documentos ostensivos e sigilosos de acordo com a legislação em vigor, implementando-se,

assim, protocolos de documentos adequados a essa classificação.

A Segurança da Informação nas Áreas e Instalações define medidas e procedimentos para preservar as informações sobre áreas e instalações.

9 | Outros Aspectos de Segurança

A sabotagem é o dano intencional contra material ou instalações, com impacto direto físico e indireto psicológico, que pode causar a interrupção de atividades. Por se constituir em um ato deliberado, possui alvo determinado e efeito esperado, aspectos que devem ser avaliados em caso de incidente de segurança.

O Plano de Segurança Institucional e os Planos de Segurança Orgânica deverão contemplar medidas de segurança que garantam ações para neutralizar eventuais atos de sabotagem contra o MPF. A negação de informação a atores hostis constitui-se em eficaz instrumento para evitar a sabotagem.

O acesso não autorizado a dados e informações constitui-se em atividade desenvolvida para subtrair conhecimento protegido de uma pessoa, organização ou instituição. O MPF, pela natureza de sua função institucional, possui dados e informações de interesse de atores antagônicos, cuja divulgação não autorizada ou prematura pode gerar desvantagem ou causar danos ao MPF.

A identificação e a proteção desses dados e informações constituem-se em atividade primordial para os integrantes do MPF. A salvaguarda da informação ocorrerá por meio da implementação de medidas de segurança orgânica integradas a práticas para desenvolver uma mentalidade de segurança.

Também é importante a conscientização por todos os integrantes do MPF de que a proteção de dados ou informações pessoais e da Instituição deve ser sempre permanente.

10 | Gestão de Riscos

A Gestão de Riscos – inclui a análise, avaliação e tratamento do risco – constitui-se em atividade fundamental para proteção do Sistema MPF, por ser um processo dinâmico e proativo de defesa do sistema.

A Gestão de Riscos precede o planejamento estratégico e tático, e o estabelecimento de processos e tomada de decisões que envolvam risco.

A sua implementação orienta a operacionalização de controles, planejamento de controle de danos e de contingência para a Instituição.

As unidades do MPF devem conduzir avaliação de risco para determinar suas necessidades de proteção, para monitorar as situações de risco e para acompanhar a escalada de ameaças, procedendo a modificações para ajustar as medidas de proteção.

Nessa concepção, as Assessorias Técnicas de Segurança (ATS), conduzidas pela Unidade de Segurança Institucional, constituem-se em eficaz instrumento de gestão de risco para as unidades do MPF. Além de avaliar e analisar os riscos, as ATS sugerem ações a realizar para tratamento do risco identificado.

11 | Planejamento de Contingência e Controle de Danos

Planejamento de contingência é a previsão de técnicas e procedimentos alternativos adotados para efetivar processos que tenham sido interrompidos ou que tenham perdido sua eficácia. Visam minimizar o impacto e restabelecer a continuidade desses processos, combinando ações preventivas e de recuperação. São fundamentais para permitir o cumprimento das funções da Instituição, mesmo diante de um incidente que atente contra a realização de processos.

O Controle de Danos é a determinação de uma série de medidas que visem avaliar a profundidade de um dano por ocasião de um incidente, o comprometimento dos ativos e as consequências para a Instituição, 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.

Os Planejamentos de Contingência e de Controle de Danos devem ser desencadeados simultaneamente em caso de crise, devem ser setoriais e exequíveis, preparados de acordo com a realidade de cada unidade do MPF. É relevante que sejam nomeados responsáveis e substitutos para cada ação a ser realizada e que os planejamentos sejam testados e reavaliados periodicamente.

12 | Atribuições

O MPF elaborará um Plano de Segurança Institucional e as unidades administrativas um Plano de Segurança Orgânica, orientados pela presente Política.

O planejamento deverá ser específico e adequado às características e realidade de cada unidade, e especial atenção deverá ser dispensada à implementação das normas e procedimentos de segurança constantes no plano.

A Unidade de Segurança Institucional deverá propor um Plano de Segurança Institucional do MPF, obedecendo a presente política, em conjunto com outras áreas da administração, como Tecnologia da Informação, Engenharia e Arquitetura, Gestão de Pessoas e Planejamento Estratégico. Esse plano deverá conter as normas específicas de cada grupo de medidas de segurança, as quais serão confeccionadas com a participação de cada setor da PGR.

Será disponibilizado pela Unidade de Segurança Institucional um modelo genérico de Plano de Segurança Orgânica para subsidiar as demais unidades do MPF. À Unidade de Segurança Institucional cabe, ainda, orientar e apoiar as unidades do MPF em situações de emergência e nos casos de ameaça. As unidades do MPF têm a incumbência de implementar os seus respectivos Planos de Segurança Orgânica, de acordo com cronograma específico.

Para obter uma concepção sistêmica da segurança, as unidades do MPF constituirão uma Unidade de Segurança Orgânica ou Assessorias de Segurança Orgânica, de acordo com a demanda e disponibilidade de recursos humanos, os quais terão atribuições regionais ou individuais, de acordo com a necessidade de cada unidade. Tais estruturas deverão estabelecer um canal técnico e operacional com a Unidade de Segurança Institucional, com ligação para assuntos de segurança, de modo a compartilhar conhecimentos, dados e informações. A existência de um canal técnico não exime os núcleos e as assessorias de sua subordinação administrativa às unidades.

O acompanhamento de cenários de interesse do Ministério Público Federal, no que se refere à segurança, para proporcionar suporte ao desempenho das funções institucionais, é uma incumbência da Unidade de Segurança Institucional, que contará com o apoio das Unidades ou Assessorias de Segurança Orgânica das unidades do MPF.

No âmbito do MPF o planejamento e a coordenação da capacitação de recursos humanos na área de segurança cabe à Unidade de Segurança Institucional, a qual, sempre que possível, realizará essa atividade em parceria com a Escola Superior do Ministério Público da União.



13 | Disposições Finais

As normas, procedimentos e técnicas de segurança devem ser exequíveis e a sua implementação precedida de um programa de capacitação e treinamento dos integrantes do MPF. Os programas de treinamento continuado, que têm por objetivo manter os integrantes do MPF em condição de executar as práticas de segurança, devem se constituir em preocupação de gestores em todos os níveis. A revisão periódica de todos os planos em prática permitirá a manutenção de níveis aceitáveis de segurança do MPF.

Os princípios de segurança constantes nesta Política também se aplicam a comissões ou grupos de trabalho designados em proveito do MPF, mesmo que atuem em áreas e instalações não pertencentes ao MPF.

A partir da data da publicação da presente Política, as unidades deverão confeccionar um Plano de Segurança Orgânica, de acordo com os prazos previstos em um programa de implementação. Depois de período de ajustes, o plano deve ser encaminhado à Unidade de Segurança Institucional para análise e avaliação.

Ao final do primeiro ano de vigência da presente Política e periodicamente deverão ser revisados os planos de segurança e a própria Política, para perfeita adequação às necessidades do MPF.

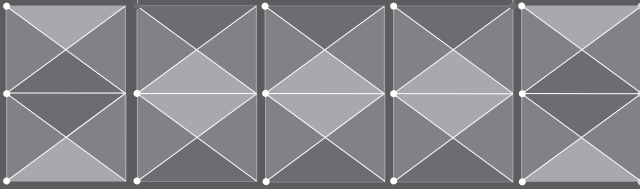
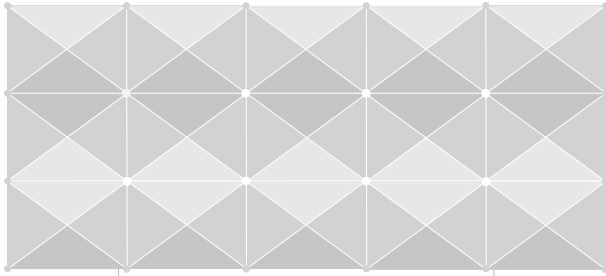
A Unidade de Segurança Institucional deverá estudar e propor uma Política de Contraineligência para o MPF, que amplie o conceito de segurança e proporcione a salvaguarda dos interesses do MPF. Nesse estudo, deverá ser prevista a criação de práticas, estruturas e normas para execução da atividade.

O equilíbrio entre a funcionalidade dos diversos setores do MPF e as restrições impostas pelas normas de segurança é impositivo para todo planejamento de segurança.



PARTE II

Plano de Segurança Institucional



PARTE II

Plano de Segurança Institucional

CAPÍTULO I

Apresentação

O presente Plano de Segurança Institucional tem por finalidade orientar e desenvolver a atividade de segurança no âmbito do Ministério Público Federal – MPF, estabelecendo princípios e diretrizes complementares à Política de Segurança Institucional.

1.1 | Considerações gerais sobre Segurança Institucional

Segurança Institucional compreende o conjunto de medidas adotadas para prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes.

A Segurança Institucional, no âmbito do MPF, é estratificada em níveis de gestão administrativa e se estrutura por meio da Política de Segurança Institucional, do Plano de Segurança Institucional e dos Planos de Segurança Orgânica.

A Política de Segurança Institucional refere-se ao nível de gestão política e estabelece as diretrizes gerais de segurança e áreas afins, alinhadas ao planejamento estratégico.

O Plano de Segurança Institucional abrange todos os grupos de medidas de segurança previstos na Política de Segurança Institucional e se refere ao nível de gestão administrativa estratégica, definindo as ações, projetos e programas necessários ao alcance dos objetivos específicos de Segurança Institucional.

Os Planos de Segurança Orgânica estabelecem normas de segurança específicas para cada unidade da Instituição, de acordo com suas características e peculiaridades, adequadas às necessidades de segurança locais e regionais.

Referem-se ao nível de gestão administrativa tática e se desdobram em normatização de rotinas e procedimentos

1.2 | Princípios da Segurança Institucional

A Segurança Institucional baseia-se nos seguintes princípios:

- I - ética profissional, cultuando e preservando os direitos fundamentais e os demais valores do MPF;
- II - antecipação às ações hostis das diversas ameaças de forma preventiva e proativa;
- III - caráter permanente, interligando-se a outras áreas para proteção do MPF;
- IV - consideração das ameaças reais ou potenciais ao MPF, inclusive as decorrentes de fenômenos naturais; e
- V - salvaguarda da Instituição de modo a evitar sua exposição midiática negativa.

