Computadores

Apoio de Divulgação:

INSTITUTO FEDERAL
Ceará
Campus Limoeiro do Norte

Produção:

cert.br nic.br cgi.br

FAÇA SUA PARTE: PROTEJA SEU COMPUTADOR

Manter seu computador seguro evita que ele seja usado para ataques na Internet e protege seus dados, como senhas de acesso a contas, informações financeiras, fotos, vídeos e outros arquivos importantes.

Veja aqui dicas de como proteger seu computador.

USE APENAS PROGRAMAS ORIGINAIS

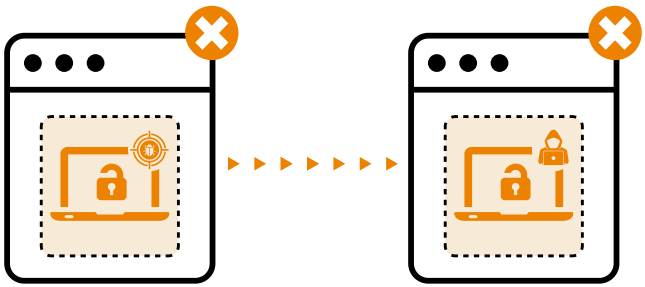
O uso de sistemas operacionais e aplicativos não originais coloca em risco sua segurança e a de seus dados, pois podem conter *malware*, não funcionar corretamente, não receber atualizações de segurança nem suporte.

- Compre licenças apenas do fabricante ou de revendas autorizadas
  - faça a ativação no fabricante
- Se quiser usar um sistema ou aplicativo pago, mas não puder arcar com os custos, avalie:
  - versão com licença mais barata
  - alternativas com funcionalidades semelhantes e menor custo ou gratuitas
- Dê preferência à versão mais recente (e atualizada)

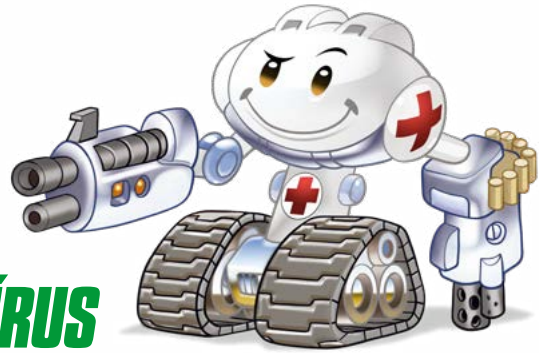
ATIVE ATUALIZAÇÕES AUTOMÁTICAS

Atacantes exploram vulnerabilidades em programas com o objetivo de invadir computadores, coletar dados e instalar *malware*. Para corrigir as vulnerabilidades, fabricantes lançam correções que precisam ser aplicadas para manter seu computador seguro.

- Configure atualizações automáticas
  - em sistemas, navegadores e demais aplicativos
- Adicionalmente, cheque por novas atualizações de tempos em tempos
  - garanta que as atualizações sejam feitas
  - fique atento: **infecção por *malware* pode desativar atualizações**
- Lembre-se de atualizar também a BIOS do computador



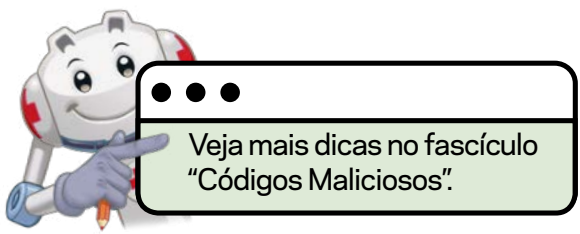
Vulnerabilidade é uma falha no projeto, na implementação ou na configuração de programas, serviços ou dispositivos.
Ao explorar uma vulnerabilidade, um atacante ou *malware* pode comprometer seu computador e os dados nele contidos, e ainda usá-lo para atacar outros computadores.



USE ANTIVÍRUS

Ferramentas antivírus (*antimalware*) podem ajudar a detectar uma infecção, preveni-la e/ou remover *malware* do computador. Mas, para serem efetivas contra a infinidade de variantes e novos *malware* que surgem todos os dias, precisam de atualização contínua.

