Manaus
Prefeitura Municipal

SUBTI – SEGURANÇA DA INFORMAÇÃO

DICAS DE SEGURANÇA

Ransomware

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR
https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt

Ransomware (1/5)

Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário

fonte: cartilha.cert.br

Ransomware (2/5)

- **Tipo de código malicioso**
  - **assim como vírus, *trojan*, *backdoor*, *worm*, *bot* e *spyware***
- **Pode infectar:**
  - **computadores**
    - como *desktop*, *notebook* e servidores
  - **equipamentos de rede**
    - como *modems*, *switches* e roteadores
  - **dispositivos móveis**
    - como *tablets*, celulares e *smartphones*

fonte: cartilha.cert.br

Ransomware (3/5)

- **Ações mais comuns**
  - **impede o acesso ao equipamento (*Locker ransomware*)**
  - **impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia (*Crypto ransomware*)**
- **Extorsão é o principal objetivo dos atacantes**
  - **pagamento feito geralmente via *bitcoins***
  - **não há garantias de que o acesso será restabelecido**
    - mesmo que o resgate seja pago
  - **normalmente usa criptografia forte**
- **Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também**

fonte: cartilha.cert.br

Ransomware (4/5)

- **Infecção pode ocorrer pela execução de arquivo infectado:**
  - **recebido:**
    - via *links* em *e-mails*, redes sociais e mensagens instantâneas
    - anexado a *e-mails*
  - **baixado de *sites* na Internet**
  - **acessado:**
    - via arquivos compartilhados
    - via páginas *web* maliciosas, usando navegadores vulneráveis

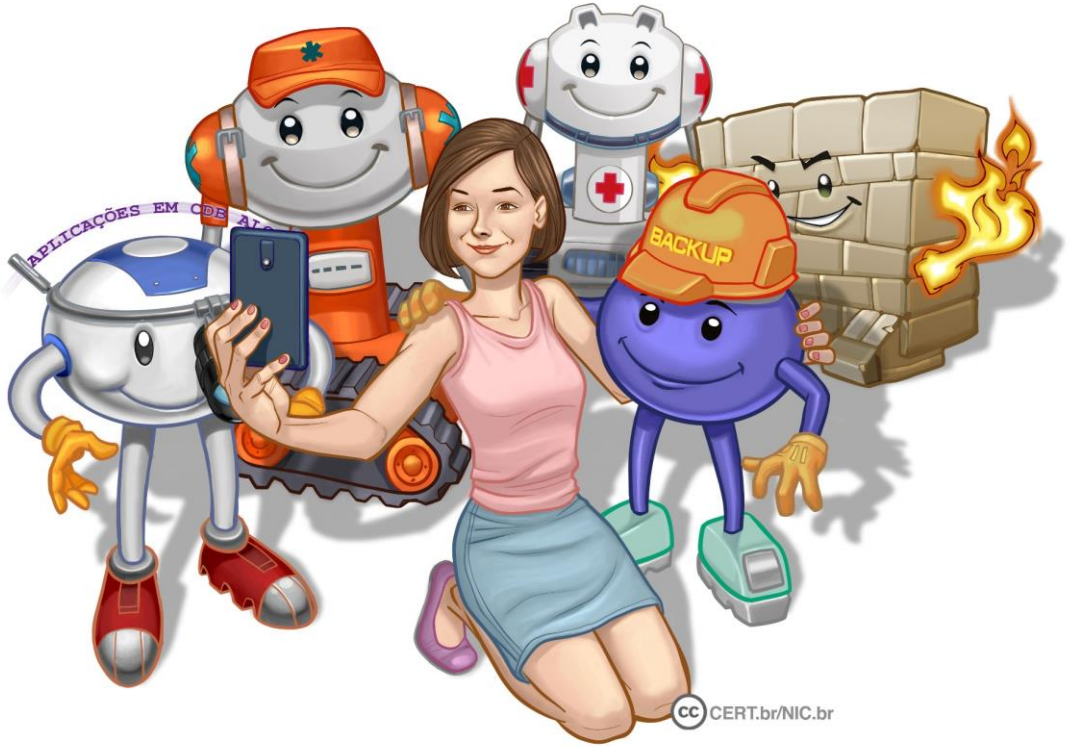
fonte: cartilha.cert.br

Ransomware (5/5)

