Manual do Gestor de

Segurança Institucional do Ministério Público

Brasília, 2026

CNMP
Conselho Nacional do Ministério Público

Manual do Gestor de Segurança Institucional do Ministério Público

Brasília, 2026

CNMP
Conselho Nacional do Ministério Público

B823 Conselho Nacional do Ministério Público (Brasil).

Manual do Gestor de Segurança do Ministério Público / Conselho Nacional do Ministério Público; Comissão de Preservação da Autonomia do Ministério Público. – Brasília : CNMP, 2026.

81 p. : il.

ISBN: 978-65-89260-88-2

1. Ministério Público - Atuação. 2. Segurança Institucional. 3. Gestão de Incidentes. 4. Interoperabilidade entre Órgãos de Segurança. 5. Inteligência e Contrainteligência. 6. Gestão de Riscos. I. Título. II. Comissão de Preservação da Autonomia do Ministério Público (CPAMP).

CDD – 341.413

Ficha catalográfica por Felipe Belo da Silva
CRB: 2655-DF

EXPEDIENTE

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP)

Paulo Gustavo Gonet Branco
Presidente

Fernando da Silva Comin
Corregedor Nacional

Ivana Lúcia Franco Cei
Conselheira Nacional

Edvaldo Nilo de Almeida
Conselheiro Nacional

Fabiana Costa Oliveira Barreto
Conselheira Nacional

Karen Luise Vilanova Batista de Souza
Conselheira Nacional

Greice Fonseca Stocker
Conselheira Nacional

Thiago Roberto Morais Diaz
Conselheiro Nacional

Gustavo Afonso Sabóia Vieira
Conselheiro Nacional

José de Lima Ramos Pereira
Conselheiro Nacional

Alexandre Lacerda Magno
Conselheiro Nacional

Editorial

A segurança institucional constitui um dos pilares fundamentais para a preservação da autonomia, da integridade e da capacidade operacional do Ministério Público brasileiro. Numa perspectiva de transformações aceleradas, marcada por riscos complexos e por novas formas de ameaça física e digital, faz-se indispensável estabelecer parâmetros claros e padronizados que orientem a atuação dos gestores responsáveis pela proteção das pessoas, das informações e das estruturas que sustentam a missão constitucional da Instituição.

Nesse contexto, o Conselho Nacional do Ministério Público (CNMP) tem consolidado, ao longo dos últimos anos, um arcabouço normativo que fortalece as bases da segurança orgânica no âmbito ministerial. A essas normas somam-se outros instrumentos e protocolos desenvolvidos pelo Sistema Nacional de Segurança Institucional do Ministério Público, todos orientados pela necessidade de garantir um ambiente organizacional seguro, resiliente e apto a responder, de maneira tempestiva e coordenada, a situações que possam comprometer a atividade finalística.

A atuação do gestor de segurança, nesse cenário, exige visão estratégica, atualização permanente, capacidade de articulação interinstitucional e estrita observância às normas que regem o tema. Assim, este Manual do Gestor de Segurança Institucional nasce exatamente com este propósito: oferecer orientações objetivas, práticas e atualizadas, facilitando a aplicação uniforme das regras de segurança orgânica e fortalecendo a cultura institucional de prevenção. Mais do que um compêndio normativo, trata-se de um instrumento de apoio à tomada de decisões, à formação contínua e à consolidação de boas práticas que assegurem a proteção do Ministério Público em todas as suas dimensões.

Ao disponibilizar este material, o CNMP, por meio da Comissão de Preservação da Autonomia o Ministério Público (CPAMP), reafirma seu compromisso com a construção de ambientes de trabalho cada vez mais seguros, com a sustentabilidade da atividade ministerial e com a defesa do Estado Democrático de Direito. Que este Manual contribua para o aprimoramento das ações de segurança institucional e para o fortalecimento da atuação integrada de todos que têm a missão de zelar pela salvaguarda da Instituição e daqueles que a servem.

JOSÉ DE LIMA RAMOS PEREIRA
Conselheiro Nacional do Ministério Público
Presidente da Comissão de Preservação da Autonomia do Ministério Público
(Gestão 2026)

Apresentação

A segurança institucional é uma área estratégica de gestão do Ministério Público brasileiro, haja vista se dedicar à proteção da Instituição na sua integralidade, por meio da antevisão de riscos de ações adversas, bem como do manejo de medidas neutralizadoras ou restauradoras dos danos ocasionados por tais ações aos ativos institucionais, sem os quais pode comprometer o cumprimento pelo Ministério Público da sua missão constitucional.

A crescente complexidade das demandas contemporâneas — incluindo riscos físicos, tecnológicos, reputacionais e operacionais — exige que a atuação do gestor de segurança institucional seja estratégica, técnica e alinhada aos valores constitucionais que regem o Ministério Público.

A elaboração deste manual fundamenta-se na Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público (CNMP) — e demais normativos relacionados —, que institui a Política Nacional de Segurança Institucional no Ministério Público e estabelece princípios, diretrizes e competências essenciais para a atuação integrada e eficiente das unidades de segurança institucional, especialmente aos novos coordenadores de segurança institucional designados para esta função.

Nesse sentido, a colaboração de membros integrantes do CPSI foi fundamental para o seu êxito, pois, com suas experiências à frente dos seus respectivos órgãos de segurança institucional, possibilitou enriquecer o conteúdo deste Manual com seus conhecimentos teóricos e práticos. Iniciativas como esta contribuem para a sustentabilidade da Instituição à medida que transmitem e fazem a gestão do conhecimento.

Assim, respeitando a autonomia e as especificidades de cada unidade e ramo, este Manual apresenta orientações práticas, parâmetros mínimos e procedimentos recomendados para subsidiar a gestão da segurança orgânica, da segurança de pessoas, da proteção de informações e da prevenção e resposta a incidentes. Mais do que um conjunto de normas, este material busca consolidar uma cultura organizacional de segurança, promovendo a integração entre membros, servidores e equipes especializadas, sempre com foco na proteção do interesse público e na continuidade da missão institucional.

Esperamos que este Manual contribua para a construção de ambientes institucionais cada vez mais seguros, resilientes e preparados para enfrentar os desafios atuais e futuros.

FERNANDO DA SILVA COMIN
Conselheiro Nacional do Ministério Público
Presidente da CPAMP/CNMP (Gestão 2024/2025)

GÉBER MAFRA ROCHA
Promotor de Justiça – MPAM
Membro Auxiliar da CPAMP

NÍSIO EDMUNDO TOSTES RIBEIRO FILHO
Procurador de Justiça – MPDFT
Coordenador do CPSI/MP

GILBERTO COSTA DE AMORIM JÚNIOR
Promotor de Justiça – MPBA
Vice-Coordenador do CPSI/MP

RODRIGO ALVES BARCELLOS
Promotor de Justiça – MPTO
Integrante da SESI

MARIANO PAGANINI LAURIA
Promotor de Justiça – MPRN
Integrante da SESI

MAURO ZAQUE DE JESUS
Promotor de Justiça – MPMT

JESSÉ MINEIRO DE ABREU
Promotor de Justiça – MPPI

CARLOS LUIZ WOLFF DE PINA
Promotor de Justiça – MPGO

JOÃO BARBOSA LIMA
Assessor-Chefe da CPAMP/CNMP

JUCÉLIA FERREIRA DE ALBUQUERQUE
Técnica Administrativa da CPAMP/CNMP

Sumário

Siglas e abreviaturas

AI	Atividade de Inteligência
CFTV	Circuito Fechado de Televisão
CICC	Centro Integrado de Comando e Controle
CMVT	Contramedidas de Vigilância Técnica
CNMP	Conselho Nacional do Ministério Público
CPAMP	Comissão de Preservação da Autonomia do Ministério Público
CPSI	Comitê de Políticas de Segurança Institucional
ESMP	Escola Superior do Ministério Público
GPS	*Global Positioning System* (Sistema de Posicionamento Global)
IA	Inteligência Artificial
LED	*Light Emitting Diode* (Diodo Emissor de Luz)
LGPD	Lei Geral de Proteção de Dados
MP	Ministério Público
NAC	Núcleo de Análise e Contramedidas
NFC	*Near Field Communication* (Comunicação por campo de proximidade)
PGJ	Procuradoria-Geral de Justiça
PGRS	Plano de Gerenciamento de Resíduo Sólido
PM	Polícia Militar
PNCiber-MP	Política Nacional de Cibersegurança do Ministério Público
POP	Procedimento Operacional Padrão
PSI/MP	Política de Segurança Institucional do Ministério Público
QR Code	*Quick Response Code* (Código de Resposta Rápida)
RFID	*Radio-Frequency Identification* (Identificação por Radiofrequência)
RTR	Relatório Técnico de Risco
SAMU	Serviço de Atendimento de Urgência
SESI	Secretaria Executiva de Segurança Institucional
SGRI	Sistema de Gestão de Riscos e Incidentes
SIGR	Sistema Integrado de Gestão de Riscos
SIMP	Sistema [Nacional] de Inteligência do Ministério Público
SNSI	Sistema Nacional de Segurança Institucional
SNS/MP	Sistema Nacional de Segurança Institucional do Ministério Público
TI	Tecnologia da Informação

1. Introdução

1.1. FINALIDADE DO MANUAL

Assumir a gestão da Segurança Institucional em uma unidade do Ministério Público representa um dos maiores compromissos com a preservação da autonomia e integridade da Instituição. A missão confiada ao gestor não se limita à proteção física e moral de membros, servidores e instalações, mas se estende à salvaguarda da própria estrutura do Estado Democrático de Direito diante de um contexto cada vez mais complexo e sensível que envolve ameaças internas e externas.

Este manual tem por finalidade orientar a função do Coordenador de Segurança Institucional, visando garantir a continuidade, a padronização e a efetividade das ações de proteção e o resguardo de pessoas, áreas, instalações, patrimônio, dados e a boa imagem do Ministério Público.

Serve também como instrumento de consulta técnica e normativa, permitindo que o gestor compreenda:

a. a) A estrutura e o funcionamento da segurança institucional;
b. b) Os processos operacionais e estratégicos;
c. c) Os procedimentos de resposta a riscos e incidentes;
d. d) As práticas de governança e melhoria contínua da área.

Assim, o manual configura-se como um guia prático que possibilita ao gestor compreender sua função, adotar medidas eficazes de proteção e, sobretudo, garantir a continuidade das ações de segurança institucional, fornecendo diretrizes estratégicas, operacionais e normativas para a gestão uniforme da segurança institucional em todos os ramos e unidades do Ministério Público brasileiro.

1.2. DEFINIÇÃO DE SEGURANÇA INSTITUCIONAL

Segurança institucional é o conjunto de princípios, medidas, processos e estruturas destinados a preservar o funcionamento ininterrupto e seguro da Instituição, seus integrantes e seus ativos – físicos, humanos, informacionais e simbólicos. Compreende ações preventivas, reativas e de inteligência voltadas à proteção do Ministério Público perante ameaças externas e internas, acidentais ou intencionais. Logo, a segurança institucional engloba um conjunto de ações visando à salvaguarda institucional como um todo (seus integrantes, materiais, comunicações e áreas e instalações), com o objetivo de prever e neutralizar eventuais ameaças protagonizadas por atores hostis e eventos da natureza.

Nos termos do art. 3º da Resolução CNMP nº 156/2016, ela abrange tanto ações de caráter orgânico — composta por medidas de segurança de pessoas, dos materiais, comunicações e das áreas e instalações — quanto ações de segurança ativa, com foco na contrassabotagem, contraespionagem e contrapropaganda, priorizando a atuação em caráter preditivo e proativo.

1.3. IMPORTÂNCIA DA SEGURANÇA INSTITUCIONAL

A segurança institucional é condição essencial para que membros e servidores desempenhem suas funções com independência, tranquilidade e respaldo. Diante da crescente complexidade das ameaças, da atuação contra o crime organizado e da crescente exposição dos agentes públicos, a segurança institucional deixou de ser uma atividade meramente acessória e se tornou um eixo estratégico de governança.

Além disso, sua correta aplicação protege a imagem e a credibilidade do Ministério Público perante a sociedade, garantindo confiança no cumprimento de sua missão constitucional.

1.4. PRINCÍPIOS FUNDAMENTAIS

Conforme a Resolução CNMP nº 156/2016, os princípios que regem a segurança institucional são:

a. Legalidade e proteção aos direitos fundamentais: busca valorizar as garantias constitucionais e o respeito aos princípios constitucionais da atividade administrativa;

b. Ética profissional e valores do Estado Democrático de Direito: como princípio orientador das práticas, valorizando o Estado Democrático de Direito, respeitando-se os direitos e os interesses legítimos dos usuários, intervenientes e colaboradores sem comprometimento da segurança;

c. Da Prevenção à Hostilidade: orienta a desenvolver suas atividades com foco na antecipação às ações hostis com viés preventivo e proativo;

d. Profissionalização e perenidade da atividade: possui um caráter profissional e permanente, interligando-se a outras áreas para proteção integral da Instituição e de seus ativos;

e. Integração com órgãos de segurança pública e de inteligência: busca integrar o Ministério Público com outros órgãos essenciais à atividade de segurança institucional;

f. Orientação às ameaças reais ou potenciais: a atividade de segurança institucional deve ser orientada para prevenir, detectar e neutralizar ameaças reais ou potenciais, independentemente da origem ou motivação dos atores hostis;

g. Preservação da imagem institucional: visa salvaguardar a imagem da Instituição, evitando sua exposição e exploração midiática negativa.

É importante evidenciar que a ética, o culto e a preservação dos valores fundamentais da organização são basilares para o exercício das atividades de Segurança Institucional.

1.5. CARACTERÍSTICAS E ESPECIFICIDADES DA SEGURANÇA INSTITUCIONAL

A segurança institucional se distingue por:

a. envolver simultaneamente segurança orgânica (pessoal, comunicações, materiais e áreas e instalações) e segurança ativa (voltada à contrassabotagem, contraespionagem, combate ao crime organizado e à contrapropaganda);

b. atuar sob regime de sigilo e confidencialidade, com tratamento adequado aos conhecimentos sensíveis;

c. utilizar profissionais com formação contínua e capacitação técnica especializada;

d. demandar resposta ágil a incidentes e ameaças reais ou potenciais, com foco em prevenção e neutralização;

e. interagir com diversos sistemas e instituições externas, de forma coordenada e integrada;

f. ser orientada por protocolos e normas próprias, com alinhamento à política nacional de segurança ministerial, garantindo uniformidade de procedimentos e integração ao Sistema Nacional de Segurança Institucional (SNSI/MP).

Para garantir um nível de segurança adequado na Instituição, devemos contar com a participação de todos os integrantes, em suas respectivas esferas de atribuições. Para isso, é necessário plano permanente de capacitação de modo a se desenvolver uma cultura de segurança sólida, com o objetivo de estabelecer atitudes alinhadas, por parte dos integrantes da Instituição, em relação às exigências de segurança.

