

# VIAGENS AO EXTERIOR



**10 DICAS DE**  
**SEGURANÇA**  
PARA  
**LEVAR NA MALA**



# Viagens ao Exterior

**10 DICAS DE SEGURANÇA  
PARA LEVAR NA MALA**

2019

# **AGÊNCIA BRASILEIRA DE INTELIGÊNCIA**

Produção

**Departamento de Contrainteligência**

**Programa Nacional de Proteção do Conhecimento Sensível (PNPC)**

Projeto Gráfico

**Assessoria de Relações Institucionais e Comunicação Social**

Impressão

**Divisão de Serviços Gráficos**

# APRESENTAÇÃO

Países, empresas e grupos de interesse estão em competição permanente na busca de um melhor posicionamento estratégico no cenário internacional.

A *Espionagem* é uma ameaça real, que emprega diversas técnicas para enganar, manipular ou explorar a confiança das pessoas, a fim de obter informações privilegiadas.

Também é real a intenção de influenciar os rumos políticos do País para favorecer interesses estrangeiros em detrimento dos nacionais. Chamamos essa ameaça de *Interferência externa*.

No Brasil, ainda existe uma baixa percepção dessas ameaças, que são difíceis de detectar e, por isso, frequentemente ignoradas. Em solo estrangeiro, autoridades e servidores públicos em missão oficial precisam ter consciência das próprias vulnerabilidades, redobrar a atenção e observar algumas medidas de segurança.

"Por que eles estariam interessados em mim?"

Porque, como servidor público e representante do Governo brasileiro, você tem acesso a informações sigilosas

ou privilegiadas, o que o torna uma atraente fonte de informações estratégicas sobre nossa política externa, comércio, agricultura, energia, etc.

Este guia de orientações para viagens ao exterior é uma iniciativa do Programa Nacional de Proteção do Conhecimento Sensível (PNPC), da Agência Brasileira de Inteligência (ABIN). A reprodução é autorizada, desde que citada a fonte.



**Aperte os cadeados e boa viagem!**

# ROTEIRO

---



**Antes de Partir**

*pág.*

**7**

**Durante a Viagem**

*pág.*

**13**

**Depois da Missão**

*pág.*

**21**

**Diário de Bordo**

*pág.*

**26**







# Antes de Partir

# 1

## ANTECIPE O DISCURSO

---



**O que dizer?** Antes da viagem, reflita sobre informações pessoais e profissionais que podem ou não ser compartilhadas com entidades estrangeiras. Antecipe perguntas e planeje respostas - essa medida ajuda a não ser pego de surpresa quando questionado sobre sua rotina ou temas de trabalho.

**Sem contradições.** Se a missão for em equipe, combine o discurso com os colegas. Na alfândega, o grupo deve informar o mesmo motivo para entrada no país. Prepare-se ainda para a possibilidade de ser chamado para uma segunda inspeção no aeroporto, com novas perguntas.

**Por onde andei.** Os carimbos de viagens anteriores do seu passaporte revelam dados sobre outros projetos de cooperação do Brasil, no caso dos passaportes oficiais, e sobre os interesses pessoais do servidor, quando o documento apresentado é o pessoal. Essas informações, assim como os dados do questionário que você preencheu para o visto, podem ser usadas por serviços de Inteligência estrangeiros. Antecipe perguntas relacionadas a viagens anteriores.

**Quem sou?** Tenha consciência de suas características, como *background* étnico, geográfico ou religioso. Reflita sobre eventual sociabilidade excessiva, vaidade, ambição, indiscrição, abuso de bebidas alcoólicas e uso de drogas. Essas características podem ser exploradas em uma eventual abordagem.



*Frase do dia:* **Dados cotidianos para você podem ser valiosos para os outros.**

# 2

## DEIXE FORA DA MALA

---



**Preciso disso?** Esvazie bolsas e carteiras, leve apenas o necessário. A medida evita informar, sem querer, dados sobre você em certas ocasiões, como em inspeções no aeroporto. Lembre-se de que sua mala pode ser aberta e checada por autoridades estrangeiras sem o seu conhecimento. Uma oportunidade perfeita para conseguir cópias de seus documentos.

