Backup
o básico cada vez mais essencial

Miriam von Zuben
CERT.br / NIC.br
miriam@cert.br

Qual o valor dos seus dados?

- **Difícil mensurar**
- **Vão sendo acumulados e muitas vezes são “esquecidos”**
- **Geralmente só se percebe o valor:**
  - quando já é tarde demais
  - da maneira mais difícil
- **Dados:**
  - possuem valor emocional, financeiro, acadêmico, jurídico, etc.
  - levam tempo ou são impossíveis de serem refeitos
  - são vitais para a maioria das empresas
    - perda pode levar a falência
- **Como protegê-los?**
  - impedir que as ameaças cheguem até eles

Como proteger os dados

- **Mantenha seus equipamentos seguros**
  - instale a versão mais nova do sistema operacional
  - aplique todas as atualizações
    - reinicie o equipamento sempre que solicitado
  - desabilite os serviços desnecessários
  - instale antivírus e mantenha-o atualizado
- **Adote uma postura preventiva**
  - seja cuidadoso ao abrir arquivos anexos e ao clicar em *links*
- **Realize *backups***
  - cópias de segurança
  - devem ser considerados como última linha de defesa
    - quando todas as anteriores tiverem falhado

Fonte - https://cartilha.cert.br/

Funções do *backup*

- **Recuperação de versões**
  - versão antiga de um arquivo alterado
  - imagem original de uma foto manipulada
- **Arquivamento**
  - guardar dados raramente alterados ou pouco usados
- **Proteção de dados**
  - furto/perda de equipamentos
  - problemas de *hardware*
  - atualização malsucedida de sistemas
  - falhas em aplicativos
  - apagados
    - sem querer
    - por querer (*hackers*, funcionários descontentes, *malware)*
  - sequestrados

Ransomware

- **Impede o acesso aos dados**
  - criptografia
  - bloqueio do equipamento (MFT, MBR)
- **Exemplos:**
  - CryptoLocker, Cryptowall, WannaCry, Petya
- **Costuma**
  - procurar por extensões típicas de *backup*
    - .back, .bak, .tar, .zip, .gz, .rar
  - cifrar também *backups* na nuvem

Ransomware

- **O que fazer se for infectado?**
  - tente recuperar com alguma ferramenta (e cruze os dedos) ☹
  - esqueça os dados e se conforme ☹
  - pague o resgate ☹☹
    - não garante a recuperação total
    - pode não haver comunicação com o atacante
      - por exemplo, conta de *e-mail* desativada
    - incentivo ao crime
      - pode levar a outros pedidos de extorsão
  - **recupere o *backup*** ☺☺☺

Não basta ter um *backup*

- **Ele deve ser adequado as suas necessidades**
  - garantir a segurança dos seus dados
  - adequar-se aos seus objetivos
- **Conheça as opções existentes**
  - *backups* inadequados podem resultar em:
    - perdas
    - gastos excessivos
    - esforços desnecessários (operacional)
- **Não existe uma politica de *backup* pré-determinada**
  - o que copiar? onde copiar? quando copiar? como copiar?
  - depende dos recursos e do valor dos dados para cada um

O que copiar

- **Somente dados**
  - confiáveis
  - realmente importantes
    - binários (executáveis e bibliotecas) devem ser evitados
      - podem conter cavalos de troia ou arquivos corrompidos, que serão recuperados na reinstalação
    - crie uma lista de arquivos que não serão copiados

- **Todo o sistema (imagem)**
  - sistema operacional, programas instalados, configurações, dados

Onde copiar

- ***Off-line***
  - mídias
    - *pen-drive*, CD, DVD, Blu-Ray, disco (interno e externo), cartão SD, fita, etc.

- ***Online***
  - nuvem (*cloud*)
  - *datacenter*
  - na rede:
    - discos de rede
    - área compartilhada

Off-line – Mídias

- **Cuidado com mídias obsoletas**
  - como recuperar disquetes e CDs????
    - dificuldade de encontrar leitores
    - tempo de vida útil limitado
- **Mantenha as mídias etiquetadas e nomeadas**
  - com informações que facilitem a localização
  - especificando o tipo do dado armazenado e a data de gravação
- **Cuidado ao descartar as mídias**
  - privacidade
  - confidencialidade das informações

Off-line – Armazenagem das mídias

- **Local**
  - ideal para recuperação rápida (mídia facilmente acessível)
  - mantenha as mídias em lugar:
    - seguro e com acesso restrito
      - à prova de fogo e protegido contra furto e pessoas não autorizadas
    - bem condicionados
      - proteção contra agentes nocivos naturais (poeira, calor, umidade)
- **Remoto (*off-site*)**
  - garante a disponibilidade, em caso de problemas nas instalações
  - velocidade de envio depende de:
    - frequência e tempo de restauração
    - finalidade: arquivamento (mídia pode estar distante)
  - pode comprometer a confidencialidade e integridade
    - criptografar e gerar *checksum* antes de enviar
    - verificar o *checksum* antes da restaurar

Online – Na rede

- **Lembre-se sempre de gravar na área ou disco compartilhado**
  - outras áreas provavelmente não serão copiadas
- **Faça uso consciente dos recursos**
  - copie apenas o que for necessário
  - sistemas de cotas ajudam a controlar o mau uso
    - mas devem ser de acordo com a necessidade
    - o que custa mais? os dados ou a compra de mais/maiores discos?