- **Formas de propagação:**
  - **através de *e-mails* com o código malicioso em anexo ou que induzam o usuário a seguir um *link***
  - **explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança**

fonte: cartilha.cert.br

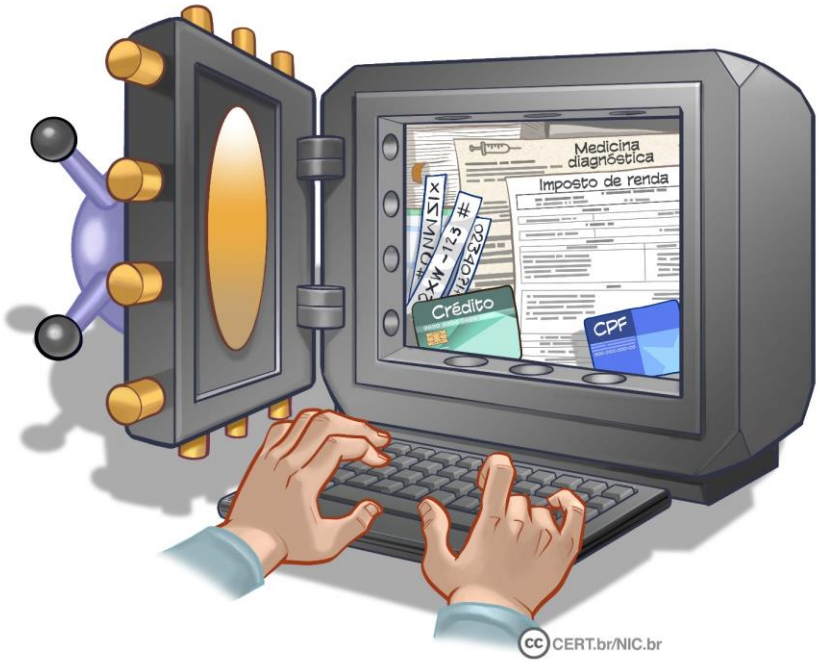
Como se prevenir



fonte: cartilha.cert.br

Não deixe que a infecção ocorra

- A melhor prevenção é impedir a infecção inicial
- Nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados



fonte: cartilha.cert.br

Faça *backups* regularmente (1/3)

Backup é a solução mais efetiva contra *ransomware*

fonte: cartilha.cert.br

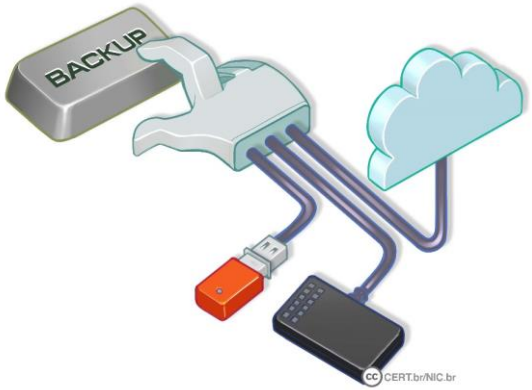
Faça *backups* regularmente (2/3)

- Mantenha os *backups* atualizados
  - de acordo com a frequência de alteração dos dados
- Configure para que seus *backups* sejam realizados automaticamente
- Certifique-se:
  - de conseguir recuperá-los
  - de que eles estejam realmente sendo feitos

fonte: cartilha.cert.br

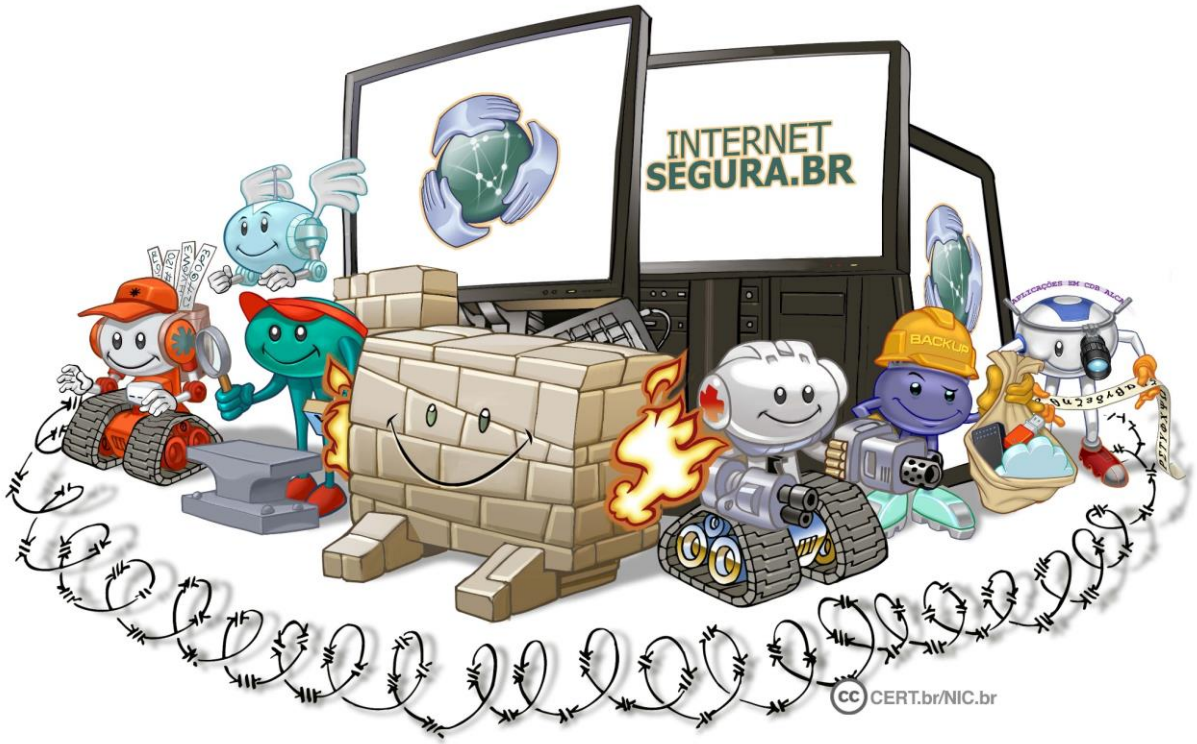
Faça *backups* regularmente (3/3)