**Sem papel.** Não leve documentos impressos e outros materiais de trabalho que, se apreendidos por autoridades de segurança locais, possam gerar riscos aos servidores ou à instituição.

**Meu celular, minha vida.** No caso de aparelhos eletrônicos, como celular, *laptop*, *tablet* e *smartwatch*, é preciso avaliar a real necessidade de levá-los. Fique atento às informações que estão armazenadas: dados sensíveis da instituição em que trabalha, fotos, contatos, notas, etc. Faça uma "limpa" antes de partir e também um *backup* para reduzir prejuízos em caso de perda, roubo ou confisco durante a viagem.

**O que passou, passou.** Apague os históricos de navegação, *cookies*, dados e conteúdos armazenados em sites, assim como senhas memorizadas. Esse recurso está disponível nas configurações do navegador. Avalie também apagar o histórico de conversas em aplicativos de mensagem, como *WhatsApp*.

**Mala diplomática.** Para os órgãos da Administração Pública Federal que possuem adidâncias em países de destino dos servidores, recomenda-se optar pelo transporte de documentos classificados por mala diplomática.

**Etiqueta.** Evite identificações funcionais na bagagem e prefira etiquetas fechadas para proteger seus dados de olhares curiosos.



*Frase do dia:* **Menos é mais.**



# 3

## PESQUISE SOBRE O DESTINO



**O que me espera?** Pesquise sobre possíveis ameaças do país de destino que possam comprometer sua segurança. Informe-se sobre leis e regulamentos, especialmente em relação ao controle na fronteira e uso de criptografia. Busque ainda conhecimentos sobre cultura e costumes. Essas informações podem ser úteis tanto em abordagens de autoridades locais quanto em conversas cotidianas com taxistas, recepcionistas e outros contatos eventuais.

**Quem são eles?** Procure saber mais sobre seus interlocutores estrangeiros, além de informações sobre o local de encontro ou reunião oficial, se for o caso.

**S.O.S.** Tenha em mãos contatos do consulado ou da embaixada do Brasil, em caso de emergência.



*Frase do dia:* Informação é poder.



# Durante a Viagem

## 4 NÃO CRIE EXPECTATIVA DE PRIVACIDADE

---



**Não estou em casa.** Lembre-se de que você fica mais vulnerável em solo estrangeiro e tem controle limitado sobre os ambientes frequentados, podendo ser monitorado ou ter conversas gravadas. Não crie expectativa de privacidade em ambientes públicos nem mesmo em privados, como quartos de hotel.

**No avião.** Leve todos os aparelhos eletrônicos na mala de mão e observe atitudes suspeitas de passageiros e da tripulação. Por que você ganharia um *upgrade* para primeira classe? O novo assento pode ter equipamento de gravação.

**Em inspeções.** Cuidado com abordagens que possam proporcionar contato com seus pertences, como por exemplo o manuseio de casaco, paletó, bolsa etc. Nessas ocasiões, podem ser inseridos dispositivos para geolocalização e captação de áudio.

**No hotel.** Só passe informações estritamente necessárias para a recepção do hotel e acompanhe sua bagagem até o quarto. Ao atender o telefone, não informe seu nome. Alguém pode querer apenas confirmar que você está hos-



pedado naquele quarto com a intenção de invadi-lo depois. Este tipo de ação faz parte do modo de agir de alguns serviços de inteligência estrangeiros. Sua bagagem (e até o lixo) podem ser revirados na sua ausência.

**No cofre.** Caso seja imprescindível deixar dispositivos eletrônicos e documentos no cofre do hotel, deixe as cortinas fechadas, coloque o aviso *Do Not Disturb* na porta e leve a chave com você.

