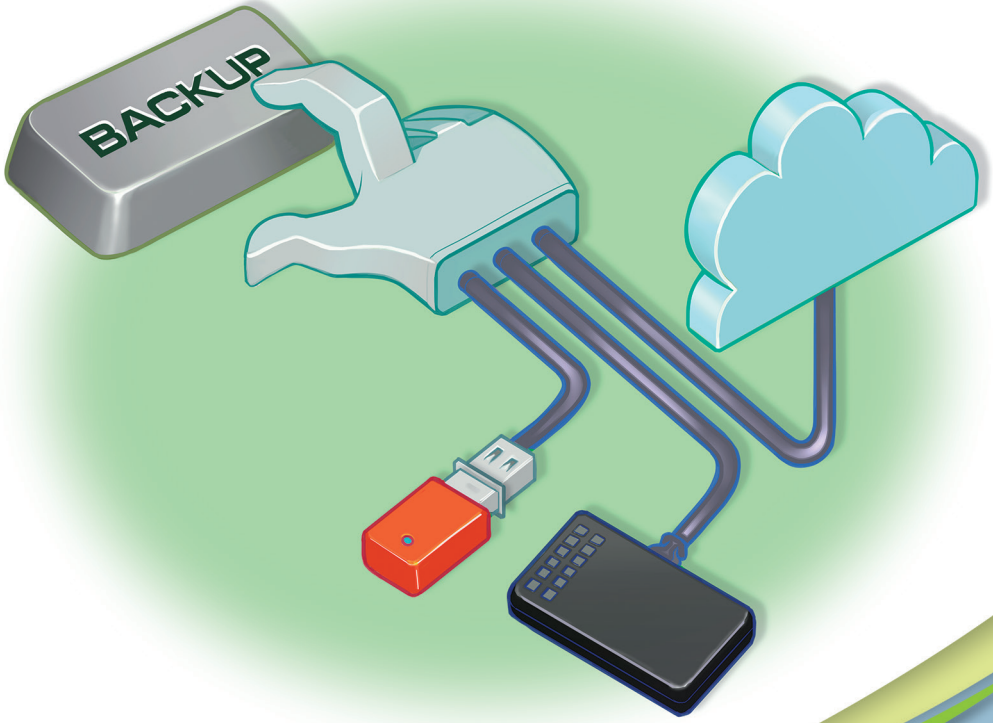
Publicação cert.br

Cartilha de Segurança para Internet

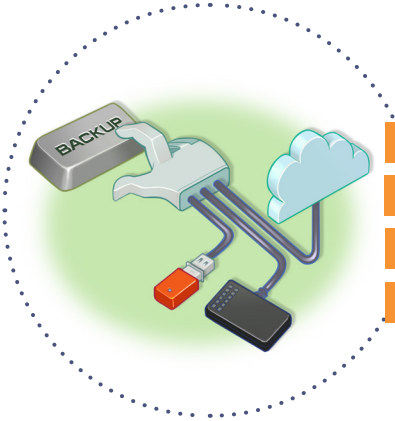
Fascículo Backup



https://cartilha.cert.br/

nic.br

cgi.br



Você já imaginou o que aconteceria se, de uma hora para outra, perdesse alguns ou até mesmo todos os arquivos armazenados nos seus equipamentos?

Você já parou para pensar no valor dos seus arquivos? Qual é a importância deles para você? Não é nada fácil responder essas questões pois, com o passar do tempo, acumulamos tantos vídeos, imagens, músicas, documentos, *e-mails* e mensagens que já nem nos lembramos de todos eles. Geralmente, só quando o pior acontece e já é tarde demais para recuperar nossos arquivos, é que percebemos o quanto eles são essenciais para nós.

Para evitar perder seus dados é preciso que você mantenha seus equipamentos seguros e adote uma postura preventiva, o que inclui, entre outras coisas, fazer cópias de segurança dos seus arquivos, ou seja, realizar ***backups***.

O *backup* permite que você:

- ✓ recupere seus arquivos em situações inesperadas, como acidentes e infecção por códigos maliciosos;
- ✓ recupere versões antigas, como a versão original de um arquivo que você alterou ou de uma imagem que você manipulou;
- ✓ arquive aquilo que você deseja ou que precisa guardar, mas que não é necessário no seu dia a dia e que raramente é alterado.

Para fazer *backups* que garantam a segurança dos seus arquivos e que sejam adequados às suas necessidades, é importante que você conheça as opções existentes e tente responder algumas questões, como:

- ✓ quantas cópias devo fazer?
- ✓ quais arquivos devo copiar?
- ✓ onde os arquivos devem ser copiados?
- ✓ qual opção melhor me atende?

Não existem respostas certas, já que elas dependem dos recursos disponíveis, da quantidade de arquivos e da importância dos dados para cada um.

A seguir apresentamos algumas dicas para tentar ajudá-lo a criar uma solução que melhor se adapte às suas necessidades.

Lembre-se: Não precisa ser nada complicado, o importante é fazer *backups*.

