SEGURANÇA NA INTERNET

GUIA PARA PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS

PNPC | PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

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

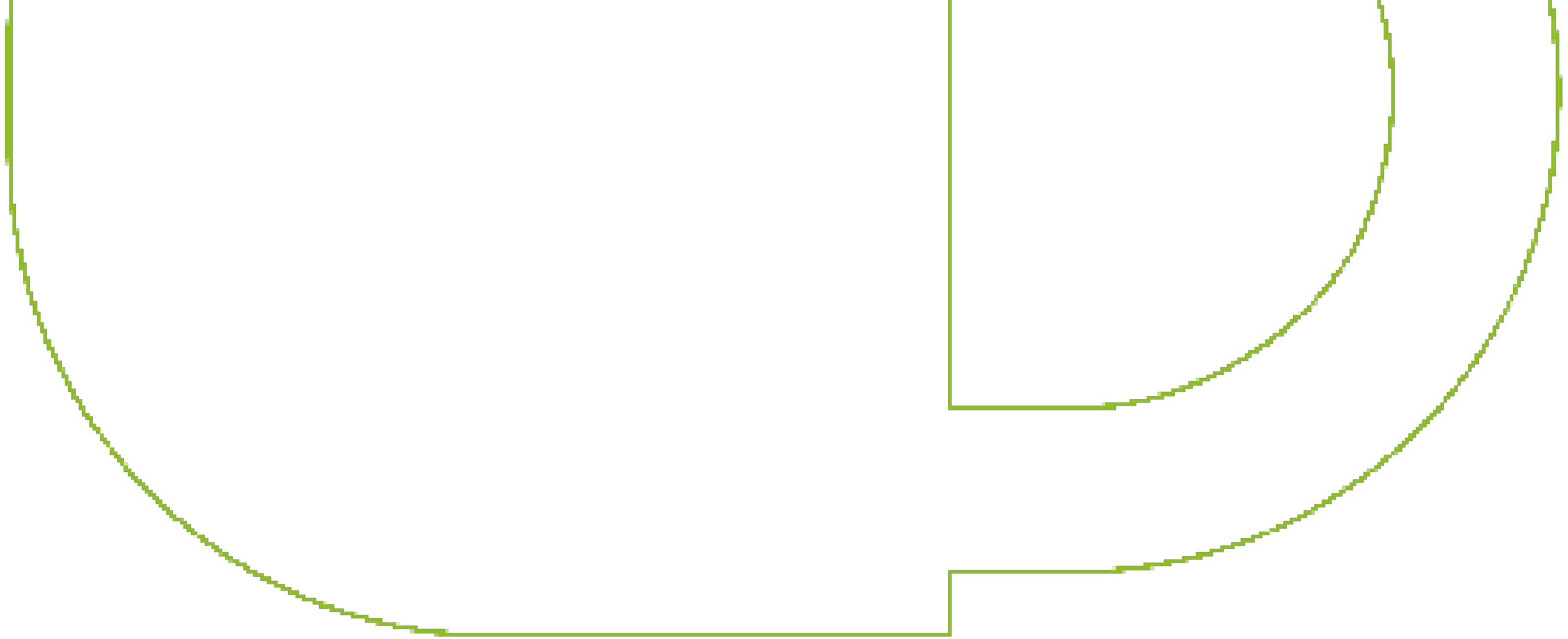
Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação

