PROTEÇÃO DE CONHECIMENTO SENSÍVEL PARA **GESTORES**

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção
Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação

Impressão
Divisão de Serviços Gráficos

PROTEÇÃO DE CONHECIMENTO SENSÍVEL PARA **GESTORES**

2021

CONTEÚDO

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

ABIN E OS CONHECIMENTOS SENSÍVEIS

Dentre as atribuições legais da Agência Brasileira de Inteligência (ABIN) está “planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade” (art. 4o, II, Lei n° 9.883/1999).

Para atender a essa atribuição, a agência desenvolve o Programa Nacional de Proteção do Conhecimento Sensível (PNPC). Criado em 1997, o PNPC é uma assessoria de segurança que busca promover cultura de proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas, com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

PNPC
PROTEGER COM INTELIGÊNCIA

1

CONHECIMENTO SENSÍVEL

PNPC
PROTEGER COM INTELIGÊNCIA

CONHECIMENTO SENSÍVEL

É todo conhecimento, sigiloso ou estratégico, cujo acesso não autorizado pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos ao país, necessitando de medidas especiais de proteção.

E O QUE É CONHECIMENTO SIGILOSO?

Conhecimento sigiloso é aquele cuja divulgação ou acesso irrestrito acarreta risco à segurança da sociedade e do Estado e, desse modo, recebe grau de sigilo por órgãos da Administração Pública Federal.

A Lei de Acesso à Informação (Lei nº 12.527/2011) estabelece os parâmetros de classificação dos documentos públicos, restringido o acesso à informação, a partir de sua produção, pelos prazos de 25 anos, no caso de classificação ultrassecreta; 15 anos, para secreta; e 5 anos, para reservada.

Leis de proteção da informação também podem incidir sobre instituições privadas, como as que protegem o sigilo bancário e as informações pessoais. Além disso, empresas e instituições podem criar suas próprias normas e classificações de sigilo.

REFLETINDO...

• Sua instituição possui **informações cobiçadas** por governos, empresas e outras instituições?

• Quanto um ator adverso estaria disposto a investir para ter **acesso antecipado** a decisões da alta administração?

• Quão **protegidos** estão os conhecimentos sensíveis da sua instituição?

• Quais prejuízos o **vazamento** de informações estratégicas traria para sua instituição ou para o país?

Nenhum sistema é 100% seguro

Por isso, é necessário:

• Criar cultura institucional de segurança.

• Sensibilizar e treinar a equipe quanto a medidas de proteção.

• Usar recursos seguros para comunicações e armazenamento de informações sensíveis.

• Levar a segurança em conta em todos os processos da instituição.

VOCÊ É UM ALVO?

As informações sensíveis que um gestor possui podem torná-lo alvo potencial de ações adversas que buscam obter vantagens ou prejudicar o país.

Um método comum é a engenharia social, utilizado para enganar, manipular ou explorar a confiança das pessoas, a fim de obter informações sensíveis ou realizar ação de interesse do agente. Há manipulação de fatores humanos como a ilusão, a influência, a adulação ou a pressão.

PNPC
PROTEGER COM INTELIGÊNCIA

2

PERCEPÇÃO DE AMEAÇAS

As ameaças aos conhecimentos sensíveis (sigilosos ou estratégicos) são constantes.

No Brasil, há um baixo nível de sensibilização sobre os riscos decorrentes dessas ameaças.