1.3 | Amplitude

O disposto no Plano de Segurança Institucional aplica-se às unidades do MPF e aos seus integrantes naquilo que se refere às práticas e aos procedimentos nas suas respectivas esferas de atribuições.

CAPÍTULO II

Estrutura Organizacional e Atribuições

As funções de gestão de segurança institucional no MPF serão desempenhadas pelo Secretário-Geral, no âmbito nacional; pelos Procuradores-



Chefes, no âmbito das respectivas unidades; e pelo Procurador, designado pelo Procurador-Chefe do respectivo Estado, nas Procuradorias da República nos Municípios.

A coordenação técnica e operacional da atividade de segurança institucional será de responsabilidade da Unidade de Segurança Institucional, no âmbito da Procuradoria Geral da República - PGR, e das respectivas Unidades de Segurança, no âmbito das Procuradorias Regionais da República - PRRs e das Procuradorias da República nos Estados - PRs. Nas Procuradorias da República nos Municípios - PRMs, a atividade será desempenhada pelo Coordenador de PRM ou, de forma justificada, por outro servidor indicado pelo Procurador responsável pela segurança da unidade.

2.1 | Atribuições das Unidades de Segurança

2.1.1 Compete à Unidade de Segurança Institucional, vinculada à PGR:

- I - planejar, coordenar, executar, orientar e supervisionar as atividades de segurança institucional do MPF;
- II - propor a atualização e o aprimoramento periódico da Política de Segurança Institucional e do Plano de Segurança Institucional do MPF;
- III - subsidiar as unidades do MPF na elaboração do Plano de Segurança Orgânica;
- IV - assessorar o Secretário-Geral na homologação dos Planos de Segurança Orgânica das unidades do MPF e nos demais assuntos referentes à segurança institucional;
- V - propor regulamentação para atividade de gestão de riscos no MPF;

- VI - desenvolver a doutrina de segurança do MPF para proteção de membros e servidores, as situações de emergência, o planejamento de contingência, a gestão de riscos, a investigação de incidentes e outros assuntos relacionados à segurança;
- VII - executar atividades de assessoria técnica de segurança e elaborar manuais técnicos para subsidiar a realização de tais atividades pelas unidades do MPF;
- VIII - planejar, coordenar e executar, quando assim determinado pelo Procurador-Geral da República ou pelo Secretário-Geral, a atividade de proteção de membros, de servidores e, se necessário, de seus familiares, para garantia do exercício das funções institucionais;
- IX - supervisionar e avaliar, quando solicitado, as medidas de proteção adotadas em favor de membros, servidores e seus familiares;
- X - realizar a fiscalização documental, fiscal e física dos contratos de segurança e de bombeiro civil da PGR;
- XI - propor, em conjunto com os setores da PGR, o estabelecimento das normas de segurança para cada grupo de medidas de segurança previstos na Política de Segurança Institucional;
- XII - desenvolver uma cultura de inovação para a área de segurança institucional do MPF, inclusive promovendo estudos, avaliações e aplicações de novas tecnologias, táticas, técnicas e procedimentos de segurança;
- XIII - promover a conscientização dos integrantes da Instituição quanto à importância da segurança institucional;
- XIV - supervisionar, coordenar e fiscalizar, tecnicamente, as atividades de segurança institucional desenvolvidas nos setores da PGR e no âmbito das unidades do MPF;



- XV - propor programas de formação de recursos humanos ou treinamentos continuados para os membros e servidores com funções de segurança;
- XVI - estabelecer os mecanismos e procedimentos necessários às comunicações e ao intercâmbio de informações e conhecimentos no âmbito do MPF, observando as medidas necessárias para manutenção da segurança e sigilo, com base na legislação em vigor;
- XVII - estabelecer um canal de comunicação com as Unidades de Segurança do MPF, de modo a compartilhar conhecimentos, dados e informações;
- XVIII - propor instrumentos de cooperação técnica com o Poder Judiciário, com órgãos de inteligência nacionais e internacionais e com outras instituições, no que se refere às questões de segurança institucional;
- XIX - orientar e apoiar as unidades do MPF nas questões de segurança institucional, sobretudo em situações de emergência;
- XX - propor uma Política de Contrainteligência para o MPF, que proporcione a salvaguarda dos interesses da Instituição;
- XXI - elaborar e implementar o Plano de Segurança Orgânica da PGR;
- XXII - levantar informações e desenvolver ações de inteligência com vistas a subsidiar as atividades de segurança institucional, quando autorizado pelo Procurador-Geral da República ou pelo Secretário-Geral;
- XXIII - planejar e executar ações relativas à obtenção e integração de dados e informações, produzindo conhecimentos para a segurança institucional;
- XXIV - acompanhar, permanentemente, os cenários de interesse do MPF, no que se refere à segurança institucional, de modo a proporcionar suporte adequado ao desempenho das funções;

- XXV - desenvolver atitudes favoráveis ao cumprimento de normas de segurança no âmbito do MPF, estimulando o comprometimento e o apoio das áreas do MPF; e
- XXVI - desenvolver outras atividades correlatas determinadas pelo Procurador-Geral da República ou pelo Secretário-Geral.

2.1.2 Compete às Unidades de Segurança das PRRs e das PRs:

- I - planejar, coordenar, executar, orientar e supervisionar as atividades de segurança institucional no âmbito da respectiva unidade do MPF;
- II - assessorar o Procurador-Chefe nas questões relativas à segurança institucional;
- III - elaborar e implementar o Plano de Segurança Orgânica da respectiva unidade do MPF, observando as recomendações da Unidade de Segurança Institucional;
- IV - subsidiar as respectivas PRMs na elaboração dos Planos de Segurança Orgânica;
- V - orientar e apoiar as respectivas PRMs no que se refere as questões de segurança institucional, assim como em situações de emergência e nos casos de ameaça;
- VI - acompanhar os cenários regionais e locais de interesse do MPF, no que se refere à segurança, a fim de proporcionar suporte ao desempenho das funções institucionais;
- VII - realizar a fiscalização documental, fiscal e física dos contratos de segurança e bombeiro civil da respectiva Unidade Gestora do MPF;
- VIII - seguir as recomendações e orientações técnicas da Unidade de



Segurança Institucional e com ela compartilhar conhecimentos, dados e informações, sem prejuízo da subordinação administrativa à respectiva unidade do MPF;

- IX - executar atividades de assessoria técnica de segurança;
- X - planejar e executar, quando assim determinado pelo Procurador-Geral da República, Secretário-Geral ou Procurador-Chefe, atividade de proteção de membros, de servidores e, se necessário, de seus familiares, para garantia do exercício das funções institucionais;
- XI - supervisionar e avaliar, quando solicitado, as medidas de proteção adotadas em favor de membros, servidores e seus familiares;
- XII - propor, em conjunto com os setores da unidade do MPF, o estabelecimento das normas de segurança para cada grupo de medidas de segurança previstos na Política de Segurança Institucional;
- XIII - promover a conscientização dos integrantes da Instituição quanto à importância da segurança institucional;
- XIV - supervisionar, coordenar e fiscalizar as atividades de segurança institucional desenvolvidas nos setores da unidade do MPF;
- XV - levantar informações e desenvolver ações de inteligência com vistas a subsidiar as atividades de segurança institucional, quando autorizado pelo Procurador-Chefe;
- XVI - planejar e executar ações relativas à obtenção e integração de dados e informações, produzindo conhecimentos para a segurança institucional;
e
- XVII - desenvolver outras atividades correlatas determinadas pelo Procurador-Chefe.

2.1.3 Compete ao Coordenador de PRM ou a outro servidor designado:

- I - planejar, coordenar, executar, orientar e supervisionar as atividades de segurança institucional no âmbito da PRM;
- II - assessorar o Procurador responsável pela segurança da PRM nas questões relativas à segurança institucional;
- III - acompanhar os cenários locais de interesse do MPF, no que se refere à segurança, a fim de proporcionar suporte ao desempenho das funções institucionais;
- IV - realizar a fiscalização documental, fiscal e física dos contratos de segurança e bombeiro civil da PRM;
- V - elaborar e implementar o Plano de Segurança Orgânica da PRM, observando as recomendações da Unidade de Segurança Institucional e da Unidade de Segurança da PR no Estado;
- VI - seguir as recomendações e orientações técnicas da Unidade de Segurança da PR no Estado e com ela compartilhar conhecimentos, dados e informações;
- VII - propor, em conjunto com os setores da PRM, o estabelecimento das normas de segurança para cada grupo de medidas de segurança previstos na Política de Segurança Institucional;
- VIII - promover a conscientização dos integrantes da Instituição quanto à importância da segurança institucional;
- IX - supervisionar, coordenar e fiscalizar, tecnicamente, as atividades de segurança institucional desenvolvidas nas áreas da PRM; e



X - desenvolver outras atividades correlatas determinadas pelo Procurador-Chefe ou pelo Procurador responsável pela segurança da PRM.

2.1.4 Sem prejuízo das atribuições das Unidades de Segurança e da Coordenação de PRM, os setores de cada unidade do MPF serão responsáveis pela aplicação das normas de segurança institucional, assim como pela propositura e implementação de outras medidas de segurança específicas em sua esfera de atribuições.

CAPÍTULO III

Gestão Estratégica

O planejamento estratégico de segurança institucional tem a finalidade de atender às diretrizes elencadas na Política de Segurança Institucional por meio de ações e projetos que devam ser implementados em cada unidade do MPF.

3.1 | Objetivo Estratégico Geral

3.1.1 Objetivo: fortalecer a segurança institucional.

3.1.2 Descrição: estruturar um sistema capaz de garantir, de modo efetivo, a segurança de pessoas (membros, servidores, terceirizados e estagiários), dados, informações, materiais, processos, documentos, áreas e instalações de todas as unidades do MPF, além de criar e desenvolver uma cultura de segurança institucional apta, entre outras coisas, a manter todo

o corpo funcional do MPF em permanente atenção no cuidado com as questões afetas a tal objetivo estratégico.

3.2 | Objetivos Estratégicos Específicos

3.2.1 objetivo estratégico geral desdobra-se nos seguintes objetivos estratégicos específicos:

- I - normatizar os itens de segurança previstos nos grupos de medidas de segurança;
- II - capacitar recursos humanos para atividades referentes à segurança institucional;
- III - desenvolver a consciência da segurança institucional no MPF;
- IV - realizar planejamento de contingência para processos sensíveis;
- V - implementar o Plano de Segurança Orgânica em todas as unidades do MPF;
- VI - estabelecer uma doutrina de segurança específica para o MPF;
- VII - desenvolver cenários de segurança;
- VIII - estruturar a segurança institucional do MPF;
- IX - dotar a Instituição de meios que permitam desenvolver a atividade de segurança nas melhores condições;
- X - estabelecer estruturas de gerência, auditoria e validação de processos; e
- XI - estabelecer processos de gestão de riscos.