Impressão
Divisão de Serviços Gráficos

SEGURANÇA NA INTERNET

GUIA PARA PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS

2021



Conteúdo

PNPC

PROTEGER COM INTELIGÊNCIA

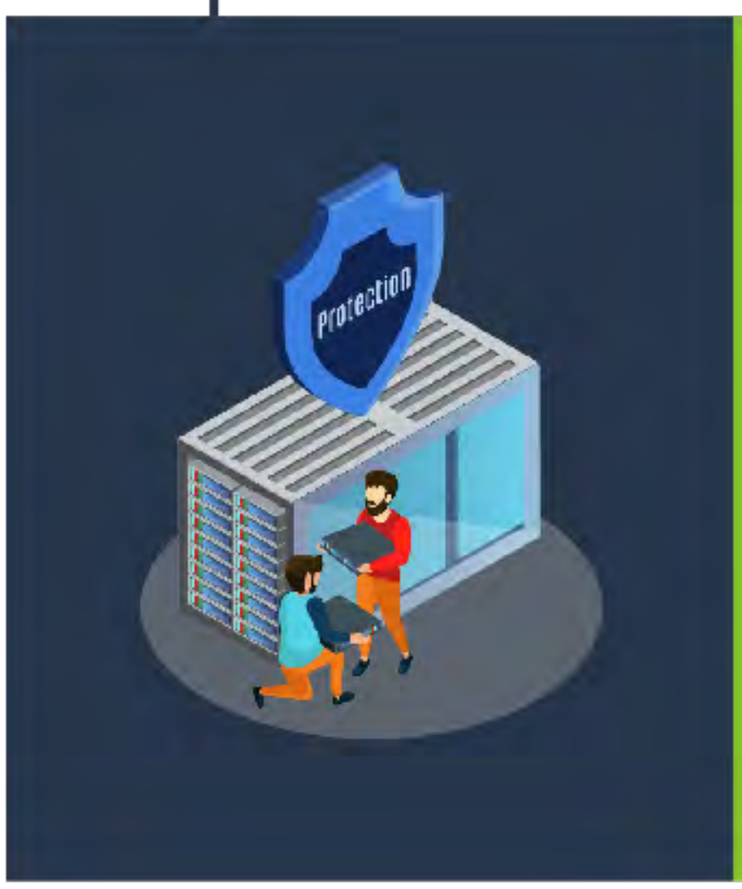
A ABIN E OS CONHECIMENTOS SENSÍVEIS

A expansão da internet acrescentou uma série de melhorias no cotidiano das pessoas, seja no trabalho ou no lazer. Ao mesmo tempo, esse avanço tecnológico abriu espaço para potenciais vulnerabilidades que os usuários nem sempre estão preparados para evitar. Os riscos vão desde o comprometimento de equipamentos até ameaças à segurança de instituições.

Cibercrime é um termo utilizado para delitos que abarquem práticas ilícitas ocorridas na internet e redes de computadores. São exemplos: invasão de sistemas, disseminação de vírus, roubo de dados pessoais, falsidade ideológica e acesso a informações confidenciais. Uma de suas características é a predominância transnacional, o que dificulta as investigações e a produção de provas contra o acusado.

Esta cartilha foi elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), da Agência Brasileira de Inteligência (ABIN), para que você conheça as ameaças mais comuns e as técnicas para proteger seus equipamentos e a si mesmo.

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.



Ransomware é um software malicioso que infecta o computador bloqueando arquivos de funcionamento do sistema operacional ou criptografando dados do usuário.

Ameaça nº 1: *Ransomware*

Pode ser que alguma vez você tenha ouvido esse termo ou lido alguma referência sobre ele em jornais. Ransomware é um software malicioso que infecta o computador bloqueando arquivos de funcionamento do sistema operacional ou criptografando dados do usuário, condicionando a restauração do acesso ao dispositivo ou o fornecimento de chave para decifração ao pagamento de resgate a quem o programou.

Embora a forma de infecção seja variada, a mais comum acontece por meio da distribuição de anexos por e-mail com links para falsos sites de aparência autêntica. Para impedir ou dificultar as ações de ransomware, seguem algumas recomendações.

Para se prevenir

· Tenha cuidado ao abrir documentos de **emissores desconhecidos** ou questionáveis.

· Utilize uma ferramenta de filtragem de e-mail, além de um **antivírus** eficaz e constantemente atualizado.

· Atualize o sistema operacional e os programas com frequência.

· Faça **backup** de seus dados rotineiramente para poder restaurá-los em caso de problemas.

Em caso de infecção

· Evite pagar o resgate para limitar a atratividade dessas práticas e não arriscar um novo ataque. O pagamento não garante a recuperação de dados ou o desbloqueio do equipamento.

· Procure **ajuda especializada** de técnicos em segurança cibernética.