Tipos de ameaça

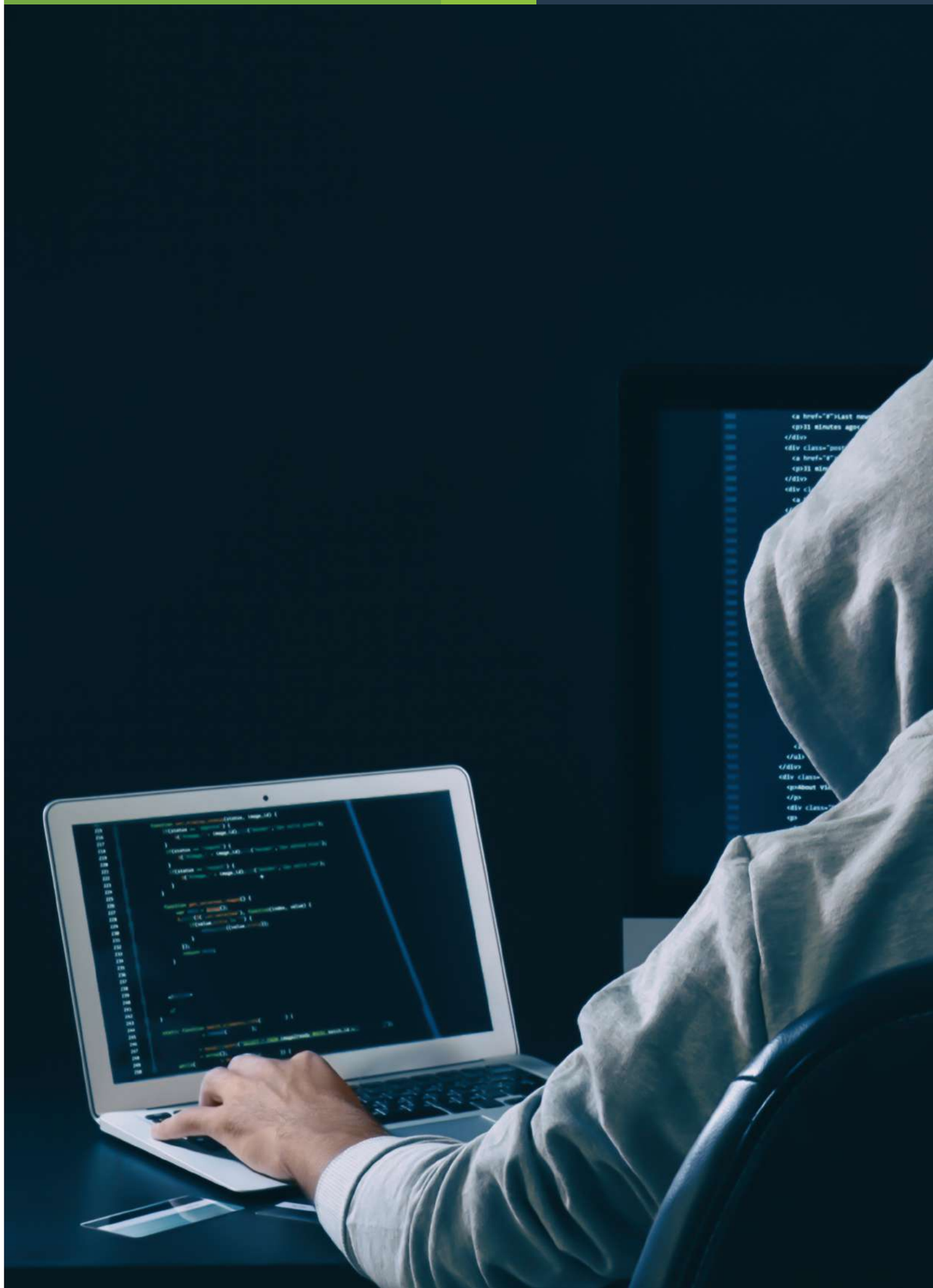
• **Espionagem:** ação que visa à obtenção de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos. As mais comuns são a espionagem de Estado e a espionagem industrial ou comercial.

• **Sabotagem:** tem o objetivo de paralisar atividades ou destruir conhecimentos, equipamentos ou instalações, sobretudo aqueles necessários ao funcionamento das infraestruturas críticas do país.

• **Vazamento:** divulgação não autorizada, acidental ou intencional, de dados ou conhecimentos sensíveis, realizada por agente interno (servidor, empregado, terceirizado etc.), também chamado de *insider*.

• **Interferência externa:** é a atuação deliberada de governos, grupos de interesse, pessoas físicas ou jurídicas que possam influenciar os rumos políticos do país com o objetivo de favorecer interesses estrangeiros em detrimento dos nacionais.

• **Ataques cibernéticos:** são ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visam a interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado.



PNPC
PROTEGER COM INTELIGÊNCIA

3

CULTURA INSTITUCIONAL DE SEGURANÇA

Pessoas são as maiores causadoras de incidentes de segurança da informação, os quais podem acarretar também perdas financeiras.

Uma parte dos profissionais que muda de emprego leva consigo dados institucionais confidenciais, planejando utilizá-los em seu novo trabalho.

Muitos gestores ainda não veem a proteção de dados como prioridade para os negócios.