3.2.2 A Unidade de Segurança Institucional deverá desenvolver ações estratégicas, por meio de programas e projetos, para atender a cada um dos objetivos estratégicos específicos.

3.3 | Plano de Segurança Orgânica

O Plano de Segurança Orgânica – PSO, composto por normas e procedimentos de segurança das unidades do MPF, deve ser orientado para as necessidades e especificidades locais.

3.3.1 O PSO será integrado por:

- I - normas de segurança para cada grupo de medidas de segurança e anexos que regulamentem procedimentos de proteção relativos a cada grupo de medidas;
- II - regras de segurança para orientação de portarias que regulamentem assuntos locais; e
- III - atribuições de responsabilidade.

3.3.2 A implementação do PSO é de responsabilidade de cada unidade do MPF, que contará com o apoio técnico (modelo de plano, capacitação e revisão) da Unidade de Segurança Institucional.

3.4 | Doutrina de Segurança Institucional

A doutrina de segurança institucional traduz a consolidação dos princípios, conceitos básicos, procedimentos, orientações, metodologias e processos referentes à área de segurança que viabilizem o adequado cumprimento da missão do

MPF. A sua codificação em cadernos doutrinários e manuais técnicos permite a divulgação do conhecimento e a padronização de procedimentos.

O detalhamento da normatização dos procedimentos de segurança constantes neste Plano constitui-se em documentação para orientar e regular as atividades de segurança a serem executadas, tais como Assessoria Técnica de Segurança, Operação de Segurança, Visita de Avaliação de Segurança, Gestão de Riscos, Oficina de Lições de Segurança Institucional Aprendidas e outros eventuais projetos desenvolvidos pela unidade. Poderá, ainda, abordar os demais aspectos ligados ao tema, para as diversas unidades do MPF.

3.5 | Cenários de Segurança

A Unidade de Segurança Institucional, com a colaboração das Unidades de Segurança das PRRs e PRs, deverá criar cenários de segurança com o objetivo de orientar os trabalhos, tanto os específicos de segurança, quanto os rotineiros dos membros e servidores das unidades do MPF.

Tais cenários, além de fornecerem subsídios para a elaboração de planejamentos de segurança, permitirão melhor ambientação dos Procuradores da República, ao serem removidos para determinada unidade ou por ocasião de sua primeira lotação.

3.6 | Gerência e Validação de Processos

Os sistemas e os serviços necessários ao MPF, que envolvam aspectos de segurança, devem possuir gerência definida e, ainda, serem submetidos à avaliação de conformidade de critérios e à validação de processos.

Os sistemas e serviços das unidades do MPF, que envolvam quesitos de segurança e cujo incidente possa redundar em interrupção ou prejuízo e causar impactos negativos à Instituição, devem ser mapeados e identificados.

Após a identificação dos sistemas e serviços, deverá ser designada uma gerência para exercer os controles de segurança e realizar as auditorias e a validação de processos. A gerência será responsável pelo acompanhamento do sistema ou serviço e por realizar as modificações e aperfeiçoamentos necessários à sua otimização.



As auditorias têm caráter interno e deverão ser realizadas periodicamente, visto que objetivam analisar criticamente os processos, atividades, ações e procedimentos do próprio sistema ou serviço e de seus operadores, verificando se estão em conformidade. Os relatórios decorrentes das auditorias deverão formar um registro para consultas posteriores, formando um banco de dados que poderá subsidiar a administração das unidades do MPF em decisões futuras.

A validação de processos tem por finalidade verificar se o sistema ou o serviço cumpre com a finalidade de atender aos requisitos da segurança institucional.

CAPÍTULO IV

Segurança Institucional

4.1 | Medidas de Segurança

A Segurança Institucional compreende o conjunto de medidas de segurança orgânica e de segurança ativa.

4.1.1 A segurança orgânica é composta pelos seguintes grupos de medidas:

- I - segurança de recursos humanos;
- II - segurança de materiais;
- III - segurança das áreas e instalações; e
- IV - segurança da informação, que se desdobra em:
 - a) segurança da informação nos meios de tecnologia da informação;

- b) segurança da informação no pessoal;
- c) segurança da informação na documentação; e
- d) segurança da informação nas áreas e instalações.

4.1.2 A segurança ativa é composta pelos seguintes grupos de medidas: contrassabotagem e contraespionagem.

4.1.3 Na implementação das medidas de segurança, além das normas constitucionais e legislação infraconstitucional, deverão ser observados a Política de Segurança Institucional, o Plano de Segurança Institucional, os Planos de Segurança Orgânica, os atos normativos expedidos pelo Procurador-Geral da República, pelo Secretário-Geral e pelos Procuradores-Chefes, as ordens de serviço, os procedimentos operacionais padrão, as orientações técnicas, as instruções e as rotinas.

4.2 | Segurança de Áreas e Instalações e Segurança da Informação nas Áreas e Instalações

A Segurança de Áreas e Instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade do MPF ou onde se realizem atividades de interesse da Instituição.

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.

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



interagem com os demais grupos de medidas, integrando a segurança como um todo.

A 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.

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

4.2.1 A Segurança das Áreas e Instalações engloba:

- I - Sistema Físico: composto por vigilantes que executam diversos serviços de vigilância;
- 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 etc; e
- III - Sistema de Barreiras: envolve as diversas barreiras para segurança dos perímetros.

4.2.2 Barreiras e Instalações Físicas

As unidades do MPF devem seguir as seguintes orientações:

- I - Devem-se instalar barreiras para impedir o acesso físico de pessoas não autorizadas às instalações das unidades do MPF. As barreiras são obstáculos de qualquer natureza que impedem, dificultam ou detectam os acessos físicos que podem se constituir em uma ameaça.
- II - Os perímetros das unidades do MPF 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. Em áreas de alto risco de invasão, as cercas ou muros podem conter concertinas ou cercas elétricas nas suas extremidades. Nos casos em que existem cercas eletrificadas, devem ser afixados avisos de advertência ao longo de todo 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 MPF.
- V - Os prédios e instalações devem possuir serviço de portaria com equipamentos: computadores e telefone, sistema para cadastro de pessoal.
- 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 nas unidades do MPF.
- IX - O cabeamento da rede elétrica ou do sistema de CFTV, quando houver, 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. 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, quando necessário.
- 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. Respeitando-se a arquitetura das edificações, as áreas de atendimento ao público, cantina, restaurante, setor de comunicação social, sala do Plan-Assiste, serviço de saúde e outras repartições de uso similar devem ser dispostas em locais que evitem o trânsito de visitantes por instalações sensíveis.
- XVI - As unidades do MPF 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 - As unidades do MPF devem regular em seus respectivos Planos 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 e, se necessário, posto armado, além de controle específico de chaves, CFTV e fechadura eletrônica.

4.2.3 Controle de Acesso

As unidades do MPF devem seguir as seguintes orientações:

- I - As entradas dos prédios ou instalações devem possuir um serviço de portaria, com vigilante 24 horas, destinado à segurança do local.
- II - As portarias de acesso devem ter um serviço de recepcionistas, para realizar o registro de visitantes que entram no prédio. Os registros devem 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. Tais registros devem ser realizados, preferencialmente, por meio de sistemas informatizados que permitam fotografar os visitantes ou digitalizar documentos de identificação. Antes do acesso do visitante à área desejada, deve ser feito contato com uma pessoa do setor de destino para a devida autorização. 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.
- III - As portarias das unidades devem possuir um sistema de catracas com leitores de cartão (ou similar) para registros de servidores, estagiários, prestadores de serviço, adolescentes aprendizes, terceirizados e visitantes.
- IV - É obrigatório o uso de crachá de identificação para acesso às áreas e instalações das unidades do MPF e permanência em seu interior, exceto pelos membros do MPF que poderão utilizar credencial específica.
- V - 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.
- VI - As portas devem possuir dispositivos de fechadura com chave. As janelas devem possuir dispositivos de fechadura com trancamento interno.



Locais que exigem maior controle de acesso devem possuir fechadura eletrônica controlada por equipamento de controle de acesso e os relatórios de acesso devem ser auditados periodicamente.

- VII - A entrada de servidores e estagiários em dias e horários sem expediente ou após o expediente deve ser regulada e controlada. Os dados de acesso devem constar em registro específico. Terceirizados não devem acessar as áreas e instalações das unidades do MPF nos dias e horários sem expediente, exceto em situações de prestação de serviços devidamente autorizados e monitorados.
- VIII - O estacionamento das unidades do MPF deve ter o seu procedimento de controle de acesso regulado por norma específica. A entrada e a saída de veículos devem ser registradas em controle específico.
- IX - 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. Quando for necessário tal acesso, este deve ser feito por vigilantes e com controle de registro. Os relatórios de acesso a claviculários devem ser auditados periodicamente.
- X - Os registros de retirada e entrega de chaves devem possuir itens de controle que permitam auditorias posteriores.
- XI - As áreas que abriguem instalações sensíveis e que sejam de acesso restrito devem ser sinalizadas com placas indicativas desta situação.
- XII - Nos casos necessários, o acesso a determinadas áreas será condicionado à credencial de segurança compatível com o grau de sigilo do local.
- XIII - Os locais onde se processam dados e informações sigilosas devem ser separados fisicamente de locais onde trabalham terceirizados.
- XIV - 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.

