CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

CARTILHA DE SEGURANÇA

INTRODUÇÃO

O Ministério Público, com o advento da Constituição de 1988, sofreu amplas transformações institucionais ocasionadas pela aposição normativa de vastas responsabilidades de defesa social e do ser humano nas mais diversas necessidades de proteção, bem como pela disponibilização de relevantes instrumentais processuais para a concretização dessa tutela.

Em razão dessa realidade constitucional houve o engrandecimento da Instituição em todas as vertentes imprescindíveis à concretização daquelas árduas missões em prol da defesa da ordem pública e do regime democrático. Por outras palavras, os ativos humanos, materiais, prediais e tecnológicos robusteceram quantitativamente e qualitativamente, como consequência da imprescindibilidade de bem cumprir os papéis outorgados pela Lei Maior.

Como consequência do exercício das responsabilidades constitucionais adveio um enorme protagonismo social e uma maior exposição aos riscos de ações adversas de naturezas plúrimas, destinadas a barrar a disseminação da distribuição da Justiça e as ações em prol da outorga de dignidade e do bem comum aos titulares dos direitos.

Paralelo a esse panorama constitucional, mutações sociais e comportamentais avolumaram-se nas últimas décadas decorrentes da globalização e da evolução tecnológica, e com elas novos riscos passaram a ser diagnosticados, vulnerantes não apenas aos seres humanos, mas também aos órgãos do Ministério Público (nesse contexto destacam-se as ações hostis engendradas no ambiente cibernético).

Nesse atual contexto social e constitucional é que se insere o principal objetivo deste trabalho: a conscientização da necessidade de adoção de medidas

protetivas ao Ministério Público para a preservação dos seus ativos imprescindíveis à concretização dos deveres institucionais hodiernos.

A cartilha agora apresentada é composta de cinco partes: a primeira dedicada a orientações para a preservação do ativo humano ministerial (segurança de pessoas); a segunda concernente a sugestões de medidas para a proteção das informações sensíveis tanto à Instituição, como aos servidores e aos membros; a terceira atinente à segurança do ativo físico predial (as áreas e as instalações); a quarta destinada a dicas de proteção do ativo físico móvel (os materiais); e a última referente a dicas para o controle no ingresso e no desligamento do material humano.

Dessa forma, com a elaboração desta cartilha, o Comitê de Políticas de Segurança Institucional (CPSI) segue a concretização do principal ditame da resolução nº 156/2016, do Conselho Nacional do Ministério Público, qual seja, o fomento da cultura da segurança dos ativos dos ramos do Ministério Público em todas as suas vertentes de vulnerabilidades: pessoas, informações, materiais, áreas e instalações. E espera contribuir para que o Ministério Público Brasileiro permaneça alicerçado nas firmes balizas humanas e idealistas que o galgaram ao posto de Instituição imprescindível à preservação do nosso Estado Democrático de Direito.

Brasília, 11 de setembro de 2018.

ELISA FRAGA DE REGO MONTEIRO
Promotora de Justiça do Ministério Público do Estado do Rio de Janeiro

GIORDANE ALVES NAVES
Promotor de Justiça do Ministério Público do Estado de Goiás

JERUSA CAPISTRANO PINTO BANDEIRA
Promotora de Justiça do Ministério Público do Estado do Maranhão

JOÃO SANTA TERRA JÚNIOR
Promotor de Justiça do Ministério Público do Estado de São Paulo

SUMÁRIO

4 SEGURANÇA DA INFORMAÇÃO

1. SEGURANÇA DE PESSOAS

1.1. CONCEITO

Segurança de pessoas é o conjunto de medidas destinadas a proteger a integridade física de membros, servidores e familiares, quando comprometida, em face do desempenho das funções institucionais. Pela especificidade e circunstâncias é fundamental que os integrantes do Ministério Público, em particular os membros, desenvolvam uma cultura de conscientização e sensibilização quanto às prováveis ameaças, estabelecendo procedimentos de proteção e preservação de sua integridade.

1.2. MEDIDAS DE SEGURANÇA PARA INCLUSÃO OU DESLIGAMENTO DE PESSOAL

NA INCLUSÃO

a. Com o apoio do órgão de Inteligência, serão efetuados os levantamentos, avaliações e verificações da vida pregressa dos candidatos, além dos conhecimentos e habilidades.

b. Caberá ao setor interessado apresentar os nomes dos servidores ao chefe do setor de pessoal, para as providências de rotina, enquanto as referências de sua vida pregressa serão avaliadas, com base na documentação de comprovação solicitada, bem como através de levantamentos feitos pelo setor de inteligência.

c. Serão buscadas ainda informações sociais do pretendente àquela função, a fim de aquilatar sua conduta na vida social.

d. Depois de finalizados os procedimentos de verificação, os resultados serão apresentados à autoridade encarregada da nomeação que tomará os procedimentos cabíveis ao caso.

e. Os estagiários a serem selecionados para funções nos setores do Ministério Público deverão sofrer avaliação proporcional ao nível de acesso que a função lhes permitirá. Neste caso, a autoridade à qual o estagiário ficará subordinado, realizará acompanhamento e avaliação de desempenho quanto ao exercício das funções de que estiver encarregado.

NO DESLIGAMENTO

a. Recolhimento de documentos, chaves, crachás e outros que permitam qualquer tipo de acesso exclusivo para integrantes e funcionários do Ministério Público.

b. Cancelamento de senhas de acesso, chaves de bancos de dados e similares.

1.3. ORIENTAÇÕES GERAIS DE SEGURANÇA

a. Não fornecer dados pessoais de integrantes do Ministério Público a solicitantes, pessoalmente ou via telefone.

b. Não informar a solicitantes horários de chegada, saída ou presença de integrantes do Ministério Público, sem antes solicitar autorização para tal.

c. Autorizações para visitas a integrantes do Ministério Público deverão ser precedidas de solicitação de autorização ao interessado.

d. Não fornecer informações sobre rotinas internas.

