SEGURANÇA INSTITUCIONAL

# DICAS DE SEGURANÇA PARA SERVIDORES DO MPF

MPF
Ministério Público Federal

# DICAS DE SEGURANÇA PARA SERVIDORES DO MPF

## MINISTÉRIO PÚBLICO FEDERAL

Procuradora-Geral da República
Raquel Elias Ferreira Dodge

Vice-Procurador-Geral da República
Luciano Mariz Maia

Vice-Procurador-Geral Eleitoral
Humberto Jacques de Medeiros

Ouvidor-Geral do Ministério Público Federal
Juliano Baiocchi Villa-Verde de Carvalho

Corregedor-Geral do Ministério Público Federal
Oswaldo José Barbosa Silva

Secretário-Geral
Alexandre Camanho de Assis

Secretário de Segurança Institucional
Delfim Loureiro Queiroz

Secretário de Segurança Institucional Adjunto
José Benedito Ramos Andrade

MINISTÉRIO PÚBLICO FEDERAL
Secretaria de Segurança Institucional

# DICAS DE SEGURANÇA PARA SERVIDORES DO MPF

Brasília - DF
MPF
2019

Disponível em: http://intranet.mpf.mp.br/areas-tematicas/administrativas/seguranca-institucional-2/campanhas

Dados Internacionais de Catalogação na Publicação (CIP)

B823d

Brasil. Ministério Público Federal. Secretaria de Segurança Institucional.
Dicas de segurança para servidores do MPF – Brasília : MPF, 2019.
29 p. : il.

Disponível também em: http://intranet.mpf.mp.br/areas-tematicas/administrativas/seguranca-institucional-2/campanhas

1. Segurança pessoal. 2. Direito à integridade física. 3. Violência urbana. I. Título.

CDD 363.22

Elaborado por Isabella de Oliveira e Nóbrega – CRB1/3131

Coordenação e organização
Secretaria de Segurança Institucional (SSIn)

Projeto gráfico, revisão e diagramação
Secretaria de Comunicação Social (Secom)

Normalização Bibliográfica
Coordenadoria de Biblioteca e Pesquisa (Cobip)

Procuradoria-Geral da República
SAF Sul Quadra 4 Conj. C
CEP 70050-900 Brasília – DF
Telefone: (61) 3105-5100

www.mpf.mp.br/pgr

# SUMÁRIO

# APRESENTAÇÃO

Constantemente somos informados pela mídia a respeito de situações relacionadas à falta de segurança em nosso país. Isso gera uma sensação de desproteção cada vez maior e, assim, a impressão de que somos apenas expectadores do que está acontecendo.

Por isso, a Secretaria-Geral do Ministério Público Federal, por intermédio da Secretaria de Segurança Institucional, elaborou esta Cartilha de Segurança Pessoal, contendo orientações básicas de segurança, as quais podem prevenir ou evitar que membros e/ou servidores do Ministério Público Federal se tornem vítimas da violência urbana.

## 1 CONCEITOS E DEFINIÇÕES

Segurança Institucional: é 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 à reputação. Compreende a Segurança Orgânica e a Segurança Ativa.

## Grupos de Medidas

## 2 SEGURANÇA DE RECURSOS HUMANOS

A Segurança de Recursos Humanos 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.

## 3 DICAS GERAIS

- Evite exposições públicas de informações em meios de comunicação e em mídias sociais;
- Evite colocar seus dados pessoais (endereço, CPF, telefones etc.) em cadastros de redes sociais, mesmo que selecione modo privado, pois esses dados são frequentemente roubados e publicados em outros sites;
- Tenha cuidado ao expor fotografias pessoais ou de familiares no perfil do WhatsApp;
- Fique atento ao risco de engenharia social, não só em redes sociais, mas também por telefonemas, e oriente funcionários e familiares quanto ao perigo;
- Altere itinerários e rotina;
- Evite locais de pouca circulação de pessoas;
- Evite festas ou reuniões em locais abertos, em que não haja policiamento ou força policial próximos; e
- Para todo e qualquer fato adverso, fica a melhor dica: NÃO REAJA!

