

VISITA DE DELEGAÇÃO ESTRANGEIRA

GUIA PARA PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS



PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

Visita de Delegação Estrangeira

Guia para Proteção de
Conhecimentos Sensíveis

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção

Departamento de Contraineligência

Programa Nacional de Proteção do Conhecimento Sensível
(PNPC)

Projeto Gráfico

Coordenação-Geral de Relações Institucionais e Comunicação
Divisão de Serviços Gráficos

Impressão

Divisão de Serviços Gráficos

APRESENTAÇÃO

Em busca de acordos e parcerias, é comum instituições nacionais receberem visitas de delegações estrangeiras. Porém, por mais vantajosa que seja a cooperação, é preciso ficar atento a medidas de segurança para proteção de conhecimentos estratégicos, que contribuem para melhor competitividade do Brasil no cenário internacional.

Além de riquezas naturais e biodiversidade, o país destaca-se na produção de pesquisa e inovação tecnológica em áreas como agricultura, energia e defesa. Esses conhecimentos chamam a atenção de agentes estrangeiros, que também possuem interesse em informações que envolvem o processo decisório nacional e nossa política externa.

Interações colaborativas, em contexto de troca de informações, geram oportunidades para coleta de dados sobre projetos nacionais. Agentes públicos podem fornecer informações sensíveis de boa-fé, imbuídos de espírito de cooperação, sem conhecer o destino e o usuário final das informações.

Agentes de serviços de Inteligência estrangeiros de variados países usam cobertura diplomática para dificultar sua identificação, obter acessos e facilitar sua circulação em ambientes sociais de interesse. Eles também podem estar infiltrados em empresas, institutos culturais, organizações sem fins lucrativos, veículos de imprensa estrangeiros etc.

Os agentes encobertos buscam construir rede de informantes e colaboradores com acesso privilegiado a órgãos da Administração Pública, para obter informações sobre decisões de grande relevância, com impactos econômicos, por exemplo.

Essas técnicas potencializam ações de espionagem, sabotagem e interferência externa. Neste último caso, são utilizadas técnicas de influência visando a persuadir autoridades a direcionar seus posicionamentos, em sintonia com interesses de parceiros ou patrocinadores estrangeiros.

O estabelecimento de políticas de segurança organizacional e de protocolos institucionais para o relacionamento com agentes externos é o caminho adequado para mitigar o risco de ação dessas fontes de ameaças.

Quando você for o anfitrião, lembre-se de estabelecer limites entre a cordialidade e a preservação da informação sensível. Isso vale tanto para visitas institucionais quanto para cursos, fóruns, palestras, reuniões e outros eventos.

Algumas medidas também podem ser adotadas para visitantes nacionais, potenciais investidores ou parceiros prospectivos. Eles podem ter a intenção de obter alguma vantagem competitiva ou mesmo estar a serviço de governos estrangeiros, e o resultado de suas ações pode comprometer a sua instituição.

Este guia 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.

A group of business professionals are gathered around a large, reflective conference table in a modern office. One man stands and speaks to the group, while others are seated, some looking at documents. The background features a large window with a view of a city skyline at dusk. The word "PREPARAÇÃO" is overlaid in large, bold, white letters at the bottom right.

PREPARAÇÃO

1) PREPARAÇÃO

Agenda. Visitas de estrangeiros à sua instituição devem ocorrer sempre com dia e horário agendados.

Curriculum. Solicite dados dos visitantes e envio prévio de informações profissionais. Elabore hipóteses sobre possíveis motivações para a visita. Uma delas pode ser a identificação de projetos estratégicos em desenvolvimento no Brasil ou, mais especificamente, na sua empresa/instituição.

Discurso. Em cursos, palestras e reuniões oferecidas pela sua instituição, tenha claro quais assuntos podem ser compartilhados com entidades estrangeiras e quais informações devem ser omitidas. Avalie a necessidade de tratar detalhes técnicos. Discuta e combine com colegas o mesmo discurso.