- XV - A presença de fornecedores nas unidades do MPF deve ser sempre acompanhada de um servidor ou vigilante previamente designado.
- XVI - O material do patrimônio somente poderá sair de uma unidade com autorização da área competente, devendo ser registrado na portaria.
- XVII - Não será permitido o ingresso de pessoas nas unidades do MPF portando arma de qualquer natureza, ressalvados os seguintes casos: membros do Ministério Público; membros da magistratura; oficiais das Forças Armadas; policiais Federais, Cíveis e Militares; servidores com atribuição de segurança do MPF; profissionais de segurança de empresas de escolta de cargas e valores e vigilantes da segurança contratada, quando em serviço; outros profissionais de segurança, participantes de solenidades ou eventos promovidos pelo MPF, desde que previamente autorizados; e os demais casos amparados pela Lei nº 10.826/2003. Não será permitido o acesso de tais pessoas armadas, se forem investigadas ou acusadas em quaisquer espécies de procedimentos instaurados pelo MPF. Em qualquer hipótese, as armas deverão ser portadas de forma velada, salvo se acondicionadas de maneira própria nas vestimentas especialmente talhadas para tanto, a exemplo de fardas e uniformes militares e/ou operacionais. Salvo nos casos expressamente permitidos, aquele que for oficialmente autorizado a portar arma, será orientado a depositá-la, após o respectivo desmuniamento, em cofre com abertura digital, localizado nas dependências da unidade mediante registro pela vigilância, para que possa transitar pelas dependências do MPF.
- XVIII - Os profissionais de segurança de empresas de escolta de cargas e valores deverão ser acompanhados por vigilante, sendo proibida a transferência de valores entre caminhões caixa-forte nas dependências do MPF. Os profissionais deverão ser orientados quanto ao horário de realização do serviço e o itinerário a ser percorrido nas unidades do MPF, evitando



ao máximo a circulação em horários de grande deslocamento ou aglomeração de servidores.

- XIX - As portarias de acesso das unidades do MPF devem possuir cofre com abertura digital ou, na sua ausência, artefato similar para guarda de armas, assim como uma caixa de descarga para ações de desmuniamento do armamento, que deve ser instalada em local reservado.
- XX - É vedado o ingresso nas dependências das unidades do MPF de pessoas: para a prática de comércio e propagandas diversas ou angariação de donativos e congêneres, salvo as campanhas institucionais; para a prestação de serviços autônomos não vinculados a contrato ou convênio firmado com o MPF; fazendo uso de trajas inadequados, incompatíveis com o decoro, ou de vestimenta que possa atentar contra a moralidade do serviço público, respeitadas as especificidades culturais; portando instrumentos sonoros, fogos de artifícios ou quaisquer objetos que por sua natureza representem risco à incolumidade física ou patrimonial e perturbem o andamento dos serviços; com qualquer espécie de animal, salvo cão-guia de pessoa portadora de deficiência visual, mediante apresentação da carteira de vacina atualizada do animal; e que sejam identificadas como possível ameaça à segurança, à ordem, à integridade patrimonial e física nas dependências da Instituição e cuja forma de apresentação ou atitudes forem consideradas suspeitas para os fins propostos, caso em que o responsável pela segurança na unidade será imediatamente acionado.
- XXI - Sempre que as condições técnicas permitirem, os sistemas de registro de pessoas nas portarias das unidades do MPF devem ser integrados a sistemas de identificação de pessoas e pesquisa de antecedentes.
- XXII - Em situações de solenidades e eventos organizados nas unidades do MPF, os integrantes de serviços de segurança armada de autoridades devem ser previamente identificados para eventuais autorizações de entrada e permanência com armamento.

- XXIII - O ingresso de equipamentos de propriedade e de uso particular nas dependências do MPF deverá ser precedido de registro nas portarias de acesso. A saída dos equipamentos particulares deverá ser autorizada somente mediante a apresentação do protocolo de registro ou documento comprobatório da propriedade do bem.
- XXIV - Não é permitida a filmagem ou fotografia no interior das unidades do MPF sem prévia autorização da autoridade competente, comunicada à respectiva área de segurança institucional.
- XXV - A cobertura jornalística, filmagem e fotografia realizadas nas dependências do MPF serão feitas por profissionais de imprensa previamente credenciados pelo setor de comunicação social da unidade, que deverá manter informada a respectiva área de segurança institucional.

4.2.4 Sistemas de Vigilância Eletrônica

As unidades do MPF devem seguir as seguintes orientações:

- I - As unidades do MPF, em regra, devem possuir um sistema de Circuito Fechado de Televisão - CFTV com cobertura das áreas e locais sensíveis. Obrigatoriamente, este sistema deve monitorar o perímetro externo, estacionamentos, portarias, entradas de instalações sensíveis (almoxarifado, gabinetes de Procuradores, ASSPA etc.), interior da sala de equipamentos de informática, Centro de Processamento de Dados - CPD, interior da sala da central telefônica, locais de circulação e locais de atendimento ao público.
- II - Os sistemas de CFTV devem ser monitorados em tempo real e possuir capacidade de armazenar, no mínimo, cento e oitenta dias de gravação de imagens de forma ininterrupta. As salas destinadas aos equipamentos de CFTV devem ter o acesso restrito por sistema de controle de acesso.
- III - O acesso aos itens de configurações do sistema de CFTV ou opções de



edição de imagens é restrito ao responsável pela Unidade de Segurança ou servidor autorizado. Os terceirizados, envolvidos em atividades de segurança, somente poderão ter acesso ao sistema de CFTV para visualização das imagens em tempo real. As imagens do CFTV devem ser classificadas e armazenadas em locais com acesso restrito. O acesso às imagens gravadas pelo CFTV é vinculado à necessidade do serviço e deve ser autorizado pela autoridade competente. 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 Secretário-Geral ou pelo Procurador-Chefe.

- IV - As salas que abrigam instalações sensíveis - como servidores de informática, CPD, almoxarifado, ASSPA, central telefônica - devem possuir, sempre, sensores de presença ligados a central de alarme e sistema de controle de acesso, com suporte a registro dos acessos permitidos e das tentativas de acesso inválidas.
- V - Os perímetros externos ou áreas sensíveis no interior das unidades do MPF, sempre que necessário, devem ser monitoradas por sensores de presença ligados a central de alarme.
- VI - Em caso de utilização de alarme, a central deve ser monitorada por vigilante durante 24 horas por dia, 7 dias por semana.

4.2.5 Serviço de Segurança dos Vigilantes

As unidades do MPF devem seguir as seguintes orientações:

- I - Os perímetros das unidades do MPF devem ser protegidos por um serviço de vigilantes. A disposição dos respectivos postos deve ser meticulosa e judiciosamente avaliada.
- II - Os Procedimentos Operacionais Padrão para cada posto de segurança

devem conter os seguintes dados: composição do posto, discriminando o número de vigilantes; finalidade do posto; atribuições dos vigilantes, com detalhamento do que os vigilantes fazem no local; procedimentos comportamentais, em que são discriminados os procedimentos em relação ao tratamento com pessoas, apresentação individual e outros; e procedimentos operacionais, em que é detalhado o que fazer em diversas situações.

- III - Nas unidades do MPF com elevado número de vigilantes, deve-se prever no respectivo instrumento um supervisor para fiscalizar o serviço dos vigilantes e fazer cumprir as normas de segurança por eles.
- IV - 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 serviço de segurança.
- V - Os postos de vigilância devem ser dotados de um equipamento de comunicação para uso dos vigilantes, ligado à área de segurança da unidade do MPF.

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

As unidades do MPF devem seguir as seguintes orientações:

- I - Todas as unidades do MPF devem possuir um planejamento de prevenção e combate a incêndio em conformidade com a legislação e com as normas técnicas em vigor. Os planos devem ser simples, exequíveis, viabilizar ações com pessoal e material existentes 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. Os relatórios de manutenções preventivas programadas ou corretivas devem ser arquivados. Devem ser realizados testes periódicos, simulando incêndio, previstos em cronogramas de manutenção preventiva.
- IV - As condições de manutenção e recarga dos extintores de incêndio devem ser verificadas periodicamente. Especial atenção deve ser dada aos contratos de manutenção e aos seus prazos.
- V - A sinalização de segurança contra incêndio e pânico deve ser disposta nas instalações das unidades, para orientação do pessoal em situações de emergência.
- VI - Cada unidade do MPF deve possuir um serviço de Bombeiro Voluntário, com a participação de servidores e treinamento específico.
- VII - As saídas de emergência não podem ser obstruídas com equipamentos, móveis ou outro tipo de material que impeça a livre movimentação de pessoas.
- VIII - 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.
- IX - A área de segurança de cada unidade do MPF deve prever planejamento de capacitação para os integrantes da Brigada de Combate a Incêndio.
- X - Os equipamentos e a sinalização de prevenção e combate a incêndio devem ser instalados nas dependências das unidades do MPF e verificados periodicamente, em particular: sistema de detecção com alarme de incêndio; rede de hidrantes e extintores; rede de sprinklers; e sinalização de segurança contra incêndio e pânico.

- XI - 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. Tais procedimentos devem ser executados e treinados sistematicamente pelos integrantes da área de segurança e Brigada de Combate a Incêndio. Em cada treinamento, os itens a seguir relacionados 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 MPF; procedimentos para evacuação das instalações; e procedimentos para trato com o objeto da emergência.
- XII - Devem ser realizados exercícios de evacuação das dependências, de acordo com as especificidades locais.
- XIII - As unidades do MPF devem possuir iluminação auxiliar para situações de emergência, independente da rede de energia elétrica convencional.
- XIV - Os sistemas essenciais que constem na infraestrutura crítica do MPF devem possuir dispositivos de *no break* que evitem interrupção do serviço.
- XV - As unidades do MPF devem possuir um planejamento para situações extraordinárias e de emergência, que inclua evacuação de pessoal, documentos sigilosos e equipamentos sensíveis das instalações.

4.2.7 Auditoria em Serviços e Planejamentos

As unidades do MPF devem seguir as seguintes orientações:

- I - Devem ser auditados periodicamente os seguintes serviços e sistemas de segurança em funcionamento nas unidades do MPF: controle de acesso nas portarias; controle de acesso de veículos nas garagens ou estacionamento; controle de acesso de servidores e estagiários em dias ou



horários sem expediente; controle de acesso a áreas e instalações sensíveis; controle de acesso aos claviculários; controle de saída de material do patrimônio; verificação do funcionamento dos equipamentos dos sistemas de detecção de intrusão; verificação do funcionamento dos equipamentos do sistema de CFTV; e verificação do funcionamento dos equipamentos do sistema de prevenção e combate a incêndio.

- II - Os planejamentos de contingência ou de emergência devem ser revistos periodicamente, avaliando-se a pertinência de seu conteúdo. 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.