Outros problemas frequentes são:

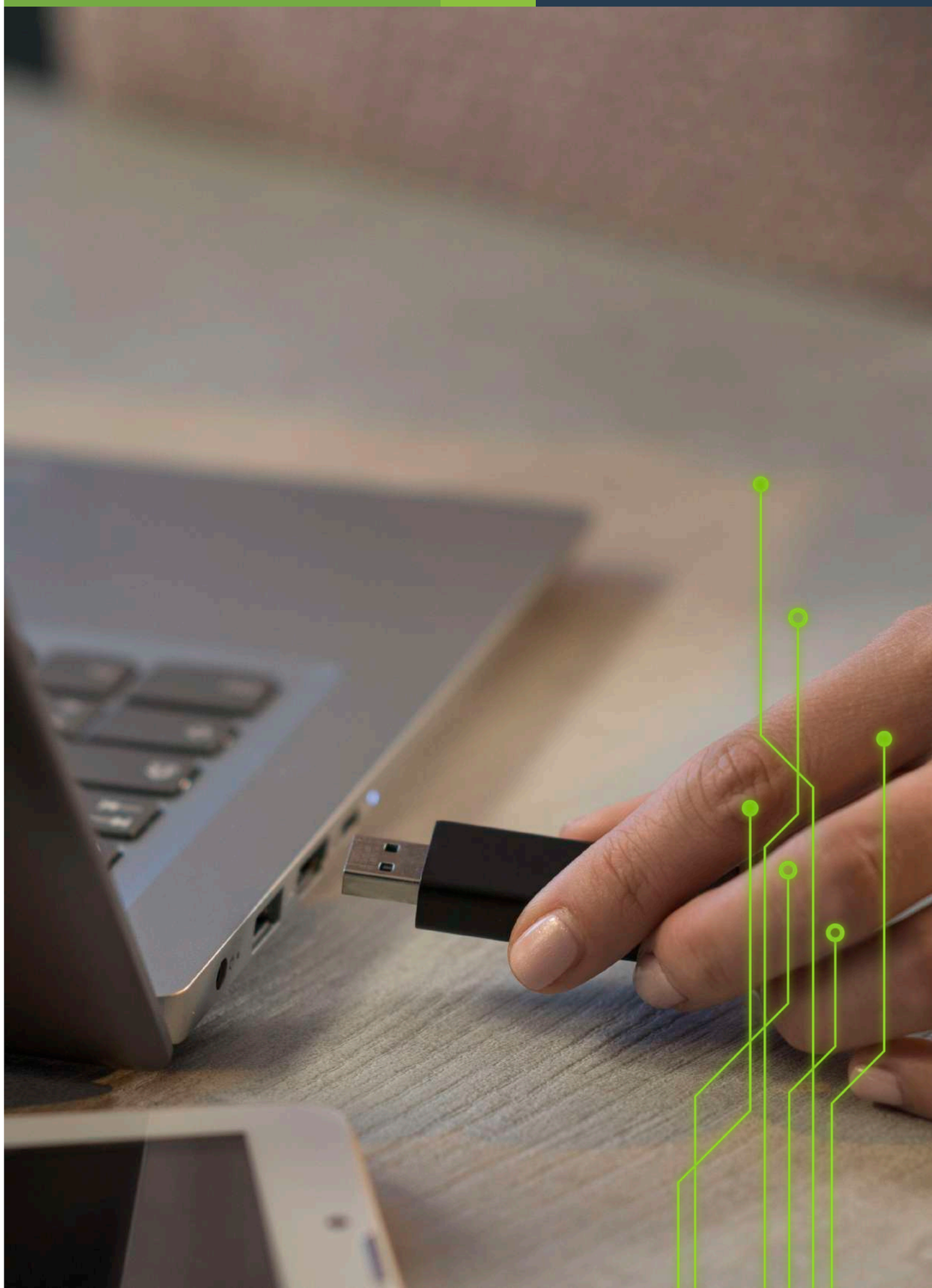
• Movimentação de documentos de trabalho para apps de compartilhamento de arquivos sem permissão.

• Transferência de arquivos de trabalho para tablets ou smartphones pessoais.

• Pen drives pessoais utilizados para fins de trabalho.

• Notebooks perdidos ou furtados, principalmente em aeroportos, carregando informações sensíveis.

• Ausência de sanção quando funcionários usam informações confidenciais em desacordo com políticas da instituição.



12 passos para construção de uma cultura de segurança institucional

Para que sua instituição construa cultura de segurança forte e perene, é necessário seguir alguns passos:

1. Estabeleça equipes de segurança institucional

Forme duas equipes: a executiva e a de segurança institucional. A primeira será responsável pela elaboração e implementação das políticas internas de segurança; a segunda, transversal, será responsável pela execução dos controles de segurança na instituição.

2. Mapeie seus ativos

Defina quais são os conhecimentos sensíveis de sua instituição.

