Campanha de Conscientização Cibernética

PROTEÇÃO DE DADOS

EXÉRCITO BRASILEIRO

Produção:

COM D CIBER

E NA D CIBER

PROTEJA SEUS DADOS

REDUZA DADOS SOBRE VOCÊ NA INTERNET

O **excesso de exposição** *online* pode comprometer sua privacidade e dar a golpistas a oportunidade de usar seus dados para, por exemplo, tentar se passar por você.

» **Pense bem** antes de postar algo
  • depois que algo é postado, dificilmente poderá ser excluído
» Ao fazer cadastros em sites e aplicativos, só forneça dados que sejam obrigatórios
» Seja **seletivo** ao aceitar seus contatos
  • quanto maior sua rede de contatos, mais pessoas terão acesso a seus dados
» Respeite também os dados de outras pessoas

Veja mais dicas na Cartilha
PRIVACIDADE

REDUZA A COLETA DE DADOS POR SITES

Os sites que você acessa podem **coletar dados de seu navegador**, usá-los para traçar seu perfil comportamental (*profiling*) e, com base nele, oferecer conteúdos personalizados para influenciá-lo ou limitar suas opções.

» Avalie e ajuste as **configurações de privacidade** de seu navegador
» Limite a coleta de dados por ***cookies***
  • aceite somente *cookies* necessários
  • configure o navegador para **não aceitar *cookies* de terceiros**
» Limpe com frequência o **histórico** de navegação
  • use **navegação anônima**, se possível

Veja mais dicas na Cartilha
PRIVACIDADE

LIMITE PERMISSÕES DE ACESSO DOS APLICATIVOS

Para funcionar, muitos aplicativos solicitam **acesso a seus dados**, além de acesso à câmera, microfone, geolocalização, redes e contatos. Alguns acessos são essenciais, mas outros podem ser **abusivos**.

» Ao instalar e usar um aplicativo, autorize apenas **acessos essenciais** a seu funcionamento e operação
» **Apague** os aplicativos que não usa mais

CUIDADO COM E-MAILS E MENSAGENS ELETRÔNICAS

Ataques de *phishing* procuram **induzi-lo** a fornecer seus dados. É comum que atacantes utilizem técnicas como o envio de e-mails e mensagens eletrônicas **falsas** para coletar dados.

» **Não clique** em todos os *links* recebidos
  - antes de clicar, analise o contexto e os detalhes e, na dúvida, não clique!
  - desconfie até de mensagens enviadas por "conhecidos"

» Desconfie sempre de **arquivos anexos**
  - cheque o arquivo com antivírus antes de abri-lo e, na dúvida, não abra!

» Só leia códigos QR se tiver certeza de que a fonte é confiável

» Acesse o site digitando o endereço (URL) diretamente no navegador
  - use sempre **conexão segura** (https)

CUIDADO COM PERFIS FALSOS

Para ter acesso a seus dados, golpistas podem criar **perfis falsos em redes sociais**, tentando se passar por pessoas ou empresas conhecidas.

» Antes de aceitar ou seguir alguém nas redes sociais, tenha certeza de que o **perfil é legítimo**
  • busque pelo **selo indicativo** de conta verificada
» Se receber um pedido de conexão e ficar na dúvida:
  • busque o **perfil oficial** da pessoa ou empresa
» **Bloqueie** e denuncie perfis falsos