**Redes sociais.** Evite publicar fotos da viagem em redes sociais até voltar ao Brasil. Elas podem revelar suas rotinas e sua localização.



*Frase do dia:* **Nenhum lugar é 100% seguro.**

# 5

## PROTEJA SEUS ELETRÔNICOS



**Roubo de dados.** Dispositivos eletrônicos estão sujeitos não somente a inspeções por agentes de fronteira, mas também a extravio, furto ou ações de espionagem.

**Na alfândega.** Em alguns países, os postos de controle migratório podem revistar dispositivos eletrônicos dos viajantes sem mandados judiciais. A medida pode resultar em confisco dos aparelhos e em cópias de dados para análise futura. Essas inspeções geralmente implicam a checagem de arquivos, mensagens, e-mails, mídias sociais e fotos. Além disso, pode ser exigida a disponibilização de senhas de desbloqueio dos dispositivos, assim como senhas e chaves para decifrar dados criptografados.

**Com você.** Carregue seus dispositivos eletrônicos sempre com você (desconfie até do cofre do hotel), a não ser que saiba que serão retidos em reunião com estrangeiros, quando são guardados em armários, por exemplo. Nesses casos, é possível a instalação de *spywares* (vírus espião), que podem roubar informações e mesmo monitorar câmeras e microfones.

**Em todo lugar.** Desligue o *bluetooth* e não utilize *wi-fi* de

hotéis, aeroportos, restaurantes e locais turísticos. Prefira usar os próprios aparelhos, em vez de computadores oferecidos por hotéis e cybercafés, por exemplo. Evite carregadores públicos (algo comum em aeroportos), especialmente aqueles conectados em portas USB.

**Indecifrável.** Use senhas fortes para bloqueio dos aparelhos eletrônicos, de preferência, diferentes daquelas utilizadas em outras contas e dispositivos pessoais. Outra sugestão é não utilizar a opção de salvar senhas em sites ou navegadores.

**Medidas extras.** Use filtro de proteção de tela para evitar que alguém leia ou fotografe enquanto você usa o computador. Também é interessante usar pastas coloridas ou outros sinais distintivos para evitar trocas de equipamentos, especialmente no transporte.

**Criptografados.** Use dispositivos de criptografia para transportar informações sensíveis ou sigilosas. Não use *WhatsApp* ou e-mail particular para esse fim. Limpe os arquivos que já foram transferidos para o órgão onde trabalha por meio de criptografia ou outros serviços de mensagem seguros.



*Frase do dia:* **Pare, pense, conecte.**

# 6

## NÃO CONTE "SEGREDOS" EM PORTUGUÊS



**What?** Em viagem ao exterior, você já fez algum comentário em língua portuguesa sem se preocupar por achar que ninguém estava entendendo?

**Ooops.** O Português não é uma linguagem cifrada. É possível que serviços de Inteligência estrangeiros gravem conversas ou infiltrem pessoas fluentes na língua portuguesa em ambientes onde representantes brasileiros se encontram. O intuito é coletar dados diante da menor preocupação dos brasileiros. Evite usar o português como proteção a dados sensíveis em *Uber*, táxi, restaurantes...

**Alô?** Também evite conversar sobre assuntos sensíveis ao telefone, pois autoridades locais podem monitorar as conversas e os números discados.



*Frase do dia:* **Eles também falam português.**



# 7

## FUJA DE PROVOCAÇÕES

---



**Ação e reação.** Alguns governos estrangeiros usam técnicas de provocação entre membros da delegação brasileira para avaliar a coesão, observar a ascendência de uns sobre outros ou analisar a reação a alguns temas, como a atual conjuntura política brasileira.

**Aliados.** É comum instigarem discussões sobre outros países, especialmente os parceiros do Brasil. Também há interesse em informações sobre grupos dos quais o País participa, como G20, Mercosul e BRICS. Críticas buscam fomentar a opinião do servidor: positiva ou negativa em relação a outras nações. É preciso ter cautela, pois a resposta pode ser considerada uma posição oficial do Governo brasileiro sobre o assunto.