· Apresente queixa à autoridade competente.

· Restaure o sistema usando backups.

· Guarde a **mídia de armazenamento infectada**, pois profissionais de segurança cibernética disponibilizam regularmente métodos ou ferramentas para decifrar os dados depois desses ataques.

· Se você for gestor, promova feedback sobre gestão de crises, a fim de limitar os impactos de um ataque cibernético futuro. Converse com a equipe sobre o que ocorreu, como a crise foi superada e formas de se evitar novas infecções.

Ameaça nº 2: *Cryptojacking*

Cryptojacking é um termo em inglês que une “crypto”, de criptomoedas, e “jacking”, em referência à obtenção de algo de forma ilegal ou irregular. Essa ameaça acontece quando um hacker se utiliza de um dispositivo de outra pessoa para fazer **mineração de criptomoedas**, que é um processo de criação de novas moedas.

Os problemas causados pelo cryptojacking não são relacionados diretamente com danos e roubos de dados, como outras vulnerabilidades de segurança, e sim com o uso irregular de recursos do seu sistema para gerar riqueza para terceiros.

Existem também maneiras de cryptojacking que se utilizam de vírus, o que aumenta consideravelmente os riscos de interceptação de dados e de causar outros danos na sua instalação.

Como você poderia fugir desta ameaça? Veja algumas regras básicas de segurança:

- Fique atento à principal consequência desse ciberataque: a lentidão do computador.
- Instale um **bloqueador de anúncios** ou uma extensão dedicada ao bloqueio de scripts em navegadores de internet.
- Bloqueie pop-ups.
- Atualize regularmente o antivírus.
- Verifique se a opção anti-adware do antivírus está habilitada.


S&P 500
S&P 500
AAPL
BRK-
Berkshire

Ameaça nº 3:
Uso incorreto da nuvem

Computação em nuvem é um conjunto de tecnologias capaz de realizar diferentes tarefas nos mais variados dispositivos (celular, computador etc.), entre elas, acessar arquivos por meio da internet. Adotada por instituições no mundo inteiro, é uma realidade nos negócios e no uso pessoal.

Os dados hospedados na nuvem, no entanto, acarretam riscos significativos para a **segurança das informações**, pois além de o usuário não saber a sua exata localização, podem ser interceptados ou capturados em qualquer momento de seu ciclo de vida. Isso acontece porque, para agilizar e otimizar o fluxo de dados, estes são transferidos e armazenados em datas centers, distribuídos geograficamente em vários centros. Ademais, os dados em servidores localizados no exterior estão sujeitos aos regulamentos dos Estados que os hospedam.

O que se percebe, entretanto, é que os riscos da hospedagem baseada em nuvem ainda são amplamente desconhecidos pelos usuários em geral. É importante ressaltar que as empresas são responsáveis pela segurança, integridade e confidencialidade de seus próprios dados, sendo, portanto, recomendável que se observem as indicações abaixo:

- Prefira **provedores nacionais** e com servidores localizados no Brasil.

- Não utilize serviços de hospedagem em nuvem que permitam acesso aos dados para fins publicitários.

- Separe o processamento de dados não sensíveis, armazenáveis na nuvem, de informações com elevado valor econômico ou estratégico, que devem ser mantidas nas **redes internas** da instituição.