- Habilite o antivírus nativo do sistema ou instale um de sua preferência
- **Mantenha o antivírus atualizado**
- Configure o antivírus para verificar automaticamente seus arquivos

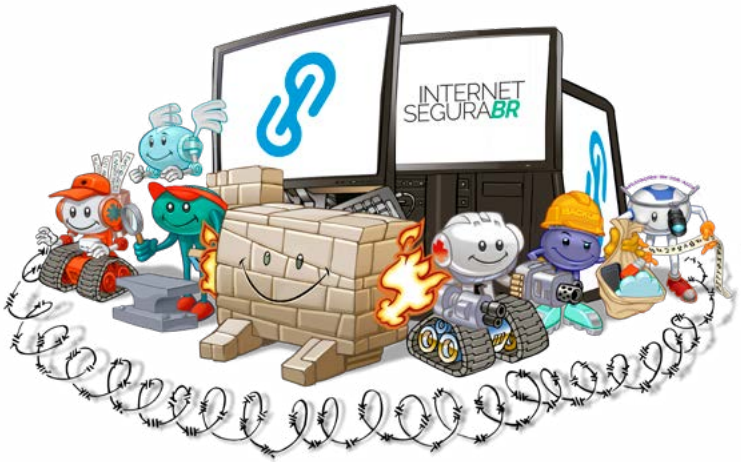


Veja mais dicas no fascículo "Códigos Maliciosos".

MANTENHA O FIREWALL PESSOAL ATIVADO

O *firewall* protege seu computador contra ataques vindos pela rede. Ele bloqueia conexões não autorizadas de entrada para programas e serviços executando em seu computador.

» Assegure-se de ter um *firewall* pessoal instalado e ativado
  - use a opção nativa do sistema ou instale um de sua preferência
  - algumas ferramentas antivírus podem incluir funcionalidades de *firewall* pessoal



AJUSTE AS OPÇÕES DE SEGURANÇA E PRIVACIDADE

Além de *firewall* e antivírus, os sistemas costumam oferecer outros recursos nativos de segurança e privacidade. É importante conhecer as opções e configurá-las conforme suas necessidades e boas práticas.

- Configure quais serviços e aplicativos podem acessar, por exemplo, localização, contatos, calendários, lembretes, fotos, *bluetooth*, microfone, câmera e arquivos
- Ative a localização remota
  - recurso chamado "Buscar Mac" no macOS e "Localizar meu dispositivo" no Windows
- Instale aplicativos extras de segurança, caso deseje recursos adicionais

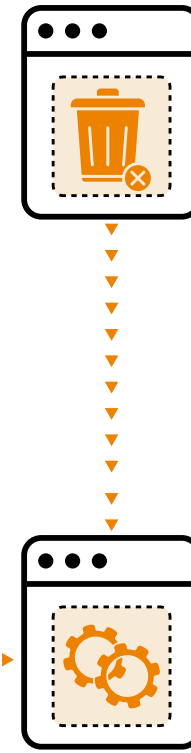
BAIXE APLICATIVOS SOMENTE DE LOJAS OFICIAIS

Infelizmente, existem aplicativos criados com fins maliciosos. As lojas oficiais costumam ter políticas mais rígidas e mecanismos mais rápidos de exclusão desses aplicativos quando detectados.

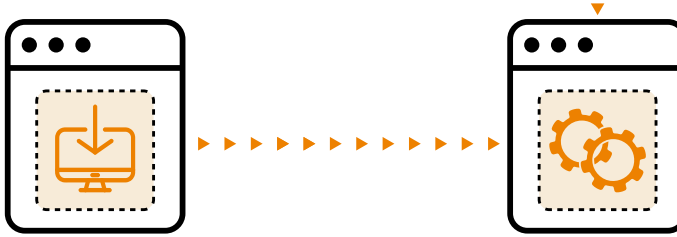
- Use apenas a loja oficial do sistema ou do fabricante do computador
  - nunca instale aplicativos recebidos via mensagens ou *links*
- Mesmo assim, cuidado com aplicativos falsos
  - antes de instalar o aplicativo, confirme seu nome e se seu desenvolvedor é mesmo quem deveria ser

MANTENHA SÓ OS APLICATIVOS QUE USA

Quanto mais aplicativos instalados, maior a chance de que vulnerabilidades sejam descobertas e exploradas por atacantes e *malware*. Deixar instalados apenas aplicativos que realmente usa facilita a atualização e reduz as chances de ser comprometido.



