Backup

Produção:

cert.br nic.br cgi.br

FAÇA BACKUPS!

Já imaginou o que aconteceria se perdesse todos seus dados, como fotos e documentos? Seja no celular, *tablet* ou computador, não espere o pior acontecer para perceber o quanto seus dados são importantes.

Veja aqui dicas para não perder seus dados.

FAÇA BACKUPS DOS SEUS DADOS

A qualquer momento você pode perder seus dados, seja por acidente, furto, falha de sistema, atualização malsucedida ou defeito físico em seu dispositivo. Se tiver *backups*, será possível recuperá-los, reduzindo os transtornos.

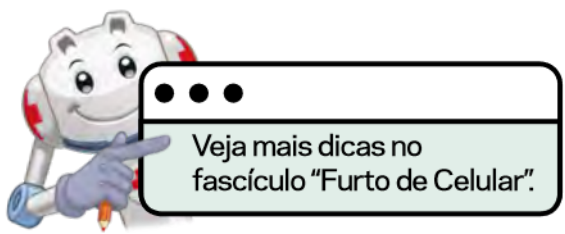
» Utilize uma ou mais opções, como:

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

NÃO ESQUEÇA DOS BACKUPS DO CELULAR

Celulares são visados para furto e fáceis de serem perdidos ou danificados. O *backup* permite restaurar fotos, *e-mails*, mensagens, aplicativos e configurações, facilitando inclusive a troca do aparelho.

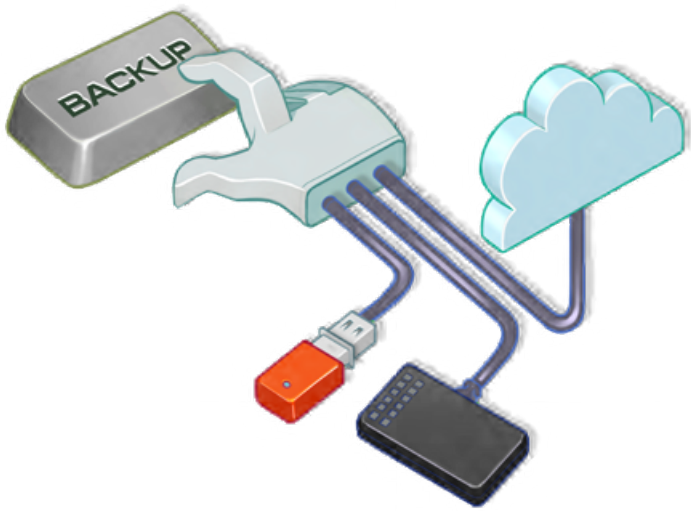
- Habilite a opção de *backup* nativa do sistema
  - configure para usar apenas Wi-Fi, se não tiver plano de dados
- Busque também outras alternativas, como *pen drive* ou sincronização com computador



HABILITE BACKUPS AUTOMÁTICOS

Backups automáticos estão menos propensos a erros e esquecimentos, o que ajuda a manter cópias atualizadas e a restaurar os dados, caso você troque ou perca seu celular ou computador.

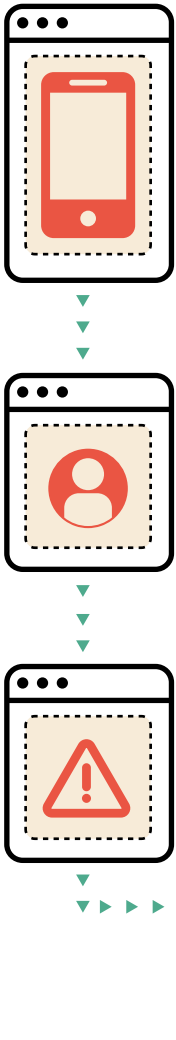
- Selecione a frequência de acordo com suas necessidades, como a cada hora, dia ou semana
- Se usar discos externos ou *pen drives*, lembre-se de conectá-los para que o *backup* seja realizado



FAÇA BACKUPS MANUAIS, EM CASOS ESPECIAIS

Em situações de risco, como viagem, atualização de sistema, envio para manutenção e troca de aparelho, complemente os *backups* automáticos com cópias manuais para garantir que arquivos importantes ou recentemente alterados tenham sido copiados.

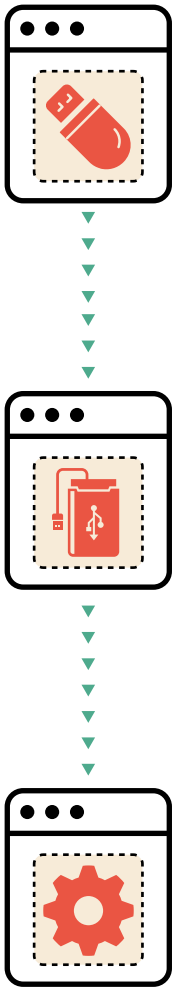
» Use opções como "Fazer *backup* agora" para garantir que seus *backups* estejam atualizados



NÃO COPIE DADOS DESNECESSÁRIOS

Dados ocupam espaço e podem exigir áreas cada vez maiores de armazenamento. Selecionar quais dados serão copiados ajuda a reduzir custos e as velocidades de cópia e restauração.

- Se possível, selecione os itens a serem excluídos dos *backups*, como arquivos e diretórios específicos
- Verifique em quais aplicativos o *backup* está ativado e desabilite os que não precisar



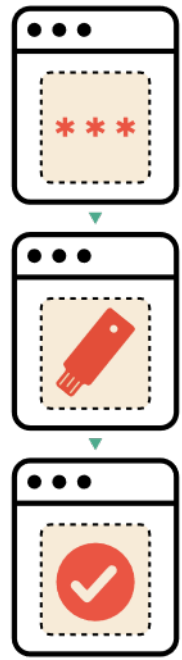
FAÇA MAIS DE UMA CÓPIA DE SEGURANÇA

A expressão "Quem tem 1 não tem nenhum" reforça a importância de ter várias cópias, pois se precisar restaurar um *backup* e ele falhar, será possível recorrer à outra cópia.