- ***Notebooks*:**
  - lembre-se de realizar o *backup* sempre que ficar períodos desconectados da rede (viagens a trabalho, férias, etc.)

Online – Backup na Nuvem

- **Atenção às senhas**
  - crie senhas bem elaboradas
  - evite a reutilização de senhas
  - ative a verificação em duas etapas
- **Não confunda:**
  - sistemas de armazenamento em nuvem
    - armazenam arquivos na nuvem
      - mas não necessariamente fazem *backup*
      - apesar de poderem ser usados para tal
    - oferecem facilidade de acesso
    - exemplos: OneDrive, Amazon Cloud Drive, Dropbox, iCloud, Google Drive
  - serviços de *backup* em nuvem
    - fazem cópia dos arquivos na nuvem
    - exemplos: Azure Backup, Amazon S3 ou Glacier, iCloud, Google Drive

Off-line ou *Online*

"There are two kinds of people in the world:
those who have had a hard drive failure,
and those who will"
Peter Krogh

- **Quantas cópias manter?**
  - "quem tem um não tem nenhum"
- **Onde armazenar as cópias?**
- **Regra 3-2-1**
  - tenha pelo menos três cópias dos dados (uma primária e 2 *backups*)
  - armazene as cópias em duas mídias diferentes
  - mantenha ao menos uma das cópias *off-site* (ou ao menos *off-line*)

Como fazer

- **Programe *backups* automáticos**
  - *backups* manuais estão mais propensos a erros e esquecimento
  - certifique-se de que eles estão realmente sendo feitos
- **Podem ser feitos via:**
  - programas integrados ao sistema operacional
  - aplicativos específicos
  - programas específicos da mídia usada
  - ferramentas
    - desenvolvidas internamente
    - de terceiros
- **Soluções simples**
  - enviar uma cópia por *e-mail* pode ser suficiente
  - andar com um *pen-drive*

Periodicidade

- **Mantenha os *backups* atualizados**
- **Conforme a frequência de criação ou modificação**
  - quantos dados você está disposto a perder?
  - quanto maior a frequência:
    - menor será a perda de dados
    - maiores serão os gastos
    - mais complexa poderá ser a recuperação
- **Faça cópias sempre que houver indícios de risco iminente**
  - mal funcionamento, mensagens de *logs* sobre falhas
  - atualização de sistemas
  - envio a serviços de manutenção
  - grandes alterações no sistema
    - adição de *hardware*, atualização do sistema operacional, etc.

Tipos de *backups*

Tipo	Descrição	Vantagens	Desvantagens
Completo	Copia todos os dados; serve como referencial para os demais tipos	Mais básico e completo; cópia de todos os dados em um único conjunto de mídia; recuperação simples	Mais demorado; ocupa mais espaço
Incremental	Copia apenas os dados alterados ou criados após o último completo ou incremental	Menor volume de dados; mais rápido; ocupa menos espaço de armazenamento	Recuperação mais complexa (primeiro um completo e depois todos os incrementais)
Diferencial	Copia os dados alterados ou criados desde o último *backup* completo	Recuperação mais rápida que o incremental (precisa só do último completo enquanto o incremental precisa do completo e dos incrementais)	Ocupa mais espaço que o incremental e menos que o completo; gasta mais tempo que o incremental e menos que o completo
Progressivo	Similar ao incremental mas com maior disponibilidade dos dados	Recuperação automatizada e mais eficiente (não precisa descobrir os conjuntos a serem recuperados)	Recuperação mais lenta que o diferencial e o completo (precisa analisar diferentes conjuntos para terminar o processo)

Fonte - https://cartilha.cert.br/

Restauração / Recuperação (1/3)

"No one cares if you can back up,
only if you can recover."