1.6. ORGANIZAÇÃO, GESTÃO E GOVERNANÇA DO GABINETE DE SEGURANÇA INSTITUCIONAL

A gestão do Gabinete de Segurança Institucional envolve uma abordagem de gerenciamento que se concentra no desenvolvimento de diretrizes, contemplando:

a. o planejamento, consubstanciado na definição dos objetivos e na escolha dos melhores caminhos para alcançá-los;

b. a organização, que é a estruturação dos recursos disponíveis, como pessoas, materiais e equipamentos que possam ser utilizados de forma eficiente e eficaz;

c. a direção, marcada pela condução das atividades do órgão, liderando e motivando as equipes para que atinjam os objetivos estabelecidos;

d. o controle, que implica a avaliação constante de resultados obtidos, comparando-os com os objetivos definidos e adotando medidas corretivas quando necessário.

A governança do Gabinete de Segurança Institucional refere-se ao sistema de regras, regulamentos, práticas e estruturas de uma organização que visa promover a transparência, a responsabilidade, a integridade, a eficiência e a eficácia na tomada de decisões para o adequado funcionamento do serviço. A boa governança da segurança institucional envolve a tomada de decisão e a gestão de riscos baseadas em evidências e no profissionalismo. Prover governança significa respeitar os valores, as estruturas éticas e legais e gerenciar riscos de acordo com as metas comuns.

Atuar com responsabilidade significa que o Gabinete de Segurança Institucional deve ser responsável por suas ações e decisões. Mecanismos de prestação de contas, como relatórios periódicos e auditorias, devem ser utilizados para garantir que o órgão mantenha a transparência e a qualidade das atividades desenvolvidas.

O Gabinete de Segurança institucional deve pautar sua atuação pela eficiência e eficácia, garantindo que os recursos públicos sejam utilizados com a maior utilidade possível para alcançar os objetivos da organização. Isso envolve a definição de metas claras, o monitoramento constante dos indicadores de desempenho e a adoção de medidas corretivas quando necessário.

A integridade e a ética devem permear todas as ações do Gabinete de Segurança Institucional, pois desempenham papel fundamental na confiança dos demais integrantes do Ministério Público nas atividades ali desenvolvidas. Isso inclui estabelecimento de padrões éticos de conduta, somado ao trabalho efetivo de contrainteligência, a fim de evitar-se a infiltração da criminalidade na Instituição, a prevenção da corrupção e do vazamento de informações entre outros riscos.

Portanto, ao assumir o Gabinete de Segurança Institucional, o gestor deve:

a. entrevistar o substituído (transição);

b. inventariar os bens patrimoniais (estrutura, parque tecnológico, equipamentos, materiais etc.);

c. avaliar os recursos humanos (lideranças, aspirações, relacionamentos e eventuais conflitos);

d. conhecer programas, projetos e ações em curso;

e. integrar e interagir com a comunidade de segurança institucional e inteligência;

f. identificar as necessidades de capacitação;

g. conhecer o modelo de governança;

h. identificar os mecanismos de controle;

i. auditar os sistemas de tecnologia da informação;

j. conhecer as normas internas e do CNMP relativas à segurança institucional.

Os órgãos de segurança institucional dos ramos e unidades do Ministério Público deverão estar preparados também para a gestão de projetos, acompanhando-os em todas as suas fases, o planejamento, a execução e o controle (fiscalização), para atingir seus objetivos específicos dentro de prazo e orçamento definidos.

1.7. O GESTOR DE SEGURANÇA INSTITUCIONAL

A atividade de segurança institucional no Ministério Público será coordenada, fiscalizada e controlada por membro do Ministério Público especificamente designado como coordenador da área por ato do Procurador-Geral do respectivo ramo ou unidade ministerial, sob as diretrizes do CNMP (art. 29 da Resolução nº 156/2016).

De acordo com essa Resolução, os membros que forem designados para coordenar a segurança institucional na sua respectiva unidade ou ramo ministerial integram, automaticamente, o CPSI, instância que tem a função de promover o direcionamento das ações de segurança institucional do Ministério Público brasileiro. Deste modo, ao ocorrer a mudança de gestor, essa substituição deve ser comunicada ao CNMP, por meio da CPAMP, para que a composição do CPSI esteja sempre atualizada e o membro legitimado para participar do colegiado.

Ainda, é recomendável que o membro indicado para coordenar a atividade de segurança institucional do Ministério Público deva possuir qualificações técnicas específicas que o habilite ao desempenho da função, pois deverá conduzir projetos e processos, atendendo às necessidades dos integrantes da Instituição, solucionando problemas e gerenciando riscos e crises.

1.8. LIMITES DE ATUAÇÃO DA SEGURANÇA INSTITUCIONAL

A discussão acerca dos limites de atuação da segurança institucional no Ministério Público, sua natureza, objeto e limites é imprescindível a fim de balizar a atividade e melhor proteger os ativos institucionais de cada ramo e unidade ministerial.

A falta de clareza de propósito, e das balizas que naturalmente dela decorrem, tradicionalmente criar cenários múltiplos de emprego dos órgãos de segurança ministeriais, tais como a aplicação em se-

gurança e levantamentos para questões desvinculadas da atuação funcional, assessorias para registros e providências policiais, orientações em segurança privada, entre outras.

Ainda, a ausência de limites pode submeter a atividade às determinações dos gestores de cada período, sem a devida cautela e com graves riscos de exposição dos entes.

Da mesma maneira, cria-se um cenário de total multiplicidade na prestação dos serviços entre os diferentes ramos e unidades do Ministério Público, culminando em comparativos equivocados entre realidades absolutamente diversas, reforçando o casuísmo e a ausência de uniformidade.

Lado outro, a consciência clara de suas atribuições permite aos gestores ministeriais de segurança a padronização de fluxos, investimentos em capacitação, direcionamento de recursos e a evasão de atuações casuísticas, melhorando sobremaneira os serviços prestados.

Tudo considerado, em que pese a forma de atuar de cada órgão de segurança seja uma opção política da Administração Superior de cada instituição, cabe ao Coordenador de Segurança, na condição de assessor direto do Procurador-Geral, indicar os melhores caminhos e boas práticas, explicitando vantagens, desvantagens e riscos de cada modelo.

Iniciando-se pela natureza da atividade de segurança institucional, não se pode olvidar que foi em parte ancorada com lastro doutrinário no campo da contrainteligência da Atividade de Inteligência (AI), como se pode ver no disposto no artigo 3º da Resolução CNMP nº 156/2014:

> Art. 3º A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação.

Não por acaso, a disposição coincide com a definição da atividade de contrainteligência trazida ao item 4 da recente Doutrina da Atividade de Inteligência editada pela Agência Brasileira Inteligência[1]:

> A contrainteligência é o ramo da atividade de inteligência que desenvolve ações especializadas voltadas para prevenir, detectar, identificar, avaliar, obstruir e neutralizar ações da inteligência adversa que constituam ameaça: a interesses do Estado e da sociedade; ao processo decisório; e à salvaguarda de conhecimentos, informações e dados sensíveis, dos meios que as retenham ou em que transitem, de seus detentores e de áreas e instalações.

1 Aprovada pela Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023.

Não por outro motivo, a Resolução CNMP nº 260/2023 – Doutrina de Inteligência do Ministério Público –, marco normativo da atividade de inteligência ministerial, trouxe exatamente o mesmo conceito em seu bojo, incluindo definitivamente a natureza da atividade de segurança institucional no âmbito da Atividade de Inteligência, em seu ramo Contrainteligência.

Essa aproximação necessária exige a observância dos pertinentes postulados da AI, num alinhamento como atividades coirmãs, porém sem confundir as atividades que, normativamente, possuem sistemas claramente distintos, como se pode ver no art. 18 da Resolução CNMP nº 156/2016 e no art. 2º da Resolução CNMP nº 292/2024, que se reporta a anexo de acesso restrito:

> Art. 18 O Sistema Nacional de Segurança Institucional do Ministério Público — SNS/MP é composto:
>
> I — pela Comissão de Preservação da Autonomia do Ministério Público — CPAMP;
>
> II — pela Secretaria Executiva de Segurança Institucional — SESI;
>
> III — pelo Comité de Políticas de Segurança Institucional — CPSI;
>
> IV — pelos membros coordenadores da segurança institucional dos ramos do Ministério Público da União e Ministérios Públicos dos Estados.
>
> Parágrafo único. Compete a CPAMP, pelo seu presidente, a gestão e coordenação estratégica do SNS/MP.
>
> Art. 2º Fica instituído o Sistema de Inteligência do Ministério Público, na forma do Anexo II, a esta Resolução, com a finalidade de:
>
> I — permitir a salvaguarda e a difusão oportuna e segura de dados, informações e conhecimentos de inteligência entre os Ministérios Públicos;
>
> II — viabilizar a inserção dos Ministérios Públicos nos demais sistemas e subsistemas de inteligência do país, possibilitando o intercâmbio direto de conhecimentos com outros órgãos e unidades de inteligência, via canal técnico, resultando em maior segurança economicidade, agilidade, eficiência e legitimidade;
>
> III — desenvolver a Atividade de Inteligência (AI) do Ministério Público.
>
> Parágrafo único. O Anexo II dessa resolução deve ser considerado documento de acesso restrito, em consonância com arts. 23, VIII, e 24 da Lei nº 12.527/2011 (Lei de Acesso à Informação).

Em destaque, na mencionada ancoragem doutrinária entre a Inteligência e a Segurança Institucional no MP, há significativas diferenças nas finalidades principais, nos produtos e entregas, nos métodos e na postura operacional, como também nos limites de atuação de ambas as atividades.

Contudo, há uma intersecção controlada que não pode ser esquecida, de modo que se torna imperioso existir um especial inter-relacionamento entre a Segurança Institucional e a Inteligência, a saber:

a. A Segurança Institucional utiliza os conceitos próprios da contrainteligência, nos segmentos de segurança orgânica e ativa, embora não se limite a esses conceitos;

b. Inteligência e Segurança Institucional visam à preservação da instituição, seus integrantes e demais ativos, bem como ao alcance dos objetivos estratégicos;

c. Deve haver o permanente compartilhamento de informações apenas quando necessário e conforme fluxos claramente definidos;

d. A Inteligência subsidia a Segurança Institucional com cenários e alertas;

e. A Inteligência produz conhecimento de suporte às ações executivas da Segurança Institucional;

f. A Segurança Institucional realimenta a Inteligência com incidentes e observações;

g. Cada área mantém métodos, sigilos e competências próprios;

h. No tocante à governança e à gestão, há a possibilidade de convívio das atividades em um mesmo órgão, desde que observadas claramente as suas divisões, com maior cuidado quando órgão também acumular funções tipicamente executivas de segurança, inclusive ostensivas.

Por outro lado, a inobservância dessa necessária interseção entre as aludidas atividades, principalmente em modelos organizacionais em que estejam atribuídas a distintos órgãos, quanto à segurança institucional, por exemplo, pode enfraquecer o desempenho dessa última pela redução do espectro de dados, informações e conhecimentos oportunamente disponíveis e minorar o controle dos efetivos de segurança empregados.

Portanto, convém estabelecer um adequado nível de inter-relacionamento entre as atividades de Segurança Institucional e de Inteligência, sem confundi-las, entretanto, assegurando interseções necessárias em prol de resultados sinérgicos.

Indo para outro aspecto limitante, não se pode prescindir ou minorar a relevantíssima contribuição dos efetivos policiais aos órgãos ministeriais, os quais tradicionalmente prestam valorosos serviços aos Ministérios Públicos de todo o Brasil, tanto na orientação, instrução e apoio como na proteção diuturna de membros e servidores.

Entretanto, o quanto possível, deve-se buscar a progressiva alocação de servidores próprios do Ministério Público para integrar os órgãos de segurança, cabendo a cada instituição, de forma autônoma e independente, a seleção, formação, controle e gestão de tais recursos humanos.

Nesse âmbito, merecem destaque as normas que permitiram o porte de arma funcional aos integrantes dos órgãos de segurança ministeriais[2] além da possibilidade de criação das Polícias Institucionais dos Ministérios Públicos[3], avanços significativos na consolidação da sua autonomia.

Vencida a questão da natureza da atividade de segurança institucional, cabe discutir acerca do objeto da atividade, seu foco e consequentes limites de atuação.

Note-se que, no âmbito da salvaguarda de dados sensíveis, áreas e instalações, materiais e imagem do Ministério Público, remanescem poucas dúvidas acerca de quando e como a segurança institucional deve atuar, observando-se sempre a devida parceria com os demais setores que tratam de cada área, incluindo-se gestão patrimonial, gestão de pessoas, assessorias de imprensa e cybersegurança.

Em relação à segurança de pessoas, especialmente na proteção dos integrantes das instituições, o gestor de segurança se depara com diversas dúvidas em relação à forma de atuar.

Nesse patamar, a primeira norma que enfrentou a questão foi a Resolução CNMP nº 116/2014, que dispõe em seu artigo 1º:

> Art. 1º Ao tomar conhecimento de fato ou notícia que implique risco ou ameaça à integridade física de membro ou de seus familiares, em razão do exercício funcional, o Procurador-Geral de cada ramo ou unidade do Ministério Público deverá adotar, por meio do órgão de segurança institucional, todas as medidas protetivas que o caso requeira, inclusive a proteção pessoal, sem prejuízo da comunicação à Polícia Judiciária.

Note-se que a norma limita a atuação nos casos de risco ou ameaça apenas à integridade física de membros, ou seus familiares, em razão do exercício funcional, excluindo-se as demais situações ou integrantes.

Após, a Resolução CNMP nº 156/2016, que instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, ampliou sobremaneira o espectro de atuação, consubstanciando em seu artigo 4º:

.....

2 Resolução CNMP nº 303, de 26 de novembro de 2024.

3 Portaria PGR/MPU nº 202, de 31 de dezembro de 2022.

> Art. 4º A segurança de pessoas compreende o conjunto de medidas voltadas a proteger a integridade física e moral de membros, ativos e inativos, de servidores e de seus respectivos familiares em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais.

Note-se a inclusão da proteção da integridade moral dos membros, inclusive inativos, além de servidores e familiares. Além disso, o dispositivo manteve a necessidade de vínculo com a atividade funcional ao instar que os riscos/ameaças devem ser decorrentes do desempenho das funções institucionais.

Em resumo, coligindo as normativas vigentes, tem-se que a atividade de segurança institucional no âmbito da segurança de pessoas tem como objeto a proteção à integridade física ou moral de membros, ativos ou inativos, e servidores, incluindo-se seus familiares, em casos de risco ou ameaça concreta ou potencial em decorrência da função.