4.2.8 Prescrições Diversas

As unidades do MPF devem seguir as seguintes orientações:

- I - As pessoas que trabalham em cantinas, restaurantes ou postos avançados de agência bancária nas dependências da unidade do MPF devem ser registradas na respectiva área de segurança e possuir crachá de identificação.
- II - As unidades do MPF devem possuir um número de telefone destinado a emergências, que deverá ser amplamente divulgado entre os integrantes da unidade.
- III - Os projetos de construção e ocupação de áreas das unidades do MPF 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; e
 - f) áreas de atendimento ao público: devem ser posicionadas em local que evite o fluxo de pessoas pelo interior da unidade do MPF.
- IV - Os projetos de arquitetura para construções de unidades do MPF devem prever layouts de ambientes internos que privilegiem os aspectos de segurança.
- V - A Unidade de Segurança 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 MPF, com a devida coordenação de ações entre os dois setores para a execução de projetos de construção, desde a sua primeira etapa.
- VI - As unidades do MPF devem 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.
- VII - As informações sobre o fluxo de circulação de pessoas nas dependências das unidades do MPF, 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.



4.3 | Segurança do Material

A segurança do material é um conjunto de medidas de segurança voltadas para proteger o material pertencente ou em uso no MPF. O material constitui-se em um ativo economicamente importante para a Instituição, englobando genericamente os equipamentos, componentes, acessórios, mobiliários, veículos, matérias-primas, armas de fogo, munições e demais itens empregados nas atividades da Instituição.

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

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

4.3.1 Além dos procedimentos de controle patrimonial previstos em ato normativo específico da PGR, devem ser adotadas as seguintes medidas:

- I - A produção (quando for o caso), 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. O acesso às áreas ou locais de armazenamento ou acondicionamento de tais materiais deve ser restrito, com a devida sinalização.
- III - As áreas de segurança das unidades do MPF devem expedir orientação para membros, servidores, estagiários, prestadores de serviços voluntários,

menores aprendizes e terceirizados a respeito de medidas adicionais de segurança a serem atendidas em face das características técnicas de cada material.

- IV - 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. O emprego de medidas adicionais de segurança será proporcional à sensibilidade do material, ao seu valor, à relevância da informação nele contida ou ao impacto de sua subtração para a Instituição.
- V - A saída de material das unidades do MPF deve atender normas administrativas e constar em registro, mantido pelas áreas de segurança das unidades, em conjunto com os demais setores.
- VI - Equipamentos e outros materiais portáteis, em viagens, devem ser conduzidos como bagagem de mão.
- VII - A doação de material seguirá norma administrativa específica. A respectiva Unidade de Segurança realizará visita inopinada à entidade recebedora da doação para certificação das condições exigidas em norma, expedindo relatório. O material a ser doado contendo dados e informações sigilosos deve ter o seu conteúdo descartado pela área competente de forma segura antes da sua entrega.
- VIII - Todo incidente de segurança envolvendo material deve ser informado às áreas de segurança das unidades do MPF.
- IX - 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.



- X - O armazenamento ou o acondicionamento de materiais que exijam condições especiais deve seguir o constante em normas técnicas específicas.
- XI - Os equipamentos e outros materiais do MPF devem ser instalados de forma a reduzir riscos ambientais em caso de um incidente de segurança; reduzir acessos desnecessários às áreas de trabalho; permitir a sua utilização de forma segura; e atender parecer técnico da área específica.
- XII - Todos os equipamentos ou outros materiais que exijam cuidados de manutenção devem ser incluídos em planejamentos de manutenção coordenados pelas respectivas áreas responsáveis.
- XIII - Os equipamentos e outros materiais que exijam capacitação técnica para sua operação somente podem ser utilizados por pessoa capacitada.
- XIV - As atividades de operação e manuseio de equipamentos e outros materiais nas unidades do MPF devem estar em conformidade com as normas de segurança no trabalho.
- XV - As bibliotecas das unidades do MPF devem possuir sistemas de controle do acervo.
- XVI - 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 MPF 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.
- XVII - A Secretaria de Administração deverá estabelecer normas de controle e armazenamento de material.

4.4 | Segurança de Recursos Humanos e Segurança da Informação no Pessoal

A segurança de recursos humanos é um conjunto de medidas destinadas a proteger a integridade física de membros e servidores do MPF, assim como de seus respectivos familiares, quando comprometida em face do desempenho das funções institucionais.

Pela especificidade e circunstância do trabalho, é fundamental que os integrantes do MPF desenvolvam uma cultura de conscientização e sensibilização quanto às prováveis ameaças, estabelecendo procedimentos de proteção e preservação de sua integridade física.

A segurança da informação no pessoal refere-se ao conjunto de medidas voltadas a estabelecer comportamentos adequados dos integrantes do MPF que proporcionem a proteção da informação. Engloba medidas de segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição.

As normas de segurança deste item reduzem a possibilidade de ingresso de pessoas nos quadros do MPF envolvidas com atores adversos ou que possam causar comprometimento da segurança para a Instituição, assim como orientam as chefias a respeito da seleção, acompanhamento e desligamento de servidor, estagiário ou prestador de serviço no exercício de suas funções.

Os recursos humanos constituem-se no ativo mais importante do MPF, o que requer medidas especiais para sua proteção e para o estabelecimento de normas de segurança. Programas de capacitação e treinamento voltados para aspectos de segurança devem ser desenvolvidos em coordenação com a Unidade de Segurança Institucional, com a finalidade de se buscar uma atitude de segurança adequada.

A seguir serão elencadas as principais medidas de segurança de recursos humanos e de segurança da informação no pessoal.

4.4.1 Segurança da Integridade Física

As unidades do MPF devem seguir as seguintes orientações:



- I - A Unidade de Segurança Institucional expedirá orientações a respeito da conduta a ser observada pela pessoa que estiver submetida ao sistema de proteção.
- II - Deverão ser elaborados atos normativos específicos para otimizar as ações de proteção pessoal e padronizar procedimentos.
- III - Os servidores, estagiários, vigilantes, recepcionistas e terceirizados devem ser orientados a respeito das normas de segurança do MPF, notadamente sobre a necessidade de: não fornecer dados pessoais de integrantes do MPF aos solicitantes, pessoalmente ou via telefone; não informar aos solicitantes horários de chegada, saída ou presença de integrantes do MPF nas unidades sem antes solicitar autorização para tal; não permitir a visita a integrantes do MPF sem prévia autorização do interessado; não fornecer informações sobre rotinas internas das unidades do MPF; registrar o ingresso e saída de todos os visitantes em controle específico; monitorar, por meio de CFTV, o deslocamento de visitantes no interior das dependências do MPF; somente autorizar a entrada de pessoas armadas de acordo com o previsto em ato normativo específico; e fazer verificação detalhada de documentação apresentada pelos visitantes.
- IV - As informações que possam revelar dados pessoais que comprometam a segurança individual de integrantes do MPF não poderão constar nas páginas eletrônicas da Instituição.
- V - A área de segurança de cada unidade deverá expedir orientação ao pessoal sobre procedimentos a serem executados em caso de emergência.

4.4.2 Segurança no Processo Seletivo

As unidades do MPF devem seguir as seguintes orientações:

- I - Os concursos de admissão para as carreiras de membros e servidores do MPF devem conter medidas e procedimentos em seus respectivos

editais que contemplem ações para evitar o ingresso de pessoas com características ou antecedentes que possam comprometer a segurança da Instituição. Inclui a realização de sindicância de vida pregressa e investigação social para os aprovados por ocasião da convocação. O resultado da pesquisa deverá ser levado em conta para a posse. Procedimento similar será executado para contratação de pessoas em cargos comissionados.

- II - A documentação normativa sobre o concurso regulará a sindicância de vida pregressa e investigação social. 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, sendo emitido parecer para a comissão de concurso ou autoridade contratante.
- III - Na escolha de servidor para as funções que envolvam o trato com assuntos sigilosos ou sensíveis, devem ser considerados, entre outros, os seguintes aspectos: tarefas sensíveis pertinentes à função; grau de acesso a assuntos sigilosos pelo servidor; capacidade de iniciativa e decisão do servidor; concessão de credencial de segurança; e investigação social atualizada.
- IV - As funções que pela sua natureza exigem avaliação psicológica para ingresso no MPF devem constar em seus respectivos editais de concurso, a critério da autoridade superior.

4.4.3 Segurança no Desempenho das Funções

As unidades do MPF devem seguir as seguintes orientações:

- I - Os novos integrantes do MPF devem ser submetidos a um curso de ingresso ou adaptação, 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 prestadores de serviço do MPF assinarão Termo de Compromisso de Manutenção do Sigilo -TCMS. Nos casos de exercício de função que trate diretamente com assuntos sigilosos, além da assinatura de TCMS atualizado, deve-se exigir ainda a credencial de segurança.
- III - Os integrantes do MPF que desempenham função com acesso a dados e informações sigilosas devem ser submetidos a avaliação periódica para renovação da credencial de segurança. As vulnerabilidades pessoais que possam comprometer o desempenho da função na Instituição devem ser observadas e consideradas para renovação da credencial.
- IV - Todos os integrantes do MPF que possuam credencial de segurança serão submetidos periodicamente a treinamento específico para o trato com assuntos sigilosos.

4.4.4 Segurança no Desligamento

As unidades do MPF devem seguir as seguintes orientações:

- 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.
- III - Para efeito do item anterior, as chefias imediatas e os setores de recursos humanos devem informar aos gerentes de cada sistema ou serviço sobre o afastamento das funções por membros e servidores. Os gerentes de cada sistema ou serviço que trate de assuntos sigilosos devem auditar

periodicamente os seus respectivos sistemas ou serviços para identificar acessos indevidos.

- IV - Em situações de desligamento de membro, servidor, estagiário ou prestadores de serviço da Instituição, devem ser adotadas medidas de segurança adicionais, tais como: entrevista com o desligado, orientando-o sobre a necessidade de manter discrição sobre os assuntos institucionais; verificação de entrega de material ou equipamento acautelado com o desligado; verificação da existência de pendências de ordem individual na Secretaria de Gestão de Pessoas; e verificação da existência de pendências em projetos, serviços ou trabalhos realizados pelo desligado.

4.4.5 Credencial de Segurança

As unidades do MPF devem seguir as seguintes orientações:

- I - A credencial de segurança é um documento que habilita membros, servidores, estagiários e prestadores de serviços do MPF 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 MPF 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. É vinculado à credencial de segurança o compromisso de manutenção do sigilo, consubstanciado em termo próprio.
- II - A credencial de segurança será objeto de regulamentação em ato normativo específico do MPF, 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 MPF.
- VI - Os servidores públicos externos à Instituição que necessitarem, em razão do serviço, ter acesso a assuntos sigilosos referentes ao MPF somente podem acessar dados e informações sigilosos 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 MPF e à assinatura do Termo de Compromisso de Manutenção do Sigilo.