Como os arquivos *podem ser perdidos*

Infelizmente há situacões em que seus arquivos podem ser perdidos, tais como:

- ✓ seus arquivos serem acidentalmente apagados;
- ✓ seus equipamentos serem perdidos, furtados ou roubados;
- ✓ seus equipamentos serem danificados de forma irrecuperável (por exemplo, por umidade ou queda);
- ✓ seus equipamentos apresentarem mau funcionamento (por exemplo, uma falha no disco);
- ✓ seus equipamentos serem invadidos e seus arquivos apagados;
- ✓ 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;
- ✓ alguém descobrir a senha da sua conta de *e-mail*, acessá-la e remover todas as suas mensagens.

Como fazer *backups*?

Para fazer *backups* você pode usar programas integrados ao sistema operacional, aplicativos específicos, ferramentas desenvolvidas internamente ou, ainda soluções simples, como andar com um *pendrive* na mochila e enviar uma cópia para seu *e-mail* ou repositório externo de arquivos. Às vezes, basta pesquisar na Internet ou recorrer à "Central Ajuda" ou ao "*Help*" do sistema que você usa para descobrir as soluções disponíveis.

- ✓ **Programe seus *backups* para serem feitos automaticamente, já que cópias manuais estão mais propensas a erros e esquecimentos.**

- ✓ **Certifique-se de que realmente os seus *backups* estão sendo feitos, não confie somente no "automático".**

Você pode fazer *backups*:

- em mídias, como *pendrives*, discos rígidos, CDs, DVDs e discos de *Blu-ray*;
- *on-line*, usando serviços na nuvem (*cloud*), em datacenter ou na rede.

A escolha de como fazer depende do tipo do seu equipamento (se é um *notebook*, *desktop*, celular, *tablet*, etc.), do aplicativo que será usado e de questões como conectividade, capacidade de armazenamento, custo e confiabilidade. Por exemplo:

- *backups* na nuvem podem ser muito práticos, mas dependem de conectividade e podem consumir muita banda de rede;
- *backups* em rede podem ser simples, mas, geralmente, dependem do equipamento estar fisicamente conectado a uma rede específica, o que pode ser difícil em caso de ausências prolongadas;
- CDs podem bastar para pequenas quantidades de dados, mas, atualmente, é cada vez mais difícil encontrar gravadores e leitores deste tipo de mídia;
- *pendrives* oferecem portabilidade, podem ser indicados para arquivos constantemente modificados e ajudam a liberar espaço nos dispositivos (há modelos especiais para celulares e *tablets* que possuem aplicativos de gerenciamento de arquivos que permitem fazer *backup*) mas podem ser facilmente perdidos;
- discos rígidos podem ser usados para grandes volumes de dados, mas podem apresentar falhas.

- Cuidados ao fazer *backups* em mídias:
  - tenha cuidado para não perder seus *pendrives*;
  - 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.
  - cuidado ao descartar as mídias, pois, se os arquivos não estiverem criptografados, alguém pode tentar acessá-los, expondo a sua privacidade e a confidencialidade das informações;
  - mantenha as mídias em locais seguros, à prova de fogo, bem acondicionados (longe de poeira, calor ou umidade) e com acesso restrito (apenas de pessoas autorizadas);
  - mantenha as mídias 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, pois com o tempo torna-se cada vez mais difícil encontrar leitores e elas possuem tempo de vida útil limitado.

- Cuidados ao fazer *backups on-line:*
  - 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. Afinal, o que custa mais? Os dados ou a compra de discos maiores ou de mais discos?
  - 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

Os serviços de *backup* na nuvem fazem cópia dos arquivos na nuvem. Os sistemas de armazenamento na nuvem gravam os arquivos na nuvem, mas não necessariamente fazem *backup* (apesar de poderem ser usados para tal).

Cuidados ao escolher serviços de *backup* na nuvem

Antes de escolher um serviço de *backup* na nuvem você deve observar alguns pontos, como por exemplo:

- ✓ 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
- ✓ 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*?

Você pode guardar seus *backups* localmente (no mesmo local dos arquivos originais) ou remotamente (*off-site*).

- ✓ Armazenamento local:
  - a recuperação é mais rápida já que os arquivos estão próximos;
  - não protege em caso de acidentes naturais (como incêndio e inundações), pois tanto a cópia como os originais podem ser perdidos.

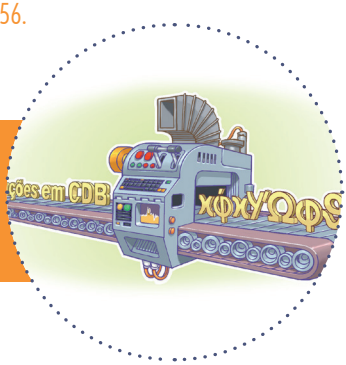
- ✓ Armazenamento remoto:
  - garante a disponibilidade em caso de problemas no local onde estão os arquivos originais;
  - a recuperação pode ser mais demorada, pois depende da velocidade da rede ou da distância do local onde as mídias estão armazenadas;
  - pode comprometer a confidencialidade e integridade dos dados, caso não estejam criptografados, pois o acesso às mídias é mais difícil de ser controlado.