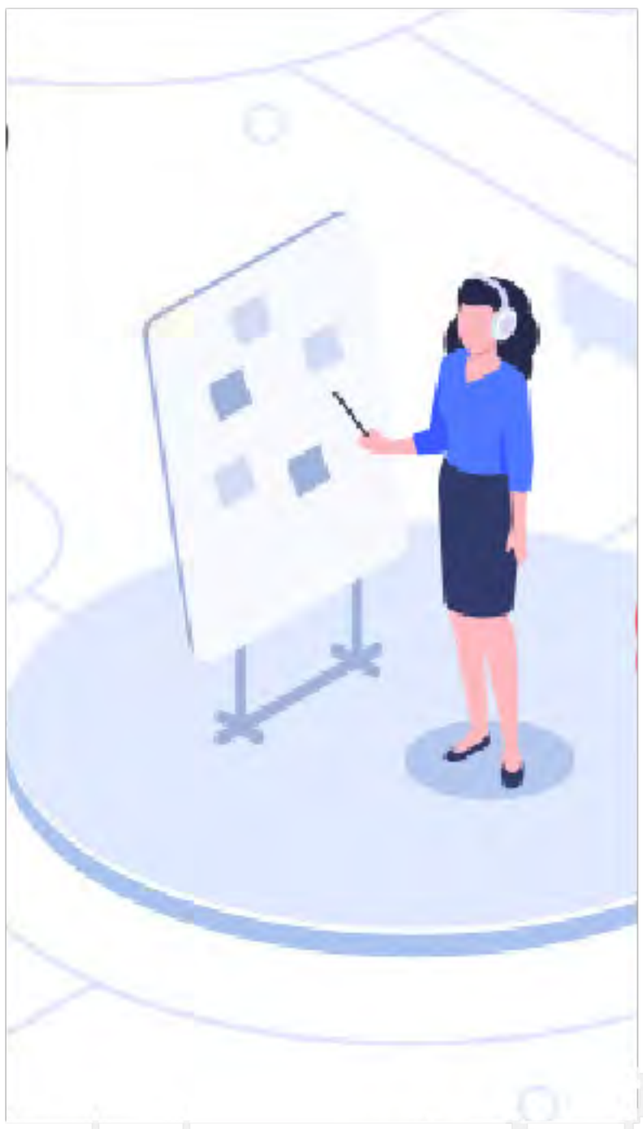
- Cifre sistematicamente todos os dados sensíveis transferidos para serviço de hospedagem remota.

Se você for gestor

- Garanta que o contrato de hospedagem de dados de sua instituição não permita a transferência dos dados do Brasil para um país estrangeiro.

- Limite os direitos dos usuários de serviços em nuvem, não use conta de administrador para tarefas diárias, monitore os eventos de registro de conexão e garanta o **gerenciamento rigoroso** dos direitos de acesso para evitar roubo de identidade.

Ameaça nº 4:
Uso inadequado da internet das coisas



Você já deve ter percebido que "conectividade" é a palavra-chave de nosso tempo. A internet das coisas ou IoT (sigla do inglês Internet of Things) permite a interconexão de objetos ou coisas com a internet. Apesar do avanço tecnológico, esses equipamentos, que são geralmente **controláveis** de forma remota por meio do uso de sensores inteligentes, como bluetooth, podem apresentar vulnerabilidades intrínsecas ao uso como falhas na segurança das informações. Elencamos algumas recomendações para que você utilize a tecnologia de maneira mais segura:

- Desative a interface de administração para acesso público via internet, se oferecida pelo fornecedor do produto.

- Altere a senha padrão.

- **Atualize os softwares** dos produtos regularmente.

- Desconecte os dispositivos quando não estiverem em uso.

Ameaça nº 5:
Uso inadequado de wi-fi público

Apesar de serem bastante convenientes, as redes wi-fi trazem riscos, principalmente os acessos públicos. Hackers e serviços de inteligência estrangeiros possuem capacidade técnica para criar redes wi-fi falsas, com nomes de marcas conhecidas, acesso gratuito e sem necessidade de senha.

Utilizando essa estratégia, **invasores podem acessar seu dispositivo** e, consequentemente, os dados manuseados em tais equipamentos, além de ativar seu microfone ou câmera sem seu conhecimento e até mesmo registrar cada tecla pressionada. Essa manobra permite o acesso a dados pessoais e sensíveis, facilitando novas intrusões.