**Discrição.** Evite entrar em situações comprometedoras: seja cético, discreto e vigilante em ambiente de trabalho ou de lazer. Cuidado com abordagens de estrangeiros sobre suas necessidades e interesses pessoais. Seja evasivo quanto ao seu salário e sua satisfação com o trabalho. Resista a bajulações, facilidades e benefícios.

**Não sei...** Desinforme seu acesso a informações e use dados ostensivos, que estão em leis e decretos, para responder a perguntas delicadas. Ou, simplesmente, diga que não sabe. O mesmo vale em relação a colegas de trabalho: não passe informações pessoais ou profissionais sobre eles.

**Dupla.** Evite andar sozinho em passeios e compromissos de trabalho. Cuidado com investidas de estrangeiros para encontros fora do período e local de reunião ou curso. Desconfie de encontros casuais e frequentes.



*Frase do dia:* **Não existe almoço grátis.**



# Depois da Missão

# 8

## DESCARTE CERTOS PRESENTES



**Presente de grego.** É cada vez mais comum a entrega de *pen drives* como brindes em eventos (conferências, palestras, cursos, etc.). Mais comum ainda é o que vem dentro desses "presentes": vírus. Esses *malwares* são usados para que o governo ou entidade estrangeira consiga acesso a informações de seu computador pessoal ou funcional. Em hipótese alguma utilize *pen drives*, HD externos e outros dispositivos presenteados.



*Frase do dia:* Presente de grego, literalmente, é Cavalo de Troia.



# 9

## FAÇA O CHECK-UP DOS APARELHOS



**Pós-evento.** Não abra anexos de e-mail ou *links* enviados depois de eventos patrocinados por estrangeiros, como apresentações de *Power Point*. Muitas vezes eles vêm com vírus para roubar as informações dos seus aparelhos eletrônicos. Se o conteúdo for importante para o seu trabalho, peça para o setor de tecnologia de informações avaliar o material antes de acessá-lo.

**Spear Phishing.** Outra técnica utilizada é o *spear phishing*, em que informações pessoais ou específicas são usadas para criar falsa legitimidade e gerar confiança do usuário para, por exemplo, abrir um *link* de e-mail com vírus.

**Check-up.** Verifique se houve contaminação de *malware* nos seus aparelhos eletrônicos. Também é recomendável trocar senhas utilizadas durante a viagem.



*Frase do dia:* **Antes seguro que curioso.**

# 10

## REPORTE INCIDENTES

---



**Rede de contatos.** Serviços de Inteligência estrangeiros tentam formar redes de fontes humanas em outros países e, para isso, oferecem cursos, equipamentos, informações, apoio e verbas para órgãos públicos. Essas ações buscam gerar uma sensação de dívida de gratidão nos servidores. Atente para contatos de pessoas que você conheceu durante a viagem e para eventual insistência em manter um relacionamento amigável a distância.

**Avalie a viagem.** Troque experiências com colegas de trabalho sobre as situações vivenciadas e reflita sobre prós e contras. Faça um relatório ou memória da viagem.

**Ficou para trás.** Verifique se algum material de trabalho se perdeu ou foi roubado.

**Será?** Caso você tenha percebido algum comportamento "estranho" de estrangeiros ou tenha desconfiado de algumas situações, informe seu chefe e o setor de segurança do seu órgão.

**Reporte.** Você também pode enviar um e-mail para ABIN: [reporte@abin.gov.br](mailto:reporte@abin.gov.br). Às vezes parece ser uma questão boba ou passageira, mas na verdade você pode ter sido espionado durante a missão!



*Frase do dia:* Qualquer semelhança não é mera coincidência.





## DIÁRIO DE BORDO

Contatos do consulado/embaixada brasileira: \_\_\_\_\_

Contatos de emergência no Brasil: \_\_\_\_\_

Registros de incidentes: \_\_\_\_\_