3. Avalie conformidade e normas regulatórias

Analise as leis e normas que sua instituição precisa seguir, tais como a Lei de Acesso à Informação (LAI), Lei Geral de Proteção de Dados (LGPD), normas emanadas pelo Gabinete de Segurança Institucional (GSI) ou normas ISO.

4. Avalie ameaças e vulnerabilidades

Faça uma lista de ameaças à sua instituição e de suas vulnerabilidades. Depois, faça uma lista de prioridades baseada no risco que representam.

5. Gerencie os riscos

Evite, mitigue ou transfira os riscos. Os cenários de risco são fruto da atuação potencial de fontes de ameaças contra os ativos da instituição e são avaliados de acordo com a probabilidade de sua ocorrência e o impacto que podem causar, determinando sua priorização.

Neste item, uma das medidas importantes é a classificação dos documentos sensíveis.

6. Crie plano de gerenciamento de incidentes e recuperação de desastres

Elabore normas de contingência e conduta em situações de incidentes, para garantir atitudes apropriadas no caso de imprevistos.

7. Crie uma política de segurança institucional

A política de segurança institucional é o principal documento para a proteção dos conhecimentos sensíveis na instituição. Para se ter uma política eficaz, alguns itens devem ser considerados:

- Alinhe os processos da instituição à política para garantir a aderência e o cumprimento das normas, em conexão com a cultura e objetivos da instituição.
- Implemente um termo de confidencialidade a ser assinado pelos funcionários, com medidas de acompanhamento e divulgação de penalizações administrativas e legais no caso de incidentes.
- Elabore orientações que abranjam e sejam seguidas por todos os funcionários

e terceirizados.

◆ Faça um texto curto e objetivo em cada assunto abordado, para facilitar e estimular a leitura e tornar mais leve e eficaz o processo de divulgação e treinamento de pessoas.

◆ Depois de elaborada a política, crie normas específicas para controle de acesso, divulgação e tratamento de dados.

8. Gerencie terceiros

Estabeleça processos de gestão dos funcionários terceirizados, vendedores, fornecedores e intermediários que possam ter acesso aos conhecimentos sensíveis da instituição.

Certifique-se de que, nos contratos de terceirização, constem cláusulas de confidencialidade e de responsabilização da empresa contratada em caso de vazamento de informações sensíveis realizado por seus funcionários.

9. Implemente controles de segurança

Crie controles de tecnologia da informação, operacionais e gerenciais, que podem ser de prevenção ou de detecção de violações.

Neste item, é essencial destacar a importância da boa gestão dos funcionários, englobando três etapas: seleção, acompanhamento e desligamento.

a) Seleção

Estabeleça requisitos de segurança para cargos com acesso a informações sensíveis.

b) Acompanhamento

Realize o acompanhamento do funcionário desde seu ingresso até o desligamento, abrangendo sua aderência às regras de segurança, às condutas de ética e participação nos treinamentos da instituição.

c) Desligamento

Realize entrevista de desligamento e interrompa os acessos do funcionário aos sistemas internos da instituição.

10. Realize treinamentos

Treine rotineiramente os colaboradores para evitar confusões, dúvidas e ações errôneas. Ensine medidas básicas de segurança e estabeleça um canal de esclarecimentos para evitar que elas sejam descumpridas por falta de compreensão.

Nos treinamentos, é importante construir cenários de riscos e alertar para hábitos inseguros do cotidiano da instituição.

É necessário, ainda, que cada colaborador compreenda o negócio da organização, conheça seus valores e seu código de ética, saiba o que é importante para a instituição. Se não entender e não absorver isso, dificilmente protegerá as informações adequadamente.

Por fim, promova campanhas periódicas de conscientização na instituição.

11. Crie um ponto focal para acompanhamento e reporte

Estabeleça um ponto focal na instituição para assegurar que a política de segurança institucional seja efetiva e de amplo conhecimento dos colaboradores. Esse setor poderá, também, receber relato de suspeitas de espionagem, sabotagem ou vazamentos.

12. Faça auditorias

Realize auditorias periódicas (internas e/ou externas), para averiguar o cumprimento das condutas de segurança na instituição.

Necessidade de conhecer, restrição de privilégios e compartimentação

Os conhecimentos sensíveis necessitam de um grau maior de proteção. Para tanto, alguns conceitos importantes devem ser aplicados em sua instituição, visando a aumentar o nível de segurança da informação e das comunicações:

• **Necessidade de conhecer:** só permita o acesso a assuntos sensíveis a pessoas com necessidade de conhecê-los para realizar uma tarefa.