A par da objetividade da conclusão, a prática do cotidiano apresenta situações que nem sempre são de simples resolução e, ainda, geram diversas discussões.

Nesse contexto, aponte-se desde logo o dissenso causado pela questão do denominado "vínculo indireto" dos sinistros com a função ministerial, ou seja, apesar de não decorrer de alguma atuação do integrante da instituição, tem como justificativa sua mera condição funcional.

Como exemplo, há os ataques à imagem dos integrantes por intermédio de redes sociais ou outros meios de comunicação, os quais incidem diretamente na imagem de todo o Ministério Público, ativo de elevada importância às Instituições.

Para além disso, cabe destaque ainda às situações de ameaça ou risco que, apesar de desvinculadas da atividade funcional, podem perturbar o livre desempenho das funções, como os casos de assédio e todos os tipos de importunações ofensivas efetivadas por quaisquer meios.

Nos casos expostos, enquadrados na categoria de vínculo indireto com a função ministerial, cabe ao gestor a análise acurada de cada situação a fim de aferir a possibilidade e – principalmente – a extensão do atendimento que será prestado, a evitar a banalização da atuação e, ainda, efetivar a proteção dos ativos institucionais de maior relevância.

No que se refere à extensão do atendimento, rememore-se que pode consubstanciar-se desde em orientações e acionamento dos órgãos de apoio, até no deslocamento de equipes próprias para escolta aproximada, a depender de cada caso.

Para além de tais situações de vínculo indireto, não se pode esquecer de situações que, apesar de totalmente desvinculadas da atividade ministerial, colocam o membro ou servidor em situação de grave vulnerabilidade ou risco relevante, como os casos de desastres, acidentes ou crimes graves, como casos de violência de gênero, agressões no âmbito familiar, crimes sexuais graves, entre outros.

Não há dúvida que nesses casos é devida a atuação do órgão de segurança institucional com o objetivo de prestar orientações e atendimentos urgentes e possíveis, acionar e encaminhar a vítima às autoridades competentes e, ainda, prestar suporte ao servidor ou membro até a estabilização da situação.

Discussão interessante também decorre da atuação da instituição na apuração direta de delitos relacionados a ameaças ou ataques aos seus integrantes, instalações, informações e imagem, na medida em que o Ministério Público é titular da ação penal e, ainda, possui poder investigatório amplo já plenamente reconhecido.

Não se mostra razoável que, em determinadas situações de urgência ou gravidade, o Ministério Público relegue a outros órgãos a investigação de ataques ou ameaças a seus ativos, a exemplo dos encaminhamentos para a polícia judiciária.

Nessa quadra, muitas possibilidades se abrem para tais situações, tais como a designação de membros especificamente para determinadas apurações, a atuação dos núcleos dos GAECO ou até mesmo a designação dos próprios membros que desempenham atividades de segurança institucional para presidir a investigação, sempre com ciência e anuência do promotor natural.

Atenção maior deve existir nessa última possibilidade, se há apenas uma estrutura orgânica destinada a exercer as Atividades de Inteligência e de Segurança Institucional, em que o membro exerce certamente atividade de coordenação, uma vez que não se pode confundir a Atividade de Inteligência com a de Investigação, como expressamente previsto na Doutrina de Inteligência do MP.

Em tempo, inexiste qualquer vedação ou impedimento para a providência que, a um só tempo, reforça a apuração em determinados casos e desonera a polícia judiciária de mais uma incumbência, sempre observando-se o caso concreto.

Outro ponto do qual exsurge alguma discussão é a atuação dos órgãos de segurança institucional no âmbito do apoio e assessoria para aquisição de armas de fogo por membros, em virtude do argumento de que, de tal providência, adviria um incremento de segurança. Desde logo aponte-se que há enorme divergência em relação a tal afirmação, ao passo que a posse ou o porte de arma, quando descuidados, sem o devido zelo ou formação, inobservado ainda o treinamento e a manutenção regulares, pode gerar ainda mais risco ao membro ou à sua família.

Nessa seara, respeitadas as opções políticas de cada unidade ministerial, a atuação do órgão de segurança deve limitar-se às orientações gerais em relação à aquisição de armas e/ou ocorrências vinculadas ao porte funcional do membro, além da tramitação documental referente às aquisições que dependem de anuência do órgão, excluindo-se as demais situações, a exemplo dos colecionadores, atiradores e caçadores.

Situação diversa emerge no sentido da disponibilização de cursos de formação e aperfeiçoamento regulares dos membros que optaram por adquirir arma de fogo, como essencial medida preventiva e de fomento à cultura de segurança das instituições.

Da mesma maneira, deve se afirmar no caso de providências de aquisição, guarda e gestão de armas de fogo adquiridas pela própria Instituição, nos termos das normativas vigentes, a qual deve ser tutelada integralmente pelo órgão de segurança, tratando-se de notória atividade de contrainteligência, no viés da segurança orgânica voltada à segurança de materiais.

2. O Sistema Nacional de Segurança Institucional

Considerando a necessidade de instituir um sistema nacional e uma política uniforme de segurança institucional no Ministério Público, com o estabelecimento de diretrizes gerais e mecanismos capazes de garantir, em todo o país, e a despeito das especificidades locais, as condições necessárias para o pleno exercício das atividades da Instituição e de seus integrantes, o Conselho Nacional do Ministério Público instituiu a Política de Segurança Institucional (PSI/MP) e o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP) no ano de 2016.

Nesse contexto, a PSI/MP e o SNS/MP foram criados com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito do Ministério Público, bem como garantir o pleno exercício das suas atividades.

2.1. MARCOS NORMATIVOS

A segurança institucional do Ministério Público é fundamentada em normas nacionais e locais, que estruturam sua política, seu sistema e sua operacionalização.

Os principais marcos normativos são:

a. Lei nº 12.694/2012 – Dispõe sobre medidas protetivas aos membros do MP e do Judiciário em situação de risco;

b. Resolução CNMP nº 116/2014 – Estabelece regras gerais de proteção pessoal de membros do Ministério Público;

c. Resolução CNMP nº 156/2016 – Institui a Política de Segurança Institucional do Ministério Público e o Sistema Nacional de Segurança Institucional (SNS/MP);

d. Resolução CNMP nº 294/2024 – Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências;

e. Resolução CNMP nº 303/2024 – Regulamenta, no âmbito dos ramos e unidades do Ministério Público, os arts. 6º, inciso XI, e 7°-A, ambos da Lei n° 10.826, de 22 de dezembro de 2003, com as alterações promovidas pela Lei n° 12.694, de 24 de julho de 2012, e os arts. 7º, § 1º, incisos III, alíneas “l” e “o”, e IV, alíneas “k” e “m”, 53 e 54, §§ 1º e 2º, do Decreto nº 11.615, de 21 de julho de 2023.

Essas normas estruturam o alicerce técnico e jurídico para a atuação do gestor de segurança institucional.

O gestor deve garantir que as atividades de segurança institucional estejam em plena conformidade com os marcos legais e normativos aplicáveis, incluindo Constituição Federal, Lei Geral de Proteção de Dados (LGPD), resoluções do CNMP e tratados internacionais de direitos humanos.

O cumprimento da legalidade deve ser monitorado de forma contínua, por meio de mecanismos de controle interno e externo, assegurando o respeito à proporcionalidade, à razoabilidade e à dignidade da pessoa humana.

2.2. ORGANIZAÇÃO E FUNCIONAMENTO DO SISTEMA NACIONAL DE SEGURANÇA INSTITUCIONAL

O Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP), coordenado pelo CNMP, é composto por órgãos e estruturas voltadas à uniformização, articulação e fortalecimento da segurança institucional em todo o país, quais sejam:

a. CNMP: Conselho Nacional do Ministério Público – coordenação nacional e definição de diretrizes;
b. CPAMP: Comissão de Preservação da Autonomia do Ministério Público – responsável pela gestão estratégica do sistema;
c. SESI: Secretaria Executiva de Segurança Institucional – unidade operacional executiva do sistema;
d. CPSI: Comitê de Políticas de Segurança Institucional – órgão consultivo e deliberativo;
e. Coordenadores Estaduais de Segurança Institucional – responsáveis pela implementação e integração nos ramos e unidades do Ministério Público.

O SNS/MP garante:

a. Integração e padronização de normas e protocolos;
b. Troca de informações e experiências;
c. Apoio técnico aos ramos e unidades do Ministério Público;
d. Coordenação de medidas em situações de risco de maior gravidade;
e. Capacitação em caráter geral e/ou pontual conforme demanda dos ramos e unidades do Ministério Público.

2.3. PROTEÇÃO PESSOAL DE MEMBROS E SEUS FAMILIARES DIANTE DE SITUAÇÃO DE RISCO

A proteção pessoal é uma das expressões mais sensíveis da segurança institucional. É regulamentada pela Lei nº 12.694/2012 e pela Resolução CNMP nº 116/2014.

Conforme Dalabrida (2019), o cumprimento da missão institucional reservada ao Ministério Público naturalmente atinge agentes e organizações que, visando à preservação de seus interesses ilícitos, se valem da prática de atentados e ameaças contra membros da Instituição para desencorajá-los do exercício de suas funções institucionais. Ações dessa natureza atentam contra a ordem jurídica, desafiam o Estado Democrático de Direito e ameaçam a independência do Ministério Público brasileiro.

Nesse ínterim, visando à garantia de condições para o pleno exercício das atividades da Instituição e de seus integrantes, a Resolução CNMP nº 116, de 6 de outubro de 2014, estabelece regras gerais para a proteção pessoal de membros do Ministério Público e de seus familiares diante de situação de risco decorrente do exercício da função.

O referido ato normativo prescreve que, ao tomar conhecimento de fato ou notícia que implique risco ou ameaça à integridade física de membro ou de seus familiares, em razão do exercício funcional, o Procurador-Geral de cada ramo ou unidade do Ministério Público deverá adotar, por meio do órgão de segurança institucional, todas as medidas protetivas que o caso requeira, inclusive a proteção pessoal, sem prejuízo da comunicação à Polícia Judiciária.

Além disso, a prestação de proteção pessoal pela Instituição deverá ser precedida de análise de risco e necessário planejamento técnico, operacional e logístico, assim como da alocação de recursos para execução das atividades, nos limites orçamentários e financeiros disponíveis.

A operacionalização da proteção pessoal ao membro será realizada mediante o estabelecimento de medidas de proteção pessoal, em que o protegido será submetido a determinadas normas de conduta e protocolos de segurança, previamente estabelecidos, de modo a minimizar os riscos pessoais, inclusive de terceiros, e institucionais. A implementação e a manutenção de tais medidas deverão ser condicionadas pela Instituição em termo próprio.

Importante ainda instituir uma comissão de segurança composta por membros do Ministério Público para analisar as situações de risco ou ameaças detectadas. A comissão de segurança institucional atuará imediatamente via provocação do Gabinete de Segurança Institucional, ao tomar conhecimento de eventual ameaça em desfavor de membros e/ou servidores. Essa comissão deliberará de forma colegiada sobre a concessão, prorrogação, suspensão, alteração e término de medidas protetivas em favor de membros ou servidores em situação de risco em decorrência do exercício funcional. Esse modelo de gestão possibilita o compartilhamento da responsabilidade pelas decisões tomadas pela Instituição, além de agregar conhecimento e experiência de seus integrantes na análise de cada situação.

Embora a Lei nº 12.694/2012, em seu art. 9º, estabeleça que, diante de situação de risco, decorrente do exercício da função, das autoridades judiciais ou membros do Ministério Público e de seus familiares, o fato será comunicado à polícia judiciária, que avaliará a necessidade, o alcance e os parâmetros da proteção pessoal, após o julgamento da ADI nº 5157 pelo Supremo Tribunal Federal (STF), foi declarada a inconstitucionalidade das seguintes expressões: (i) respeitado o limite máximo de 50% do número de servidores que exerçam funções de segurança, constante do § 2º do art. 7º-A da Lei nº 10.826/2003; (ii) que avaliará a necessidade, o alcance e os parâmetros da proteção pessoal, constante do *caput* do art. 9º da Lei nº 12.694/2012; (iii) de acordo com a avaliação realizada pela polícia judiciária, inscrita no § 1º do art. 9º da Lei nº 12.694/2012; (iv) segundo a avaliação a que se referem o *caput* e o § 1º deste artigo, do § 2º do art. 9º da Lei nº 12.694/2012; e (v) definidos pela polícia judiciária, a que se refere o § 4º do art. 9º da Lei nº 12.694/2012.

Nesse contexto, os procedimentos de segurança serão definidos pelo órgão de segurança institucional e podem compreender, entre outros:

a. Solicitação do interessado ou provocação da Administração;

b. Avaliação técnica do risco;

c. Decisão administrativa pela Procuradoria-Geral;

d. Acompanhamento periódico da situação;

e. Revisão semestral da necessidade de proteção.

Por sua vez, as medidas de segurança a serem prestadas podem incluir:

a. Reforço de segurança orgânica;

b. Fornecimento de colete balístico;

c. Proteção armada de membros, servidores e familiares (escolta);

d. Transferência temporária de lotação;

e. Utilização de veículos blindados;

f. Sigilo de endereço funcional ou pessoal;

g. Apoio psicológico em situações de risco prolongado;

h. Remoção provisória do integrante, a pedido;

i. Trabalho remoto.

Importante ressaltar que as medidas protetivas não podem ser impostas, devendo ser precedidas da aquiescência formal da pessoa sob proteção. Nesse sentido, seguem em anexo alguns modelos de termos de mobilização e desmobilização de escolta.

Outrossim, a eficácia das medidas protetivas depende diretamente do acatamento pelo protegido das orientações e protocolos recomendados pelo órgão de segurança. O descumprimento de tais orientações pode comprometer todo o trabalho de proteção, colocando em risco não apenas seu destinatário como também os agentes de segurança empenhados.

Deferida a prestação de proteção pessoal, a unidade ou ramo deverá comunicá-la ao CNMP, nos termos do § 3º do art. 9º da Lei nº 12.694/2012. A comunicação deverá ser acompanhada da inserção de dados sobre a situação no sistema informatizado mantido pela CPAMP, para fins de registro dos casos de riscos ou ameaça à integridade física dos membros e das respectivas medidas protetivas adotadas.

2.4. INTEGRAÇÃO E INTEROPERABILIDADE ENTRE OS SISTEMAS DE SEGURANÇA INSTITUCIONAL DO MP

O gerenciamento das políticas nacionais de segurança institucional se desenvolve de forma integrada, harmônica e em regime de corresponsabilidade entre cada ramo do Ministério Público e o Conselho Nacional do Ministério Público.