## 4 CONDUÇÃO DE VEÍCULOS

- Não coloque no carro adesivos que possam identificar onde você mora, onde trabalha, a academia que frequenta, faculdade etc. Isso pode ser usado contra você; e
- Ao entrar no veículo, ligue-o, trave as portas e saia imediatamente. Após isso, coloque o cinto e só depois ligue o rádio etc.; quanto mais tempo parado, maior o risco de uma abordagem.

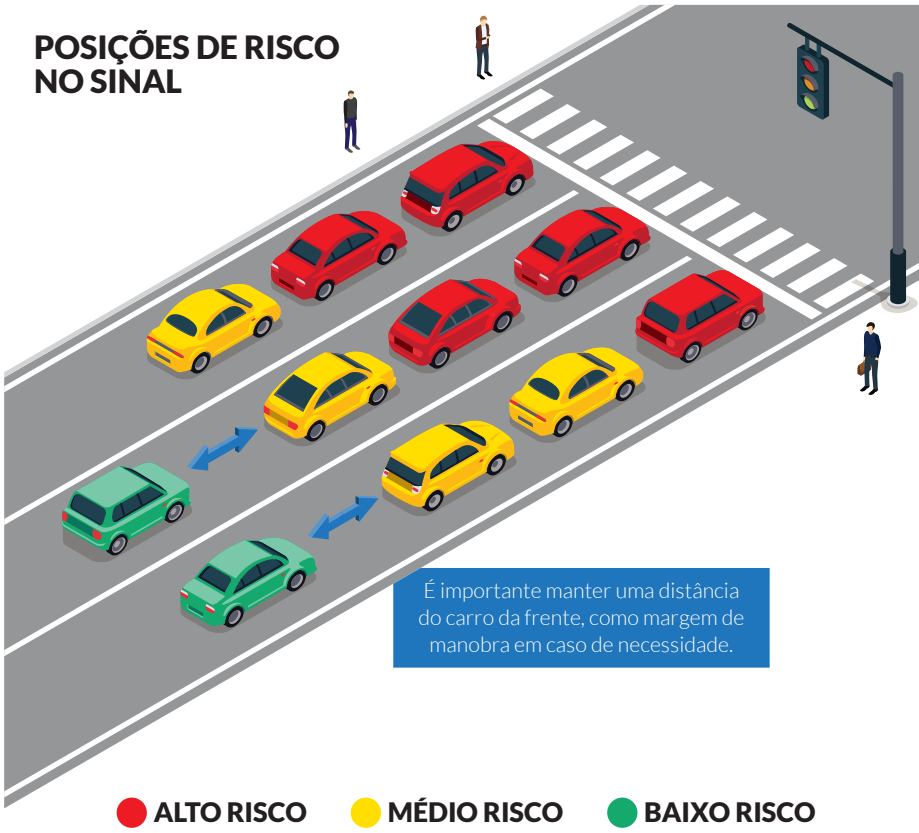
O bandido não quer ter surpresas desagradáveis e, em regra, escolhe os alvos mais fáceis, sendo assim as películas escuras (insulfilme) são interessantes para inibir a ação de assaltantes.

Se alguém colidir em seu veículo, em trânsito, tenha cuidado e desconfie, pois pode ser uma "manobra de colisão" para dissimular o cometimento de algum delito. Observe quantas pessoas se encontram no interior do outro veículo; verifique se há outros veículos em apoio, principalmente motos. Nesse caso, não pare! Tente registrar a placa e sinalize para que os demais envolvidos possam lhe seguir até o posto policial ou delegacia mais próxima.

- Antes de estacionar (ou quando retornar), olhe ao redor, veja se existe alguém ou alguma situação suspeita;
- Se desconfiar de alguma coisa, passe direto por seu carro e reavalie a situação. Na dúvida, chame a polícia;
- Ao estacionar, feche totalmente seu veículo, certificando-se, tentando abrir as maçanetas das portas, de que seu alarme foi efetivamente acionado e suas portas estão devidamente trancadas;
- Tranque seu veículo mesmo que a saída seja por apenas alguns minutos ou que esteja na garagem de sua casa ou edifício;
- Ao sair de seu veículo, nunca o deixe ligado ou mesmo com ocupantes em seu interior (especialmente crianças), mesmo que seja apenas por alguns instantes;
- Nunca fique dentro do carro estacionado. Você se transforma na vítima perfeita, seja em via pública, seja em estacionamento privado. Essa é uma ótima oportunidade para ser surpreendido. Se for necessário, faça-o em local que permita uma ampla visão do ambiente e permaneça sempre alerta à aproximação de estranhos; e
- Lembre-se: carro parado é alvo fácil!