1.4 ORIENTAÇÕES DE SEGURANÇA NO CONTROLE DE ACESSO E PERMANÊNCIA

a. Registrar o ingresso e a saída de todos os visitantes em controle específico.

b. Monitorar, por meio de CFTV, o deslocamento de visitantes no interior das dependências das unidades.

c. Anunciar e confirmar o visitante que deseja ingressar no Ministério Público.

d. Cumprir as normas do Ministério Público para o controle de acesso, notadamente de pessoas portando armas de fogo e pacotes ou mochilas onde possam ser transportados substâncias ou artefatos nocivos.

e. Registrar o nome da pessoa que ingressa no Ministério Público, com anotação de um número de documento de identidade e, se possível, a retirada de fotografia com câmeras digitais acopladas em computadores.

f. Caso note nervosismo ou irritação de alguém, procure não confrontá-lo diretamente, mantenha a calma e, caso necessário, acione a segurança ou a polícia local.

1.5 ORIENTAÇÕES DE SEGURANÇA ESPECÍFICAS A MEMBROS

a. Procure não demonstrar raiva ou externar comportamento agressivo/vingativo em relação a terceiros ou investigados, pessoalizando atos que devem ter natureza institucional e impessoal.

b. Evite expor excessivamente sua imagem nos meios de comunicação, prevenindo a personalização desmedida de seus atos funcionais. Não havendo prejuízo para o interesse público protegido no caso, busque sempre o órgão de comunicação para a transmissão de informações oficiais.

c. Evite ter rotinas precisas e conhecidas de todos em relação a horários de chegada e saída da sua promotoria, especialmente de saídas no período noturno, chegadas e saídas da comarca ou de itinerário de trânsito.

d. Caso provocado por partes, testemunhas, réus ou terceiros, mantenha sempre a calma, evitando discutir com os mesmos. Mostre-se seguro, requerendo sempre o que for necessário para manter a dignidade pessoal e do cargo imaculada, sem se afetar emocionalmente com a disputa.

e. Planeje a chegada e a saída das audiências, evitando aproximação descuidada com réus, parentes ou terceiros fora do recinto da audiência em caso de situação de incremento do risco, como condenação a penas elevadas em sessões do tribunal do júri.

f. Prefira sempre ser técnico, evitando desprezar ou ridicularizar em conversas sobre outras pessoas ou autoridades de seu convívio funcional permanente.

g. No planejamento de acompanhamento de execuções de mandados judiciais, como busca e apreensões, preocupe-se com as questões de segurança. Nesses casos, pondere sempre a necessidade de ser acompanhado de agentes de segurança próprios da sua instituição ou mesmo de fora, de eventual apoio de outros colegas para despersonalizar sua atuação, bem como a necessidade de utilização de equipamentos como coletes balísticos e veículos blindados.

h. Em casos como interrupção de vias por protestos de grupos sociais organizados, manutenção de reféns em cativeiro e outros semelhantes, caso o Ministério Público seja chamado ao local das negociações por outras instituições, notadamente policiais, ligue sempre para o órgão de segurança de sua instituição antes de tomar qualquer medida, de modo a receber orientações sobre como proceder em casos como esses, em que há estrito protocolo a ser seguido com o objetivo de prevenir riscos desnecessários ao membro e à instituição.

1.6 ORIENTAÇÕES DE SEGURANÇA QUANTO A SUSPEITA DE ARTEFATOS EXPLOSIVOS

Caso receba algum volume ou pacote, geralmente em caixa, que não esteja esperando, sem remetente ou de remetente desconhecido, e se houver a suspeita de que pode se tratar de algum artefato explosivo, adote as seguintes providências:

a. Acione imediatamente a autoridade policial, para mobilização do grupo especializado em casos de ameaça de bomba.

b. Mantenha a calma e acalme a todos.

c. Em hipótese alguma o artefato deve ser mexido ou movimentado.

d. Busque retirar todos das proximidades do local onde está o artefato, indo para o local a pelo menos 100 (cem) metros.

e. Se possível, fique em local onde exista algum anteparo sólido entre você e o artefato, como paredes de alvenaria e armários de aço.

f. Solicite e respeite as orientações da autoridade policial quanto à evacuação e isolamento do prédio.

1.7 ORIENTAÇÕES GERAIS DE SEGURANÇA FORA DO AMBIENTE DE TRABALHO

a. Desconfie de terceiros que desejem se aproximar ou obter informações sobre sua vida de forma muito rápida e se mostrando muito prestativo.

b. Mantenha sempre seu celular carregado, para ser utilizado em caso de urgência ou emergência. Tenha carregadores de celular portáteis e/ou veiculares.

c. Memorize sempre seus dados pessoais, dados de seus familiares e de seu veículo. Eles serão necessários caso algo ocorra e você precise acionar a polícia.

d. Esteja atento ao ambiente. Evite uso de aparelhos celulares e outros equipamentos que tirem sua atenção enquanto não tiver chegado ao local de destino.

e. Não ostente objetos de valor em excesso, como joias chamativas e vultosas quantias em dinheiro.

f. Ao conduzir bolsas, recomenda-se que o zíper ou outro mecanismo de abertura dos compartimentos esteja voltado para frente do corpo.

g. Caso note que esteja sendo seguido, busque um local movimentado, como lojas e supermercados, e peça ajuda. Ligue imediatamente para a Polícia Militar ou para algum número do órgão de segurança de sua instituição.

h. Desconfie de pessoas que se aproximam para pedir informações. Se for prestá-las, faça em movimento.

i. Busque caminhar contra o sentido da via e no centro da calçada.

j. Não dê atenção caso alguém comece a discutir com você sem razão aparente. Pode ser apenas o início de golpe. Mantenha o movimento e se afaste.

k. Em caso de necessidade de locomoção por meios de transporte particular, evite sair procurando pela rua, especialmente à noite. Ligue para uma das centrais que prestam serviço de teleatendimento ou aplicativo de celular e solicite um veículo.

l. Antes de entrar ou sair, verifique o entorno do veículo, especialmente a presença de pessoas estranhas ou de veículos ligados com pessoas dentro em atitude anormal. Na dúvida, chame a segurança do local ou acione a Polícia Militar.

m. Estacione apenas em locais iluminados e movimentados.

n. Nunca deixe armas ou documentos relevantes no automóvel, especialmente os que informem o seu endereço.

o. Caso precise deixar objetos valiosos em veículo estacionado na rua, pare em algum ponto antes do local de destino e coloque-os na mala.

p. Busque estacionar o carro em condições de saídas rápidas, de preferência sem precisar dar marcha ré para se evadir.

q. Nunca fique por mais de cinco minutos no veículo parado na rua, aguardando alguém. De preferência, dê a volta no quarteirão até que a pessoa chegue ao local de encontro.

r. Ao aguardar por alguém no interior do veículo na rua, não se distraia com telefone celular ou outro dispositivo. Esteja atento à aproximação de estranhos.

s. Em semáforos, pare na faixa central, um pouco distanciado do veículo da frente (evite a primeira fila), com vidros fechados e primeira marcha engatada.

t. Evite trafegar por bairros que você não conhece e que tenham reputação de perigosos, especialmente à noite.

u. Se achar que está sendo seguido, mantenha a calma, tente memorizar a placa e características do veículo, dirija-se a algum posto policial e nunca ingresse em ruas pouco movimentadas ou mal iluminadas, ainda que seja para tentar escapar.

v. Evite andar sozinho, principalmente à noite. Se estiver caminhando de madrugada, evite se posicionar nos cantos das calçadas, preferindo ocupar a sua beirada ou até mesmo a pista de rolamento, se não houver movimento de veículos.

