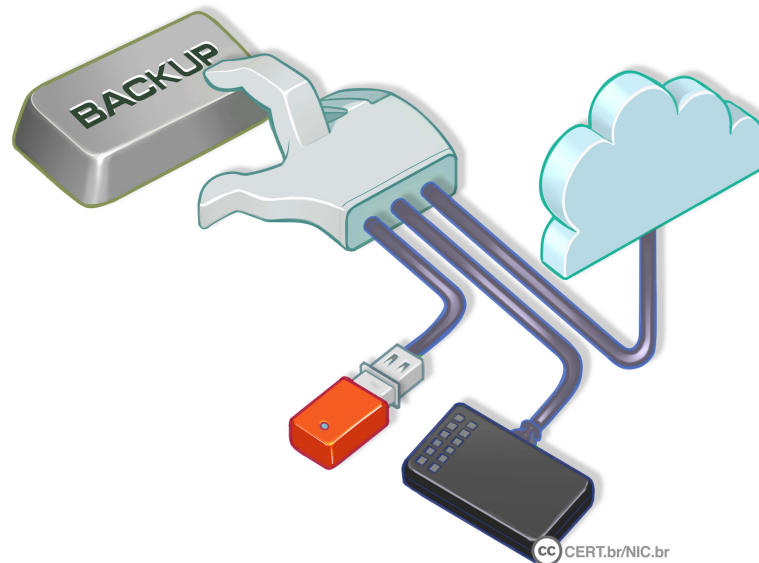


BACKUP

<Nome>
<Instituição>
<e-mail>

Agenda

- Importância dos dados
- Funções do *backup*
- Como seus arquivos podem ser perdidos
- Questões a serem consideradas
- Cuidados com *ransomware*
- Outros cuidados
- Saiba mais
- Créditos



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 e 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**
 - **fazer cópias de segurança (*backups*)**

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**

Como seus arquivos podem ser perdidos (1/2)

- **Seus arquivos podem ser accidentalmente apagados**
- **Seus equipamentos podem:**
 - **ser perdidos, furtados ou roubados**
 - **ser danificados de forma irreversível**
 - por exemplo, por umidade ou queda
 - **apresentar mau funcionamento**
 - por exemplo, uma falha no disco
 - **ser invadidos e seus arquivos apagados**



Como seus arquivos podem ser perdidos (2/2)

- **Algum aplicativo apresentar mau funcionamento**
- **Uma atualização de sistema malsucedida obrigá-lo a reinstalar seus equipamentos**
- **O servidor em que seus arquivos estão armazenados apresentar problemas**
- **Algum código malicioso infectar seus equipamentos e apagar ou cifrar todos os seus arquivos**
- **Alguém descobrir a senha:**
 - **da conta do seu repositório de arquivos, acessá-la e apagar todos seus arquivos**
 - **da sua conta de *e-mail*, acessá-la e remover todas as suas mensagens**

Questões a serem consideradas



Como fazer *backups* (1/2)

- **Você pode fazer *backups*:**
 - em mídias: *pen drives*, discos rígidos, CDs, DVDs, etc.
 - *online*: usando serviços na nuvem, em *datacenter* ou na rede
- **Você pode usar:**
 - programas integrados ao sistema operacional
 - aplicativos específicos
 - ferramentas desenvolvidas internamente
 - soluções simples, como:
 - andar com um *pen drive* na mochila
 - enviar uma cópia para seu:
 - *e-mail*
 - repositório externo de arquivos

Como fazer *backups* (2/2)

- **Programe seus *backups* para serem feitos automaticamente**
 - cópias manuais estão propensas a erros e esquecimentos
- **Certifique-se de que realmente eles estão sendo feitos**
 - não confie somente no “automático”

Cuidados ao fazer *backups* em mídias (1/2)

- Tenha cuidado para não perder seus *pen drives*
- Proteja as mídias com senhas, sempre que for possível
- Criptografe seus *backups*
 - para evitar que alguém consiga acessá-los em caso de perda
 - você pode gravar os arquivos já criptografados ou criptografar a mídia de forma que, para acessá-la, será necessário o fornecimento de senha

Cuidados ao fazer *backups* em mídias (2/2)

- **Cuidado ao descartar as mídias**
 - se os arquivos não estiverem criptografados, alguém pode tentar acessá-los, expondo:
 - a sua privacidade
 - a confidencialidade das informações
- **Mantenha as mídias:**
 - bem acondicionadas, em locais seguros, à prova de fogo e com acesso restrito
 - etiquetadas e nomeadas, com informações que facilitem a localização e especificando o tipo do arquivo armazenado e a data de gravação
- **Cuidado com mídias obsoletas**

Cuidados ao fazer *backups online* (1/3)