Nesse sentido, o SNS/MP promove a interoperabilidade técnica, informacional e operacional entre os Ministérios Públicos da União e dos Estados, por meio de:

a. Compartilhamento de protocolos e boas práticas;

b. Padronização de planos de segurança orgânica e ativa;

c. Programas de capacitação conjunta;

d. Sistemas de informação integrados;

e. Apoio mútuo em operações críticas ou emergenciais.

Os órgãos de segurança institucional de cada unidade do Ministério Público devem atuar em conformidade com o sistema nacional e manter fluxo contínuo de informações com a SESI/CNMP.

Para tanto, o CPSI realiza semestralmente reunião com os coordenadores e chefes da segurança institucional para alinhamento de atuação e nivelamento de conhecimento.

2.5. SEGURANÇA INSTITUCIONAL E SEGURANÇA PÚBLICA

Embora distintas, segurança institucional e segurança pública são áreas complementares. A capilaridade das forças policiais, somada à larga experiência no enfrentamento da criminalidade e de situações de crise, além da possibilidade de pronto emprego a qualquer momento, contribui de forma inequívoca para o sucesso das ações de segurança institucional.

Portanto, o gestor de segurança institucional de cada ramo ou unidade do Ministério Público deve manter interlocução direta, constante e qualificada com:

a. a Polícia Militar: apoio à proteção de membros e grandes operações;

b. a Polícia Civil/Polícia Federal/Polícia Rodoviária: cooperação investigativa e apoio técnico especializado;

c. o Corpo de Bombeiros Militar: prevenção e resposta a sinistros;

d. a Polícia Penal: monitoramento de ameaças a membros envolvidos em persecuções criminais;

e. a Segurança Institucional do Poder Judiciário: articulação de medidas conjuntas.

Necessariamente, o tráfego de dados, as informações e os conhecimentos de Inteligência devem ser realizados exclusivamente por intermédio do Canal Técnico de Inteligência[4] junto à coordenadoria de inteligência , conforme o Anexo II da Resolução CNMP nº 292/2024.

Com vistas a enfatizar a importância de uma atuação sistêmica e integrada entre a segurança institucional e as forças de segurança pública, a Resolução CNMP nº 156/2016 dispõe que o CNMP e os ramos do Ministério Público, em parceria com a Polícia Federal, a Polícia Rodoviária Federal, as Polícias Estaduais e outros órgãos afins, de natureza policial, de segurança ou de inteligência, celebrarão termos de cooperação para realização, anualmente, de cursos sobre segurança institucional, com ênfase em inteligência e contrainteligência, planejamento de operações, crime organizado, grupo de extermínio, estatuto do desarmamento, armamento e tiro, técnicas e equipamentos menos letais, direção operacional e defensiva, defesa pessoal, uso seletivo da força, conduta da pessoa protegida, técnicas operacionais, prevenção e combate a incêndios, entre outros.

É imperioso, quanto aos assuntos de inteligência e contrainteligência, que haja definições e trato direto pela coordenadoria de inteligência de cada ramo ou unidade do MP, dada a sua responsabilidade pela sustentação da Doutrina de Inteligência do MP e pela adoção de medidas de contrainteligência circundantes, conforme o Anexo II da Resolução CNMP nº 292/2024.

4 Órgão central de assessoria especializada capacitado a exercer a Atividade de Inteligência nas unidades e ramos do MP que o representa no Sistema de Inteligência do Ministério Público (SIMP). Não há denominação padronizada desse órgão nos Ministérios Públicos.

2.6. SEGURANÇA INSTITUCIONAL E INTELIGÊNCIA

Segundo Caron e Bueno[5], a segurança institucional tem como princípios a abrangência, o enfoque sistêmico e a proatividade, e deve ser entendida como a capacidade de prevenção, considerando atitudes, comportamentos e a consciência a respeito das normas de segurança de uma instituição.

Intimamente relacionada às atribuições da segurança institucional está a atividade de inteligência, com a finalidade de subsidiar o processo decisório e o planejamento estratégico, por meio da produção de conhecimentos avaliados, relevantes, úteis e oportunos, contribuindo para a redução de incertezas e para a antecipação de cenários futuros. No âmbito da Contrainteligência, essa atuação visa à proteção permanente da Instituição, mediante a neutralização de ações hostis, com enfoque preventivo e proativo.

Nesse sentido, a segurança institucional depende da Inteligência nos âmbitos estratégico, tático e operacional, sendo fundamental:

a. Produção de conhecimento sensível e sigiloso;

b. Antecipação de ameaças e identificação de vulnerabilidades;

c. Cruzamento de dados internos e externos;

d. Atuação coordenada com a inteligência da unidade ministerial da sua unidade ou ramo.

O trato técnico e sistêmico com os sistemas de inteligência de outras instituições (entre elas a Polícia Civil, Polícia Militar, Polícia Penal, Polícia Federal, Polícia Rodoviária, Ministério da Justiça e Poder Judiciário) deve ser realizado necessariamente pela coordenadoria de inteligência da unidade ou ramo do MP.

Sobre essa temática, convém registrar que a Resolução CNMP nº 292, de 28 de maio de 2024, instituiu a Política Nacional de Inteligência do Ministério Público e o Sistema de Inteligência do Ministério Público.

2.7. SEGURANÇA INSTITUCIONAL E SEGURANÇA CIBERNÉTICA

A Resolução CNMP nº 156/2016 amplia a segurança institucional para a proteção das informações digitais e dos sistemas críticos. Nesse sentido, a segurança cibernética envolve:

.....

5 CARON, Ricardo; BUENO, Vani Antônio. Inteligência e segurança institucional: uma abordagem sobre a segurança de áreas e instalações no Ministério Público. In: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Ministério Público Brasileiro**. Brasília: CNMP, Comissão de Preservação da Autonomia do Ministério Público, 2019. Publicação on-line. Disponível em: <https://www.cnmp.mp.br/portal/images/Comissoes/CPAMP/Estudos_de_Seguran%C3%A7a_Institucional.pdf>.

a. Controle de acesso lógico a sistemas sensíveis;
b. Criptografia de dados sensíveis ou estratégicos;
c. Certificação digital nos assuntos que necessitam de sigilo e validade jurídica;
d. Monitoramento de tentativas de invasão ou vazamento;
e. Integração com a TI e a segurança orgânica para proteção de redes, arquivos e dados institucionais.

A atuação do gestor inclui:

a. Interação com a área de tecnologia da informação;
b. Participação em projetos de segurança da informação;
c. Acompanhamento da classificação e do ciclo de vida de dados sensíveis.

Importa mencionar que a Resolução CNMP nº 294/2024 instituiu a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP), a qual é parte integrante da Política de Segurança Institucional do Ministério Público (PSI/MP), instituída pela Resolução nº 156, de 13 de dezembro de 2016, e com ela se compatibiliza para regulamentar o subgrupo de medidas voltadas à segurança da informação nos meios de tecnologia da informação e comunicação, em consonância com o disposto no art. 7º, § 2º, inciso I, e no art. 8º da citada Resolução.

Desse modo, os planos de segurança institucional das unidades e ramos do Ministério Público deverão contemplar o planejamento, a organização, a coordenação das atividades e do uso de recursos para a execução das ações estratégicas e o alcance dos objetivos da PNCiber-MP, com a atribuição de responsabilidades, a definição de cronogramas e a apresentação da análise de riscos e das ações de continuidade que garantam o atingimento dos resultados esperados.

Além disso, a Resolução CNMP nº 294/2024 prevê a criação de um Comitê de Gerenciamento de Crise Cibernética, que será instituído nos casos em que o incidente cibernético relevante inviabilizar o regular funcionamento dos ramos e unidades ministeriais e terá em sua composição, entre outros, o gestor de segurança institucional, da informação, cibernético ou semelhante, da unidade ou ramo ministerial.

3. Estrutura Organizacional e Responsabilidades

3.1. PAPÉIS E RESPONSABILIDADES

No âmbito dos ramos e unidades do Ministério Público brasileiro, a segurança institucional é conduzida por uma estrutura especializada, vinculada à Procuradoria-Geral, para tratar das questões afetas à área, criando mecanismos para garantir as atividades de gerência, auditoria e validação de processos sensíveis.

Dessa feita, cada ramo e unidade do Ministério Público, respeitada a autonomia administrativa, normatizará as diretrizes impostas pela Política de Segurança Institucional do Ministério Público (PSI/MP) e pelo Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP), estabelecidas na Resolução nº 156 do CNMP, com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito do Ministério Público e garantir o pleno exercício das suas atividades.

De acordo com o referido ato normativo, a atividade de segurança institucional no Ministério Público será coordenada, fiscalizada e controlada por membro do Ministério Público especificamente designado como coordenador da área por ato do Procurador-Geral do respectivo ramo, sob as diretrizes do CNMP.

3.2. HIERARQUIA DE SEGURANÇA

A hierarquia funcional da segurança institucional de cada ramo e unidade do Ministério Público brasileiro será organizada segundo critérios de conveniência e oportunidade da Administração Superior, consideradas as diferentes realidades locais, orçamentárias e organizacionais dos Ministérios Públicos Estaduais e da União.

Recomenda-se que a estrutura seja composta, no mínimo, por um membro Coordenador, que ficará incumbido de liderar, supervisionar e representar o órgão de segurança institucional, e um membro Subcoordenador ou Coordenador Adjunto, que substitui o Coordenador nos impedimentos e afastamentos.

O órgão poderá ser estruturado ainda por divisões, gerências ou núcleos especializados, que estarão diretamente subordinados ao Coordenador e cuja composição e dimensionamento podem variar conforme o porte e a demanda da unidade do Ministério Público.

Cumpre ressaltar que deve haver integração da área de segurança institucional com a corregedoria, ouvidoria e áreas administrativas, sempre com respeito à independência funcional.

É fundamental que todas as áreas da Instituição que possuem correlação com a segurança compreendam suas responsabilidades individuais e o impacto de suas decisões: o setor de engenharia deve conhecer os preceitos de segurança orgânica ao elaborar projetos de construção e reforma predial; o departamento de recursos humanos deve seguir as orientações destinadas a mitigar os riscos durante o recrutamento de novos integrantes e colaboradores; e a alta administração deve prever recursos para a aquisição de dispositivos e sistemas de segurança.

O enfoque sistêmico da segurança é determinado pela integração e interrelação de todos os setores da Instituição que possuem pertinência temática com a segurança, visando ao estabelecimento de um sistema de proteção verdadeiramente eficiente que proporcione a continuidade das atividades do órgão, e, para tanto, é importante que eventuais medidas administrativas que possam repercutir na segurança sejam previamente alinhadas com o gabinete de segurança institucional.

3.2.1. ESTRUTURA MÍNIMA RECOMENDÁVEL DE UMA UNIDADE DE SEGURANÇA INSTITUCIONAL

A unidade de segurança institucional deve possuir uma estrutura mínima capaz de assegurar a execução de suas atividades. Essa estrutura pode variar conforme o porte do Ministério Público e sua cultura organizacional.

3.3. COMITÊS E EQUIPES DE SEGURANÇA

Além da estrutura permanente da unidade de Segurança Institucional, o gestor poderá:

a. Propor à Procuradoria-Geral a criação de comissões temporárias para resposta a eventos específicos (por exemplo, comissão de crise, comitê de risco cibernético);

b. Designar equipes de resposta rápida para operações críticas ou emergências;

c. Atuar em conjunto com comitês nacionais, como o CPSI do CNMP.

Equipes externas podem ser mobilizadas por meio de convênios com forças policiais, bombeiros ou órgãos de inteligência.

Insta pontuar, ainda, que a Resolução nº 156 do CNMP, de 13 de dezembro de 2016, estabelece que cabe às instituições que compõem o SNS/MP, além da criação do órgão de segurança institucional, instituir comitê vinculado ao Procurador-Geral com o fim de realizar a gestão estratégica da segurança institucional e de articular os diversos setores da Instituição para a concretização das ações relativas à área, tudo dentro de uma concepção sistêmica de proteção e salvaguarda institucionais.

3.4. COMUNICAÇÃO INTERNA

A comunicação interna é um elemento crítico da gestão de segurança. O Coordenador deve garantir canais diretos, rápidos e seguros com:

a. Procurador-Geral de Justiça;

b. Membros do órgão de segurança institucional;

c. Servidores da segurança orgânica e ativa;

d. Diretoras e diretores administrativos e de TI;

e. Coordenadoria de inteligência do seu Ministério Público[6];

f. Demais integrantes da Instituição.

São boas práticas de comunicação:

a. Escalas de plantão com nomes e contatos atualizados;

b. Relatórios periódicos de situação e ocorrências relevantes;

c. Procedimentos Operacionais Padrão (POPs) e orientações operacionais com linguagem clara;

d. Sigilo e compartimentação da informação sensível;

e. Reuniões mensais de alinhamento com os gerentes e chefes de núcleo, se houver.

A comunicação também deve garantir a padronização de respostas, especialmente em incidentes, ameaças, crises ou acidentes.

6 Órgão central de assessoria especializada capacitado a exercer a Atividade de Inteligência nas unidades e ramos do MP que o representa no SIMP. Não há denominação padronizada desse órgão nos Ministérios Públicos.

4. Gestão de Riscos

A gestão de riscos na segurança institucional tem como finalidade antecipar ameaças, minimizar vulnerabilidades e reduzir os impactos de eventos que possam comprometer a integridade de pessoas, informações, instalações e da própria Instituição. Deve ser conduzida com base em metodologia técnica, continuada, oportuna e proativa.

4.1. METODOLOGIA E TÉCNICAS DE GESTÃO DE RISCOS

O processo de gestão de riscos pode ser conduzido com base em metodologias como a ISO 31000 e princípios da análise de riscos corporativa adaptada à segurança institucional, com foco nos seguintes eixos:

a. Etapas principais:

- Identificação dos riscos: reconhecimento das ameaças (internas e externas);
- Análise dos riscos: determinação de probabilidade e impacto;
- Avaliação dos riscos: hierarquização e definição de resposta;
- Tratamento dos riscos: adoção de medidas de mitigação, transferência, aceitação ou eliminação;
- Monitoramento e revisão: acompanhamento contínuo e reavaliação a cada seis meses (no mínimo).

b. Técnicas aplicáveis:

- Matriz de riscos (probabilidade x impacto);
- Indicadores de ameaça (boletins, investigações, relatórios de inteligência);
- Entrevistas e formulários sigilosos;
- Contramedidas de vigilância técnica (CMVT) ambiental (física e eletrônica) e simulações.

A análise documental e situacional de ambientes, rotinas e pessoas em risco é conduzida pelos núcleos técnicos da unidade de Segurança Institucional.