Para a entrada em residências ou condomínios, sugere-se:

- analise o perímetro para verificar situações ou atitudes suspeitas;
- não menospreze incongruências ou situações incomuns;
- alterne a rota de chegada;
- sempre avance para averiguar pontos de guarida. Caso necessário, faça uma volta completa antes de iniciar a entrada à residência;
- posicione o carro, no acesso à garagem, de modo que seja possível a rápida evasão e diminua a probabilidade de encurralamento. Evite posicionar-se perpendicularmente;
- mantenha o carro engatado em primeira marcha ou ré, a depender do caso;
- não reduza a atenção ao perímetro;
- após entrar, certifique-se de que não houve acesso simultâneo não autorizado; e
- mesmo no interior da garagem, seja rápido ao desembarcar.




Áreas de risco no semáforo:

A. em geral, a faixa central é a mais segura, pois o bandido irá agir pelas calçadas ou pelo canteiro central;
B. procure manter distância do veículo da frente, o suficiente para visualizar as rodas de trás do carro, assim, caso precise, você poderá se evadir rapidamente do local sem fazer manobras;
C. se a intenção for roubar o veículo, as primeiras posições são mais perigosas, pois o bandido terá a sua frente livre para deixar o local rapidamente; e
D. se a intenção for roubar objetos, as últimas posições também se tornam perigosas, já que o bandido não irá se expor demasiadamente e terá maior facilidade para fugir por trás do veículo sem ter que transitar entre outros carros parados.

## 5 CAMINHANDO NAS RUAS

- Esteja sempre atento ao modo de se vestir, aos locais por onde irá transitar, aos objetos que esteja ostentando. Utilize somente o que tenha necessidade de uso. Nunca leve objetos que não tenham utilidade;
- Evite locais desertos e/ou com pouca iluminação, bem como cortar caminhos por becos, vielas, ruas, terrenos, construções, entre outros locais desconhecidos, ermos, ou pouco utilizados por você;
- Evite atender pedidos ou informações que lhe despertem desconfiança;
- Desconfie de estranhos com conversas envolventes e que tentem se aproximar de você; e
- Cuidado ao atender seu telefone celular em ambientes públicos e/ou de grande aglomeração de pessoas. Você estará distraído e poderá ser alvo de furto.

## 6 CAMINHANDO NAS RUAS – CRIANÇAS

Por ainda estarem no processo de maturidade psicológica e social, as crianças tornam-se alvos fáceis de ações de meliantes. Indivíduos podem se aproximar delas para obter algum tipo de vantagem. Com isso, todo cuidado é pouco.

- Orientem e cobrem para que sempre estejam acompanhadas de algum adulto. Nunca deixem suas crianças sozinhas;
- Avisem de que, em caso de estarem sendo seguidas por estranhos na rua, devem pedir ajuda a um policial ou a alguém uniformizado. Pode-se, também, entrar na primeira casa habitada que encontrar ou em qualquer estabelecimento comercial;
- Em caso de serem atacadas por alguém, ou tentarem agarrá-las, ensinem a gritar bem alto e espernear, repetidas vezes, pedindo ajuda;
- Orientem a nunca aceitar carona de pessoas desconhecidas e, se alguma delas as chamar, diga para não darem atenção e nunca se aproximarem do veículo de estranhos; e
- Orientem seus filhos a não aceitarem nada de pessoas estranhas, principalmente, comida e bebida.

## 7 DURANTE UM ASSALTO

- Mantenha-se o mais calmo possível e não esboce qualquer tipo de reação. Lembre-se de que não há dinheiro ou patrimônio que valha sua vida;
- Evite gritar ou discutir com o criminoso, entregue o que lhe for exigido e faça apenas o que ele mandar. Seu nervosismo poderá aumentar a tensão do meliante e provocar uma atitude mais agressiva em seu desfavor;
- Comunique-se com tranquilidade e faça movimentos lentos;
- Responda com calma o que lhe for perguntado e avise antecipadamente sobre qualquer gesto ou movimento que você precise fazer; e
- Evite olhar diretamente para o meliante. Isso normalmente é visto como uma intimidação, ameaça ou uma afronta.