1.8 ORIENTAÇÕES DE SEGURANÇA CASO SEJA ABORDADO POR CRIMINOSO

Caso seja surpreendido por um criminoso e ele determine sua saída do veículo, aja da seguinte forma:

a. Não reaja, caso não tenha absoluta segurança e não tenha treinamento específico, pois os criminosos quase nunca estão sozinhos.

b. Saia por trás do veículo evite passar entre a porta aberta e o criminoso.

c. Se estiver usando cinto ou algo que tenha que ser removido para sair, avise com tranquilidade que vai retirá-lo, para que sua conduta não seja interpretada como reação.

d. Não grite, não buzine, não acelere o veículo e não faça movimentos bruscos.

e. Não tente negociar a devolução de qualquer objeto, ele não é mais importante que a sua vida.

1.9. ORIENTAÇÕES DE SEGURANÇA EM CASOS DE SEQUESTROS RELÂMPAGOS

a. Evite discutir ou gritar.

b. Tente manter-se calmo e não realize movimentos bruscos.

c. Responda apenas ao que for perguntado.

d. Entregue ao criminoso o que ele pedir.

e. Busque não olhar diretamente para os criminosos.

f. Memorize detalhes como cor da pele, sotaques, roupas e outras características de identificação.

g. Nunca se identifique como membro do Ministério Público.

h. Após ser solto, ligue imediatamente para 190.

i. Caso seja mantido como refém, procure não conversar com outros reféns.

1.10. ORIENTAÇÕES DE SEGURANÇA EM VEÍCUOS

a. Faça revisões periódicas em seu veículo, evitando assim, paradas inesperadas em locais de risco.

b. Coloque película protetora (*insulfilm*) nos vidros dos carros. O acessório dificulta que se enxergue o interior do veículo.

c. Planeje, antecipadamente, seu itinerário, conhecendo caminhos alternativos e pontos de apoio (delegacias, unidades militares, hospitais etc).

d. Use GPS (*global position system*) e evite utilizar vias conhecidamente perigosas, principalmente em horários tardios. Ao digitar o endereço de destino no sistema GPS, certifique-se que o local encontrado situa-se no bairro e município desejados, pois existem ruas com mesmo nome, em bairros ou municípios diferentes.

e. Evite trafegar em vias secundárias, sobretudo em horário noturno.

f. Mantenha as portas do veículo travadas.

g. Trafegue com os vidros fechados.

h. Não abra os vidros para atender a ambulantes e a pedintes.

i. Evite portar na sua carteira a identidade funcional.

j. Evite exibir joias e relógios.

k. Não use adesivos nos vidros e lataria que possibilitem identificar dados pessoais e sua família, como escola dos filhos, clube que frequenta e condomínio que reside.

l. Coloque bolsas, pastas e objetos chamativos no porta-malas ou no assoalho do veículo. Processos devem ser guardados na mala do veículo, dentro de bolsas ou caixa de papelão, de maneira que não fiquem aparentes.

m. Esteja sempre atento à movimentação de pessoas e veículos, utilizando os retrovisores.

n. Reduza a velocidade na aproximação de semáforos fechados, de maneira a permanecer o menor tempo possível parado.

o. A maioria das abordagens por meliantes ocorre pelo lado do motorista. Geralmente, eles partem das calçadas e canteiros. Portanto, utilize, preferencialmente, as faixas centrais.

p. Quando inevitável a parada em semáforos, procure não ficar nas primeiras filas.

q. Ao parar em semáforos, posicione-se de maneira a fechar o “corredor” utilizado por motociclistas.

r. Mantenha distância do veículo da frente, de maneira a visualizar os seus pneus traseiros para realização de manobras evasivas, se necessário.

s. Se você tem o hábito de guardar documento do veículo no seu interior, acomode-o sob o banco ou em local que não apareça. Em caso de furto ou roubo, se o condutor vier a ser abordado por policiais não disporá do documento para apresentação.

1.11. ORIENTAÇÕES SOBRE SEGURANÇA EM LIGAÇÕES TELEFÔNICAS.

a. No caso de uma ligação em que o interlocutor pergunte: “QUEM ESTÁ FALANDO?” ou “DE ONDE ESTÃO FALANDO?”, não forneça nenhuma dessas informações. Responda fazendo outra pergunta ”COM QUEM DESEJA FALAR?” ou “QUE NÚMERO DISCOU?”.

b. Quando receber ligação pedindo confirmação do endereço para a entrega de presentes, brindes ou flores, procure saber de onde fala e qual é o nome do estabelecimento, dizendo que ligará em seguida dando a informação solicitada.

c. Ao receber um telefonema comunicando que um familiar ou amigo está doente ou sofreu um acidente, peça e anote todas as informações possíveis, como quem está falando e qual o telefone para a confirmação. Servidores públicos nunca ligam a cobrar de telefones celulares.

d. Quando receber uma ligação comunicando que algum familiar ou amigo foi sequestrado, insista para falar diretamente com ele. Ao mesmo tempo e sem informar ao suposto sequestrador, tente localizar a vítima utilizando todos os recursos possíveis, acionando amigos e familiares, mas sem fazer comentários de um possível sequestro.

Peça alguém para ligar incessantemente para os telefones da vítima, é possível que esteja momentaneamente fora de área de cobertura ou desligado.

Mantenha a calma. Não aja impulsivamente. Não forneça nenhuma informação, nem confirme dados. Havendo dúvidas, trate a ligação como se fosse realmente um caso de sequestro. Se tiver que tomar alguma atitude e se deslocar para algum lugar, peça ajuda e não faça nada sozinho. Comunique o fato à polícia.