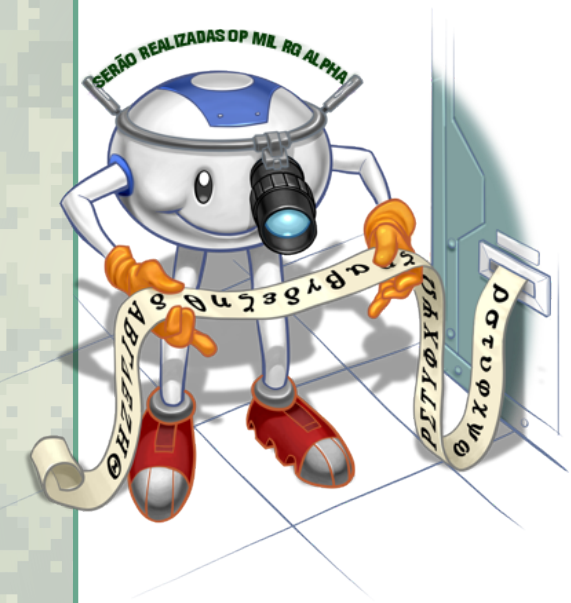
USE AUTENTICAÇÃO FORTE

Reforçar a autenticação ajuda a proteger suas contas e dispositivos **contra invasões** e a minimizar o impacto do vazamento de senhas. Atacantes se aproveitam de dados obtidos via **vazamentos** ou *malware* para tentar invadir contas e dispositivos e, então, coletar mais dados ou usá-los para **aplicar golpes**.

- Ative a **verificação em duas etapas** em todas suas contas
- Crie **senhas fortes**, difíceis de adivinhar, e **não as repita**
- Configure seus dispositivos para **exigir autenticação** na tela inicial
- Troque imediatamente suas senhas se desconfiar que vazaram ou foram usadas em um dispositivo infectado
- Habilite **notificações de *login***, sempre que possível

Veja mais dicas na Cartilha
AUTENTICAÇÃO

PREFIRA SERVIÇOS COM CRIPTOGRAFIA



Dados podem ser **indevidamente acessados** se transmitidos sem criptografia. A criptografia cifra os dados para que, mesmo que um atacante os capture, **não seja possível entender**.

» Use **conexões seguras**, como https, para acesso a *sites*
  - além de cifrar os dados, garantem que você está conectando no destino correto

» Escolha serviços de nuvem que:
  - usem conexões seguras (https)
  - ofereçam verificação em duas etapas

» Prefira aplicativos de mensagem com **criptografia ponta a ponta**

ATUALIZE SEUS DISPOSITIVOS

Seus dispositivos têm grande quantidade de dados sobre você, por isso são **visados por ladrões** e atacantes, que tentam invadi-los explorando vulnerabilidades, ou infectá-los, usando *malware*.

» Instale **atualizações de segurança** regularmente
  • ative a **atualização automática**, sempre que possível
» Utilize mecanismos de proteção, como antivírus e *firewall* pessoal

FAÇA *BACKUPS* PERIÓDICOS

Seus dados podem ser **perdidos** a qualquer momento, seja por acidente, furto, falha de sistema, atualização malsucedida ou defeito físico em seu dispositivo. Ter **cópias** permite recuperá-los, reduzindo os transtornos.

- Utilize uma ou mais opções, como:
  - serviço de nuvem
  - sincronização com outro equipamento
  - disco externo ou *pen drive*
- Em celulares, habilite a opção de ***backup* nativa** do sistema
- Tenha pelo menos um *backup offline*
- Evite colocar na nuvem arquivos com **dados confidenciais**

Veja mais dicas na Cartilha
BACKUP

PROTEJA DADOS SENSÍVEIS COM CRIPTOGRAFIA

Muitas informações **sensíveis**, que você pode preferir manter privadas, são **hoje arquivos digitais**, por exemplo documentos, fotos ou informações de saúde. Guardá-las criptografadas protege-as contra **acesso indevido** por atacantes ou *malware*.

» Se possível, ative a **criptografia nativa** do sistema em celulares, *tablets* e computadores
  • alternativamente, crie uma partição criptografada
» Criptografe arquivos sensíveis se precisar colocá-los na nuvem

PROTEJA MÍDIAS E DISCOS EXTERNOS

Mídias portáteis, como *pen drives* e discos externos, podem ser perdidas ou furtadas e, se **desprotegidas**, ter os dados acessados indevidamente. Além disso, os dados gravados podem ser apagados ou criptografados por *malware*, impedindo que sejam acessados.

» Não deixe as mídias conectadas o tempo todo
  - conecte-as apenas quando for realmente usá-las

» Guarde as mídias em **local seguro**

APAGUE DADOS ANTES DE DESCARTAR OU REPASSAR DISPOSITIVOS

Dados armazenados em seus dispositivos e mídias podem ser indevidamente acessados, por isso é importante garantir que sejam apagados antes de você descartá-los ou repassá-los a terceiros.