## 8 SEGURANÇA RESIDENCIAL

Imagine sua residência como se fosse composta por uma série de perímetros de proteção, para salvaguardá-la da ação de meliantes. Percorra todo o perímetro interno e externo, verificando a segurança que eles lhe oferecem, tais como: iluminação ao redor da residência, janelas seguras, portas reforçadas, câmeras de segurança, barreiras físicas (muros de alvenaria, cercas, muro natural, entre vários outros).

- Muitos invasores acessam as residências por meio de portas ou janelas que foram esquecidas abertas ou destrancadas. Antes de dormir ou de sair de casa, verifique se todas as portas e janelas estão devidamente trancadas;
- Grades de proteção em portas e janelas aumentam o grau de segurança. Sua casa deve parecer de difícil acesso para o meliante. Assim, a probabilidade de você se tornar uma vítima será menor;
- Oriente familiares e empregados a não comentarem com estranhos os hábitos, as rotinas, os bens e as atividades sociais e profissionais da família;
- Ao sair e ao chegar em sua residência, verifique se há movimento de pessoas estranhas na rua;
- Ao regressar para sua residência, caso verifique sinais de arrombamentos ou qualquer sinal de anormalidade (luzes acesas, portas ou janelas abertas, marcas de pés nas paredes próximas às janelas, cortinas movimentadas etc.), não entre! Chame imediatamente a polícia;
- Atenda à porta somente após identificação prévia;
- Mantenha a porta da garagem sempre fechada;

- Faça uso de dispositivos eletrônicos de segurança. Instale sistema de CFTV, ofendículos, sensores de movimento. Lembre-se do amparo legal para uso de alguns itens de segurança, como a cerca eletrificada, em que há normas específicas a serem observadas;
- Fique atento ao nível de segurança adotado pelas residências vizinhas. Observe se são utilizados sistema de CFTV, cerca eletrificada, concertinas etc. Procure adotar o mesmo nível de segurança;
- Portas externas devem ser maciças e o mais reforçadas possível;
- Evite espaços a serem revestidos por vidros, próximos à fechadura, eles poderão ser facilmente quebrados e a fechadura estará à mercê da ação dos meliantes;
- Janelas de vidro, que tenham espaço razoável, podem ser invadidas por meliantes de pequeno porte ou por crianças;
- Lembre-se de que o pavimento superior deverá ter o mesmo nível de segurança do pavimento inferior;
- Plantas e arbustos espinhosos podem ser utilizados pelo lado de dentro do jardim junto aos muros, grades, cercas ou janelas, formando uma barreira natural;
- No quintal, não deixe escadas ou outros objetos que possam facilitar o acesso a pavimentos superiores;
- Mantenha os acessos à residência bem iluminados, inclusive em áreas que ligam a residência à via pública; e
- Na maioria dos casos, a invasão às residências é realizada por escalada, ou seja, pulando grades e muros ou acessando janelas. Nesse caso, evite detalhes ou barras transversais que possam ser utilizadas como degraus.

## 9 ESTABELECIMENTOS BANCÁRIOS

- Evite conversar com pessoas estranhas dentro ou fora do ambiente bancário, principalmente acerca de suas operações financeiras;
- Observe atentamente as pessoas em atitudes suspeitas próximas ao local de caixas eletrônicos. Observe também a existência de dispositivos implantados com intuito de capturar informações de seu cartão eletrônico;
- Evite ao máximo realizar saques de alto valor. Caso seja imprescindível, solicite o recebimento em uma sala reservada, evitando fazer a contagem em frente a estranhos ou no próprio caixa. Verifique se não está sendo observado e/ou seguido por alguém.

## 10 CONTRATAÇÃO DE FUNCIONÁRIOS DOMÉSTICOS

- Contrate apenas pessoas que tenham ótimas referências de parentes ou de amigos. Pessoas que você conheça muito bem e em quem confie. Ao sair de casa, deixe todas as orientações de como deve ser o procedimento em casos de emergências;
- Em caso de apartamentos, mostre onde se encontram os extintores de incêndio e saídas de emergência;
- Faça uma relação de números de telefones (Polícias, Corpo de Bombeiros Militar, Samu, farmácia mais próxima...) que podem ser necessários em casos de emergência; e
- Os funcionários não devem receber visitas no local de serviço sem que estejam devidamente autorizados.