4.4.6 Termo de Compromisso de Manutenção do Sigilo

As unidades do MPF devem seguir as seguintes orientações:

- I - 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.
- II - 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.

- III - Compete à Unidade de Segurança Institucional elaborar o(s) modelo(s) de TCMS, que serão disponibilizados a todas as unidades do MPF.
- IV - O TCMS deve ser arquivado em local seguro e estar disponível para consulta e auditoria.
- V - As empresas ou órgãos contratados ou conveniados e seus respectivos empregados ou servidores, devem assinar o TCMS quando, por necessidade do serviço junto ao MPF, tiverem acesso a informações sigilosas.

4.5 | Segurança da Informação nos Meios de Tecnologia da Informação

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.

Ressalta-se que os recursos de tecnologia da informação disponíveis no MPF destinam-se exclusivamente ao suporte das atividades desempenhadas pelos membros, servidores e estagiários.

A seguir são relacionadas medidas de segurança da informação nos meios de tecnologia da informação.

4.5.1 Uso de Recursos de Tecnologia da Informação

As unidades do MPF devem seguir as seguintes orientações:

- I - Os recursos de informática e comunicações disponíveis para os usuários do MPF 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 comunicando qualquer defeito ou comportamento anormal às áreas de tecnologia da informação das unidades do MPF.
- III - Os programas adquiridos pelo MPF 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 MPF. Apenas programas e sistemas homologados pela Secretaria de Tecnologia da Informação da Instituição podem ser instalados.
- IV - É vedada a instalação e/ou execução de qualquer outro programa ou sistema que não tenha sido adquirido ou desenvolvido pelo MPF, exceto em casos de comprovada necessidade do serviço, mediante anuência técnica das áreas de tecnologia da informação das unidades do MPF e com a autorização da autoridade competente. A autorização de instalação e/ou execução de programa ou sistema que não tenha sido adquirido ou desenvolvido pelo MPF será autorizado pelo Secretário-Geral, na Procuradoria-Geral da República, e pelos respectivos Procuradores-Chefes, nas demais unidades do MPF.
- V - As áreas de tecnologia da informação das unidades do MPF 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 patrimônio e das áreas de tecnologia da informação das unidades do MPF.

4.5.2 Segurança de Rede e Internet

As unidades do MPF devem seguir as seguintes orientações:

- 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 MPF 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. Para tanto, será elaborado ato normativo específico regulamentando o uso de tais recursos no âmbito do MPF. A Secretaria de Tecnologia da Informação e Comunicação - STIC deverá elaborar estudos e prover os meios necessários para viabilizar tais providências.
- III - A retirada de dados e informações sigilosos ou sensíveis da Rede Nacional do MPF 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 MPF.



- 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 chefia do setor do usuário às áreas de tecnologia da informação das unidades do MPF, informando o perfil de utilização. O desligamento ou afastamento da função deverá ser informado.
- VII - As senhas de acesso deverão ser individuais, sigilosas e intransferíveis. A STIC definirá as regras de formação de senhas e de suas reutilizações e período de validade.
- VIII - O acesso às redes institucionais e à Internet dar-se-á por meio disponibilizado e configurado pelas áreas de tecnologia da informação das unidades do MPF. 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. O acesso aos registros somente será realizado mediante autorização do Secretário-Geral.
- IX - É vedado o acesso às páginas ou serviços que possuam características diversas das atividades institucionais do MPF, 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 MPF, deverá ser realizada solicitação ao Secretário-Geral para a respectiva liberação.
- 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. É vedado o uso dos recursos do correio

eletrônico para a veiculação de mensagens desvinculadas do exercício das funções institucionais.

- XII - As áreas de tecnologia da informação das unidades do MPF poderão prover acesso sem fio às suas redes locais. Somente equipamentos autorizados e previamente homologados pelas áreas de tecnologia da informação das Procuradorias poderão atuar como pontos de acesso sem fio às redes locais.
- XIII - Os pontos de acesso sem fio às redes locais do MPF 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 MPF.
- XV - A configuração do dispositivo que irá realizar o acesso remoto será de responsabilidade do usuário solicitante, sob orientação da STIC ou das áreas de tecnologia da informação das unidades do MPF.
- 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 MPF.

4.5.3 Segurança de Mídias, Acesso Remoto e Auditoria

As unidades do MPF devem seguir as seguintes orientações:

- I - As mídias contendo dados e informações sigilosas devem ser protegidas durante o transporte externo às instalações das unidades do MPF. A proteção deverá ser realizada 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 MPF. Os recursos de tecnologia da informação que serão homologados para acesso remoto, bem como os perfis de usuários autorizados, serão definidos pela STIC. 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 STIC ou às áreas de tecnologia da informação das unidades do MPF, sendo tal acesso de uso exclusivo do usuário solicitante. A configuração do dispositivo que irá realizar o acesso remoto será de responsabilidade do usuário solicitante, sob orientação da STIC ou das áreas de tecnologia da informação das Procuradorias.
- 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 STIC e as áreas de tecnologia da informação das unidades do MPF poderão 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.

4.5.4 Segurança das Comunicações

As unidades do MPF devem seguir as seguintes orientações:

- I - É vedado o uso de aparelhos de telefones sem fio, exceto os DECT originais das próprias centrais telefônicas, nas unidades do MPF.
- 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. Preferencialmente, a instalação da central telefônica deve ser em racks com chave.
- III - Não é autorizado acesso remoto à central telefônica, inclusive por empregados de empresa de manutenção, sem monitoramento da ação pelas áreas de tecnologia da informação das unidades do MPF.
- 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 instalações físicas destinadas ao serviço de telefonistas e à central telefônica 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 - Os quadros de telefonia devem ser mantidos limpos e organizados. A planilha com identificação de ramais deve ser controlada pelo setor responsável pela central e não ser disponibilizada nos próprios quadros de telefonia.



- VIII - As empresas contratadas para realizar a manutenção da central telefônica e seus empregados que prestam serviço nas unidades do MPF devem assinar TCMS.
- IX - 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 serviço de segurança. A área de segurança das unidades do MPF deverá acompanhar o desempenho das funções com vistas a detectar eventuais vulnerabilidades.
- X - Os usuários de equipamentos de comunicações não deverão introduzir mensagens com conteúdo sigiloso ou sensível nas secretárias eletrônicas.
- XI - Os documentos sigilosos, salvo necessidade excepcional, não deverão ser transmitidos mediante equipamento de fac-símile.

4.5.5 Prescrições Diversas

As unidades do MPF devem seguir as seguintes orientações:

- I - Os usuários que necessitarem, devido à natureza de suas funções, de acesso privilegiado a recursos da rede do MPF deverão realizar solicitação formal ao Secretário de Tecnologia da Informação e Comunicação, apresentando os argumentos que justifiquem tal acesso. A STIC realizará registro de tais autorizações.
- 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 MPF, deverão ter seus dados eliminados de forma segura pelas áreas de tecnologia da informação das unidades.

- IV - As mídias inservíveis contendo dados e informações sigilosos ou sensíveis que por qualquer motivo devam ser destruídas, serão eliminadas de forma segura. As áreas de tecnologia da informação das unidades do MPF deverão 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 e prévia autorização da autoridade competente.
- VI - O ingresso e o uso de equipamentos de informática e periféricos particulares em unidades do MPF devem ser controlados. O material deverá ser registrado nas portarias das unidades do MPF pelo serviço de segurança e as respectivas áreas de tecnologia da informação comunicadas a respeito.

4.6 | Segurança da Informação na Documentação

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 MPF. Inclui, ainda, medidas de segurança no ato de produzir, classificar, tramitar, arquivar e destruir a documentação.

É relevante que se proceda à gestão documental para documentos ostensivos e sigilosos de acordo com a legislação em vigor, implementando-se protocolos de documentos adequados a essa classificação.

A seguir são elencadas as medidas de segurança da informação na documentação.



4.6.1 Classificação e Segurança

As unidades do MPF devem seguir as seguintes orientações:

- I - A documentação produzida no MPF deve ser classificada quando o seu conteúdo exigir grau de sigilo.
- II - A classificação dos documentos ou informações sigilosos do MPF e os seus respectivos trâmites e tratamentos observarão, no que couber, a Lei nº 12.527, de 18 de novembro de 2011, sem o 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.

4.6.2 Gestão de Documentos Sigilosos

As unidades do MPF devem seguir as seguintes orientações:

- 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.

4.6.3 Documentos Controlados

As unidades do MPF devem seguir as seguintes orientações:

- I - Os Documentos Controlados - DCs são documentos sigilosos cujo conteúdo requer medidas extras de segurança, que incluem guarda e custódia.
- II - A segurança do DC requer medidas adicionais de controle, tais como: identificação dos destinatários em protocolo e recibo 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. 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. O termo de transferência, por sua vez, 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.

4.6.4 Segurança na Autuação e Processamento Administrativo

As unidades do MPF devem seguir as seguintes orientações:



- 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 MPF.
- II - Quando a autuação for realizada pelo MPF, 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.

4.6.5 Marcação de Documentos Sigilosos

As unidades do MPF devem seguir as seguintes orientações:

- 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 as 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.

4.6.6 Segurança na Expedição, Tramitação e Reprodução

As unidades do MPF devem seguir as seguintes orientações:

- I - Toda a documentação sigilosa deve tramitar em grau de urgência.
- II - Os mesmos critérios de segurança aplicados no encaminhamento ao MPF 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 MPF), 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 - Salvo necessidade excepcional e devidamente justificada, a expedição de documentação sigilosa não deverá ser realizada mediante utilização de equipamento de fac-símile.
- VIII - É vedada a extração de cópia com a finalidade de colher recibo de entrega de documentação classificada segundo o grau de sigilo.
- IX - 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.

- X - O invólucro interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior.
- XI - O invólucro interno contendo a marca “pessoal” somente pode ser aberto pelo próprio destinatário.
- XII - A movimentação e o recebimento eletrônico de documentação sigilosa fica restrita aos servidores credenciados.
- XIII - 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; e guarda armada. Os responsáveis pela guarda ou custódia de documentos sigilosos os transmitirão a seus substitutos, devidamente conferidos, quando da passagem ou transferência de responsabilidade.
- XIV - 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.
- XV - 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.
- XVI - As eventuais cópias decorrentes de documentos sigilosos serão autenticadas pela autoridade devidamente constituída.