Pauta. Defina com os visitantes, por escrito, a pauta do evento. Questionar as áreas de interesse da delegação, especifique os assuntos a serem abordados e analise a possibilidade de discussão de temas sensíveis. Neste caso, verifique a necessidade de se firmar termo de compromisso de manutenção do sigilo.

Perguntas e respostas. Antecipe perguntas e planeje respostas para não ser surpreendido quando questionado sobre rotinas e temas de trabalho sigilosos ou estratégicos. Limite-se ao motivo do encontro.

Gestão. Reúna os servidores envolvidos para orientá-los quanto aos procedimentos de conduta e de reação durante a visita, além dos papéis de cada um. Faça alertas sobre possíveis abordagens maliciosas (gravações não autorizadas, furto de materiais, **engenharia social**, **entrevista**). Reveja normas de segurança - se não houver, é preciso elaborá-las para contemplar medidas adequadas para esse tipo de situação.



Engenharia social: Método utilizado para enganar, manipular ou explorar a confiança das pessoas, a fim de obter informações privilegiadas. Há manipulação de fatores humanos como a ilusão, a influência, a adulação ou a pressão.

Entrevista: técnica de obtenção de informações por meio de conversa, na qual se camuflam os reais objetivos do entrevistador. Para a Atividade de Inteligência, a entrevista é uma conversa mantida com propósito definido, planejada e controlada pelo entrevistador. Pode ser realizada para obter, confirmar ou fornecer dados ou ainda modificar o comportamento de outra pessoa.

Acompanhantes. Selecione funcionários para acompanhamento dos visitantes durante todo o período de permanência da delegação. O número de servidores deve ser proporcional ao tamanho da comitiva e ao nível de especialização suposta ou conhecida dos visitantes. É importante que os acompanhantes recebam briefing de preparação e saibam quais informações podem ou não ser compartilhadas.

Chaves. Indique previamente funcionários para trancar as portas de salas de trabalho, quando não ocupadas.

Veículo. Defina o local para estacionamento dos veículos e a portaria onde será permitida a entrada, caso haja mais de uma. Prepare-se também para a possibilidade de os visitantes chegarem de táxi ou outros serviços de transporte por aplicativos.

Crachá. Providencie crachá que destaque a condição de acesso, com a identificação de “visitante”, por exemplo.

Segurança. Avise os setores de segurança e recepção sobre a visita, envie a lista de convidados e reforce a necessidade de medidas de controle, como a verificação de documento de identidade com foto, a necessidade

de fotografia para cadastro e a proibição de entrada de quem não está na lista. Alerta também sobre horários de chegada e de saída e deixe contato de telefone na portaria em caso de imprevistos.

De última hora. Os visitantes atrasados devem ser acompanhados por um membro da instituição até que se integrem ao grupo. O mesmo vale para os que chegarem antes do horário marcado. Atente também para participantes incluídos de última hora na lista e para a presença de pessoas alheias ao evento.

De olho. Peça verificação do funcionamento do Circuito Fechado de Televisão (CFTV) e alerte os seguranças para redobrar a atenção no dia da visita, se o grupo for considerado de maior risco para realizar ações de espionagem. O ideal é que as imagens registradas durante o evento sejam guardadas por no mínimo 90 dias.

Logística. Pergunte à delegação sobre necessidades que terá no dia da visita, como uso de computador da instituição visitada. Se não houver computador reservado para esse fim, o que seria o ideal, limpe pastas armazenadas com documentos da instituição e desconecte o computador da rede corporativa, como a intranet. É preciso ter certeza de que, se houver instalação de malware

por meio de pen drive, por exemplo, não haverá furto de informações ou problemas na rede.

Regras. Informe aos participantes as regras que nortearão a visita. Em reuniões sensíveis, por exemplo, é recomendável proibir celular, tablet e outros equipamentos que possibilitem gravação de áudio ou vídeo. Providencie armário ou escaninho para guardar os eletrônicos.

Ambiente. Escolha sala ou auditório em local isolado, para reduzir o contato com outros funcionários e o acesso a instalações. Prefira por exemplo, local mais próximo à entrada de um corredor, para evitar que os visitantes caminhem por várias salas de trabalho antes de chegar ao destino. Evite ambientes habitualmente destinados ao trato de assuntos estratégicos ou sigilosos, para diminuir a possibilidade de subtração de materiais sensíveis ou mesmo inserção de aparelhos de escuta.