2. SEGURANÇA DE MATERIAIS

2.1. CONCEITO

A segurança de material compreende o conjunto de medidas voltadas a proteger o patrimônio físico, bens móveis e imóveis, pertencente ao Ministério Público ou sob o uso da Instituição.

2.2. OBJETIVOS GERAIS

a. Desenvolver estratégias uniformes dentro da instituição, para padronizar os níveis gerais de proteção adequados às reais necessidades de preservação do Ministério Público quanto ao material pertencente a ele ou que esteja sob sua responsabilidade.

b. Estruturar um sistema de proteção do material pertencente ao Ministério Público, de forma a garantir proteção integral do patrimônio material da instituição, que acompanhe a evolução temporal e natural do seu volume.

2.3. OBJETIVOS ESPECÍFICOS

a. Promover a segurança patrimonial do Ministério Público, nas suas várias classes e categorias, garantindo a sua integral preservação através de medidas preventivas e reativas necessárias para tal desiderato.

b. Estabelecer um sistema eficiente de controle de entrada e saída de materiais.

c. Manter controle permanente das condições em que se encontra tal patrimônio no que tange a sua segurança, tomando todas as medidas cabíveis quando forem constatados danos ou riscos de danos, visando evitar ou minimizar prejuízos causados

por ações humanas, decorrentes de intempérie ou degradação natural, antecipando ao órgão da administração do Ministério Público, responsável pela solução do problema constatado.

2.4. AÇÕES ESPECÍFICAS

Serão estabelecidos parâmetros operacionais para a segurança do patrimônio institucional, através de controles quanto a(o):

a. Entrada e saída de materiais,

b. Circulação de bens nas dependências da instituição;

c. Proteção a bens com maior interesse de proteção, pela finalidade a que se destinam, valor agregado, nível de interesse para a instituição ou de interesse externo lícito ou ilícito;

d. Proteção quanto a riscos de dano provocado, sabotagem, furto, roubo e outros que possam causar dano parcial, total, subtração, adulteração e destruição de itens que componham o patrimônio da instituição ou que esteja sob sua responsabilidade.

e. Controle de acesso de materiais que possam causar risco de qualquer natureza ao patrimônio da instituição, bem como aos seus integrantes, de forma acidental ou intencional, como explosivos, produtos tóxicos, contaminantes e corrosivos.

f. Sistema integrado de monitoramento, para a segurança do material da instituição, conforme levantamento técnico, levando em conta as peculiaridades e rotinas das instalações a serem protegidas.

Nos almoxarifados serão estabelecidos parâmetros operacionais para a segurança do patrimônio institucional, através das seguintes ações:

a. O material deve ser acondicionado de forma adequada, contando, inclusive, com dispositivos de segurança através de circuito interno de câmeras.

b. O controle deve ser totalmente informatizado.

c. Devem ser executadas conferências periódicas entre as quantidades apontadas pelo sistema de materiais e os saldos existentes em estoque.

d. O processo de entrada tem que ser dado diretamente no sistema de controle através de notas fiscais e as saídas efetuadas através de solicitações de setores via e-mail, ofícios ou diretamente junto ao setor, após requisições.

e. Todo material permanente deve ser registrado, recebendo numeração indicativa de patrimônio (plaquetas de identificação).

3. SEGURANAÇA DAS ÁREAS E INSTALAÇÕES

3.1. CONCEITO

Segurança de áreas e instalações constitui um grupo de medidas orientadas para proteger o espaço físico sob a responsabilidade do Ministério Público ou onde se realizam atividades de interesse da instituição, com a finalidade de salvaguardá-la.

3.2. OBJETIVOS GERAIS

a. Criar um sistema eficiente de segurança institucional quanto às suas áreas e instalações onde funcionam os diversos setores do Ministério Público, que garanta sua integridade quanto a ameaças e riscos de causas naturais ou humanas, sem que haja prejuízo ao seu bom funcionamento.

b. Garantir a expansão e aperfeiçoamento do sistema, acompanhando a evolução social da sociedade em que se insere, de forma a impedir que fatores supervenientes decorrentes de tal evolução, gerem qualquer tipo de impacto indesejável institucionalmente.

3.3. OBJETIVOS ESPECÍFICOS

a. Estabelecer medidas de proteção das áreas e instalações do Ministério Público, no que tange a acessos e permanência nos diversos setores da instituição.

b. Orientar os procedimentos a serem tomados quanto à prevenção e combate a incêndios e sinistros, sejam por causas naturais ou humanas.

c. Estabelecer um sistema eficiente de controle de entrada e saída de materiais.

3.4. AÇÕES ESPECÍFICAS

A segurança de áreas e instalações compreende, entre outras, os seguintes conjuntos de medidas:

a. Controle do acesso e permanência de pessoas no Ministério Público ou em espaços sob sua responsabilidade, identificando-as adequadamente por sistema de crachá ou outro considerado adequado para o acesso pretendido, por integrante da instituição ou público externo.

b. Detecção de invasão e monitoramento de alarme.

c. Implantação de barreiras de acesso perimetral.

d. Estabelecimento de perímetros de proteção.

e. Proteção do sistema de cabeamento e quadros das diversas naturezas presentes.

f. Proteção do sistema de energia, água, gás e ar condicionado.

g. Estruturação de sistemas de prevenção e combate a incêndio.

h. Instalação de câmeras de segurança e alarme monitorado.

i. Organização de brigadas de incêndio.

j. Instalação de equipamento para detecção de metais, pelo qual deverão passar todas as pessoas que venham a acessar as dependências do Ministério Público.

k. Todas as reformas e projetos de construção deverão passar pelo crivo do órgão de segurança institucional, tendo em vista o interesse da segurança da instituição como um todo, para evitar que se crie através de tais alterações, vulnerabilidades que reduzam os níveis de segurança já estabelecidos ou que estejam sendo buscados.

l. Quanto à área de estacionamento, deverá ser desenvolvido projeto de segurança estrutural, de forma a não permitir que isto torne vulnerável a segurança desta instituição.