- **Ao usar recursos compartilhados, como discos em rede:**
 - lembre-se de fazer uso consciente, copiando apenas o que for necessário, pois outras pessoas também usarão o mesmo espaço
 - sistemas de cotas ajudam a controlar o uso mas é necessário que o tamanho da área seja de acordo com a necessidade
- **Se tiver dispositivos móveis:**
 - lembre-se de fazer *backups* sempre que eles ficarem longos períodos desconectados da rede (viagens a trabalho, férias, etc.)
- **Não confunda:**
 - serviços de *backup* na nuvem fazem cópia dos arquivos na nuvem
 - sistemas de armazenamento na nuvem gravam os arquivos na nuvem, mas não necessariamente fazem *backup*
 - apesar de poderem ser usados para tal

Cuidados ao fazer *backups online* (2/3)

- **Pontos a serem observados ao escolher serviços de *backup* na nuvem**
 - **Autenticação**
 - acesso ao sistema (se oferece opção de conexão segura, como https)
 - métodos oferecidos (sempre use a verificação em duas etapas)
 - **Realização**
 - sistemas operacionais suportados
 - possibilidade de automatização
 - restrições quanto ao tamanho e tipo de arquivos
 - tempo estimado de transmissão de dados (*upload*)
 - forma como os dados trafegam pela rede (protegidos por criptografia)
 - **Armazenagem**
 - custo, espaço de armazenagem oferecido (limitado ou ilimitado)
 - forma como os dados são armazenados (protegidos por criptografia)
 - políticas de privacidade e de segurança

Cuidados ao fazer *backups online* (3/3)

- Pontos a serem observados ao escolher serviços de *backup* na nuvem (cont.)
 - **Restauração**
 - procedimento (por meio de aplicativos ou interface *web*)
 - capacidade de transmissão de dados (*download*)
 - tempo para restauração (imediatamente, um dia, uma semana)
 - **Retenção**
 - tempo que os dados são mantidos
 - procedimento quando não ocorre o pagamento
 - **Reputação**
 - disponibilidade do serviço (quantidade de interrupções)
 - suporte oferecido, tempo no mercado, opinião dos demais usuários
 - outras referências

Onde guardar os *backups* (1/2)

- **Você pode guardar seus *backups*:**
 - **localmente**
 - recuperação mais rápida, já que os arquivos estão próximos
 - não protege em caso de acidentes naturais
 - **remotamente (*off-site*)**
 - garante a disponibilidade em caso de problemas no local onde estão os arquivos originais
 - a recuperação pode ser mais demorada
 - depende da velocidade da rede ou da distância do local onde as mídias estão armazenadas
 - pode comprometer a confidencialidade e integridade dos dados, caso não estejam criptografados
 - o acesso às mídias é mais difícil de ser controlado

Onde guardar os *backups* (2/2)

- Siga a regra “**3 – 2 – 1**”, que consiste em:
 - ter pelo menos **3** cópias dos dados (a original e 2 *backups*)
 - armazenar as cópias em **2** tipos diferentes de mídias
 - manter ao menos **1** das cópias remota (ou ao menos *off-line*)
- Cópias *off-line* são aquelas que estão desconectadas do sistema principal quando não estão sendo usadas
- Para tentar detectar alterações indevidas em uma mídia:
 - gere os *hashes* dos arquivos antes de enviá-la para locais remotos
 - gere-os novamente antes de restaurá-los
 - se os dois *hashes* forem iguais, conclui-se que o arquivo não foi alterado
 - caso contrário, pode ser um forte indício de que o arquivo esteja corrompido ou foi modificado

O que copiar

- **Você pode copiar:**
 - **apenas arquivos**
 - ocupa menos espaço (pode ser feito diariamente)
 - fácil recuperação
 - **tudo (imagem do sistema)**
 - incluindo sistema operacional, programas, configurações e arquivos
 - facilita a substituição de equipamentos
 - não é indicado para proteger arquivos constantemente alterados
 - ocupa muito espaço e a restauração é mais complexa
- **Copie apenas os arquivos confiáveis e importantes**
- **Faça uma imagem do sistema quando:**
 - substituir seus equipamentos ou fizer alterações que possam comprometê-lo

Quando copiar

- **Mantenha seus *backups* atualizados**
- **Faça cópias periódicas**
 - **conforme a frequência de criação e modificação dos arquivos**
 - arquivos frequentemente modificados podem ser copiados diariamente
 - arquivos pouco alterados podem ser copiados semanalmente ou mensalmente
- **Para determinar a frequência adequada tente se perguntar:**
“Quantos dados estou disposto a perder?”
 - **encontre um equilíbrio entre copiar demais e perder dados**
- **Faça cópias sempre que houver indícios de risco iminente**
 - **por exemplo: mau funcionamento, alerta de falhas, atualização de sistemas, envio a serviços de manutenção**