## 11 PRAIAS, RIOS OU LAGOS

Segundo a Sociedade Brasileira de Salvamento Aquático (Sobrasa), a maior *causa mortis* em crianças de 0 a 4 anos de idade é por afogamento. O afogamento é, também, a segunda maior *causa mortis* de 0 a 14 anos de idade, perdendo apenas para acidentes automobilísticos. Assim, saber nadar é também uma questão de sobrevivência, e não somente uma prática esportiva.

- Evite entrar sozinho no mar, principalmente, onde houver ondas e correntezas. Lembre-se de que câimbras sempre poderão ocorrer;
- Não entre na água à noite;
- Não entre nos locais com sinalização de risco;
- Em rios, observe a força da água, se estiver chovendo não entre, pois existe a possibilidade do aumento repentino do nível de água; e
- Mantenha a atenção em seus filhos. Não perca o contato visual.

## 12 SEQUESTRO RELÂMPAGO

- Nunca reaja! Em nenhuma circunstância se deve esboçar qualquer tipo de reação;
- Se possível, obedeça a todas as exigências do meliante;
- Tente observar as características físicas e individuais, como: tatuagens, cabelos,

olhos, altura, peso, gírias, sotaques, sinais visíveis, entre outras características e peculiaridades que possam identificá-lo; e

- Assim que for liberado, solicite auxílio à polícia.

## 13 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados podem acarretar prejuízos de qualquer natureza ao Ministério Público ou proporcionar vantagem a atores antagônicos. Visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, informação ou conhecimento. A segurança da informação, pela sua relevância e complexidade, desdobra-se nos seguintes subgrupos:

- Segurança da Informação nos Meios de Tecnologia da Informação;
- Segurança da Informação de Pessoas;
- Segurança da Informação na Documentação; e
- Segurança da Informação nas Áreas e Instalações.

## 14 SEGURANÇA DA INFORMAÇÃO DE PESSOAS

A Segurança da Informação de Pessoas compreende um conjunto de medidas voltadas a assegurar comportamentos adequados dos integrantes da Instituição ou de terceiros, que garantam a salvaguarda de informações sensíveis ou sigilosas, em especial:

I. segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição;
II. detecção, identificação, prevenção e gerenciamento de infiltrações, recrutamentos e outras ações adversas de obtenção indevida de informações;
III. identificação precisa, atualizada e detalhada das pessoas em atuação ou de inter-relação no respectivo ramo do Ministério Público; e
IV. verificação e monitoramento de ações de prestadores de serviços na Instituição.

## 14.1 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO DE PESSOAS

- Acesso é a possibilidade, oportunidade de se obter informações;
- Sigilo é tudo o que deve permanecer de conhecimento restrito, que deve ser protegido;
- Informação sensível é o dado ou conhecimento que, em decorrência de sua natureza ou conteúdo, deveria ser classificado, mas ainda não foi;
- Informação sigilosa é aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade;
- Informação ostensiva é aquela não classificada, que pode ser franqueada. Não significa livre acesso;
- Compartimentação é a restrição de acesso com base na necessidade de conhecer;
- Necessidade de conhecer é a condição inerente ao efetivo exercício do cargo, emprego ou função. O acesso a dado ou conhecimento sigiloso somente é concedido para quem dele necessite funcionalmente; e
- Credencial de segurança é a autorização oficial que habilita uma pessoa a ter acesso a documentos e informações classificados.

## 14.2 ENGENHARIA SOCIAL

Engenharia Social, no contexto de segurança, é a habilidade de conseguir acesso a informações sensíveis ou confidenciais ou a áreas importantes de uma instituição por meio de habilidades de persuasão.

Refere-se à manipulação psicológica de pessoas para se ter acesso a informações confidenciais.

Depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança. Um ataque clássico na engenharia social ocorre quando uma pessoa se passa por um alto funcionário dentro de instituições e diz que possui problemas urgentes, conseguindo, assim, o acesso a informações restritas.

É aplicada em diversos setores da Segurança da Informação, e, independentemente de sistemas computacionais, software e/ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de Engenharia Social.