4.2. PROCESSO DE GESTÃO DE RISCOS

A unidade de Segurança Institucional deve manter um processo permanente, com protocolos definidos para cada tipo de risco (pessoal, patrimonial, cibernético, institucional), observadas as seguintes fases práticas:

a. Abertura de procedimento sigiloso;
b. Coleta de informações com apoio da inteligência;
c. Inspeções em campo (residências, promotorias, sedes);
d. Elaboração de Relatório Técnico de Risco (RTR);
e. Deliberação preliminar e cautelar do Coordenador (ou da PGJ, em casos graves);
f. Aplicação de medidas preventivas ou reativas;
g. Acompanhamento com reavaliação periódica;
h. Trâmite por meio da comissão de segurança institucional.

Todos os atos devem ser documentados e protegidos por acesso restrito.

4.3. 4.3. GESTÃO DE RISCOS EM SEGURANÇA ORGÂNICA

A segurança orgânica envolve:

a. Instalações físicas (prédios, portarias, garagens);
b. Equipamentos (câmeras, escâneres de raios X, detectores de metais, alarmes, TI);
c. Documentação sensível;
d. Sistemas de comunicação e controle;
e. Segurança de pessoal (recrutamento, credenciamento, desligamento).

Ações específicas:

a. Auditorias de vulnerabilidade física e tecnológica;
b. Protocolos de controle de acesso (pessoas, veículos, chaves e entregas);
c. Estabelecimento de Procedimento Operacional Padrão (POP);
d. CMVT eletrônicas e inspeção de segurança ambiental;

e. Inventário de bens críticos;

f. Plano de manutenção preventiva;

g. Integração com a TI para controle de segurança digital;

h. Análise de vida social pregressa;

i. Protocolos de segurança para realização de concursos públicos.

O núcleo específico do órgão de segurança institucional deve executar vistorias e varreduras, elaborando relatórios sobre pontos críticos, equipamentos expostos e fluxos de risco.

Considerando a sensibilidade das atividades a serem desenvolvidas no Ministério Público, todos os integrantes que ingressarem por meio de concurso público, cedidos, nomeados para cargos em comissão, à disposição ou que possuam vínculo de prestação de serviços devem ser submetidos à criteriosa avaliação da vida social pregressa com vistas a detectar situações ou fatos que eventualmente desabonem ou contraindiquem seu ingresso ou acesso ao Ministério Público. O resultado da pesquisa deverá ser levado em conta para a posse ou contratação.

A realização de concursos públicos para seleção de servidores e de membros também enseja a implementação de protocolos específicos para prevenir a admissão de pessoas com perfil inadequado ou que possam comprometer a segurança, a imagem e a reputação da Instituição.

Para tanto, é necessário que o edital do certame seja revisado pela unidade de Segurança Institucional a fim de assegurar que suas diretrizes estejam de acordo com os princípios da segurança institucional. Outrossim, a cada etapa do processo seletivo, deve-se implementar medidas voltadas a coibir fraudes e garantir a lisura dos concursos e seleções, desde o edital até a nomeação.

Ações específicas:

a. Revisão dos editais dos concursos e seleções para estagiários e cursos de pós-graduação;

b. Proibição de uso de aparelhos celulares e outros dispositivos eletrônicos nos locais de prova;

c. Emprego de detectores de metais e de dispositivos de radiofrequência;

d. Treinamento dos fiscais de prova;

e. Reforço da segurança nos locais de prova;

f. Apoio da Polícia Militar para realização de busca pessoal em caso de fundada suspeita.

4.4. 4.4. GERENCIAMENTO DE INCIDENTES

O **incidente de segurança** é qualquer ocorrência que comprometa (ou tenha o potencial de comprometer) a integridade de pessoas, áreas e instalações ou informações institucionais.

Tipos mais comuns:

a. Ameaça direta a membros ou servidores;
b. Invasão física ou digital;
c. Sabotagem, espionagem, vandalismo;
d. Incêndios, sinistros, falhas operacionais.

Protocolo básico de resposta:

a. Acionamento da unidade de Segurança Institucional ou responsável de plantão;
b. Contenção inicial da ocorrência;
c. Comunicação ao Coordenador;
d. Registro e investigação técnica;
e. Adoção de contramedidas;
f. Elaboração de relatório pós-incidente.

A atuação deve ser rápida, sigilosa e documentada, com possível articulação com órgãos externos (Polícia Militar, Polícia Civil, Bombeiros, TI, Corregedoria etc.).

4.5. PLANEJAMENTO DE CONTINGÊNCIA E RESPOSTA A EMERGÊNCIAS

O planejamento de contingência consiste em prever cenários críticos e preparar respostas organizadas, evitando descontinuidades dos serviços institucionais e minimizando impactos.

O controle de danos compreende uma série de medidas que visam avaliar a gravidade de um dano decorrente de um incidente, o comprometimento dos ativos da Instituição e as suas consequências, incluindo a imagem institucional.

Elementos essenciais do plano:

a. Mapeamento de ativos críticos (pessoas, sistemas, instalações);
b. Procedimentos alternativos (operações remotas, realocação);

c. Protocolos de evacuação, isolamento, contenção e comunicação;

d. Escalamento de resposta e cadeia de comando;

e. Exercícios simulados e treinamentos periódicos.

f. Responsabilidade do Gestor de Segurança Institucional;

g. Elaborar e revisar planos para eventos distintos (ataques, incêndios, blecautes, vazamento de dados);

h. Testar planos ao menos uma vez por ano;

i. Integrar o plano às diretrizes institucionais de continuidade de negócios.

5. Procedimentos Operacionais de Segurança

Os procedimentos operacionais são essenciais para garantir padronização, eficiência e rastreabilidade nas atividades de segurança institucional. Devem ser claros, objetivos, revisados e compatíveis com os riscos identificados.

5.1. SEGURANÇA EM PROCESSOS E ATIVIDADES DIÁRIAS

O cotidiano do Ministério Público envolve movimentação constante de pessoas, veículos, informações e documentos sensíveis. Para isso, a unidade de Segurança Institucional deve assegurar:

Boas práticas operacionais:

a. Identificação e registro de pessoas, veículos e objetos no momento do acesso às sedes;
b. Acompanhamento de visitantes por servidores autorizados;
c. Detecção de armas e objetos que representem risco às pessoas e instalações;
d. Preservação da cadeia de custódia de documentos sigilosos;
e. Evitar exposição de rotinas ou agendas públicas de membros sob risco;
f. Avaliação de segurança em atividades externas (audiências, perícias, diligências).

Rotinas que exigem atenção reforçada:

a. Atendimento a pessoas não identificadas;
b. Presença de veículos suspeitos próximos às sedes;
c. Entregas não programadas;
d. Instalações em reforma (fragilidade de barreiras físicas);
e. Uso de equipamentos de gravação, fotografia ou drones sem autorização.

5.2. CONTROLE DE ACESSOS E INFORMAÇÃO

O controle de acesso é um pilar da segurança orgânica, tanto física quanto digital. Deve ser estruturado com níveis de permissão diferenciados.

5.2.1. MEDIDAS RECOMENDADAS

Acesso físico:

a. Identificação visual e biométrica nos prédios;
b. Catracas eletrônicas e controle de veículos;
c. Pórticos detectores de metais;
d. Escâneres de raios X;
e. Crachás com QR Code ou *chips*;
f. Áreas restritas com autorização formal;
g. Monitoramento por circuito fechado de TV (CFTV).

Acesso informacional:

a. Políticas de senhas seguras e de acesso por perfis;
b. Criptografia de dados sensíveis;
c. *Backup* automático e em servidores protegidos;
d. Bloqueio remoto de contas ou dispositivos;
e. Assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS) pelos usuários.

5.3. SEGURANÇA NO USO DE RECURSOS E FERRAMENTAS

Equipamentos de uso institucional (rádios, *notebooks*, veículos, armamento) devem ser utilizados de forma responsável, com rastreabilidade e conservação asseguradas.

Recomendações:

a. Inventário atualizado dos recursos de segurança;
b. Controle de saída e devolução de equipamentos;
c. Manutenção preventiva de veículos e equipamentos eletrônicos;

d. Uso exclusivo dos armamentos e rádios por servidores autorizados;

e. Comunicação interna sigilosa por meios seguros (*apps* criptografados, rádio digital).

5.4. PROCEDIMENTOS DE EMERGÊNCIA

Diante de eventos inesperados (ameaças, sinistros, falhas), a unidade de Segurança Institucional deve seguir protocolos preestabelecidos.

Ações imediatas:

a. Avaliação preliminar da situação;

b. Contenção de danos e evacuação, se necessário;

c. Comunicação à coordenação e, se o caso, à PGJ;

d. Acionamento das forças externas (PM, Bombeiros, SAMU, TI);

e. Registro detalhado da ocorrência (com fotos, vídeos, testemunhos);

f. Produção de relatório técnico e análise de falhas;

g. Revisão dos procedimentos e reforço das medidas preventivas.

Tipos de emergência abordados:

a. Incêndio ou pane elétrica;

b. b) Vazamento de informação sensível;

c. c) Invasão física ou digital;

d. d) Sabotagem de equipamentos em áreas sensíveis;

e. e) Ameaça a membro/servidor;

f. f) Falha de comunicação em operação.

Planos a serem mantidos:

g. a) Plano de abandono de área;

h. b) Plano de evacuação em incêndio;

i. c) Rota de fuga sinalizada;

j. d) Ponto de encontro e controle de presença;

k. e) Plantão de emergência com escala atualizada.

6. Gestão de Pessoas e Cultura de Segurança

A segurança institucional é um esforço coletivo. Seu êxito depende do engajamento dos membros e servidores, especialmente daqueles diretamente envolvidos com as ações da unidade de Segurança Institucional. Cabe ao gestor implementar práticas eficazes de seleção, capacitação, motivação e conscientização, criando uma cultura organizacional de segurança.

A gestão de pessoas talvez seja o maior desafio a ser enfrentado pelo gestor de segurança institucional, na medida em que é a abordagem que se concentra em maximizar o desempenho dos colaboradores por meio do recrutamento, qualificação, treinamento, desenvolvimento e retenção de talentos.

Não obstante, também é fundamental que o público interno da instituição compreenda a importância de se implementar as medidas de segurança recomendadas para aumentar o nível de proteção do órgão e dos seus integrantes.

Na prática, observa-se que a segurança é inversamente proporcional ao conforto. O desafio que se apresenta consiste justamente em equilibrar o desejo por comodidade da maioria das pessoas, com a necessidade da implementação de protocolos e rotinas preventivas. Muitas vezes, os destinatários dessas medidas são os primeiros a ignorar ou mesmo resistir aos protocolos destinados a neutralizar ou mitigar riscos.

Verifica-se que o sucesso das ações de segurança institucional depende diretamente da participação efetiva de todos os integrantes do órgão. Nesse sentido, deve-se difundir a cultura de segurança para que todos compreendam e assumam sua parcela de responsabilidade, adotando uma postura proativa e consciente que viabilize resultados profícuos e duradouros.

O mês de agosto foi instituído formalmente como o **Mês da Segurança Institucional** por meio de deliberação do Comitê de Políticas de Segurança Institucional do Ministério Público (CPSI-MP). Todos os anos, cada ramo do Ministério Público promove diversas ações como campanhas, publicações, cursos e atividades sobre o tema para promover a cultura de segurança na Instituição. São exemplos de ações típicas do mês da segurança institucional: instruções de armamento e tiro; curso de direção defensiva; palestras sobre boas práticas de segurança pessoal e profissional; os perigos da internet e como se proteger de golpes virtuais; oficina de blindagem de celulares e de redes sociais; seminários de defesa pessoal; oficinas de primeiros socorros; treinamento para combate a princípio de incêndio e técnicas para evacuação de áreas de risco, entre outros.

6.1. SELEÇÃO E DESLIGAMENTO DE INTEGRANTES DA UNIDADE DE SEGURANÇA E DE VIGILANTES TERCEIRIZADOS

A equipe da segurança institucional pode ser composta por:

a. Servidores do Ministério Público;

b. Policiais civis e militares;

c. Bombeiros Militares;

d. Profissionais cedidos por órgãos de segurança pública;

e. Vigilantes terceirizados.

Critérios de seleção recomendados:

a. Análise permanente de antecedentes funcionais e criminais (do agente de segurança e seus familiares);

b. Avaliação de perfil comportamental e histórico de conduta;

c. Capacidade de operar sob sigilo e em situações críticas;

d. Conhecimentos prévios em segurança, defesa pessoal, direção operacional, TI ou Inteligência;

e. Para cargos de chefia: liderança, proatividade e capacidade de tomada de decisão rápida.

O Setor de Análise e Contramedidas é responsável pela verificação da idoneidade dos candidatos (análise biográfica e funcional).

Desligamento:

a. Deve ser conduzido de forma discreta e documentada;

b. O desligado não deve manter acesso a sistemas, dependências restritas ou informações sensíveis;

c. Deve assinar termo de devolução de material e de confidencialidade pós-vínculo.

6.2. CONSCIENTIZAÇÃO E ENGAJAMENTO DE PESSOAL

Todos os integrantes do Ministério Público – mesmo fora da estrutura da unidade de Segurança Institucional – devem ter consciência da importância da segurança institucional. O Coordenador deve promover:

a. Campanhas internas de educação para a segurança (digitais, físicas, operacionais);
b. Informativos periódicos com orientações práticas;
c. Quadros de avisos e boletins sigilosos, com alertas sobre condutas suspeitas;
d. Envolvimento de chefias e diretores administrativos como multiplicadores de boas práticas.

A compreensão de que "segurança é responsabilidade de todos" fortalece a resiliência institucional.

Esse entendimento deve ser constantemente promovido não apenas entre os integrantes que atuam na unidade de segurança institucional, mas perante todo o público interno da Instituição.

6.3. MOTIVAÇÃO PARA PRÁTICAS DE SEGURANÇA INSTITUCIONAL

A atuação na segurança institucional é intensa, exigente e, muitas vezes, silenciosa. Por isso, o gestor deve investir em:

a. Reconhecimento institucional (elogios, promoções, indicações para capacitações externas);
b. Inclusão dos integrantes em grupos estratégicos de planejamento;
c. Comunicação clara sobre o impacto da segurança nas operações do Ministério Público;
d. Acesso prioritário a treinamentos e cursos de aperfeiçoamento.

Resultados positivos, como a prevenção de incidentes e a proteção de membros em risco, devem ser valorizados.

6.4. COMUNICAÇÃO E *FEEDBACK* SOBRE SEGURANÇA INSTITUCIONAL

A comunicação eficaz é vital. O gestor deve garantir que:

a. Toda a equipe tenha clareza sobre suas atribuições, limitações e canais de atuação;
b. Os protocolos e os procedimentos operacionais padrão estejam disponíveis, atualizados e acessíveis;
c. Ocorrências sejam relatadas com rapidez e precisão;
d. Haja abertura para sugestões e denúncias internas (inclusive anônimas) sobre falhas de segurança.

Reuniões periódicas com os gerentes, chefes de núcleo e operadores de campo são fundamentais para alinhar estratégias e ajustar práticas.