W. Curtis Preston - Unix Backup and Recovery

Restauração / Recuperação (2/3)

- **Pode ser:**
  - parcial (apenas um ou mais arquivos)
  - total
    - restauração do zero
      - restaurar um *backup* de sistema completo em um equipamento sem dados
    - reinstalar e após restaurar
      - instalar o sistema operacional básico e recuperar os dados
- **Quando for necessário restaurar um sistema:**
  - isole a máquina da rede
  - caso o sistema tenha sido comprometido
    - revise a configuração após a restauração
    - certifique-se de que não tenha ficado alguma porta de entrada previamente instalada pelo invasor

Restauração / Recuperação (3/3)

- **Testes**
  - **não deixe para perceber o erro quando já for tarde**
  - ***backups* devem ser verificados:**
    - logo após serem gerados
    - posteriormente, em intervalos regulares
    - não apenas para satisfazer auditorias
  - **testes periódicos evitam surpresas**
    - dados corrompidos
    - mídia ou formato obsoleto
    - programas mal configurados
    - cadê o programa de recuperação?

Retenção

- **Por quanto tempo devem ser armazenados**
  - até quando tiver espaço?
  - para cumprir obrigações legais?

Backup na nuvem - O que considerar

- **Realização**
  - sistemas suportados
  - processo automatizado
  - espaço de armazenagem
  - restrições de arquivos (tamanho, extensão)
  - tempo estimado de transmissão de dados
- **Restauração**
  - procedimento (interface Web, aplicativo)
  - tempo (imediatamente, horas, dias)
  - capacidade de transmissão de dados
- **Armazenagem/retenção**
  - tempo que os arquivos são mantidos
  - procedimento quando não ocorre o pagamento
- **Políticas de privacidade e de segurança**
  - transmissão e armazenagem (criptografia)
- **Suporte, tempo no mercado, opiniões e referências**

Fonte - https://cartilha.cert.br/

Lembre-se

Backup

- **Deve ser considerado como última linha de defesa**
  - quando todas as anteriores falharem
- **É essencial que você:**
  - mantenha os equipamentos seguros
    - instale a versão mais nova do sistema operacional
    - aplique todas as atualizações
      - reinicie o equipamento sempre que solicitado
    - desabilite serviços desnecessários
    - instale antivírus e mantenha-o atualizado
  - adote uma postura preventiva
    - cuidado ao clicar em *links* e acessar *sites*

Fonte - https://cartilha.cert.br/

Mantenha-se informado (1/3)

Cartilha de Segurança para Internet

https://cartilha.cert.br/

RSS

https://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Mantenha-se informado (2/3)

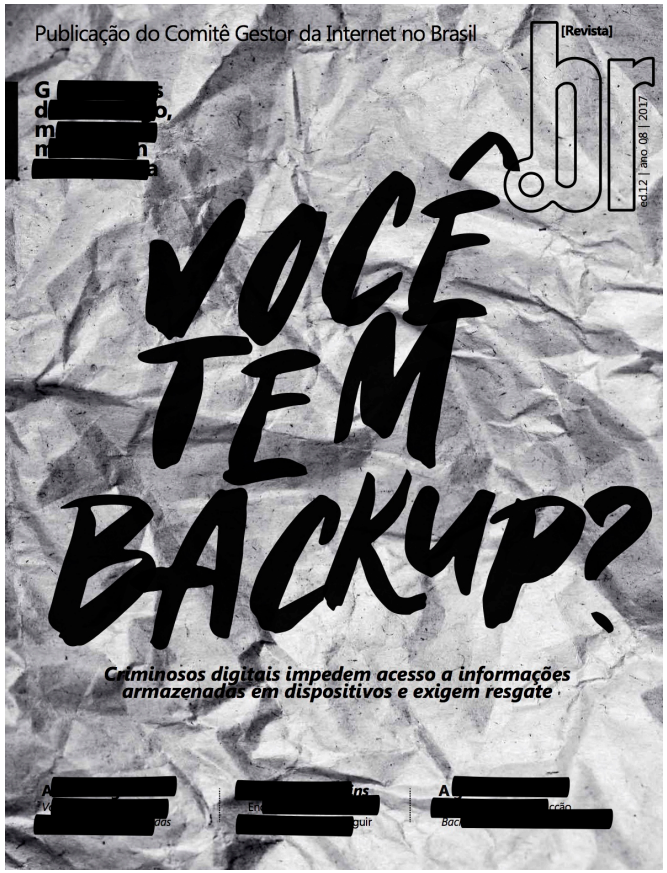
Portal Internet Segura

http://www.internetsegura.br/

Campanha Antispam.br

http://www.antispam.br/

Mantenha-se informado (3/3)



http://nic.br/publicacao/revista-br-ano-08-2017-edicao-12/
https://cartilha.cert.br/

Fonte - https://cartilha.cert.br/

Créditos

- **Cartilha de Segurança para Internet**

  https://cartilha.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

Obrigada

www.cert.br

miriam@cert.br

@certbr

15 de agosto de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br