» Reavalie regularmente os aplicativos instalados
  - exclua os que não usa mais
  - você pode reinstalá-los depois, se sentir necessidade



CONSIDERE CIFRAR O DISCO RÍGIDO

Cifrar o disco rígido ajuda a proteger seus dados contra acessos indevidos em situações de perda ou furto. Protege também em casos de descarte de equipamento ou disco quando não é possível apagar previamente os dados armazenados.

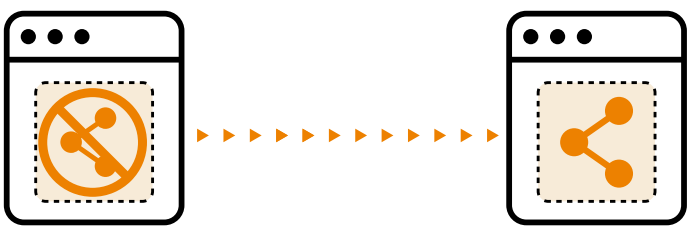
» Use recursos nativos dos sistemas
  - exemplo: FileVault no macOS e BitLocker no Windows

» Cifre também discos externos e *pen drives*

LIMITE O COMPARTILHAMENTO DE RECURSOS

Alguns sistemas permitem o compartilhamento de recursos, como arquivos e discos. Entretanto, há o risco de recursos ou informações sensíveis serem indevidamente acessados ou de receber arquivos maliciosos.

- Desabilite opções de compartilhamento, caso não as use
- Ao compartilhar recursos do computador:
  - estabeleça senhas e permissões de acesso adequadas
  - compartilhe pelo tempo mínimo necessário
  - não aceite pedidos de compartilhamento ou conexões de estranhos
- No compartilhamento por proximidade, permita acesso apenas para seus dispositivos



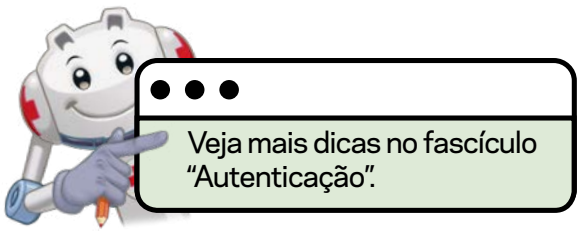
EXIJA AUTENTICAÇÃO NA TELA INICIAL

Se alguém pegar seu computador desbloqueado, poderá acessar seus dados e aplicativos, se passar por você e instalar aplicativos maliciosos para, por exemplo, espioná-lo.

» Configure o método de autenticação na tela inicial
  - **use senha forte ou biometria**

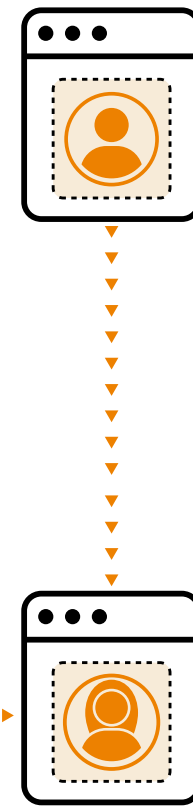
» Configure para exigir autenticação sempre que:
  - a proteção de tela for ativada, ou
  - o computador entrar em modo de repouso (inativo)

» Habilite a proteção de tela com tempo mínimo



USE CONTAS DIFERENTES PARA DIFERENTES USUÁRIOS

Ter diferentes contas permite limitar acesso a aplicativos e separar configurações e arquivos. Ajuda também a reduzir os danos em caso de invasão ou infecção, pois as ações maliciosas ficarão restritas às permissões do dono da conta comprometida.



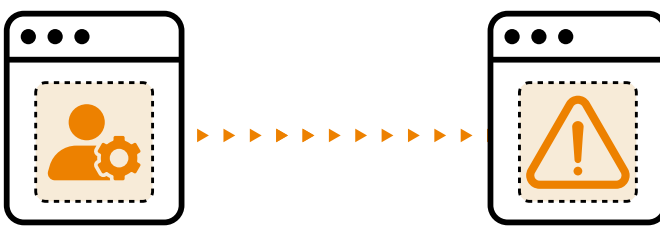
- **Crie uma conta para cada pessoa que usar o computador**
- Defina o acesso que cada conta pode ter
  - considere configurar recursos de controle parental, caso a conta seja usada por crianças