- XVII - Nas cópias expedidas devem constar marcas ou carimbos de identificação. Junto aos documentos originais, devem constar as destinações das cópias expedidas.
- XVIII - 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.
- XIX - 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.

4.6.7 Segurança na Publicação, Arquivamento e Acesso

As unidades do MPF devem seguir as seguintes orientações:

- 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 serão encaminhados ao Arquivo Central para fins de organização, preservação e acesso, conforme estabelecido em regulamento próprio.

- 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. A reconstituição obedecerá aos princípios normatizados para a restauração de autos ostensivos extraviados ou destruídos acidentalmente. 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.
- 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. Demais casos serão solicitados e concedidos na forma da legislação vigente.

4.6.8 Segurança em contratos envolvendo sigilo

As unidades do MPF devem seguir as seguintes orientações:

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

- h) definição dos dados e informações a serem protegidas e determinação do período de manutenção do sigilo;
- i) 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;
- j) critérios para registro do conhecimento e a regulamentação da propriedade intelectual, quando for o caso;
- k) regulamentação da eliminação de dados e informações sigilosos ou qualquer material sigiloso que não se prestam mais ao objetivo do contrato;
- l) medidas de gestão de incidentes de segurança da informação, estabelecendo procedimentos a serem adotados pelas partes para notificação e tratamento de incidentes de segurança;
- m) 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 MPF. Nesse caso, os terceirizados e consultores devem submeter-se às normas de segurança previstas no contrato.

III - As unidades do MPF 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 MPF 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 MPF. 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. Excetua-se os casos de traduções de documentos, quando a contratada deve assumir compromisso de manutenção do sigilo.

4.6.9 Prescrições Diversas

As unidades do MPF devem seguir as seguintes orientações:

- 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 Infra-Estrutura 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 MPF, 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.

4.7 Gestão de Riscos

A Gestão de Riscos, que inclui a identificação, análise, avaliação e tratamento do risco, constitui-se em atividade fundamental para proteção do MPF, por ser um processo dinâmico e proativo de defesa do sistema.

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

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. É fundamental para permitir o cumprimento das funções do MPF, mesmo diante de um incidente que atente contra a realização de processos.

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 MPF 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.

4.7.1 Planejamento de Contingência

O Planejamento de Contingência visa a minimizar ou neutralizar os impactos decorrentes da interrupção de atividades críticas e serviços essenciais do MPF ocasionada por falhas, desastres, indisponibilidade significativa ou ação intencional de ator hostil em processos sensíveis, permitindo a continuidade das atividades e serviços em níveis aceitáveis. Esse planejamento contempla ações de prevenção e recuperação, além de medidas de avaliação do dano, que constituem os planos de contingência e os planos de controle de danos.

Cada unidade do MPF deve identificar seus processos sensíveis e estabelecer um planejamento de contingência. A prevenção e combate a incêndio, por exemplo, constitui atividade que requer, obrigatoriamente, um planejamento de contingência.

4.7.2 Plano de Contingência

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. O planejamento deve conter, entre outras coisas:

- I - objetivos e escopo do plano;
- II - gerência do plano (planejamento e execução);

- III - ações a realizar;
- IV - previsão de ações alternativas;
- V - condições de ativação do plano;
- VI - comunicações a serem feitas;
- VII - medidas de controle de danos;
- VIII - medidas de prevenção a serem executadas; e
- IX - processos de testes e validação do planejamento.

As auditorias e validações para revisões do planejado devem ser realizadas pelo menos uma vez ao ano ou quando houver modificação de qualquer aspecto que tenha reflexo para o planejamento.

É importante que as gerências e o pessoal envolvido nas ações de contingência saibam as suas respectivas responsabilidades, procedimentos a serem executados, conheçam os equipamentos eventualmente utilizados e estejam familiarizados com o planejamento.

4.7.3 Plano de Controle de Danos

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.

Da mesma forma que o plano de contingência, pode ser previsto para atender incidentes em serviços e sistemas essenciais da Instituição ou para situações de emergência. Em regra, integra o próprio plano de contingência, entretanto, pela sua complexidade, pode ser elaborado separadamente.



O planejamento deve conter, entre outras coisas:

- I - objetivos e escopo do plano;
- II - gerência do plano (planejamento e execução);
- III - ações a realizar:
 - a) avaliação dos danos (sistemas ou serviços atingidos);
 - b) levantamento de ativos danificados;
 - c) identificação de força do serviço ou sistema afetado; e
 - d) mensuração do impacto para a Instituição.
- IV - condições de ativação do plano;
- V - comunicações necessárias;
- VI - ações de comunicação social;
- VII - ações de gerenciamento de crise; e
- VIII - monitoramento de eventos decorrentes do incidente.

4.7.4 Mapeamento de Sistemas e Serviços Essenciais e situações de emergência

É fator crítico de sucesso do planejamento de contingência o levantamento dos serviços e sistemas sob gerência de cada unidade do MPE, cuja interrupção cause dano ou prejuízo à Instituição. No caso de serviços e sistemas

gerenciados por setores distintos é necessária a integração entre as partes para coordenação de ações.

Este mapeamento deve ser estendido às situações de emergência que exijam ações de contingência, a exemplo da prevenção e combate a incêndios e da evacuação de pessoas e documentos das dependências das unidades do MPF.

4.7.5 Assessoria Técnica de Segurança

A Unidade de Segurança Institucional deverá executar atividades de Assessoria Técnica de Segurança - ATS e elaborar manuais técnicos para subsidiar a realização de tais atividades pelas unidades do MPF.

A execução da ATS objetiva:

- I - identificar vulnerabilidades reais e potenciais;
- II - orientar o estabelecimento de estruturas de controle e validação de processos de segurança;
- III - avaliar ameaças, impactos e os graus de vulnerabilidades;
- IV - sugerir o estabelecimento de ações para obtenção de atitudes favoráveis à segurança; e
- V - assessorar na implementação de medidas de segurança e contribuir para o desenvolvimento de atitudes de segurança.



CAPÍTULO V

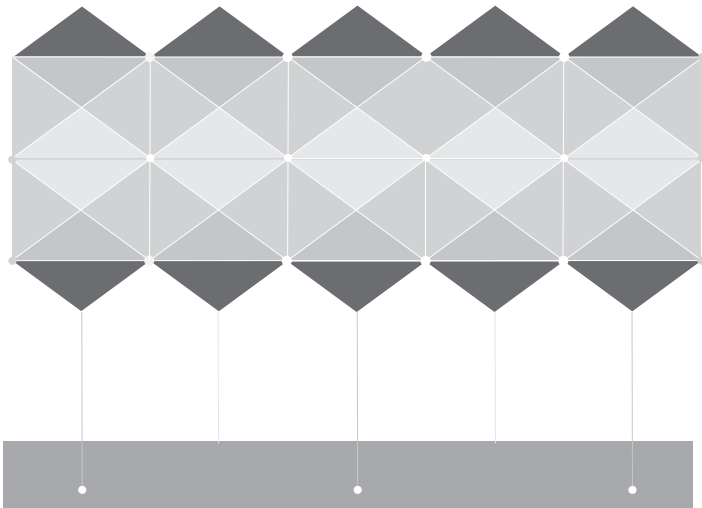
Disposições Finais

O presente Plano de Segurança Institucional tem aplicação imediata e deverá ser submetido a revisão a cada dois anos. A execução do plano receberá tratamento prioritário no âmbito da Instituição, inclusive no que diz respeito à expedição dos atos normativos que se revelem necessários ao cumprimento de todas as diretrizes e procedimentos nele previstos.



PARTE III

Anexos



PORTARIA PGR Nº. 580 DE 17 DE NOVEMBRO DE 2010

O PROCURADOR-GERAL DA REPÚBLICA, no uso das atribuições que lhe confere o artigo 49 da Lei Complementar nº 75, de 20 de maio de 1993, resolve:

Art.1º – Aprovar a Política de Segurança Institucional (PSI) do Ministério Público Federal, na forma do anexo à presente Portaria.

Art. 2º – O Procurador-Geral da República baixará os atos que se fizerem necessários à operacionalização das normas constantes desta Política.

Art. 3º – A implantação desta Política será realizada conforme cronograma a ser divulgado.

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



ROBERTO MONTEIRO GURGEL SANTOS

PORTARIA PGR/MPF Nº 124 DE 18 DE MARÇO DE 2013

O PROCURADOR-GERAL DA REPÚBLICA, no uso da atribuição que lhe confere o art. 49, inciso XX, da Lei Complementar nº 75, de 20/5/1993, e considerando o que consta no Processo Administrativo PGR/MPF nº 1.00.000.002615/2010-03, resolve:

Art. 1º Constituir Comissão para validação dos estudos e apresentação de proposta de Plano de Segurança Institucional do Ministério Público Federal.

Art. 2º A Comissão será composta pelos seguintes integrantes:

- I - WILSON ROCHA DE ALMEIDA NETO, Procurador da República;
- II - SÍLVIO PEREIRA AMORIM, Procurador da República;
- III - GUILHERME GUEDES RAPOSO, Procurador da República;
- IV - SÍLVIO ROBERTO OLIVEIRA DE AMORIM JÚNIOR, Procurador da República;
- V - EDUARDO SANTOS DE OLIVEIRA, Procurador da República;
- VI - DELFIM LOUREIRO QUEIROZ, Chefe da Unidade de Segurança Institucional da PGR;
- VII - HENRIQUE ANTÔNIO OLIVEIRA DOS SANTOS, Chefe Adjunto da Unidade de Segurança Institucional da PGR; e
- VIII - LUÍS CARLOS GALVÃO, Chefe da Unidade de Segurança da PRR3ª Região.

Parágrafo único. Designar WILSON ROCHA DE ALMEIDA NETO, Procurador da República, como presidente da Comissão.

Art. 3º Estabelecer à Comissão o prazo de trinta dias, a contar da data de publicação desta Portaria, para conclusão dos trabalhos.

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



ROBERTO MONTEIRO GURGEL SANTOS



PGR-00151780 /2013

8 1 7 /2013

PORTARIA PGR/MPF Nº 417 DE 5 DE JULHO DE 2013

Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal.

O PROCURADOR-GERAL DA REPÚBLICA, no uso da atribuição que lhe confere o art. 49, inciso XX, da Lei Complementar nº 75, de 20/5/1993, e considerando a Portaria PGR/MPF nº 124, de 18/3/2013, e o que consta no Processo Administrativo PGR/MPF nº 1.00.000.002615/2010-03, resolve:

Art. 1º Aprovar o Plano de Segurança Institucional do Ministério Público Federal, constante do Anexo desta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.