Deve-se considerar que informações, tais como dados pessoais, números de telefones, rotinas, nomes de familiares, agenda de compromissos, endereço de e-mail etc., são elementos que podem colocar em risco a segurança de servidores ou mesmo de uma autoridade do Ministério Público Federal. Para obter essas informações, muitas vezes os engenheiros sociais utilizam o telefone e possuem como objetivo se passar por algum funcionário, colega de trabalho ou algum tipo de autoridade externa.

Os primeiros alvos são secretárias, recepcionistas e seguranças, pois esses funcionários estão sempre em contato (direto ou indireto) com as autoridades – os verdadeiros alvos. Assim, por meio de pessoas mais acessíveis e com cargos menores é possível obter informações sobre aquelas mais bem posicionadas na hierarquia.

### 14.2.1 TÉCNICAS DE ENGENHARIA SOCIAL – REDES SOCIAIS

Muitas pessoas possuem perfis e contas em redes sociais, o que facilita a Engenharia Social criminosa. Ao criar perfis em sites de relacionamento, é preciso ter cautela com os dados fornecidos, pois muitas vezes eles podem ser usados na preparação de um ataque via telefone. Não é aconselhável colocar telefones, endereço, a unidade do Ministério Público que você trabalha ou qualquer tipo de informação pessoal em seu perfil.

Quando um engenheiro social precisa conhecer melhor seu alvo, essa técnica é utilizada, iniciando um estudo no site da Instituição para melhor entendimento da estrutura. Por meio de pesquisas na internet e uma boa consulta nas redes sociais, é possível encontrar informações interessantes de funcionários da Instituição, cargos, amizades, perfil pessoal, entre outros.

### 14.2.2 TÉCNICAS DE ENGENHARIA SOCIAL – CONTATO TELEFÔNICO

Com os dados já coletados, o engenheiro social pode utilizar uma abordagem via telefone para obter acesso a informações, seja se passando por um funcionário de empresa terceirizada, servidor de outra instituição, autoridades etc. Nesse ponto, o engenheiro social já conhece o nome da secretária e da autoridade.

Com um simples telefonema e técnicas de Engenharia Social, fingindo ser, de preferência, o elo de confiança da vítima, fica mais fácil conseguir um acesso ou coletar informações sensíveis e até mesmo sigilosas.

### 14.2.3 TÉCNICAS DE ENGENHARIA SOCIAL – FALAR A MESMA LÍNGUA

Cada instituição possui sua própria linguagem. No nosso caso, a linguagem do meio jurídico. A Engenharia Social criminosa estuda tal linguagem para tirar o máximo proveito.

O motivo é simples: se alguém fala com você utilizando uma linguagem conhecida é mais fácil se sentir seguro e baixar a guarda.

### 14.2.4 TÉCNICAS DE ENGENHARIA SOCIAL – MÚSICA DE ESPERA

Ataques bem-sucedidos exigem paciência, tempo e persistência.

Uma abordagem atual é colocar a música que as empresas utilizam para deixar as pessoas esperando ao telefone.

Ao ouvir a música à qual está habituado, o funcionário conclui que quem está do outro lado da linha realmente trabalha na instituição que ele afirma, baixando a guarda e fornecendo todas as informações solicitadas.

### 14.2.5 TÉCNICAS DE ENGENHARIA SOCIAL – USO DE "SPOOFING"

Uma nova técnica é a utilização do telefone falso pela Engenharia Social criminosa, para burlar o sistema de identificador de chamada.

É o denominado "spoofing" do número telefônico, que faz com que o identificador de chamadas mostre um número diferente daquele que realmente originou a ligação.

# REFERÊNCIAS


ALVES, Cássio Bastos. **Segurança da informação vs. Engenharia Social**: Como se proteger para não ser mais uma vítima. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm.

BRASIL. Resolução nº 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. **Diário Eletrônico do CNMP**, Caderno Processual, Brasília, p. 1-11, 13 dez. 2016.