Além disso, durante viagens ao exterior, comunicações sem fio podem ser monitoradas por autoridades locais ou serviços de inteligência. Seguem recomendações para que você utilize as redes wi-fi de maneira mais segura:

- Utilize uma rede privada virtual (VPN) ao se conectar a um wi-fi público.
- Proteja seus dados e comunicações utilizando uma ferramenta de criptografia, tipo Pretty Good Privacy (PGP), disponível para download gratuito.
- Utilize e-mails criptografados para trocar conteúdo sensível.
- Desligue o modo wi-fi quando não estiver em uso.
- Atualize regularmente o sistema operacional, o navegador da internet e suas extensões, antivírus e softwares.
- Opte por sites seguros, que utilizem HTTPS.
- Em caso de dúvida depois de se conectar a uma rede wi-fi pública, mude rapidamente as senhas dos aplicativos que você usa com mais frequência.
- Ao viajar, privilegie o uso de dispositivos móveis que não contenham material sensível.

Ameaça nº6: *Phishing*

Phishing é uma técnica que tem o objetivo de enganar pessoas para que compartilhem informações confidenciais. Os procedimentos consistem em criar e-mails, mensagens de texto ou janelas pop-up aparentemente reais e plausíveis para induzir o usuário a realizar ações que podem comprometer seus dispositivos, redes ou sistemas.

É importante ressaltar que esse é um tipo simples de ciberataque e, ao mesmo tempo, perigoso e eficiente. São exemplos comuns pedir que você abra um **anexo malicioso ou clique em um link falso**. Golpes de *phishing* também podem induzir você a fornecer suas informações confidenciais, o que favorece o acesso indesejado a suas contas. Essas informações podem também ser usadas pelo invasor para se passar pela vítima e enviar e-mails com software malicioso para seus contatos, visando a enganar os destinatários para que abram anexos infectados.

Spear phishing

Enquanto boa parte das campanhas de *phishing* enviam e-mails em massa para o maior número de pessoas possível, no caso do *spear phishing* você pode ser um alvo específico. Nesta ameaça, o ataque acontece a uma pessoa ou instituição específica, utilizando geralmente um conteúdo personalizado para a vítima. Para tanto, é necessário maior planejamento para descobrir nomes, cargos em empresas, endereços de e-mail etc. Assim, hackers vasculham a internet para combinar essas informações com outros dados pesquisados sobre a pessoa de interesse. Elencamos abaixo algumas recomendações para evitar esta ameaça:

- Defina senhas seguras.
- Evite compartilhar informações pessoais, mantendo discrição online.
- Não clique em **links duvidosos** e desative a opção de baixar automaticamente os anexos de e-mails.
- Use redes seguras.
- Antes de fornecer qualquer informação, cheque com a origem se eles são realmente aqueles que enviaram o e-mail.

Recomendações para trabalhos realizados em rede

Além de ser um recurso de proteção no ambiente institucional, a segurança da informação auxilia a gestão corporativa. Seguem algumas recomendações para que você trabalhe com segurança:

- Se a instituição aderiu ao teletrabalho, deve também instituir política que o regule, fornecer ferramentas adequadas (laptops profissionais, aplicativos seguros etc.) e estabelecer orientações de boas condutas para os funcionários.
- A instituição também deve disponibilizar meios de conexão protegidos ou encriptados, por meio de uma VPN, que garantam a confidencialidade e a integridade das comunicações.
- Se você está representando sua instituição on-line, pense cuidadosamente sobre o que você publica, limitando informações sensíveis sobre projetos e funcionários.
- Não presuma que as informações que você compartilha não irão além do destinatário original.
- Não disponibilize informações pessoais em mensagens automáticas ou assinaturas de e-mail, pois podem ser capturadas.
- Evite abrir mensagens sem identificação ou se houver suspeita de endereço falso.
- Não use seu e-mail profissional para cadastramento em sites.
- Não acesse e-mails de anúncios (spam).
- Use cópia oculta para enviar mensagens a vários usuários, desse modo evitará que sua lista de contatos circule pela internet.

Confie em sua importância!
Proteja sua informação.

Caso ocorra violação em dados que envolvam suas informações pessoais ou profissionais, você e sua instituição estarão expostos a uma ampla gama de riscos. Relate suas preocupações a seus superiores e ao setor de segurança de sua instituição, caso desconfie ter sofrido algum ciberataque. Também é possível relatar o caso para a ABIN pelo e-mail *reporte@abin.gov.br*.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR

WWW.GOV.BR/ABIN/PNPC