- Tenha pelo menos 2 cópias dos dados
- Armazene as cópias em locais diferentes
  - por exemplo: uma na nuvem e outra em *pen drive*

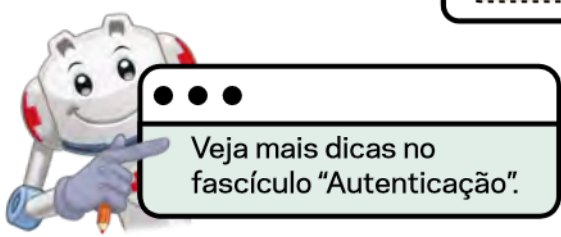
ATIVE A VERIFICAÇÃO EM DUAS ETAPAS NOS SERVIÇOS DE NUVEM

Serviços de nuvem são visados por atacantes pela grande quantidade de dados que armazenam. O uso exclusivo de senhas não é suficiente para garantir a segurança e deve ser reforçado com outras formas de autenticação.



» Escolha a opção disponível que considerar mais prática e segura, como:

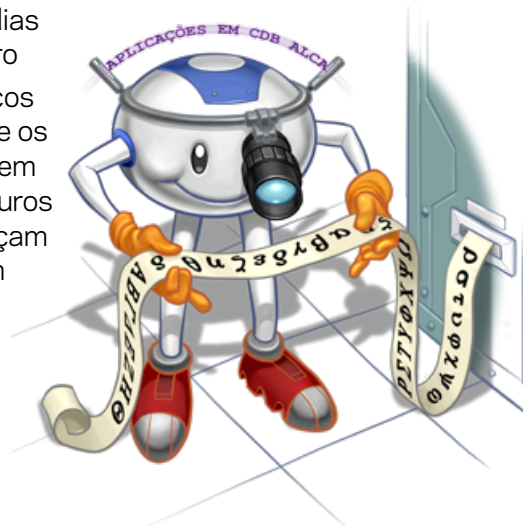
- usar uma chave de segurança física
- usar um aplicativo de celular para gerar códigos de verificação
- receber códigos por mensagem de texto ou voz



PROTEJA OS DADOS DO BACKUP CONTRA ACESSO INDEVIDO

Se as mídias não estiverem protegidas alguém pode acessar os arquivos gravados. Seus dados também podem ser indevidamente acessados se transmitidos via conexões inseguras.

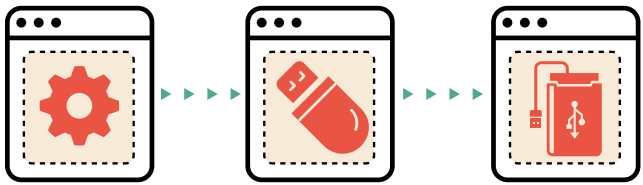
- Habilite criptografia sempre que possível
  - tanto para *backup* em nuvem como em mídias
- Não deixe as mídias conectadas o tempo todo
  - conecte-as periodicamente para fazer *backups*
- Guarde as mídias em local seguro
- Escolha serviços de nuvem onde os dados trafeguem via canais seguros (https) e ofereçam verificação em duas etapas



ACOMPANHE AS NOTIFICAÇÕES E TESTE SUAS CÓPIAS

Acompanhar as notificações do sistema e, de tempos em tempos, acessar seus *backups* evita surpresas, como arquivos corrompidos, opções mal configuradas, mídias defeituosas e áreas de armazenamento cheias.

- Verifique se as áreas de armazenamento possuem espaço disponível
- Se estiverem ficando cheias:
  - exclua *backups* antigos
  - apague arquivos desnecessários
  - aumente o tamanho da área
- Substitua as mídias com problema
- Faça um *backup* manual, para garantir uma cópia atualizada

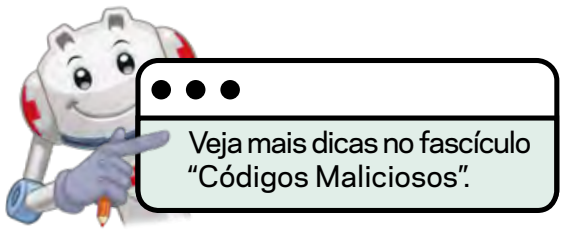


MANTENHA OS SISTEMAS E APLICATIVOS ATUALIZADOS

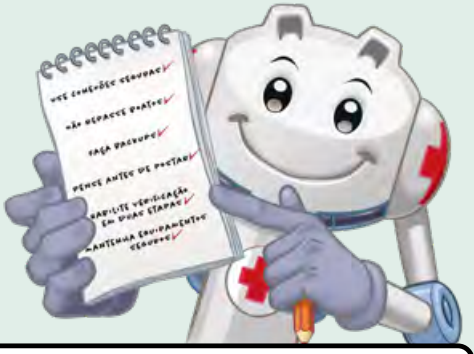
Corrigir vulnerabilidades de sistemas e aplicativos evita que elas sejam exploradas por *malware*, como o *ransomware* que cifra os dados e apaga os *backups* para que você não consiga mais recuperá-los.

» Instale atualizações regularmente
  - ative a atualização automática, sempre que possível

» Instale mecanismos de segurança, como antivírus e *firewall* pessoal, e mantenha-os atualizados



Veja mais dicas no fascículo “Códigos Maliciosos”.



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.