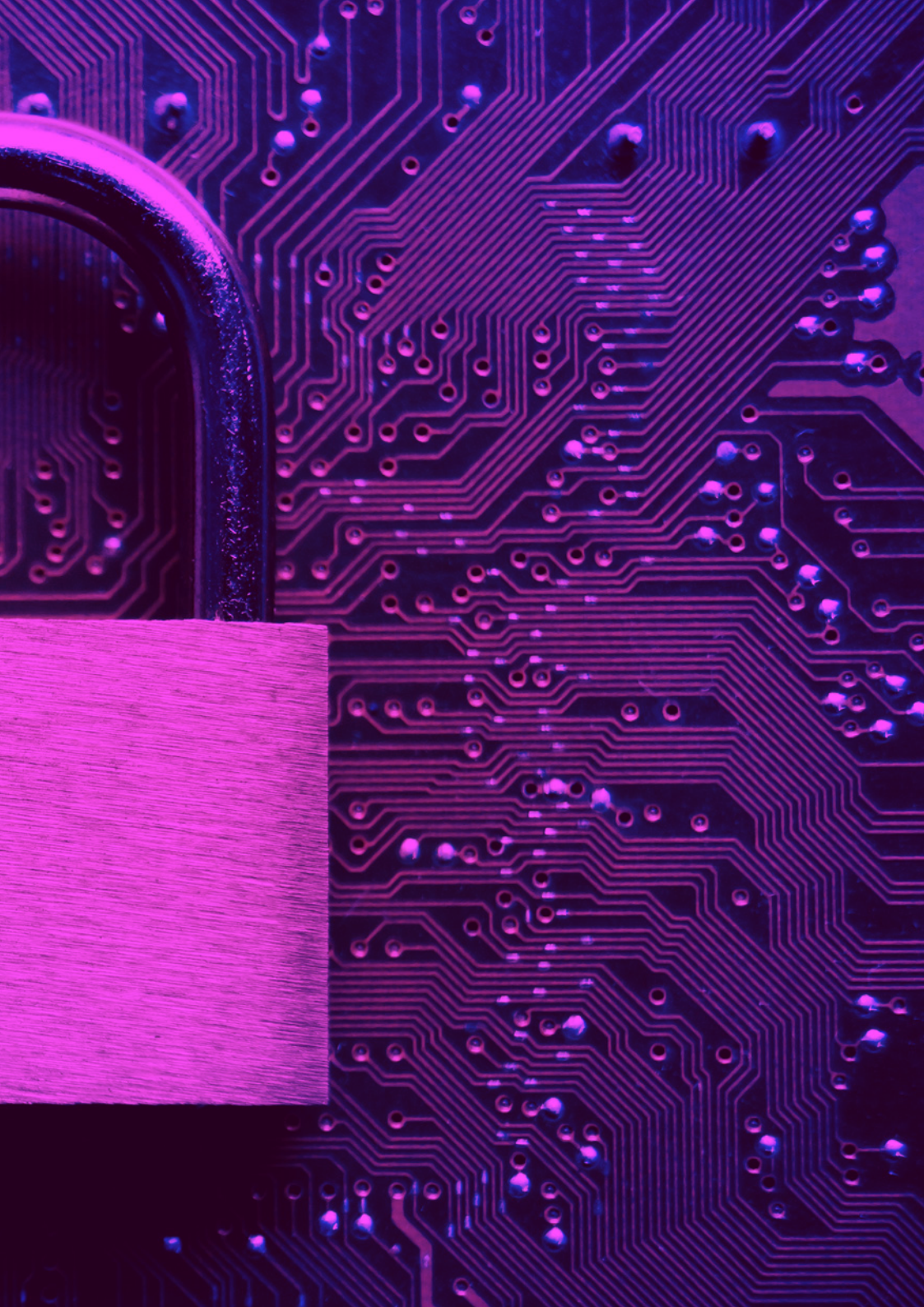
BRASIL. Ministério da Fazenda. Secretaria Executiva. Subsecretaria de Planejamento, Orçamento e Administração. Coordenação-Geral de Recursos Logísticos. **Procedimentos para classificação de informação em grau de sigilo**: cartilha. 2. ed. rev. Brasília: Coordenação-Geral de Recursos Logísticos/SPOA, 2018. 67 p.