6.5. CAPACITAÇÕES E TREINAMENTOS

A profissionalização contínua da equipe é elemento obrigatório da segurança institucional.

Capacitações recomendadas:

a. Técnicas de segurança ativa (proteção pessoal, autodefesa, tiro defensivo);
b. Análise de riscos;
c. Noções da atividade de inteligência;
d. Doutrina de segurança de autoridades;
e. Técnicas de entrevista;
f. Atendimento pré-hospitalar tático (APH);
g. Técnicas para elaboração de Planos de Segurança Orgânica;
h. Contrainteligência aplicada à segurança institucional e a varreduras ambientais;
i. Gestão de crises e resposta a emergências;
j. Segurança cibernética e proteção de dados;
k. Condução de veículos em situação crítica;
l. Relações interpessoais e atendimento a pessoas sob estresse ou ameaça;
m. Participação em feiras e eventos de segurança para conhecer novas práticas e tecnologias;
n. Técnicas de análise de percurso;
o. Técnicas de Contravigilância;
p. Capacitação em coleta de fontes abertas.

É imperioso, quanto aos assuntos de inteligência e contrainteligência, que haja definições e trato direto pela coordenadoria de inteligência de cada ramo ou unidade do MP, dada a sua responsabilidade pela sustentação da Doutrina de Inteligência do MP e pela adoção de medidas de contrainteligência circundantes.

Instrumentos para execução:

a. Parceria com a Escola Superior do Ministério Público (ESMP);

b. Convênios com Polícia Militar, Bombeiros, PC, PF e SENASP;

c. Inclusão em treinamentos do CNMP (via CPAMP e SESI);

d. Realização de exercícios simulados periódicos;

e. Visitas a unidades de segurança institucional de outros ramos e unidades do Ministério Público e outras instituições públicas e privadas para troca de experiências.

7. Tecnologias de Apoio à Segurança

A adoção de tecnologias adequadas é decisiva para garantir segurança em tempo real, prevenir ameaças e documentar evidências. O gestor de segurança institucional deve manter diálogo permanente com a área de tecnologia da informação (TI) e buscar inovação com responsabilidade, observando as exigências legais e os princípios da segurança institucional.

7.1. FERRAMENTAS E SISTEMAS DE MONITORAMENTO

O monitoramento contínuo permite à unidade de Segurança Institucional agir preventivamente, detectar irregularidades e intervir de maneira tempestiva, além de auxiliar na identificação e na responsabilização de infratores ou agentes hostis.

7.1.1. PRINCIPAIS FERRAMENTAS

As principais ferramentas são:

a. CFTV (Circuito Fechado de TV) com gravação digital: câmeras com inteligência artificial (IA), reconhecimento facial, leitura de placas veiculares e detecção de movimentos em áreas sensíveis;

b. Controle de acesso eletrônico: catracas biométricas, crachás com QR Code, RFID ou NFC, detectores de metais e escâneres de raios X, cancelas automatizadas para controlar o acesso de veículos com sistema de reconhecimento de placas ou de reconhecimento facial;

c. Sistema de alarme integrado: sensores de presença, vidros quebrados, portas forçadas e alertas silenciosos;

d. Botão de pânico em salas estratégicas;

e. Monitoramento de perímetro via drones ou sensores externos, especialmente em unidades isoladas;

f. Rastreamento de veículos oficiais e uso de rádio digital criptografado.

Integração com a unidade de Segurança Institucional:

g. O gestor deve manter acesso remoto ao sistema de monitoramento das unidades do MP;

h. Todas as imagens e *logs* devem ser arquivados com segurança e criptografia;

i. A equipe de segurança deve ser treinada para interpretar alertas e operar os sistemas.

7.2. INOVAÇÕES EM SEGURANÇA ORGÂNICA

Além dos sistemas tradicionais, o gestor de segurança institucional deve acompanhar e avaliar soluções inovadoras que possam ser adaptadas à realidade do Ministério Público:

Exemplos de inovações:

a. *Softwares* de análise comportamental por vídeo, que detectam padrões de movimentação anormal;

b. Sensores inteligentes de fumaça, gás e temperatura com acionamento remoto do Corpo de Bombeiros;

c. Sistema de iluminação tática de emergência com acionamento automatizado em caso de sinistro ou pane elétrica;

d. Revestimentos de blindagem arquitetônica (vidros, divisórias e portas);

e. Controle de acesso a documentos físicos sensíveis por RFID e tranca eletrônica;

f. Dispositivos de detecção de escutas ambientais e câmeras escondidas – CMVT;

g. Sistema de monitoramento por vídeo com reconhecimento facial.

7.3. TECNOLOGIAS DE GESTÃO DE RISCOS E EMERGÊNCIAS

A tecnologia também apoia a gestão estratégica e operacional de riscos, por meio de ferramentas e práticas recomendadas, e boas práticas de implantação tecnológica.

7.3.1. FERRAMENTAS E PRÁTICAS RECOMENDADAS

São ferramentas e práticas recomendadas:

a. Plataformas de gestão de incidentes e riscos (SIGR, SGRI, entre outras): permitem registrar, classificar, tratar e acompanhar ocorrências e vulnerabilidades;

b. *Softwares* de mapeamento de riscos georreferenciados (para promotorias em áreas sensíveis);

c. Aplicativos institucionais de alerta e emergência para membros (botão de pânico, GPS, chamada segura);

d. Banco de dados seguro para perfis de risco, ameaças e proteção de membros sob risco;

e. Integração com sistemas da segurança pública (videomonitoramento urbano, centro integrado de comando e controle – CICC).

7.3.2. BOAS PRÁTICAS DE IMPLANTAÇÃO TECNOLÓGICA

São boas práticas de implantação tecnológica:

a. Realizar estudos técnicos prévios de viabilidade e impacto;

b. Adquirir tecnologias que sigam padrões da LGPD, da segurança da informação e da normatização do CNMP;

c. Integrar a TI e a unidade de Segurança Institucional desde o início dos projetos de segurança tecnológica;

d. Testar, documentar e treinar os usuários em qualquer nova ferramenta;

e. Estabelecer protocolos de atualização, manutenção preventiva e descarte.

8. *Compliance* e Normas Regulatórias

A segurança institucional deve ser exercida com estrita observância dos princípios constitucionais, das normas legais e das boas práticas regulatórias. A conformidade – ou *compliance* – garante legitimidade, segurança jurídica e integridade das ações da unidade de Segurança Institucional.

8.1. LEGISLAÇÃO APLICÁVEL

O gestor deve assegurar que todas as atividades da unidade de Segurança Institucional estejam em consonância com os seguintes atos normativos.

8.1.1. LEGISLAÇÃO NACIONAL

a. Lei nº 12.694/2012 – Estabelece medidas de segurança para autoridades do Ministério Público e do Poder Judiciário em risco;

b. Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) – Regulamenta o tratamento de dados pessoais, inclusive aqueles utilizados na segurança institucional;

c. Lei nº 8.666/1993 e Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos) – Normas aplicáveis à contratação de serviços de segurança privada, monitoramento e tecnologia;

d. Lei nº 10.826/2003 – Dispõe sobre registro, posse e comercialização de armas de fogo e munição e sobre o Sistema Nacional de Armas (SINARM);

e. Código Penal e Lei de Abuso de Autoridade (Lei nº 13.869/2019) – Delimita o uso legítimo da força, coleta de dados, monitoramento e abordagem a pessoas.

8.1.2. 8.2.1 NORMAS DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

a. Resolução nº 156/2016 – Institui a Política Nacional de Segurança Institucional e o SNS/MP;

b. Resolução nº 116/2014 – Proteção pessoal de membros e familiares;

c. Resolução nº 303/2024 – Regulamenta a aquisição, o registro e a posse de armas de fogo por membros e servidores do MP;

d. Resolução nº 260/2023 – Aprova a Doutrina de Inteligência do Ministério Público;

e. Resolução nº 270/2023 – Assegura a proteção a membros inativos e seus familiares que estejam em situação de risco em razão do exercício da função, incluindo ex-Procuradores-Gerais;

f. Resolução nº 292/2024 – Institui a Política Nacional de Inteligência do Ministério Público e o Sistema de Inteligência do Ministério Público, e dá outras providências;

g. Resolução nº 294/2024 – Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências; e

h. Resolução nº 310/2025 – Regula a atividade do Ministério Público na investigação de crimes decorrentes de intervenções dos órgãos de segurança pública.

8.2. CERTIFICAÇÕES E PADRÕES DE QUALIDADE

Embora a segurança institucional pública não exija certificações obrigatórias, o gestor pode adotar práticas alinhadas a normas internacionais para aprimorar a qualidade e a rastreabilidade das ações:

Referências recomendadas:

a. ISO/IEC 31000 – Gestão de riscos (aplicável à estruturação do processo de análise e mitigação de riscos);

b. ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação;

c. ABNT NBR 15247 – Procedimentos e requisitos para serviços de vigilância patrimonial;

d. ABNT NBR 5410 e 17240 – Normas de sistemas de detecção e alarme de incêndio.

e. Normas Técnicas Estaduais referentes à Segurança Contra Incêndio e Pânico;

A incorporação desses padrões melhora o controle interno, facilita auditorias e promove reconhecimento técnico do trabalho da unidade de Segurança Institucional.

8.3. AUDITORIAS DE SEGURANÇA

A auditoria é instrumento de controle interno que permite avaliar a eficácia, a legalidade e a eficiência das ações de segurança. Deve ser exercida de forma periódica e pode ser:

a. Interna: conduzida pela própria Corregedoria-Geral ou setor de controle interno do Ministério Público;

b. Externa: realizada por órgãos como o CNMP, o TCE, ou mediante cooperação com forças de segurança.

8.3.1. OBJETIVOS DA AUDITORIA

A auditoria tem por objetivos:

a. Verificar conformidade com normativos legais e administrativos;
b. Identificar fragilidades operacionais e de controle;
c. Avaliar a qualidade dos serviços terceirizados;
d. Analisar a gestão de contratos, escalas, equipamentos e relatórios;
e. Emitir recomendações de ajustes, melhorias ou correções.

8.3.2. BOAS PRÁTICAS

São boas práticas relacionadas à auditoria:

a. Manter toda a documentação organizada, atualizada e rastreável;
b. Garantir acesso à informação auditável (escala, ocorrências, POPs, vídeos, registros);
c. Promover auditorias periódicas (semestrais ou anuais) com relatórios formais.

9. Segurança Ambiental e Sustentabilidade

A segurança institucional moderna deve integrar preocupações ambientais à sua atuação, garantindo não apenas a proteção de pessoas e ativos, mas também a preservação dos recursos naturais, o cumprimento de normas ambientais e a adoção de práticas sustentáveis. Essa abordagem amplia a legitimidade do Ministério Público e fortalece a imagem institucional como órgão comprometido com o desenvolvimento responsável.

9.1. PRÁTICAS SUSTENTÁVEIS E SEGURANÇA

A segurança sustentável busca reduzir impactos ambientais sem comprometer a eficácia da proteção institucional. Recomenda-se que o gestor incentive algumas práticas:

a. Substituição gradual de equipamentos por modelos com menor consumo de energia (ex.: câmeras IP com sensores de presença, iluminação LED);

b. Implantação de sistemas de energia solar em edificações do Ministério Público com alta demanda energética de segurança (CFTV, alarmes, TI);

c. Reaproveitamento de água para uso em hidrantes, jardins e limpeza externa;

d. Implantação de logística reversa para descarte adequado de baterias, rádios, cabos e equipamentos eletrônicos;

e. Racionalização do uso de papel, com digitalização de relatórios de segurança e registros operacionais;

f. Promoção de campanhas internas para reduzir o desperdício de recursos em ambientes operacionais.

9.2. GESTÃO DE IMPACTOS AMBIENTAIS

A unidade de Segurança Institucional também deve prevenir e mitigar riscos ambientais que possam gerar danos à saúde, ao meio ambiente e ao funcionamento da Instituição, especialmente em casos de:

a. Incêndios em instalações do Ministério Público;

b. Vazamento de combustíveis ou produtos químicos (ex.: geradores de energia, extintores, oficinas ou empresas contratadas para a manutenção de equipamentos ou instalações);

c. Armazenamento inadequado de materiais inflamáveis ou contaminantes;

d. Destinação incorreta de resíduos de obras ou reformas em unidades do Ministério Público;

e. Ocorrências em áreas de proteção ambiental ou zonas urbanas com risco de contaminação.

São medidas preventivas:

a. Vistorias técnicas em todas as instalações ministeriais;

b. Elaboração de planos de contingência ambiental (em conjunto com os setores de Engenharia e Meio Ambiente);

c. Inspeções periódicas nos sistemas de detecção de fumaça, dutos, fiação elétrica e geradores;

d. Inspeção periódica das edificações para certificação das condições de segurança, conforme normas técnicas do Corpo de Bombeiros Militar Estadual;

e. Realização periódica de treinamentos de combate a princípio de incêndio com o uso de extintores;

f. Parceria com o Corpo de Bombeiros e com órgãos ambientais, especialmente em construções, reformas e grandes eventos.

9.3. POLÍTICAS DE REDUÇÃO DE RISCOS AMBIENTAIS

A atuação integrada entre segurança institucional e meio ambiente é estratégica para:

a. Evitar sanções administrativas e responsabilização civil;

b. Assegurar a continuidade das operações institucionais em caso de desastre;

c. Promover cultura interna de responsabilidade ecológica e uso racional dos recursos.

Sugestões de políticas institucionais a serem apoiadas pela unidade de Segurança Institucional:

a. Inclusão de critérios ambientais nas licitações de segurança e monitoramento;

b. Implantação de Plano de Gerenciamento de Resíduos Sólidos (PGRS) nas unidades do Ministério Público;

c. Treinamento dos vigilantes e brigadistas quanto ao descarte seguro de materiais;

d. d) Avaliação de fornecedores terceirizados quanto à responsabilidade ambiental.

10. Análise de Incidentes e Lições Aprendidas

A resposta eficaz a um incidente de segurança não se encerra com o seu controle imediato. O verdadeiro aprimoramento surge da análise sistemática do ocorrido, da identificação de causas e da aplicação de mudanças para evitar reincidências. O gestor de segurança institucional deve institucionalizar esse processo.

10.1. INVESTIGAÇÃO DE ACIDENTES

Todo incidente significativo – envolvendo riscos à integridade de pessoas, falhas operacionais, exposição de dados ou danos ao patrimônio – deve ser objeto de investigação técnica sigilosa, seguindo as etapas adiante expostas:

a. Registro detalhado da ocorrência: dia, horário, local, envolvidos, imagens, documentos, testemunhas;
b. Isolamento do cenário (quando aplicável);
c. Coleta e análise de evidências físicas e digitais;
d. Entrevistas com testemunhas e operadores;
e. Emissão de parecer técnico com hipóteses e causas prováveis;
f. Classificação da gravidade e da falha (operacional, estrutural, humana, cibernética);
g. Encaminhamento do relatório ao Coordenador e à Administração Superior.