- Desconecte sua conta ID de sistema
- Restaure as configurações originais de fábrica
- Sobrescreva a mídia ou dispositivo, se possível
- Escolha empresas de manutenção com boa reputação e confiança

Veja mais dicas na Cartilha

CELULARES E *TABLETS*

PENSE BEM ANTES DE TROCAR DADOS POR DESCONTOS

Já pensou por que tantas empresas pedem para você fazer **cadastro** e **informar o CPF** a cada compra? O desconto é a **contrapartida** para que você autorize a coleta e o uso de seus dados. Assim, elas passam a conhecê-lo melhor e podem selecionar o que ofertar ou deixar de ofertar a você.

» Antes de cair na tentação dos programas de descontos, analise:
  - **para que** seus dados serão usados e com quem serão compartilhados?
  - os **valores** dos descontos compensam sua exposição?

» Reflita também sobre o potencial risco de **vazamentos de dados**
  - você pode se tornar vítima de golpes

CONHEÇA SEUS DIREITOS

SAIBA COMO SEUS DADOS SÃO TRATADOS

Antes de fornecer seus **dados pessoais** em *sites* e aplicativos, é importante saber como eles serão tratados. Isso ajuda a identificar práticas abusivas de coleta e compartilhamento de dados que possam comprometer sua **privacidade e segurança**.

» Leia **políticas de privacidade** para entender:
  - **quais** dados são coletados
  - para **quais finalidades** serão usados
  - **com quem** podem ser compartilhados e por quê
» **Leia** os termos de consentimento disponibilizados
» Não aceite e não use o serviço se não concordar com os termos

A QUEM RECORRER EM CASO DE ABUSO?

A pessoa (ou seja, Titular dos dados) que sofre algum tipo de **abuso** deve utilizar os **canais oficiais** de atendimento disponibilizados pela organização (ou seja, Controlador) ou, pela ANPD, caso não consiga exercer seus direitos perante o Controlador. A comunicação à ANPD pode se dar por meio de uma **petição de Titular**, ou, ainda, por meio de **denúncia**, em caso de suposta infração da LGPD, quando não for aplicável a petição de Titular.

- Entre em contato com o Encarregado de Dados do Controlador
- Entre em contato com a ANPD para peticionar ou denunciar qualquer infração à Lei Geral de Proteção de Dados (LGPD) https://gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/

CONHEÇA ALGUNS TERMOS DA LGPD

Toda pessoa tem o direito de saber como seus dados pessoais são tratados por organizações. A Lei Geral de Proteção de Dados (LGPD) não é aplicada quando os dados são utilizados de forma particular, mas somente quando os dados pessoais são usados por organizações públicas, privadas e terceiros para fins econômicos.

A LGPD define termos específicos com o propósito de classificar tipos de informações pessoais, instituições que tratam os dados e papéis de quem trata os dados. Conhecer esses termos ajuda a compreender as políticas de privacidade, estimar o dano e quem contatar quando tiver problemas.

Conheça a seguir alguns dos termos definidos na LGPD.

TITULAR

É a **pessoa** natural a quem se referem os dados pessoais.

DADOS PESSOAIS

São as informações de **identificação**, como nome, documentos e endereço residencial, mas também informações indiretas como seus hábitos de consumo, sua aparência e aspectos de sua personalidade, que possam ser usadas para determinar o seu perfil comportamental.

DADOS PESSOAIS SENSÍVEIS

São dados relacionados a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando **vinculado a uma pessoa** natural.

DADO ANONIMIZADO

Dado que **não permite** que o Titular seja diretamente identificado. É uma forma de manter a segurança e a privacidade dos dados.

CONTROLADOR

É o responsável pelo **tratamento** dos dados do Titular. É ele quem define como os dados são tratados e o que o Operador pode fazer.

OPERADOR

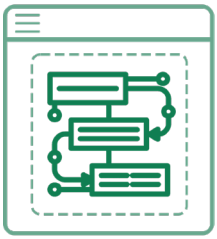
É quem **trata** os dados pessoais em nome do Controlador.

AGENTE DE TRATAMENTO

É o Controlador e o Operador.