Sigilo. Se houver discussão de assuntos sensíveis durante a visita, escolha salas sem janelas ou feche as persianas. Antes do encontro, retire aparelhos eletrônicos do local. Se for necessário, deixe à disposição um telefone fixo de linha.

Mesa limpa. Remova todos os documentos sensíveis sobre mesas, post-its em quadros e papéis em impres-

soras. Guarde-os em armários ou gavetas com chave. Esvazie lixeiras e bloqueie telas de computador.

Sem fio. Evite usar microfone sem fio em reuniões com assuntos sensíveis, porque aumenta o risco de interceptação de sinais. Também prefira teclados com fio, ao invés de bluetooth.

Roteiro. Em caso de visita guiada, selecione previamente os locais a serem visitados. Levante vulnerabilidades dos pontos a serem percorridos e reforce medidas de proteção em áreas sensíveis. Redobre cuidados em visitas a estruturas críticas, como laboratórios, campos de pesquisa etc. Deixe claro aos visitantes os locais a que terão ou não direito de acesso.



Estudo de caso: Estrangeiro é escalado de última hora para participar de visita. No fim evento, solicita a representante do governo brasileiro ajuda para encontrar uma pessoa de sua família que mora no País, mas com a qual perdeu contato. A técnica é usada para saber se o servidor está disposto a ajudá-lo para depois tentar acesso a informações.



DIA DA VISITA

2) DIA DA VISITA

Identificação. Forneça crachás aos membros da delegação e registre horários de entrada e saída de cada participante.

De perto. Os visitantes devem ser acompanhados durante todo o período, inclusive na saída, com a devolução obrigatória do crachá. A medida evita a circulação de visitantes livremente pela instituição.

Lanche. Os cuidados de segurança devem ser mantidos nos intervalos e em outras situações de descontração (coffee break, almoço, confraternização de despedida etc.), em que é comum “baixar a guarda”. É nesses momentos que o grupo costuma dispersar e visitantes mal-intencionados podem tentar subtrair ou fotografar documentos sensíveis, por exemplo. Nesses horários, todas as salas de trabalho deverão, na ausência de funcionários, ficar trancadas.

What? Caso a língua estabelecida para o encontro seja o inglês ou espanhol, por exemplo, não converse com colegas de trabalho como se ninguém entendesse por-

tuguês.

Oops. É possível que haja estrangeiros fluentes na língua portuguesa, mesmo que não se identifiquem como tal. O intuito é coletar dados diante da menor preocupação dos brasileiros.

Telefone. Ao falar no celular, fique atento ao teor da conversa; não comente assuntos sensíveis na presença de estrangeiros.

Proibido. Relembre regras de segurança logo no começo da visita. Alerta sobre a proibição de fotos e vídeos em certos momentos ou locais. Informe o que os visitantes poderão manter consigo e o que deverá ser guardado previamente em local específico (guarda-volumes, gavetas etc.), como celular, notebook, etc.

Sigilo. Alerta sobre a responsabilidade de manutenção de sigilo, se for o caso, e sobre a necessidade de se manter documentos e até o bloco de notas com anotações sensíveis em local seguro após o encontro.

Discrição. 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.

Pedido. Acenda um sinal de alerta se algum estrangeiro lhe pedir um favor, mesmo que pareça inocente. Pode ser um teste para saber se você está disposto a ajudá-lo. Também fique atento se pedirem para você detalhes do seu trabalho ou se revelarem algo sigiloso.

Não sei... Minimize seu acesso a informações e use dados ostensivos para responder a perguntas delicadas. Ou, simplesmente, diga que não sabe. O mesmo vale em relação a estruturas sensíveis do órgão em que trabalha.

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

Aliados. É comum que sejam provocadas discussões sobre outros países, especialmente parceiros do Brasil. Críticas buscam sondar 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 ou embasar decisões sobre negociações, por exemplo.

Dados pessoais. Prefira estabelecer relações institucionais do que fornecer contatos pessoais.