O relatório deve ser mantido sob sigilo e classificado conforme grau de sensibilidade, com cópias controladas.

10.2. ANÁLISE CAUSAL

A análise causal permite compreender por que o incidente ocorreu e quais fatores contribuíram para a sua materialização. As metodologias mais utilizadas são:

a. Diagrama de Ishikawa (espinha de peixe): identifica causas por categorias (pessoas, processos, equipamentos, ambiente);

b. Método dos 5 Porquês: busca a causa-raiz por meio de perguntas sucessivas;

c. Análise de Barreiras: identifica onde os controles falharam ou não existiam.

O objetivo não é buscar culpados, mas corrigir vulnerabilidades sistêmicas.

10.3. APLICAÇÃO DE LIÇÕES PARA MELHORIA CONTÍNUA

A real utilidade da investigação reside na correção de falhas e na prevenção de novos riscos. O gestor de segurança institucional deve:

a. Atualizar os Procedimentos Operacionais Padrão (POPs) conforme as conclusões;

b. Incluir o aprendizado nos treinamentos regulares;

c. Comunicar internamente as mudanças, preservando o sigilo;

d. Revisar protocolos de contingência e resposta conforme as falhas identificadas.

O "banco de lições aprendidas" pode ser estruturado internamente como um repositório seguro, para uso interno da equipe de segurança e da alta administração.

10.4. REVISÃO DE PROCEDIMENTOS APÓS INCIDENTES

Todo incidente relevante deve ensejar uma revisão específica dos procedimentos relacionados, com avaliação crítica e propostas de ajustes imediatos.

Ações recomendadas:

a. Reunião técnica pós-incidente com os envolvidos;

b. Verificação de falhas de conduta, comunicação, tempo de resposta, equipamento ou estrutura;

c. Definição de novo procedimento ou ajuste do protocolo existente;

d. Testes simulados do novo padrão;

e. Inclusão do tema no cronograma de capacitações.

O ciclo "ocorrência → análise → correção → treinamento" deve ser institucionalizado como prática obrigatória da unidade de Segurança Institucional.

11. Plano de Contingência e Recuperação

A existência de planos de contingência é indispensável para garantir que o Ministério Público possa manter ou retomar suas funções essenciais mesmo diante de situações adversas, como desastres naturais, atentados, falhas tecnológicas, incêndios ou ameaças à vida de seus integrantes. O gestor de segurança institucional deve liderar ou participar da elaboração, execução e atualização desses planos, em articulação com as áreas estratégicas da Instituição.

11.1. ELABORAÇÃO DE PLANOS DE CONTINGÊNCIA

O plano de contingência define ações emergenciais e rotinas alternativas a serem adotadas durante eventos de interrupção crítica ou risco elevado.

Elementos fundamentais:

a. Identificação de ameaças e cenários críticos (ex.: incêndio, ataque armado, sequestro, blecaute, pane de TI);
b. Mapeamento dos ativos essenciais: pessoas-chave, sistemas, instalações, documentos e informações críticas;
c. Definição de prioridades operacionais e serviços que não podem ser interrompidos;
d. Plano de ação por tipo de incidente, com responsáveis designados e protocolos claros;
e. Cadeia de comando emergencial, com contatos atualizados e mecanismos de substituição imediata;
f. Designação de pontos de apoio, sedes alternativas e meios de comunicação redundantes.

O plano deve ser documentado, testado e validado, com revisões anuais ou sempre que houver mudanças estruturais.

11.2. PLANOS DE RECUPERAÇÃO PÓS-CRISE

Após a contenção do incidente, é necessário implementar planos de recuperação voltados à normalização das atividades institucionais, com foco em:

a. Reintegração de sistemas e dados;
b. Reconstrução de infraestrutura ou instalações danificadas;
c. Acompanhamento psicológico de membros e servidores afetados;
d. Restabelecimento da confiança pública;
e. Revisão das medidas de segurança e auditoria do ocorrido.

Etapas da recuperação:

a. Avaliação de danos e impacto;
b. Mobilização de equipes técnicas (TI, Engenharia, Segurança, Comunicação);
c. Ações emergenciais de recomposição física e lógica;
d. Comunicação oficial à imprensa e órgãos parceiros, quando aplicável;
e. Relatório final e recomendação de medidas permanentes.

A recuperação também deve incluir ações de reparação de imagem e resgate da rotina institucional com segurança reforçada.

11.3. MONITORAMENTO E ATUALIZAÇÃO DE PLANOS

Planos de contingência e recuperação não são estáticos. Devem ser vivos, testáveis e revistos regularmente, com envolvimento ativo da unidade de Segurança Institucional e das demais áreas.

Boas práticas:

a. Estabelecer agenda de testes simulados, com avaliação de tempo de resposta, tomada de decisão e coordenação entre áreas;
b. Promover treinamentos intersetoriais, incluindo segurança, TI, saúde, comunicação e administração;
c. Incluir o tema nos planos de capacitação da Escola Superior do Ministério Público;
d. Realizar revisões anuais ou pós-incidente, com aprovação formal da Administração Superior;
e. Garantir que todos os envolvidos saibam onde encontrar os planos e como acessá-los rapidamente em situação real.

12. Avaliação e Melhoria Contínua

A segurança institucional não é estática. Exige monitoramento, revisão e correção contínuos, em sintonia com os princípios de eficiência, responsabilidade e inovação. Cabe ao gestor de segurança institucional implementar mecanismos periódicos de avaliação, permitindo identificar pontos fortes, vulnerabilidades e oportunidades de aprimoramento.

12.1. INDICADORES DE DESEMPENHO DE SEGURANÇA

A avaliação da segurança institucional deve ser orientada por indicadores quantitativos e qualitativos, que auxiliem na tomada de decisão e demonstrem a efetividade das ações da unidade de Segurança Institucional.

Exemplos de indicadores:

a. Quantidade de incidentes registrados por unidade e por tipologia;
b. Tempo médio de resposta a ocorrências;
c. Índice de reincidência de falhas;
d. Taxa de cumprimento de protocolos operacionais;
e. Número de inspeções preventivas realizadas;
f. Participação dos integrantes em treinamentos e simulados;
g. Índice de satisfação de membros protegidos (apuração sigilosa);
h. Percentual de planos de contingência atualizados;
i. Frequência dos agentes de segurança em cursos de especialização e capacitação continuada.

Esses dados devem constar de relatórios gerenciais periódicos e subsidiar ajustes nas políticas de segurança.

12.2. PROCESSOS DE AUDITORIA INTERNA

Além da auditoria externa e institucional (já mencionada na Seção 8), o próprio gestor da unidade de Segurança Institucional deve implementar auditorias internas regulares em seus procedimentos e controles operacionais, com os seguintes objetivos:

a. Verificar cumprimento de normas e procedimentos;
b. Avaliar a atuação de núcleos especializados;
c. Conferir integridade dos registros de ocorrências e relatórios;
d. Validar manutenção de equipamentos, escalas, rondas e monitoramento.

Sugere-se a seguinte frequência de realização das auditorias:

a. Semestral, com cronograma definido pela coordenação da unidade de Segurança Institucional;
b. Após incidentes relevantes ou alterações estruturais.

As inconformidades devem ser objeto de plano de ação corretivo, com prazos definidos.

12.3. REVISÕES PERIÓDICAS DE PROCEDIMENTOS E ESTRUTURAS

Todos os procedimentos e estruturas de segurança devem ser revisados anualmente, ou sempre que houver:

a. Mudança de sede ou reforma estrutural;
b. Alteração de equipamentos ou sistemas tecnológicos;
c. Modificação nos fluxos operacionais;
d. Incidente grave ou novo risco identificado;
e. Surgimento de novas tecnologias.

As revisões devem envolver os núcleos operacionais, a TI, a administração e, quando necessário, o setor jurídico ou a Corregedoria.

12.4. *FEEDBACK* DE COLABORADORES E *STAKEHOLDERS*

A percepção da segurança também é um termômetro de sua efetividade. O CGI deve adotar mecanismos para captar a visão dos membros, servidores e parceiros, promovendo:

a. Formulários sigilosos de avaliação após proteção pessoal;

b. b) Pesquisas de clima e percepção de segurança nas unidades;

c. c) Canais internos para sugestões de melhorias;

d. d) Reuniões periódicas com chefias e setores estratégicos;

e. e) Escuta ativa com membros lotados em áreas sensíveis.

f. O *feedback* deve ser tratado como insumo estratégico, nunca como crítica pessoal ou burocrática.

13. Transição da Gestão

A transição responsável e documentada da gestão da Coordenadoria de Segurança Institucional é essencial para garantir a continuidade das operações, preservar o sigilo de informações estratégicas e manter a eficácia do sistema de segurança.

O gestor que encerra sua função deve promover a transmissão técnica, sigilosa e organizada de informações, conforme padrões institucionais.

13.1. DOCUMENTOS

O gestor que se despede da função deve reunir e entregar ou disponibilizar acesso ao seu sucessor – ou à chefia institucional, quando cabível – os seguintes documentos, de forma física e/ou digital (em mídia criptografada ou em sistema informatizado):

a. Relatórios e Registros Operacionais:

- Relatórios técnicos de risco (ativos e arquivados);
- Relatórios de proteção pessoal em andamento;
- Registros de ocorrências e incidentes;
- Escalas operacionais dos núcleos e turnos;
- Inventário atualizado de equipamentos de segurança.

b. Planos e Protocolos:

- Planos de contingência vigentes;
- POPs atualizados e validados;
- Estratégias de segurança personalizadas para integrantes sob proteção;
- Fluxogramas e manuais operacionais internos.

c. Dados Estratégicos:

- Cadastro de pessoas protegidas (quando aplicável), com respectivos níveis de risco e medidas adotadas;
- Informações de acesso restrito (contatos de emergência, senhas institucionais, contratos sensíveis);
- Pendências operacionais, administrativas e jurídicas em curso;

- Cronograma de capacitações e treinamentos futuros.
- Projetos em desenvolvimento;
- Processos de aquisição de equipamentos em curso.

Todos os documentos devem estar organizados, com datas, autoria e grau de sigilo definido, preferencialmente assinados digitalmente ou com protocolo físico.

13.2. RELATÓRIO DE GESTÃO

O coordenador em final de mandato deverá elaborar um Relatório de Gestão, com visão estratégica e retrospectiva, contendo:

Conteúdo mínimo recomendado:

a. Período de atuação e principais atividades desenvolvidas;
b. Medidas implementadas e respectivos resultados;
c. Indicadores e números relevantes da gestão (proteções, treinamentos, incidentes, inspeções);
d. Pontos críticos, riscos remanescentes ou recorrentes;
e. Recomendações ao novo gestor ou à Administração Superior;
f. Sugestões de melhoria normativa, estrutural ou tecnológica.

O relatório deve ser objetivo, sigiloso e protocolado junto à chefia imediata (Gabinete da PGJ ou órgão superior indicado).

Boas práticas na transição:

a. Promover reunião técnica reservada com o novo gestor, esclarecendo pendências e prioridades;
b. Evitar exposição de dados sensíveis a terceiros;
c. Incentivar a continuidade das boas práticas e projetos em andamento;
d. Manter-se disponível para esclarecimentos após o encerramento formal da função, por tempo razoável.

14. Considerações Finais

A atuação na segurança institucional exige do gestor equilíbrio entre técnica, sensibilidade, sigilo, capacidade de articulação e compromisso com a missão ministerial. Mais do que proteger estruturas físicas, a segurança institucional deve salvaguardar vidas, preservar a atuação independente dos membros e garantir a integridade dos valores que sustentam o Ministério Público.

14.1. RESUMO DOS PRINCIPAIS PONTOS

Este manual apresentou diretrizes práticas e estratégicas para o gestor da Coordenadoria de Segurança Institucional do Ministério Público, com base nos seguintes eixos:

a. A função constitucional da segurança institucional e sua importância para a atuação do Ministério Público;
b. A estrutura normativa e operacional do Sistema Nacional de Segurança do Ministério Público (SNS/MP) e da unidade de Segurança Institucional;
c. A organização interna, papéis, núcleos e responsabilidades do gestor de Segurança Institucional;
d. A adoção de processos de gestão de riscos, planejamento de contingência e resposta a incidentes;
e. A valorização das pessoas, da capacitação e da cultura de segurança;
f. O compartilhamento de responsabilidades e a conscientização coletiva;
g. A aplicação de tecnologia e inovação com foco em prevenção e eficiência;
h. O compromisso com a conformidade legal, a sustentabilidade ambiental e a melhoria contínua;
i. A necessidade de uma transição transparente e responsável da função gestora.

14.2. COMPROMISSO DA ORGANIZAÇÃO COM A SEGURANÇA

O Ministério Público reafirma, por meio de seu órgão de segurança institucional, o compromisso institucional com:

a. A proteção da vida, da integridade e da atuação independente de seus membros;
b. A preservação do patrimônio público e informacional;

c. A promoção de um ambiente institucional seguro, resiliente e confiável;

d. A promoção de uma cultura de segurança permanente entre o público interno da Instituição;

e. O cumprimento das diretrizes do Conselho Nacional do Ministério Público;

f. A valorização das equipes de segurança e a sua constante formação técnica e ética;

g. O aperfeiçoamento contínuo dos protocolos de segurança orgânica, pessoal, cibernética e ambiental.

14.3. PASSOS FUTUROS E EVOLUÇÃO DA SEGURANÇA ORGÂNICA

A segurança institucional deve acompanhar as transformações da sociedade, das ameaças e das tecnologias. Nesse sentido, o gestor que assume a função deve estar atento às seguintes linhas de evolução:

a. Implantação de plataformas integradas de riscos e inteligência preventiva;

b. Desenvolvimento de modelos de proteção digital e segurança da informação mais robustos;

c. Ampliação da interoperabilidade com forças de segurança e outras unidades do Ministério Público;

d. Aperfeiçoamento do perfil técnico e comportamental das equipes;

e. Criação de um observatório interno de incidentes e boas práticas;

f. Integração da segurança institucional com a política de governança do Ministério Público.

A evolução da segurança começa na postura do gestor: comprometido, vigilante, articulado e tecnicamente preparado.

Referências

BRASIL. Agência Brasileira de Inteligência. **Doutrina da Atividade de Inteligência**. Brasília: Abin, 2023.

BRASIL. Conselho Nacional do Ministério Público. **Estudos de segurança institucional e contrainteligência no âmbito do Ministério Público brasileiro**. Brasília: CNMP, 2019.