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 <i>backup</i> 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 <i>backup</i> 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

Como recuperar os arquivos

- **A recuperação pode ser:**
 - parcial: quando um ou mais arquivos são recuperados
 - total: quando todos os arquivos são recuperados
- **Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis**
- **Para recuperar totalmente (do zero) um equipamento:**
 - use uma imagem do sistema previamente feita
- **Se precisar recuperar um sistema invadido:**
 - isole-o da rede
 - revise a configuração
 - certifique-se de que não tenha ficado nenhuma porta de entrada incluída pelo invasor

Como saber se o *backup* está funcionando

- **Testes evitam surpresas, como:**
 - dados corrompidos, mídia ou formato obsoleto
 - programas mal configurados
 - falta do programa de recuperação
- **Teste seus *backups*:**
 - periodicamente
 - logo após terem sido gerados

**Não deixe para perceber falhas quando
já for tarde demais**

Por quanto tempo manter os *backups*

- O tempo de retenção depende do tipo do arquivo copiado
 - fotos e vídeos, provavelmente, serão guardados para sempre (possuem valor emocional)
 - trabalhos de escola, talvez, possam ser descartados (ficam ultrapassados)
- Mantenha seus *backups*:
 - pelo tempo que os arquivos tiverem valor ou utilidade
 - enquanto não tiver problemas de espaço
- Lembre-se de identificar seus *backups*:
 - com informações que ajudem a localizar o tipo do arquivo armazenado e a data de gravação
 - a identificação ajuda a selecionar o que será apagado, caso necessário

Cuidados com *ransomware*



CC CERT.br/NIC.br



fonte: cartilha.cert.br

Ransomware (1/3)

- 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
- 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

Ransomware (2/3)

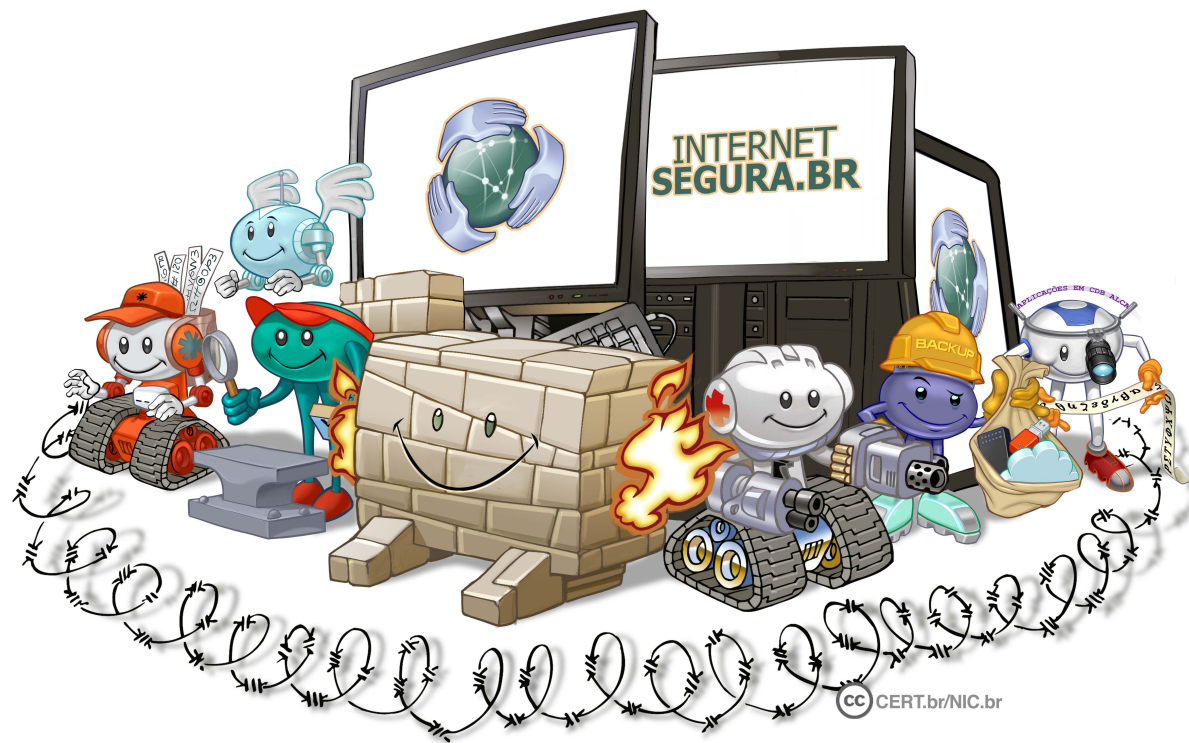
- **Além de cifrar os arquivos, também costuma:**
 - cifrar *backups* na nuvem
 - procurar por arquivos com extensões típicas de *backup* (back, .bak, .tar, .zip, .gz, .rar) e removê-los ou cifrá-los
 - buscar por outros equipamentos conectados e cifrá-los também
- **Se seu equipamento for infectado, o *backup* é a única garantia de que você conseguirá recuperar seus arquivos**
 - o pagamento do resgate
 - não garante que o acesso será restabelecido
 - pode incentivar o crime
 - pode levar a novos pedidos de extorsão