ROBERTO MONTEIRO GURGEL SANTOS



PGR-00453946/2013

017/2013

PORTARIA PGR/MPF Nº 427 DE 5 DE JULHO DE 2013

Regulamenta o serviço de proteção aos membros e servidores do Ministério Público Federal.

O PROCURADOR-GERAL DA REPÚBLICA, no uso da atribuição que lhe confere o art. 49, inciso XX, da Lei Complementar nº 75, de 20/5/1993, e tendo em vista a Lei nº 9.807, de 13/7/1999, e o que consta no Processo Administrativo PGR/MPF nº 1.00.000.008398/2012-19, resolve:

Art. 1º Regular o serviço de proteção aos membros e servidores do Ministério Público Federal - MPF nos termos desta Portaria.

Art. 2º Compete à Unidade de Segurança Institucional - USI realizar a segurança de membros e servidores do MPF, quando comprometida em razão da respectiva atuação institucional.

§ 1º O Secretário-Geral, após análise da USI, decidirá a necessidade de disponibilizar o serviço de proteção ao membro ou servidor do MPF, sem prejuízo da atuação da Polícia Federal em caráter complementar ou residual.

§ 2º Da decisão do Secretário-Geral caberá recurso ao Procurador-Geral da República no prazo de até 30 (trinta) dias.

Art. 3º Se houver comprometimento da segurança de cônjuge ou companheiro, ascendentes, descendentes e dependentes declarados oficialmente, em razão da atuação institucional do membro ou do servidor, a segurança poderá ser estendida a eles.

Art. 4º A solicitação do serviço de proteção deverá ser realizada pelo membro ou servidor do MPF, mediante requerimento a ser encaminhado ao Secretário-Geral para deliberação, constando a descrição dos fatos e as providências já adotadas.

Art. 5º A proteção concedida e as medidas dela decorrentes serão determinadas pela USI, considerando a gravidade da ameaça à integridade física e a dificuldade de preveni-la ou reprimi-la.

Parágrafo único. Em caso de risco iminente, devidamente comprovado, a USI poderá demandar a adoção imediata de providências de segurança de caráter emergencial, quando não for possível percorrer toda a extensão da via administrativa.

Art. 6º Compete à USI adotar as providências necessárias à aplicação das medidas do dispositivo de segurança, cabendo-lhe para tanto:

- I - manter contato com os órgãos de segurança pública, para agilizar a implementação de medidas de gerenciamento de incidentes de segurança; e
- II - propor a formação e capacitação de equipe técnica para realização de tarefas desenvolvidas no dispositivo de segurança.

Art. 7º A USI deverá aplicar, isolada ou cumulativamente, em benefício da pessoa protegida, segundo a gravidade e as circunstâncias de cada caso, as seguintes medidas:

- I - segurança no local de trabalho, incluindo a salvaguarda das telecomunicações institucionais e da telemática;
- II - segurança na residência, incluindo a salvaguarda das telecomunicações;
- III - escolta e segurança nos deslocamentos relacionados ao desempenho das funções institucionais em que a presença do protegido seja imprescindível;
- IV - análise de riscos com vistas a identificar pontos críticos na segurança dos membros, bem como definir medidas preventivas que possam ser adotadas nas unidades diante da existência de perigo iminente; e
- V - outras medidas correlatas que a USI esteja habilitada a implementar.

Art. 8º Antes do início do dispositivo de segurança, todos os protegidos deverão firmar compromisso assumindo as seguintes obrigações:

- I - evitar exposição desnecessária, principalmente em horário de lazer, que possa potencializar o risco de ocorrência de atentados;
- II - acatar as recomendações técnicas estabelecidas pela equipe de segurança;
- III - evitar frequentar ambientes onde o uso do veículo oficial possa parecer de cunho particular, ressalvadas, em circunstâncias excepcionais e sob risco avaliado pela equipe de segurança, as atividades cotidianas ou familiares;
- IV - abster-se de frequentar clubes, casas de diversões, estabelecimentos educacionais e locais onde se realizem competição esportiva, reunião ou aglomeração de pessoas;
- V - comunicar imediatamente à equipe de segurança qualquer fato cuja circunstância seja indicativa de possível ameaça ou hostilidade;
- VI - informar, com antecedência, a agenda de trabalho e particular à equipe de segurança para possibilitar avaliação de risco e conveniência de manutenção da atividade ou adequação da equipe;
- VII - dispensar formalmente, responsabilizando-se pelo ato, a segurança aproximada quando entender desnecessária;
- VIII - procurar, sempre que possível, manter-se fora de área hostil quando em férias ou licenças, avisando com antecedência à USI para adaptação da escala de serviço dos agentes de segurança;
- IX - orientar familiares, quando couber, sobre o cumprimento das recomendações técnicas estabelecidas pela equipe de segurança; e
- X - outras medidas de segurança recomendadas pela USI.

Parágrafo único. Caso o protegido se recuse a assumir na sua integralidade as obrigações constantes deste artigo, poderá, em comum acordo com a USI, estabelecer meios de proteção que impliquem restrições menores a sua vida pessoal, se o grau de gravidade da ameaça assim o permitir.

Art. 9º As medidas e providências relacionadas ao dispositivo de segurança serão adotadas, executadas e mantidas em sigilo pelo protegido e pelos agentes de segurança envolvidos na execução do programa.

Art. 10. O encerramento do dispositivo de segurança se dará a qualquer tempo:

- I - por solicitação formal do protegido;
- II - pelo cessamento dos motivos que ensejaram a implantação do dispositivo de segurança;
- III - por recomendação da USI e aprovação do Secretário-Geral; ou
- IV - por determinação do Secretário-Geral, no caso de desatendimento injustificado das normas estabelecidas no art. 8º, que exponham a risco desnecessário a pessoa protegida e que possam comprometer a eficiência dos serviços prestados pela equipe de segurança.

Parágrafo único. O protegido terá um prazo de 10 (dez) dias para se manifestar, antes de ser decidido o encerramento do dispositivo de segurança.

Art. 11. Os deslocamentos do protegido, quando assim julgado pela equipe de segurança, poderão ser precedidos das providências necessárias à proteção, incluindo, conforme o caso, o uso de colete à prova de balas, disfarces e outros artifícios capazes de dificultar a sua identificação.

Art. 12. A equipe de segurança terá autonomia para decidir, em situações críticas, sobre as condutas a serem adotadas, visando à segurança do protegido.

Art. 13. Aplicam-se, no que couber, as disposições desta Portaria às Unidades de Segurança descentralizadas no âmbito do MPF, sob orientação da USI.

Art. 14. Compete ao Secretário-Geral do MPF dirimir as dúvidas suscitadas na aplicação do disposto nesta Portaria, cabendo ao Procurador-Geral da República decidir os casos omissos.

Art. 15. Esta Portaria entra em vigor na data de sua publicação.


ROBERTO MONTEIRO GURGEL SANTOS

PGR-00275338/2013

13/12/2013

PORTARIA PGR/MPF Nº 902 DE 13 DE DEZEMBRO DE 2013

Altera a Portaria PGR/MPF nº 427, de 5/7/2013, que regulamenta o serviço de proteção aos membros e servidores do Ministério Público Federal.

O PROCURADOR-GERAL DA REPÚBLICA, no uso da atribuição que lhe confere o art. 49, inciso XX, da Lei Complementar nº 75, de 20/5/1993, e tendo em vista o que consta no Processo Administrativo PGR/MPF nº 1.00.000.013009/2013-58, resolve:

Art. 1º A Portaria PGR/MPF nº 427, de 5/7/2013, passa a vigorar com a seguinte redação:

"Art. 8º

Parágrafo único. Caso o protegido se recuse a assumir na sua integralidade as obrigações constantes deste artigo, poderá, em comum acordo com a USI, estabelecer meios de proteção que impliquem restrições menores a sua vida pessoal, se o grau de risco da ameaça assim o permitir.

Art. 9º As medidas e providências relacionadas ao dispositivo de segurança serão adotadas, executadas e mantidas em sigilo pelo protegido e pelos agentes envolvidos na execução do programa.

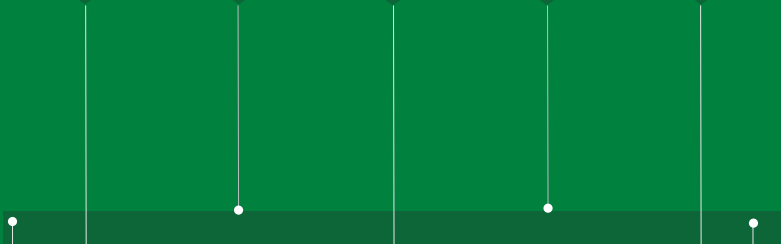
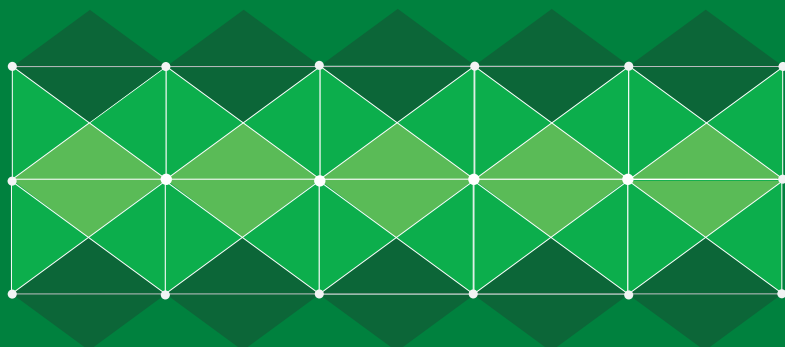
Art. 10.

§ 1º A USI deverá reavaliar a manutenção do dispositivo de proteção ao membro ou servidor protegido a cada 6 (seis) meses, a contar de sua abertura, a fim de opinar sobre a continuidade do serviço.

§ 2º O membro ou servidor protegido terá um prazo de 10 (dez) dias para manifestar-se nas hipóteses previstas neste artigo, antes de ser decidido pelo encerramento do dispositivo de segurança." (NR)

Art. 2º Esta Portaria entra em vigor na data de sua publicação.


RODRIGO JANOT MONTEIRO DE BARROS



MPF
Ministério Público Federal

www.mpf.mp.br