CARON, Ricardo; BUENO, Vani Antônio. Inteligência e segurança institucional: uma abordagem sobre a segurança de áreas e instalações no Ministério Público. In: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Ministério Público Brasileiro**. Brasília: CNMP, Comissão de Preservação da Autonomia do Ministério Público, 2019. Publicação on-line. Disponível em: <https://www.cnmp.mp.br/portal/images/Comissoes/CPAMP/Estudos_de_Seguran%C3%A7a_Institucional.pdf>. Acesso em: 30 jun. 2025.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 116, de 6 de outubro de 2014** – Estabelece regras gerais para a proteção pessoal de membros do Ministério Público e de seus familiares diante de situação de risco decorrente do exercício da função. Publicada no Diário Oficial da União, Seção 1, edição de 21/10/2014. Disponível em: <https://www.cnmp.mp.br/portal/images/Resolucoes/Resolu%C3%A7%C3%A3o-116.pdf>. Acesso em: 30 jul. 2025.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 156, de 13 de dezembro de 2016** – Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Processual, p. 1-11, de 14 de fevereiro de 2017. Disponível em: <https://www.cnmp.mp.br/portal/images/Resolucoes/2021/Resoluo-n-156-2016-v3.pdf> Acesso em: 30 jul. 2025.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 292, de 28 de maio de 2024** – Institui a Política Nacional de Inteligência do Ministério Público e o Sistema de Inteligência do Ministério Público e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Caderno Processual, edição de 11/06/2024. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-292.pdf>. Acesso em: 30 jul. 2025.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 294, de 28 de maio de 2024** – Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Processual, edição de 03/07/2024. Disponível em: <https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-294d.pdf>. Acesso em: 30 jul. 2025.

DALABRIDA, Sidney Eloy. Resolução nº 156, de 13 de dezembro de 2016: o processo de surgimento da normatização sobre segurança institucional do Ministério Público Brasileiro. In: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Ministério Público Brasileiro**. Brasília: CNMP, Comissão de Preservação da Autonomia do Ministério Público, 2019. Publicação on-line. Disponível em: <https://www.cnmp.mp.br/portal/images/Comissoes/CPAMP/Estudos_de_Seguran%C3%A7a_Institucional.pdf>. Acesso em: 30 jun. 2025.

SILVA, Paula Cristina de Moura; BARCELLOS, Rodrigo Alves. Segurança Institucional: necessidade de mudança da cultura organizacional entre os integrantes do Ministério Público do Estado do Tocantins. **Revista Jurídica do Ministério Público do Estado do Tocantins**, *[S. l.]*, v. 17, n. Especial, 2024. Disponível em: <https://cesaf.mpto.mp.br/revista/index.php/revistampto/article/view/105>. Acesso em: 6 out. 2025.

FARAH, Camel André de Godoy. **Gestão de segurança institucional** [Recurso eletrônico] / Camel André de Godoy Farah. 1. ed. Florianópolis: Ed. do autor, 2013.

JESUS, Mauro Zaque de. **Como não se tornar uma vítima**: um guia de segurança pessoal e corporativa. São Paulo: Dialética literária, 2025.

SEABRA, Marcelo Canizares Schettini. **Atividade de inteligência na polícia judicial: a gestão do conhecimento como fator determinante para a segurança institucional do Poder Judiciário** / Marcelo Canizares Schettini Seabra; Maurício Viegas Pinto (org.) - Brasília: Pró-consciência, 2024.

Apêndice A – *Checklist*

A.1 *CHECKLIST* INICIAL DO NOVO GESTOR – PRIMEIROS 90 DIAS DE GESTÃO

- ☐ Conhecer as Resoluções CNMP nº 116/2014, nº 156/2016, nº 303/2016 e demais normativos aplicáveis.
- ☐ Reunir-se com o Procurador-Geral e a chefia administrativa para alinhamento estratégico.
- ☐ Levantamento dos relatórios técnicos de riscos ativos.
- ☐ Verificação dos planos de contingência e POPs vigentes.
- ☐ Verificação do inventário de equipamentos de segurança (CFTV, alarmes, rádios, armas, viaturas) e recursos disponíveis.
- ☐ Contatos estratégicos atualizados (PM, PC, Bombeiros, Defesa Civil, TI) e estabelecimento de um canal direto com órgãos de segurança pública parceiros.
- ☐ Identificação dos membros sob proteção especial.
- ☐ Reunião reservada com equipe operacional para diagnóstico.

A.2 *CHECKLIST* OPERACIONAL – VISTORIA PREDIAL DE SEGURANÇA

- ☐ Cercas, muros e concertinas em bom estado.
- ☐ Portas e janelas com fechaduras e alarmes funcionais.
- ☐ Sistema de CFTV ativo, com gravação em nuvem/servidor seguro.
- ☐ Alarmes e sensores de presença testados.
- ☐ Iluminação externa e de emergência funcionando.
- ☐ Saídas de emergência desobstruídas e sinalizadas.

A.3 *CHECKLIST* OPERACIONAL – PROTEÇÃO PESSOAL DE MEMBROS

- ☐ Avaliação de risco atualizada.
- ☐ Conduta em redes sociais revisada.
- ☐ Rotas alternativas de deslocamento mapeadas.
- ☐ Veículo vistoriado (blindagem, combustível, manutenção).
- ☐ Contatos de emergência configurados (botão de pânico, rádio, celular funcional).
- ☐ Família orientada quanto a rotinas seguras.

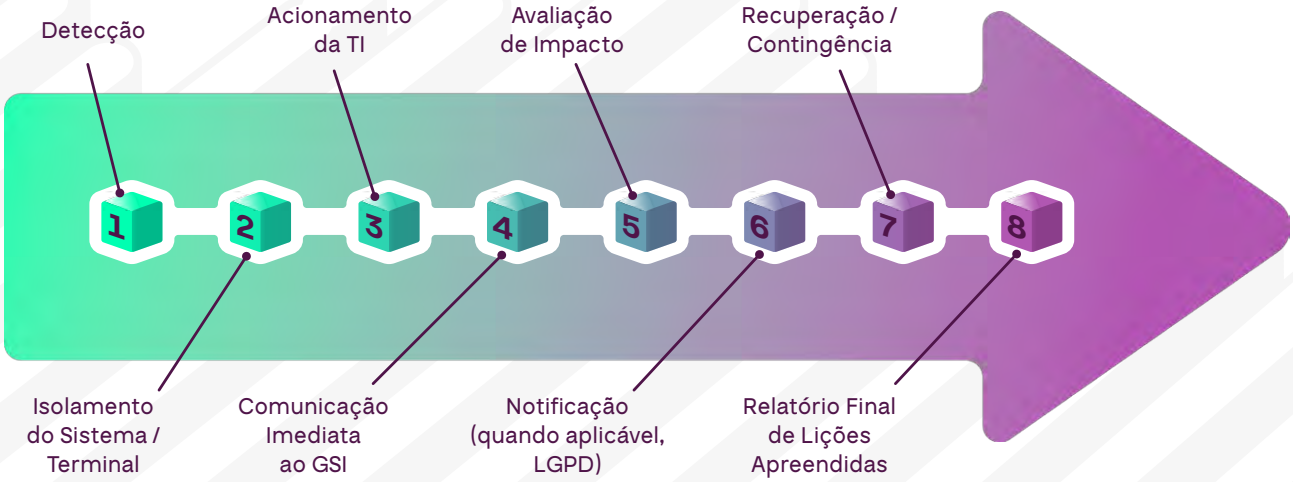
A.4 *CHECKLIST* DE COMUNICAÇÃO RÁPIDA

- ☐ Procurador-Geral de Justiça.
- ☐ Coordenação da TI.
- ☐ Chefes da PM e PC locais.
- ☐ Bombeiros – Defesa Civil.
- ☐ Coordenação do CNMP/SESI.
- ☐ Coordenadoria de Inteligência do seu MP.

Apêndice B – Fluxogramas de Decisão

B.1 RESPOSTA A INCIDENTE DE SEGURANÇA FÍSICA

B.2 RESPOSTA A INCIDENTE CIBERNÉTICO



B.3 PLANO RÁPIDO DE CRISE

Ataque Armado em Unidade	Evacuação	Acionamento PM / Bombeiros	
Vazamento de Dados Sensíveis	Isolamento de Sistema	Acionamento da TI	Acionamento da Comunicação
Protesto em Frente a Sedes	Contato PM	Contenção Preventiva	Plano de Comunicação Institucional
Ameaça a Membro	Avaliação de Risco Emergencial	Proteção Imediata	Plano Logístico

Apêndice C – Painel de Indicadores de Segurança (KPI/KRI)

- Tempo médio de resposta a incidentes.
- Nº de incidentes prevenidos/detectados.
- Índice de reincidência de falhas.
- Percentual de planos de contingência atualizados.
- % de equipe treinada no último semestre.
- Nº de vulnerabilidades físicas/digitais corrigidas.
- Satisfação dos membros protegidos (pesquisa sigilosa).

Apêndice D – Modelos de Documentos

D.1 MODELO DE RELATÓRIO TÉCNICO DE RISCO (RTR)

Relatório Técnico de Risco	
Identificação:	
Data/Hora:	
Local:	
Descrição do Risco Identificado:	**Classificação:** ☐ Baixo ☐ Médio ☐ Alto ☐ Crítico
Medidas Adotadas:	
Respensável pelo Registro:	

D.2 MODELO DE PLANO DE CONTINGÊNCIA

Plano de Contingência	
Cenário de Crise:	
Impacto Esperado:	
Recursos Necessários:	
Protocolo de Resposta:	
Responsáveis Designados:	

D.3 MODELO DE RELATÓRIO PÓS-INCIDENTE

Relatório Pós-Incidente	
Data/Hora do Incidente:	
Local:	
Descrição do Incidente:	
Medidas Adotadas:	
Falhas Identificadas:	
Ações Corretivas Propostas:	
Lições Aprendidas:	

D.4 MODELO DE TERMO DE SIGILO E RESPONSABILIDADE

Termo de Sigilo e Responsabilidade
Declaro, para os devidos fins, que me comprometo a manter o mais absoluto sigilo sobre todas as informações, documentos e dados sensíveis a que tiver acesso em razão de minhas atividades na área de Segurança Institucional, sob pena de responsabilização administrativa, civil e penal. Nome: ..... Cargo/Função: .... Assinatura Data: ..... /..... /.....

Apêndice E – Termo de Mobilização de Escolta

1. Considerando a recomendação de escolta de pessoa sob proteção constante no ATO PGJ nº XX/20XX da Procuradoria-Geral de Justiça do Estado de XXXXXX; e
2. Considerando a necessidade de se alterar a rotina do membro/servidor ...., visando potencializar sua segurança pessoal;
3. A Comissão de Segurança recomenda à pessoa sob proteção:

   a) evitar, ao máximo, atividades laborais após o expediente, principalmente no período noturno;

   b) evitar, ao máximo, expor sua imagem pessoal;

   c) não dar publicidade aos fatos envolvendo sua segurança, especialmente por meio de entrevistas ou qualquer divulgação pela mídia;

   d) não divulgar dados e informações da situação de risco;

   e) não divulgar ou comentar sobre as ferramentas de investigação e de proteção adotadas;

   f) não manter ou criar perfil profissional ou pessoal nas redes sociais;

g) não se ausentar da sede da Comarca onde exerce suas atividades profissionais;

h) não frequentar bares, boates, restaurantes e similares, bem como ginásios e quadras esportivas, estádios de futebol, espetáculos públicos, shopping center e outros locais com grande presença de público;

i) não comparecer a eventos sociais de cunho particular ou profissional que resultem em exposição física, bem como a locais que possam comprometer a atuação da segurança pessoal e potencializar o risco a sua integridade física;

j) fornecer dados de sua agenda aos responsáveis pela sua proteção, com razoável antecedência;

k) atender às recomendações dos agentes de segurança institucionais encarregados da proteção, dispensando-os, formalmente, conforme modelo próprio, em caso de discordância e assumindo voluntariamente os riscos a que está submetido;

l) comunicar os casos omissos à Comissão de Segurança para deliberação.

4. O serviço de proteção será interrompido pelos agentes de segurança, ainda que não haja sua dispensa formal, no caso de persistir a divergência do protegido quanto às orientações recebidas. Tal fato será consignado em solicitação de desmobilização de escolta, conforme modelo próprio, que será encaminhado ao coordenador da equipe e, posteriormente, à Comissão de Segurança Pessoal para fins de deliberação.

5. As viagens para outros Municípios/Estados, bem como os deslocamentos para zona rural, clubes sociais, shoppings, entre outros, onde se presumem aglomerações de pessoas ou locais ermos, serão considerados emergenciais e deverão ocorrer somente em casos estritamente necessários, mediante aviso prévio pelo próprio membro/servidor ao Coordenador da unidade de Segurança Institucional, com antecedência mínima de 48 (quarenta e oito) horas, que, após parecer, deliberará sobre a autorização, considerando que, por sua natureza, localização, comunicação, podem comprometer a segurança do membro/servidor ameaçado, além da própria equipe de escolta.

6. Eu, *(Nome completo do integrante sob proteção)*:

☐ Concordo e acato as diretrizes estabelecidas;

☐ Discordo e dispenso a escolta institucional, mesmo tendo conhecimento da situação de risco em que me encontro.

Local e data.

.....

Membro/servidor sob proteção

Apêndice F – Termo de Dispensa de Escolta

Na presente data, ciente das recomendações de escolta e da situação de risco em que me encontro, dispenso a escolta a mim concedida pelas razões abaixo discriminadas: .....
.....
.....
.....
.....
.....

Local e data.

.....

Membro/servidor

Apêndice G – Solicitação de Desmobilização de Escolta pelo Protegido

Na presente data, solicito que, a partir do dia ..... /..... /..... , seja desmobilizada a escolta a mim prestada, pelas razões abaixo discriminadas: .....
.....
.....
.....
.....
.....

Local e data.

.....

Membro/servidor

Apêndice H – Termo de Desmobilização de Escolta

Na presente data, pelas razões abaixo discriminadas (dispensa pelo membro e/ou servidor, solicitação de desmobilização pelo membro e/ou servidor, conclusão de investigação, ausência de fatos relevantes, entre outros) e conforme relatório do Gabinete de Segurança Institucional do Ministério Público do Estado *XXXXXXXXX*, fica autorizada a desmobilização da escolta prestada ao membro/servidor ...., sem prejuízo do acompanhamento da situação por esta Comissão: .....
.....
.....
.....
.....
.....

A desmobilização da escolta ocorrerá a partir do dia ..... de ..... de .....

Local e data.

.....

Membro/servidor

Conselho
Nacional do
Ministério Público

Acesse nosso portal
www.cnmp.mp.br

Siga o **CNMP** nas redes sociais:

conselhodomp

cnmpoficial

@cnmp_oficial