3.5. CLASSIFICAÇÃO EM SISTEMAS

A segurança de áreas e instalações engloba os seguintes sistemas:

a. **SISTEMA FÍSICO**: composto pelos vigilantes que executam diversos serviços de vigilância.

b. **SISTEMA ELETRÔNICO**: integrado pelos equipamentos eletrônicos para segurança, tais como sensores, sistema de câmeras de segurança, alarmes, fechaduras eletrônicas, sistemas de registro *etc*.

c. **SISTEMA DE BARREIRAS**: envolve as diversas barreiras para segurança dos perímetros.

3.6. AÇÕES VOLTADAS À SEGURANÇA DE ÁREAS E INSTALAÇÕES

São atividades relacionadas à segurança de áreas e instalações:

a – Perímetros, barreiras e instalações físicas.

b – Portaria e vigilância.

c – Controle de acesso de pessoas, veículos e objetos.

d – Controle de acesso às salas e dependências internas das edificações ocupadas.

e – Cadastro de estagiários, cessionários e prestadores de serviço.

f – Emissão, distribuição e controle dos instrumentos de identificação de pessoas e veículos.

g – Controle de acesso às áreas e dependências especiais para a realização de eventos.

h – Captação e monitoramento de imagens, por sistema de câmeras de segurança.

i – Proteção contra incêndio e pânico.

Deve-se constituir barreiras para impedir o acesso físico de pessoas não autorizadas nas instalações. As barreiras são obstáculos de qualquer natureza que impedem, dificultam ou detectam os acessos físicos que podem se constituir em ameaça.

Os perímetros internos devem possuir barreiras dispostas de acordo com avaliação de risco do local. Elas se estendem do perímetro externo e chegam até as salas e gabinetes, passando pelas portarias, constituindo-se em linhas de proteção.

Os perímetros externos devem ser cercados por muros ou cercas de metal. Em áreas de alto risco de invasão as cercas ou muros podem conter concertinas ou cercas elétricas nas suas extremidades. Nesse caso, deverão ser afixados avisos de advertência ao longo de todo perímetro, alertando sobre a existência de cerca eletrificada.

Os prédios e instalações devem possuir um serviço de portaria, com equipamentos, sistemas e pessoal para seu trancamento.

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

As áreas externas, garagens e estacionamentos devem ser iluminados para garantir uma vigilância noturna adequada. Quando a situação permitir, podem ser instalados sensores de presença ligados à iluminação auxiliar, para melhorar as condições de luminosidade no local.

Os muros e cercas dos perímetros devem estar livres de vegetação que comprometa a segurança.

O cabeamento da rede elétrica deve ser protegida, em particular nas áreas externas. Nas áreas internas, os quadros de energia elétrica devem ser de livre acesso.

O cabeamento da rede lógica, para informática e comunicações, deve ser protegida. Os quadros e racks devem possuir sistemas de fechadura com chave ou outro dispositivo similar, para impedir o acesso indevido.

O cabeamento da rede de energia elétrica deverá ser instalado separadamente do cabeamento da rede lógica.

Não é permitida a filmagem ou fotografia no interior do Ministério Público sem permissão de autoridade competente para tal. Nos casos de reportagens jornalísticas, após a autorização, a equipe de jornalistas deverá ser acompanhado por um servidor da área de comunicação social.

As salas em que são tratados assuntos sigilosos, ou que pela sua sensibilidade mereçam maior grau de segurança, deverão possuir paredes com isolamento acústico. Estes locais poderão, de acordo com a necessidade, serem submetidos a varredura eletrônica e de ambiente.

Os equipamentos de ar condicionado instalados em paredes externas deverão possuir grades de proteção que impeçam o acesso indevido retirando-se o aparelho do local.

Os quadros de disjuntores de energia elétrica deverão ter as chaves devidamente identificadas.

As mesas de trabalho em que são tratados assuntos sigilosos deverão ser dispostas nas salas de forma a evitar a observação externa pelas janelas.

O Ministério Público deverá regular, em seus respectivos Planos de Segurança, as rotinas e horários para abastecimento de valores nos caixas eletrônicos existentes nas respectivas sedes.

As salas onde se localizam as dependências do almoxarifado, notadamente os locais com material de alto custo, informática ou sensível, deverão possuir teto com laje.

As atividades de portaria e vigilância compreendem:

a. A recepção, a orientação, o registro, o controle e a fiscalização da entrada e saída de pessoas, veículos e objetos nas dependências do Ministério Público.

b. A atividade de vigilância, destinada a proteger as pessoas e os bens patrimoniais, zelando pela tranquilidade nas dependências do Ministério Público.

A atividade de portaria e vigilância será planejada, organizada, controlada e coordenada pelo órgão de Segurança Institucional.

Nas instalações do Ministério Público que funcionam em edifícios cedidos, as atividades de portaria e vigilância serão executadas em articulação com os órgãos cedentes das instalações.

O serviço de vigilância, ao final do horário de funcionamento do Ministério Público, deverá realizar vistoria nas salas e dependências internas das edificações ocupadas, tendo como atribuições desligar a iluminação e os equipamentos encontrados em funcionamento, além de fechar portas e janelas deixadas abertas.

1.7. ORIENTAÇÕES DE SEGURANÇA PARA MEMBROS E SERVIDORES

a. Não deixar as chaves da promotoria à disposição de todos, especialmente dos gabinetes de membros e dos locais onde haja informações relevantes.

b. Ficar atento sobre quem trabalha em sua sede, bem como sobre as pessoas mais próximas no convívio funcional, incluindo profissionais da área jurídica.

c. Buscar informações com as unidades administrativas da PGJ, para saber os serviços programados do mês respectivo, especialmente reformas, detetizações e instalação de equipamentos, principalmente os que forem ser realizados em fins de semana. Isso ajudará na preparação para proteger os documentos e autos de danos ou acesso indevido quando da realização do serviço.

d. Seguir sempre as normas de segurança da instituição. Elas são estabelecidas para garantir a proteção de todos, exigindo impessoalidade em sua aplicação.

e. Alertar os responsáveis pelas falhas de segurança que presenciar, notificando o órgão de segurança de sua instituição.

f. Em casos de eventos, planejar com antecedência a realização e incluir a questão da segurança como um dos tópicos de consideração. Considere na definição das necessidades de segurança o local de realização do ato, a quantidade e

características das pessoas envolvidas, o tema do evento, a possibilidade de protestos de grupos civis organizados, o histórico dos eventos similares, a sua condição pessoal (estar em situação de ameaça ou de risco incrementado), a existência de rotas de fuga, saídas de emergência e equipamentos de prevenção e combate a incêndios.