- **Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis**
- **Mantenha os *backups* desconectados do sistema**
  - **para que não sejam também criptografados**
- **Faça cópias redundantes**
  - **para evitar perder seus dados:**
    - em incêndio, inundação, furto ou pelo uso de mídias defeituosas
    - caso uma das cópias seja infectada



fonte: cartilha.cert.br

Outros cuidados a serem tomados



fonte: cartilha.cert.br

Mantenha os equipamentos atualizados

- Tenha sempre as versões mais recentes dos programas
- Remova os programas que não usa mais, eles tendem a:
  - ser esquecidos
  - ficar com versões antigas e potencialmente vulneráveis
- Configure a atualização automática dos programas
  - atualizações devem ser baixadas e aplicadas em horários em que o equipamento esteja ligado e conectado à Internet
- Cheque periodicamente por novas atualizações usando as opções disponíveis nos programas
- Use apenas programas originais

fonte: cartilha.cert.br

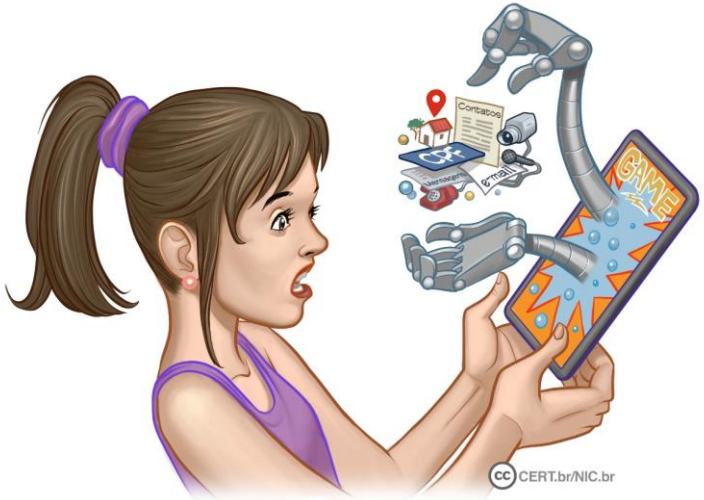
Use mecanismos de proteção

- **Instale um antivírus (*antimalware*)**
  - **mantenha-o atualizado**
  - **configure-o para verificar automaticamente:**
    - toda e qualquer extensão de arquivo
    - arquivos anexados aos *e-mails* e obtidos pela Internet
    - discos rígidos e unidades removíveis
  - **verifique sempre os arquivos recebidos antes de abri-los ou executá-los**

fonte: cartilha.cert.br

Ao instalar aplicativos de terceiros

- **Verifique se as permissões de instalação e execução são coerentes**
- **Selecione os aplicativos, escolhendo aqueles:**
  - **bem avaliados**
  - **com grande quantidade de usuários**

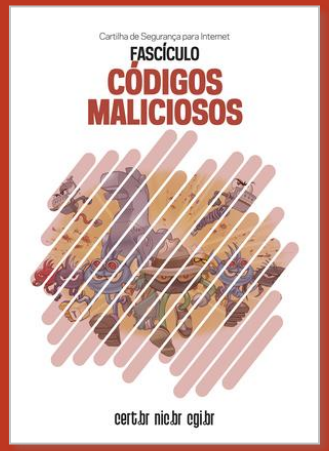


fonte: cartilha.cert.br

Créditos

- **Cartilha de Segurança para Internet**
  Fascículo Códigos Maliciosos
  Fascículo *Backup*
  cartilha.cert.br/fasciculos

- **Livro Segurança na Internet**
  cartilha.cert.br/livro



cert.br nic.br cgi.br