Ransomware (3/3)

- **Proteja seus *backups***
 - mantenha os *backups* desconectados dos seus equipamentos
 - desabilite o compartilhamento de arquivos, se não for necessário
 - escolha serviços de nuvem que ofereçam proteção *antiransomware* e habilite a verificação em duas etapas sempre que possível



Outros cuidados



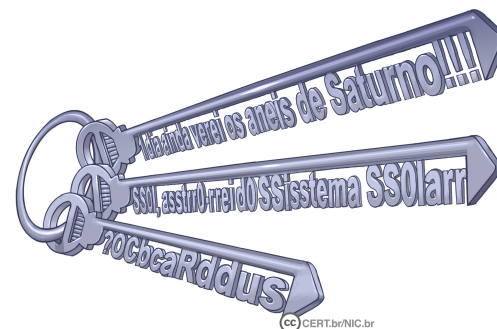
Proteja seus equipamentos

- **Backup** deve ser considerado como última linha de defesa
 - quando todas as anteriores falharem
- **Mantenha os equipamentos seguros**
 - instale a versão mais nova do sistema operacional
 - aplique as atualizações e reinicie o equipamento quando solicitado
 - desabilite serviços desnecessários
 - instale e mantenha atualizados mecanismos de segurança
 - antivírus, *antiransomware* e firewall pessoal



Proteja suas senhas

- **Procure usar senhas com:**
 - grande quantidade de caracteres
 - diferentes tipos de caracteres
- **Não utilize:**
 - dados pessoais, como nome, sobrenome e datas
 - dados que possam ser facilmente obtidos sobre você
- **Evite reutilizar suas senhas**
- **Troque periodicamente suas senhas**
- **Não informe senhas via *e-mails* ou telefonemas**
- **Use a verificação em duas etapas, sempre que disponível**

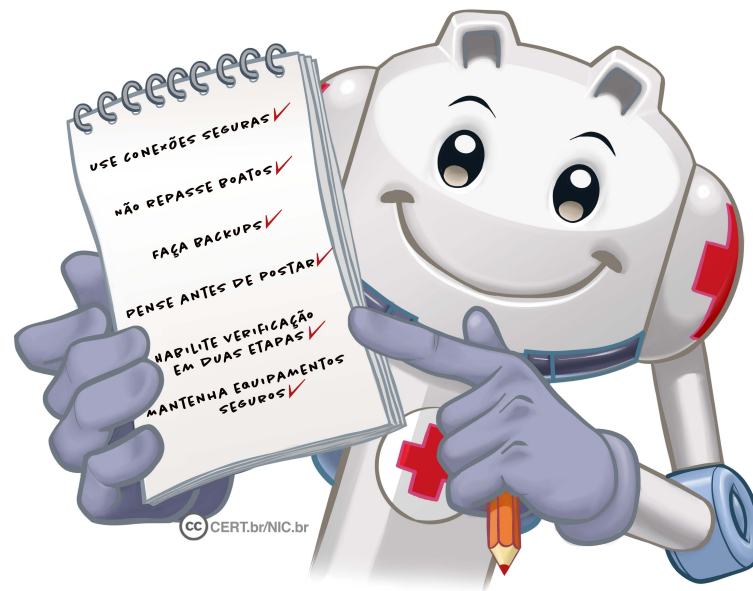


Adote uma postura preventiva

- **Seja cuidadoso ao abrir arquivos anexos e ao clicar em *links***
- **Não repasse correntes nem mensagens contendo ofertas e promoções**
 - elas podem conter *links* para *sites* falsos (*phishing*) ou instalar códigos maliciosos
- **Seja cuidadoso ao clicar em *links***
 - independente de quem os enviou
- **Não considere que mensagens vindas de conhecidos são sempre confiáveis**
 - quem enviou pode não ter verificado o conteúdo, o campo de remetente pode ter sido falsificado e elas podem ter sido enviadas de contas falsas ou invadidas

Saiba mais

- Consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet: cartilha.cert.br
- Confira os demais materiais sobre segurança para os diferentes públicos: internetsegura.br
- Acompanhe novidades e a dica do dia no Twitter do CERT.br twitter.com/certbr



Créditos

- Cartilha de Segurança para Internet
Fascículo *Backup*
cartilha.cert.br/fasciculos
- Livro Segurança na Internet
cartilha.cert.br/livro



cert.br nie.br egi.br