4. SEGURANÇA DA INFORMAÇÃO

4.1. CONCEITO

A segurança da informação refere-se ao conjunto de medidas destinadas a estabelecer comportamento dos integrantes do Ministério Público, que garanta a proteção da informação. Engloba ainda, medidas de segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição.

É um dos principais ativos de qualquer instituição e deve ser protegida em todas as suas formas. A proteção da informação dá-se por meio de um conjunto de ações, que visa a minimizar o risco de comprometimento da informação e de seus sistemas de armazenamento e transmissão.

A segurança da informação é regida por quatro propriedades básicas, que estão presentes quando falamos de proteção da informação. São elas a Disponibilidade, Integridade, Confidencialidade e Autenticidade:

a. **Disponibilidade** - A disponibilidade objetiva garantir que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade. Consiste na proteção dos dados, para que não sejam alterados ou se tornem indisponíveis, assegurando ao usuário o acesso à informação sempre que dela precisar. Isso pode ser chamado também de continuidade dos serviços.

b. **Integridade** - objetiva garantir que a informação não seja modificada ou destruída de maneira não autorizada ou acidental. A integridade consiste em proteger a informação nas suas mais variadas formas contra alteração, sem a permissão explícita do seu proprietário. Isso significa que nada deve ser acrescentado, retirado ou modificado aos dados originais.

c. **Confidencialidade** - objetiva garantir que a informação não esteja disponível, ou que não seja revelada a qualquer pessoa física, sistema, órgão ou entidade não autorizados ou não credenciados. Os dados privados devem ser apresentados somente

aos seus donos ou ao grupo por ele liberado. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo.

d. **Autenticidade** - objetiva garantir que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Está associada à identificação correta de um usuário ou do computador, à certificação e origem da informação. Normalmente, é implementada a partir de um mecanismo de senhas ou de assinatura digital.

4.2. FINALIDADE

Estabelecer medidas para a proteção de dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não-autorizados, bem como sua adulteração, destruição ou outro dano ou inconveniência propositalmente imposta, possa causar prejuízo de qualquer natureza ao pessoal, bens e serviços do Ministério Público.

4.3. SEGURANÇA DA INFORMAÇÃO NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO

a. Garantir a proteção quanto aos recursos de informática em uso na instituição.

b. Assegurar a sua plena disponibilidade, livre de riscos ou ameaças ao seu bom funcionamento.

c. Garantir a utilização segura pela instituição de recursos computacionais como certificação digital, autenticações e auditoria de dados, investigações eletrônicas, entre outras.

d. Elaborar em conjunto com o órgão de tecnologia da informação, normas específicas a respeito da segurança dos dados institucionais relevantes e que tenham considerável impacto na imagem do Ministério Público.

e. Definir programa, dentre os disponíveis no mercado, para efetuar a criptografia de todos os dispositivos de armazenamento, fixos ou móveis, atualmente utilizados por membros da instituição, dando preferência àqueles que notadamente tenham alto grau de proteção de dados encriptados.

f. Implantar rotina, em conjunto com o órgão de tecnologia da informação, para a constante verificação de ataques de intrusos nas redes lógicas do Ministério Público, através da definição de ferramentas gerenciais e visuais de tráfego de rede.

g. Implementar e disponibilizar certificação digital a todos os membros no Ministério Público, dando maior segurança e evitando possíveis fraudes.

h. Criar projeto completo de reestruturação de rede computacional lógica estruturada (*as built*), adequando todas as instalações do Ministério Público, separando inclusive a rede elétrica comum da destinada ao ambiente computacional.

i. Elaborar projeto para implementar telefonia IP após a realização da reestruturação de rede lógica e elétrica, o que dentre outras facilidades, como vídeochamadas e vídeoconferências, reduziria sensivelmente custos com telefonia.

j. Complementar a área de controle patrimonial, através da implementação de sistema de monitoramento por câmeras em todos os ambientes julgados necessários.

k. Criar protocolo de ajuste de conduta computacional junto aos membros do Ministério Público, difundindo informações práticas do dia a dia ligadas a segurança da informação.

4.4. ATRIBUIÇÕES DOS ÓRÃOS DO MINISTÉRIO PÚBLICO QUANTO À SEGURANÇA DA INFORMAÇÃO EM AMBIENTE INFORMATIZADO

Órgão de Tecnologia da informação:

a. Criar e manter cópias de segurança (*backups*) dos dados críticos, armazenados nos servidores de redes.

b. Guardar os *backups* em local seguro, separados dos equipamentos, para viabilizar a recuperação dos dados.

c. Realizar auditoria de segurança e análise de risco nos ambientes operacionais, nos sistemas de informação localizados nos prestadores de serviços e nas próprias instalações nas unidades do Ministério Público, bem como autorizar testes controlados para identificar a existência de falhas ou vulnerabilidades.

d. Realizar o programa de capacitação de servidores do Ministério Público na área de segurança da informação.

e. Atualização dos *softwares* em uso no Ministério Público.

f. Prevenção, detecção e eliminação de vírus de computador.

g. Cópia de segurança (*backup*) e recuperação.

h. Uso, armazenamento e destruição de informações.

i. Transmissão e compactação de dados.

j. Desenvolver e manter os sistemas de informação corporativos de acordo com a política de segurança da informação vigente.

k. Administrar a utilização e a configuração das bases de dados, de acordo com a política de segurança da informação vigente.

l. Orientar os usuários quanto aos procedimentos de segurança da informação.

m. Instalar ou remover componentes, fazer manutenção, homologar e controlar *hardware* e *software*.

n. Tratar os incidentes de segurança da informação em meio eletrônico.

o. Possibilitar o controle de acesso à informação em meio eletrônico de forma integrada entre os vários serviços e aplicações corporativas disponíveis.

p. Bloquear os usuários assim que desligados, bem como o acesso a qualquer recurso da rede.

q. Manter em todos os computadores antivírus instalado e atualizado periodicamente.

r. Disponibilizar aos usuários o acesso ao correio eletrônico a partir de qualquer

computador conectado à *internet*, utilizando-se do serviço de *WebMail*, sendo que este serviço poderá ser acessado através do portal do Ministério Público.