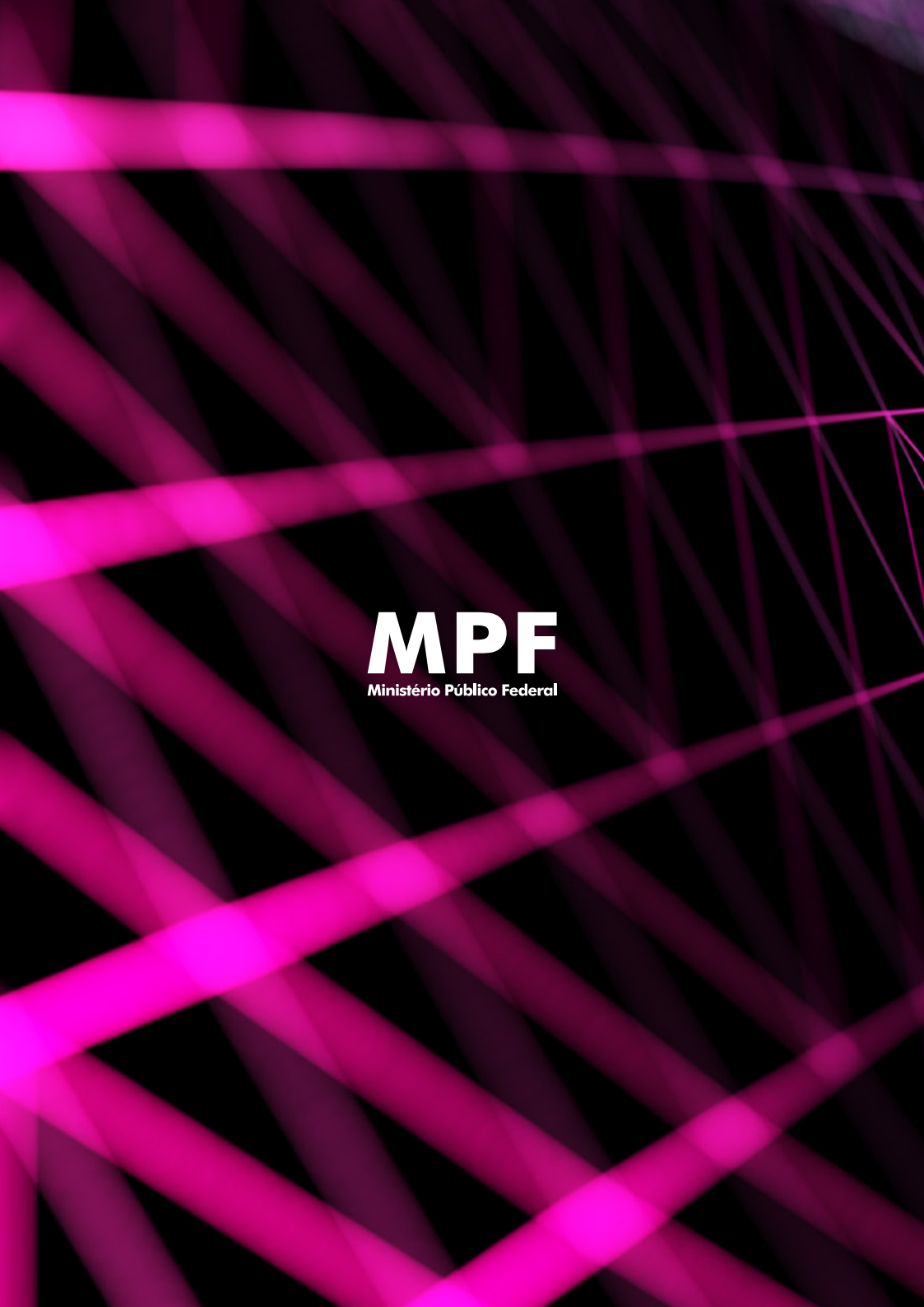
GEPROC. **Segurança pessoal em áreas de alto risco**: regras para não se tornar uma vítima da violência urbana.

MPF. Portaria/MPF nº 417, de 5 de julho de 2013. Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal. 2013. **Diário Eletrônico do MPF**, n. 87, p. 8-9, jul. 2013.

PRESIDÊNCIA DA REPÚBLICA. Secretaria de Comunicação Social. **Manual de Orientação para Atuação em Mídias Sociais**: Identidade Padrão de Comunicação Digital do Poder Executivo Federal. Brasília: Secom, 2014.

RAFAEL, Gustavo de Castro. **Engenharia Social**: as técnicas de ataques mais utilizadas. 24 out. 2013. Disponível em: https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/.




MPF
Ministério Público Federal