Estudo de caso: Em feira voltada para indústria química, estrangeiro furta amostra usando método inusitado: molhando “acidentalmente” a própria gravata em material líquido.

A group of four business professionals are gathered around a table, looking at a large document. Two men in the foreground are pointing at the document with pencils. Two women stand behind them, one holding a clipboard. They are all dressed in business casual attire. The scene is brightly lit, suggesting an indoor office or meeting space.

**APÓS O
EVENTO**

3) APÓS O EVENTO

Achados e perdidos. Ao término do evento, verifique se há documentos esquecidos ou desaparecidos.

Presente de grego. Caso sejam ofertados presentes, como pen drives, carregadores, HD externo etc., inutilize-os. Muitas vezes, esses dispositivos estão infectados com vírus para que o governo ou entidade estrangeira acesse informações do seu computador.

Antivírus. Computadores usados por estrangeiros deverão passar pelo setor de tecnologia de informações (TI) da instituição para que seja verificada eventual instalação de vírus. O computador deverá ser formatado antes de ser reconectado à rede.

Pós-evento. Não abra anexos de e-mail ou links enviados por visitantes, como apresentações de Power Point. Se o conteúdo for importante para o seu trabalho, peça para o setor de TI avaliar o material antes de acessá-lo.

Varredura. Se necessário, realize varredura nas salas de encontro para checar se houve instalação de dispositivos para captação de áudio ou vídeo.

Redes sociais. Atente para contatos que você conheceu durante a visita e na eventual insistência em manter um relacionamento pessoal. Pode haver tentativa de recrutamento para que você seja fonte de informações.

Gratidão. Na tentativa de retribuir o encontro, podem ser oferecidos convites para eventos, cursos no exterior e outras oportunidades. É preciso ficar atento aos reais interesses que envolvem essas ofertas e adotar medidas de segurança caso ocorra novo encontro, desta vez promovido por estrangeiros. Entre elas, ir acompanhado de pelo menos mais um membro da instituição, ser discreto e consumir moderadamente bebidas alcóolicas.

Banco de dados. Elabore sistema de informação que permita o armazenamento e a busca de dados sobre a visita (nome do visitante, instituição de origem etc.), para consultas posteriores por tempo determinado para fins de controle de segurança.

Avalie o evento. Troque experiências com colegas de trabalho sobre as situações vivenciadas e reflita sobre prós e contras. Faça um relatório ou memória do encontro e inclua lições aprendidas e possíveis melhorias nos procedimentos de segurança.

Será? Caso você tenha percebido algum comportamento “estranho” de estrangeiros ou tenha desconfiado de algumas situações, informe seu chefe e/ou o setor de segurança do seu órgão. Desconfie e relate se:

- Houver inclusão ou troca de pessoa de última hora com o intuito, por exemplo, de não permitir a checagem do nome.
- Os participantes marcarem reunião sobre um assunto e insistirem em outras pautas durante a visita.
- Vários visitantes fizerem a mesma pergunta de formas variadas para diversos anfitriões ou alguém perguntar a mesma coisa para várias pessoas.
- O visitante se mostrar ofendido quando o anfitrião se recusar a responder uma questão, causando um desconforto que pode favorecer a obtenção de outras informações.
- Houver uso de eletrônicos não autorizados.
- Alguém insistir em tirar fotos ou exagerar no número de imagens.
- Houver pedido de forma reiterada para visitar

área fora do roteiro de visita.

- Ocorrer tentativa de levantar nomes de pessoas com acesso a informações.

Reporte. Você também pode enviar um e-mail para **reporte@abin.gov.br** para estabelecer contato com a ABIN e relatar o caso. Às vezes parece ser uma questão boba ou passageira, mas na verdade alguém pode ter aproveitado o evento para tentar coletar informações sensíveis!



Estudo de caso: Estrangeiro entrega pen drive de presente a representante de instituição brasileira. O dispositivo estava infectado com vírus para invasão da rede interna do órgão.



PROTEGER COM INTELIGÊNCIA

pnpc@abin.gov.br

www.gov.br/abin/pnpc