ENCARREGADO DE DADOS

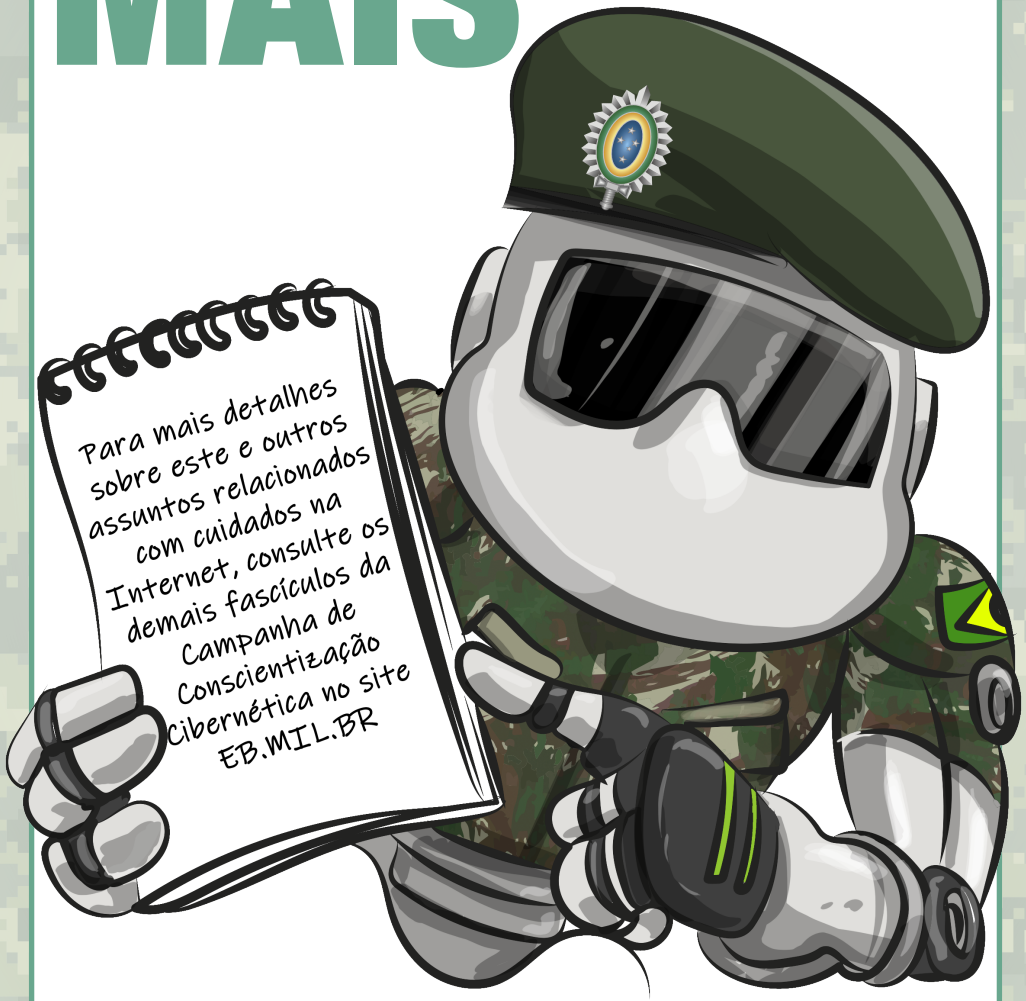
É a pessoa indicada pelo agente de tratamento para atuar como **canal de comunicação** entre o Controlador, o Titular e a ANPD. Dentre suas funções, destaca-se a **orientação** dos funcionários e dos contratados da entidade a respeito das **práticas** a serem tomadas em relação à proteção de dados pessoais.



ANPD (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS)

É a **autarquia**, de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, que tem como missão **zelar** pela proteção de dados pessoais no país, incluindo normatização, fiscalização e aplicação de sanções por violações à LGPD, que podem incluir multas de até R$ 50 milhões por infração.

SAIBA MAIS


Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais fascículos da Campanha de Conscientização Cibernética no site EB.MIL.BR

EXÉRCITO BRASILEIRO

Novos Desafios, Mesmos Valores

Produção:

Fonte:
Cartilha de Segurança para Internet - https://cartilha.cert.br/