Órgãos de Engenharia e Arquitetura

a. Verificar se as instalações prediais e infraestrutura elétrica onde estão instalados os equipamentos de informática estão compatíveis com as Normas Técnicas de Segurança e com as recomendações do fabricante.

b. Prover a proteção e segurança física do centro de processamento de dados, com:

i. Controle de acesso de entrada física.

ii. Geradores de energia e *no-breaks*.

iii. Monitoramento de câmeras CFTV.

iv. Rede de supressão a gás.

v. Meio de detecção e extinção de incêndio no ambiente.

vi. Cabeamento estruturado em piso elevado.

4.5. ORIENTAÇÕES A MEMBROS E SERVIDORES QUANTO À SEGURANÇA DA INFORMAÇÃO EM AMBIENTE INFORMATIZADO DO TRABALHO

a. Não utilizar o *e-mail* para fins ilegais e transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis.

b. Não utilizar *e-mail* para transmitir mensagens conhecidas como *spam*, *JunkMail*, correntes ou a distribuição de mensagens em massa não solicitadas.

c. Encerrar a sessão através do *logoff*, bloquear o acesso ao computador, reiniciar ou desligar o sistema, sempre que se afastar do mesmo.

d. Não configurar ou alterar as configurações de rede e de acesso à *internet* dos computadores, incluindo as seguintes: IP, DNS, WINS, *Gateway, Proxy* e a instalação ou

reconfiguração de clientes *Proxy*.

e. Não enviar, baixar (*download*) ou manter arquivos de imagens, músicas, vídeos e arquivos executáveis em geral, ou quaisquer outros de caráter pessoal.

f. Não acessar *sites* do gênero relacionamento, dos quais façam parte.

g. Não acessar *sites* de *Internet* com conteúdo pornográfico, jogos, bate-papo, *chat, blogger, cartoon*, relacionamento, música, *hacker* ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança.

h. Não acessar *sites* nem utilizar programas de troca de mensagens instantâneas ou arquivos do tipo.

i. Não utilizar sites do tipo *Proxy*.

4.6. ORIENTAÇÕES A MEMBROS E SERVIDORES ACERCA DA SEGURANÇA DA INFORMAÇÃO EM COMPUTADOR, *INTERNET* E REDES SOCIAIS

a. Certifique-se de não estar sendo observado ao digitar sua senha.

b. Não fornecer senha para outra pessoa.

c. Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senha. Use a opção de sair (*logout*), pois isso evita que suas informações sejam mantidas no navegador.

d. Elaborar senha sem nomes/sobrenomes de pessoas, datas, telefones e placas de veículos. Use senhas com letras, números e símbolos (*&#$) e nunca use dados pessoais. Lembre-se de mudar periodicamente suas senhas e crie uma senha com, no mínimo, oito caracteres.

e. Não compartilhe sua senha de rede/e-mail. É de sua responsabilidade o que acontece com seu *login*.

f. Não use a mesma senha para todos os serviços que acessa.

g. Ao usar perguntas de segurança para facilitar a recuperação de senha, evite escolher aquelas cujas respostas possam ser facilmente adivinhadas.

h. Tenha o hábito de bloquear sua estação de trabalho ao sair de perto de seu computador (Ctrl+Alt+Del e "bloquear estação de trabalho").

i. Certifique-se de utilizar serviços criptografados quando o acesso a um *site* envolver o fornecimento de senha.

j. Procure manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar sua senha, caso você não tenha sido cuidadoso ao elaborá-la.

k. Mantenha a segurança do seu computador.

l. Seja cuidadoso ao usar sua senha em computadores potencialmente infectados ou comprometidos. Procure, sempre que possível, utilizar opções de navegação anônima.

m.Lembre-se que o cuidado com a segurança da informação continua após o horário de expediente.

n. Evite compartilhar pastas de seu computador (compartilhamento de rede).

o. Examine previamente os arquivos anexados em *e-mail* com antivírus. Na dúvida, não abra.

p. Não utilizar o *e-mail* funcional para uso pessoal.

q. Realize sempre a cópia de segurança dos dados armazenados no disco rígido da estação de trabalho.

r. Evite abrir e-mails suspeitos de remetentes desconhecidos. Não clique em *link*s suspeitos.

s. Evite trazer CD, DVD, *pen drive*s ou quaisquer outros dispositivos móveis de fora do Ministério Público. Se você utilizar esses dispositivos em um computador infectado, ele poderá carregar o vírus e infectar computadores da instituição.

t. A equipe técnica do Ministério Público se encarrega de manter o antivírus

atualizado, mas nem sempre esse mecanismo de proteção conseguirá proteger contra todo tipo de invasão. Em caso de qualquer problema, abra um GLPI para que a situação possa ser corrigida.

u. Mantenha sempre seus dados digitais em pastas criptografadas, usando o programa gratuito *Truecrypt*. Ao enviá-los por *e-mail,* também use criptografia para protegê-los, podendo ser utilizado o programa *Encryptfiles,* também gratuito e eficiente. Ambos são fáceis de baixar da *internet* e de usar. Na dúvida, entre em contato com o setor de segurança ou com a diretoria de TI para agendar uma visita e aprender a utilizar as ferramentas.

v. Caso esteja digitando um documento de conteúdo sigiloso como, por exemplo, uma petição com medidas de natureza cautelar ou antecipatória, criminal ou cível, desconecte o computador da rede, de modo a não permitir que alguém, mesmo que seja servidor da instituição, capture ou leia seu arquivo indevidamente.

w. Não instale programas de computador em dispositivos funcionais sem adquiri-los de fontes seguras e sem autorização do órgão de tecnologia da informação. Em muitos programas baixados diretamente da *internet* estão contidos códigos maliciosos para acessar indevidamente informações de sua máquina ou mesmo utilizá-la para espalhar conteúdos maliciosos pela rede.

x. Mantenha sempre o antivírus atualizado de sua máquina, bem como das máquinas de sua promotoria. Cobre do órgão de tecnologia da informação as ações necessárias para não deixar tais computadores desguarnecidos dessa importante ferramenta de proteção das informações funcionais.

y. Cuidado com informações funcionais em *smartphones* e *tablets*, especialmente *e-mails*. Recomenda-se a leitura e a exclusão imediata das mesmas.