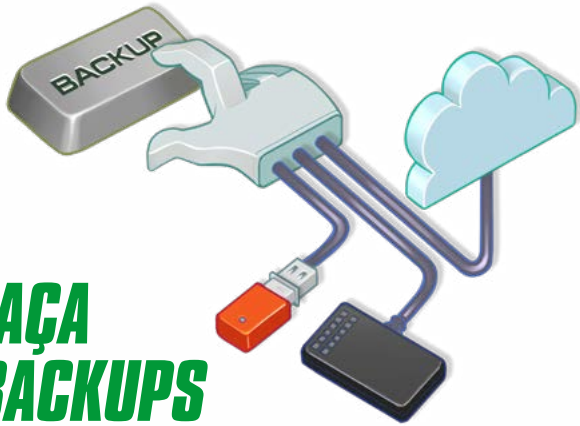
ATENÇÃO ESPECIAL ÀS CONTAS COM PERFIL DE ADMINISTRADOR

Contas com perfil de administrador requerem cuidados especiais, pois têm acessos privilegiados. Se uma conta com esse perfil for comprometida, o atacante ou malware poderá executar ações maliciosas como se fosse o administrador do computador.

» **Só atribua perfil de administrador a quem realmente necessitar**
  - e compreender as consequências

» Ao usar uma conta com perfil de administrador:
  - só confirme operações que tiver certeza
  - redobre os cuidados com a senha de acesso à conta
  - ative a verificação em duas etapas na conta ID de sistema





FAÇA BACKUPS

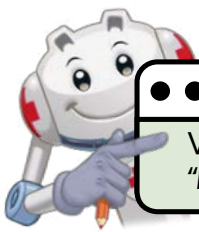
Os dados do seu computador podem ser perdidos por falhas de *hardware* ou de sistema, perda ou furto do equipamento, ou ação de *malware*, como *ransomware*. Ter cópias permite recuperá-los, reduzindo os transtornos.

» **Habilite *backups* automáticos**

» Faça *backups* manuais em casos especiais, como atualização de sistema ou envio para manutenção

» Utilize uma ou mais opções, como:

- serviço de nuvem do próprio sistema
- sincronização com outro equipamento
- disco externo ou *pen drive*

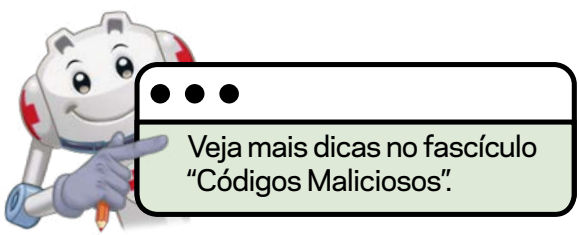


Veja mais dicas no fascículo *"Backup"*.

AJA RAPIDAMENTE EM CASO DE SUSPEITAS DE PROBLEMAS

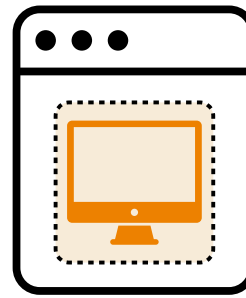
Abriu um arquivo ou clicou no *link* de um *e-mail* e depois descobriu que era *malware*? O computador está mais lento? Janelas de *pop-up* estão aparecendo? Seus arquivos estão sumindo? Nessas situações, é melhor agir rapidamente para evitar problemas maiores.

- Execute o antivírus nativo do sistema ou outro de sua preferência
- Reinstale o sistema se não for possível remover o *malware* ou os sintomas persistirem
- Altere as senhas dos serviços que costuma acessar do computador
  - faça isso em outro dispositivo que considere seguro ou
  - se usar o próprio computador, altere as senhas apenas depois que o problema inicial estiver resolvido



Veja mais dicas no fascículo “Códigos Maliciosos”.

NÃO USE COMPUTADOR PESSOAL PARA TRABALHO



Usar seu computador para trabalho é arriscado: sua privacidade pode ser exposta e você pode violar regras de segurança e proteção de dados. Além disso, vulnerabilidades em seu computador podem levar à invasão da rede da empresa, assim como vulnerabilidades em aplicativos usados pela empresa podem comprometer seu computador.