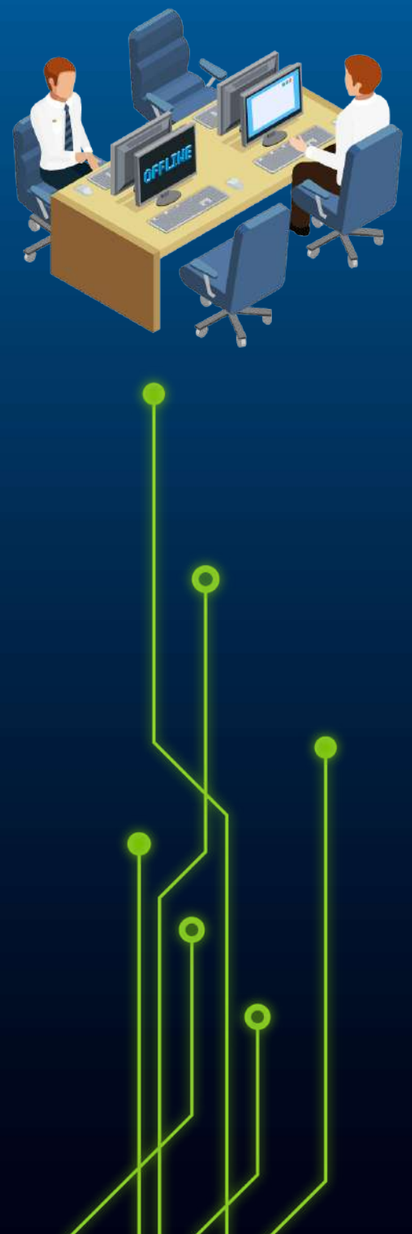
• **Restrição de privilégios:** só conceda o acesso mínimo imprescindível para executar uma operação e apenas pelo tempo necessário.

• **Compartimentação:** garanta que não haja fluxo de informações entre grupos com diferentes necessidades de conhecer.

PNPC
PROTEGER COM INTELIGÊNCIA

4

CONDUTAS DE PROTEÇÃO NO TRABALHO



Você, como gestor, ocupa uma função de liderança na instituição e é exemplo de conduta para sua equipe e seus pares. Sendo assim, é importante implementar medidas de proteção no trabalho, tais como:

• Escolha meios de comunicação e armazenamento adequados para informações sensíveis.

• Descarte pen drives recebidos como presente – eles podem estar infectados com vírus.

• Ao deixar sua estação de trabalho, mesmo que por curto período de tempo, bloqueie a tela de seu computador.

• Ao término do expediente, verifique se arquivos e gavetas com documentos com conteúdo sensível estão trancados.

• Lembre-se de que não é aconselhável levar para casa documentos sigilosos ou realizar tarefas que envolvam assuntos sensíveis fora do ambiente de trabalho.

• Cuidado com as ciladas cibernéticas — especialmente em e-mails, sites e arquivos maliciosos que provocam a propagação de malwares.

• Fique atento para o comportamento de pessoas em visita a sua instituição, especialmente as incluídas na última hora. Evite responder a perguntas que não estejam relacionadas ao objetivo da visita.

• Em reuniões com delegações estrangeiras, reúna os funcionários 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 etc.).

• Em viagens ao exterior, você fica mais vulnerável a sofrer ações de espionagem; portanto, redobre sua atenção com as condutas de segurança.

Desafio do gestor

RESGUARDAR OS CONHECIMENTOS SENSÍVEIS

x

PERMITIR O FLUXO DE INFORMAÇÕES

A solução é PROTEGER PARA COMPARTILHAR ADEQUADAMENTE!

PNPC – Assessoria de Segurança

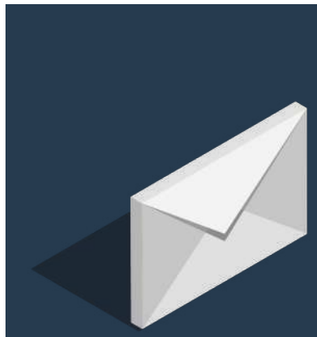
A Assessoria de Segurança realizada pelo PNPC inclui:

• Sensibilização

• Avaliação de Riscos

• Recomendações de melhoria

Se sua instituição é detentora de conhecimentos sensíveis e necessita aumentar o nível de proteção, entre em contato pelo e-mail pnpc@abin.gov.br.



Reporte

Caso acredite que sua instituição foi vítima de ação de espionagem ou sabotagem, avise o setor de segurança da sua instituição. Você também pode enviar e-mail a **reporte@abin.gov.br** para estabelecer contato com a ABIN e relatar o caso.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR
WWW.GOV.BR/ABIN/PNPC