4.7. ORIENTAÇÕES A MEMBROS E SERVIDORES ACERCA DE SEGURANÇA DA INFORMAÇÃO NO TELEFONE

a. Trate o telefone como um meio de comunicação sem segurança, principalmente o celular.

b. Quando atender ao telefone, não forneça o número dele, seu nome e demais dados pessoais. Verifique a identidade de quem chama antes de prestar qualquer informação. Se o interlocutor não sabe dizer seu nome ou indicar com quem deseja, falar encerre a ligação.

c. Evite manter seu número na lista telefônica.

d. Os empregados e membros da família devem ser orientados a nunca fornecerem dados pessoais, detalhes da localização ou movimentação.

e. Instale um identificador de chamadas (bina).

f. Tenha especial atenção com chamadas a cobrar. Lembre-se de que a maioria dos casos de extorsão é efetuada a partir destas ligações.

g. Não se iluda com prêmios e sorteios. Procure não aceitar ofertas de produtos. Não ceda às pressões por cartões telefônicos, pedidos de depósitos bancários ou saque.

h. Nunca fale ao telefone assuntos funcionais sigilosos ou mesmo a respeito de aspectos de sua vida privada, que possam ser utilizados para chantagens. Procure tratar sobre esses assuntos apenas pessoalmente.

i. Caso necessite tratar ao telefone assuntos funcionais sigilosos, comunique-se o mais truncado possível, de modo a permitir a comunicação sem revelar para terceiros que eventualmente estejam ouvindo o conteúdo integral da conversa.

4.8. ORIENTAÇÕES A MEMBROS E SERVIDORES ACERCA DE SEGURANÇA DA INFORMAÇÃO EM OPERAÇÕES BANCÁRIAS

a. Cheques, extratos, faturas de cartões de créditos e demais informações sobre suas operações bancárias são importantes documentos que devem ser guardados e manuseados com extrema cautela.

b. Cuidado ao portar talão de cheques. Se possível, tenha consigo somente a quantidade de folhas necessárias à sua utilização diária.

c. Não entregue folhas de cheques para terceiros preencherem. Sempre que possível, identifique o nome do favorecido.

d. No caso de perda ou furto de talões de cheque ou cartões, comunique imediatamente ao seu banco.

e. Confira periodicamente o seu extrato. Em caso de transação suspeita, comunique imediatamente ao seu banco.

f. Mantenha o corpo próximo ao caixa eletrônico, de maneira a impedir a visualização dos dados expostos na tela.

g. Esteja atento a pessoas suspeitas ou curiosas no interior da cabine ou nas proximidades. Na dúvida, não realize a operação.

h. Suas senhas não devem ser escritas em locais de fácil acesso. Procure gravá-las e destruí-las em seguida. É recomendável a troca de senhas periodicamente.

i. Nunca escolha senhas que possam ser facilmente descobertas por terceiros (data de nascimento, número de identidade, placas de automóveis etc).

j. Nunca forneça senhas ou demais dados confidenciais por telefone, mesmo em caso de informação sobre o recebimento de prêmios.

4.9. ORIENTAÇÕES A MEMBROS E SERVIDORES ACERCA DE OPERAÇÕES BANCÁRIAS PELA *INTERNET*

a. Não utilize computadores de terceiros, como *lan houses*, aeroportos, *cybercafés* e *stands* de eventos para fazer operações financeiras.

b. Para compras pela *internet*, use apenas *sites* conhecidos, seguros e recomendados por terceiros.

c. Não use redes de *wi-fi* públicas em seu celular, *tablet* ou *notebook*. Seu equipamento pode ser monitorado, além de suas informações e fotos serem copiadas.

4.10. ORIENTAÇÕES A MEMBROS E SERVIDORES ACERCA DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE TRABALHO

a. Antes de deixar seu local de trabalho, certifique-se que todos os documentos, materiais e mídias contendo informações relevantes ou sigilosas estão protegidos contra terceiros não autorizados. Mantenha-os sempre trancados em armários, retirando as chaves após trancá-los.

b. Ao receber alguém em seu gabinete, não permita a exposição de conteúdo de autos ou de documentos, impressos ou em mídia, que não devam ser conhecidos pelo visitante. De preferência, deixe sua mesa limpa de documentos e a tela do computador sem documento digital aberto.

c. Providencie para que o acesso aos feitos judiciais e extrajudiciais de sua promotoria seja realizado apenas por servidor autorizado. Em caso de autos com assunto sigiloso, de preferência, deixe apenas um servidor ou assistente autorizado a consultá-lo.

d. Compartimente informações funcionais, evitando repassá-las apenas por amizade ou coleguismo. Apenas repasse dados conhecidos para quem pode e precisa conhecê-los, para a realização da respectiva função.

e. Os documentos e autos sigilosos devem ter tratamento diferente dos demais

documentos, sem risco quanto ao seu conteúdo. Tal diferença deve abarcar a produção, a transmissão, o transporte, o armazenamento, o arquivamento, a reprodução e a destruição, de modo que em cada um desses momentos os conteúdos sigilosos tenham salvaguardas maiores do que os demais, para proteger o respectivo conteúdo de vazamentos, subtrações ou adulterações.

f. Triture sempre documentos, borrões e anotações com conteúdos relevantes ou sigilosos que serão descartados.

g. Guarde os documentos mais sensíveis de sua promotoria nos cofres disponibilizados pela instituição.

h. Atenção sempre na forma como os procedimentos são manejados na secretaria de sua unidade, especialmente se as regras de tratamento de documentos sigilosos são seguidas.

i. Zele para que todos os documentos da sua unidade estejam guardados em armários trancados ou em cofres, bem como todas as portas das salas trancadas, quando do fechamento da mesma para o período noturno ou, especialmente, para o fim de semana.

j. Estabeleça também de forma clara, para os servidores e terceirizados de sua unidade, o que pode e o que não pode ser repassado a terceiros por telefone, orientando sempre para que não sejam repassadas informações pessoais sobre membros ou mesmo sobre as rotinas deles e da própria promotoria.

k. Antes de reuniões sobre investigações ou outros assuntos sigilosos, verifique se a sala onde será realizada permite a escuta da conversa por terceiros fora da sala. Em caso de risco desse tipo de vazamento, tome providências para reduzir ao máximo as possibilidades de ocorrência, como o isolamento de corredores de acesso ou mesmo a definição de outro horário ou local para a conversa.

l. Agende periodicamente com o órgão de segurança de sua instituição a realização de varreduras eletrônicas em sua promotoria, com o objetivo de identificar instalação ilegal de equipamentos de espionagem.