» Separe o pessoal do profissional. Não use seu computador pessoal para:
  - acessar a rede corporativa
  - instalar aplicativos do trabalho
  - armazenar dados da empresa ou de clientes

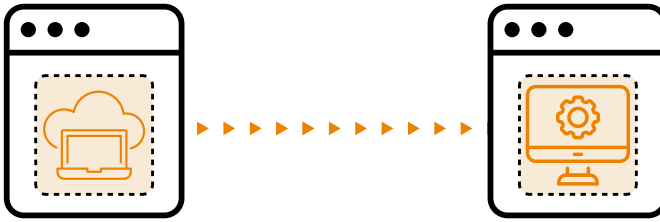
» Respeite as regras e políticas da empresa onde trabalha

Veja mais dicas no fascículo "Trabalho Remoto".

TOME CUIDADOS AO ENVIAR O COMPUTADOR PARA MANUTENÇÃO

Para evitar acessos indevidos a informações sensíveis ou perda de dados em caso de reinstalação do sistema, é importante tomar alguns cuidados ao levar seu computador para manutenção.

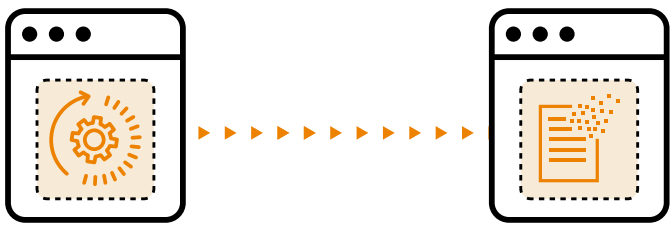
- Procure empresas com boas referências
- Faça *backup* antes, se possível
- Solicite a instalação de programas originais
- Se trocar o disco, garanta que os dados do disco antigo sejam apagados ou mantenha-o com você
  - se o disco antigo estiver cifrado, isso não é necessário
- Após a manutenção, verifique se atualizações automáticas, antivírus e *firewall* continuam ativos



APAGUE OS DADOS ANTES DE REPASSAR SEU COMPUTADOR

Vai vender, doar ou descartar seu computador? Para evitar que alguém acesse seus dados, é melhor apagar tudo antes. Se por algum motivo você não conseguir apagar o conteúdo, ter cifrado previamente o disco previne esse acesso.

- Restaure o sistema operacional e as configurações originais de fábrica
  - selecione opções para apagar todo conteúdo e sobrescrever o disco
- Caso seu sistema não tenha opções de apagar dados de forma segura, sobrescreva o disco rígido ou use ferramentas de segurança que tenham essa funcionalidade



MANTENHA DATA E HORA CORRETAS

Data e hora corretas no computador são essenciais para que recursos de seu computador, como aplicativos de verificação em duas etapas, funcionem corretamente. Ajudam também na correlação de sequência de eventos e na identificação de problemas de segurança.

- Configure seu computador para definir o horário automaticamente
- Sincronize seu computador com um servidor de horário
  - veja dicas de como fazer isso em **https://ntp.br/**

NTP significa *Network Time Protocol* ou Protocolo de Tempo para Redes. É o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede, como servidores, estações de trabalho, roteadores e outros equipamentos, a partir de referências de tempo confiáveis.

CUIDADO COM USO EM LOCAIS PÚBLICOS

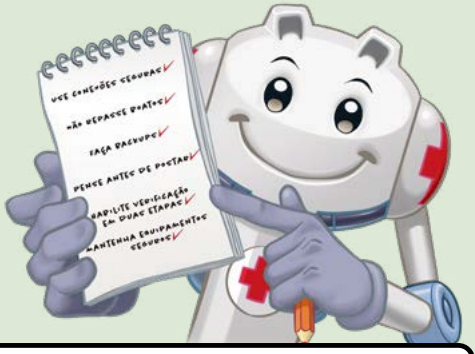
Computadores são visados por ladrões, tanto pelo valor do equipamento como pelas informações que contêm. Por isso, é importante não deixá-los sozinhos em locais públicos.

» Mantenha controle físico sobre seu computador

» Bloqueie a tela ao sair de perto do computador

» Em caso de furto ou perda:

- tente localizar, bloquear ou apagar os dados remotamente **https://icloud.com/find/** para macOS e **https://account.microsoft.com/devices/** para Windows
- faça um boletim de ocorrência



SAIBA MAIS

- Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **https://cartilha.cert.br/**
- Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores. Confira em: **https://internetsegura.br/**

cert.br

O CERT.br **(https://cert.br/)** é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br **(https://nic.br/)** é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

cgi.br

O Comitê Gestor da Internet no Brasil **(https://cgi.br/)**, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

https://cartilha.cert.br/cc/

abril / 2024