- ✓ 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. Pode ser um *pendrive* que só é colocado no momento da cópia ou até um serviço de nuvem que apenas é conectado quando necessário.

- ✓ Para tentar detectar alterações indevidas em uma mídia, gere os *hashes** dos arquivos antes de enviá-la para locais remotos e gere-os novamente antes de restaurá-los.
  - se os dois *hashes* forem iguais então você pode concluir que o arquivo não foi alterado;
  - caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado;
  - exemplos de métodos de *hash* são SHA-1 e SHA-256.

* *Hash* é o resultado único e de tamanho fixo gerado quando uma função de resumo (tipo de método criptográfico) é aplicada sobre uma informação.



O que copiar?

Apenas arquivos: Geralmente é o mais comum, já que pode ser feito diariamente, ocupa menos espaço e a recuperação é mais fácil.

- ✓ **Copie apenas os arquivos confiáveis e importantes.**
- ✓ **Evite copiar arquivos do sistema ou de aplicativos, pois eles podem ser facilmente reinstalados posteriormente.**

Tudo (imagem do sistema): Incluindo sistema operacional, programas instalados, configurações e arquivos. Facilita a substituição de equipamentos, mas não é indicada para proteger arquivos constantemente alterados, já que ocupa muito espaço e a restauração é mais complexa.

- ✓ **Faça uma imagem do sistema quando for substituir seus equipamentos ou fazer alterações que possam comprometê-los.**

Quando copiar?

- ✓ **Mantenha seus *backups* atualizados, fazendo cópias periódicas, de acordo com a frequência com que você cria ou modifica seus arquivos.**
  - arquivos frequentemente modificados devem 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?"**
  - fazer *backups* pode ser trabalhoso e custoso, por isso é importante encontrar um equilíbrio entre copiar demais e perder dados.
- ✓ **Faça cópias sempre que houver indícios de risco iminente, como mal funcionamento, alerta de falhas, atualização de sistemas, envio a serviços de manutenção, grandes alterações no sistema e adição de *hardware*, etc.**

Para tentar otimizar as cópias você pode escolher entre os diferentes **tipos de *backups*:**

- *Backup* completo, total ou *full*: Copia todos os arquivos.
- *Backup* incremental: Copia apenas os arquivos alterados ou criados após o último *backup* completo, incremental ou diferencial.
- *Backup* diferencial: Copia os arquivos alterados ou criados após o último *backup* completo (diferente do incremental que se baseia no último *backup*, independente do tipo).

Uma politica de proteção bastante comum é fazer um *backup* completo pelo menos uma vez por semana e nos demais dias fazer *backups* incrementais.

Como recuperar os arquivos?

A recuperação de um *backup* pode ser parcial (quando um ou mais arquivos são recuperados) ou total (quando todos arquivos são recuperados).

- ✓ Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis.
- ✓ Para recuperar totalmente (do zero) um equipameno você pode usar uma imagem do sistema previamente feita.
- ✓ Se precisar recuperar um sistema invadido, isole-o da rede, revise a configuração e certifique-se de que não tenha ficado alguma porta de entrada incluida pelo invasor.

Como saber se o *backup* está funcionando?

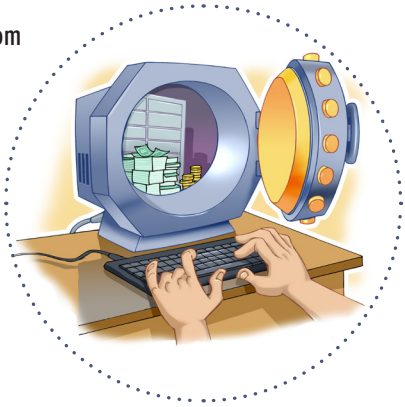
Testes evitam surpresas, como dados corrompidos, mídia ou formato obsoleto, programas mal configurados ou falta do programa de recuperação. Não deixe para perceber falhas quando já for tarde demais.

- ✓ Teste seus *backups* periodicamente e logo após eles terem sido gerados.

Por quanto tempo deve-se manter os *backups*?

O tempo de retenção dos *backups* depende do tipo de cada arquivo que foi copiado. Suas fotos e seus vídeos, provavelmente, você vai querer guardar para sempre, pois possuem valor emocional. Seus trabalhos de escola, talvez, você queira se desfazer após um tempo, pois o conteúdo vai ficando ultrapassado.

- ✓ Mantenha seus *backups* pelo tempo que os arquivos tiverem valor ou utilidade para você ou 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, pois isso ajuda a selecionar o que será apagado em caso de necessidade.



Cuidados com *ransomware*

O *ransomware* é um tipo de código malicioso 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.

As formas mais comuns de propagação de *ransomware* são:

- 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.

Além de cifrar os arquivos, o *ransomware* também costuma:

- cifrar *backups* na nuvem;
- procurar por arquivos com extensões típicas de *backup*, como .bak, .zip, .gz e .rar;
- buscar por outros equipamentos conectados, locais ou em rede, e criptografá-los também.

Se seu equipamento for infectado por *ransomware* a única garantia de que você conseguirá acessar novamente seus arquivos é possuir *backups* atualizados. O pagamento do resgate não garante que o acesso será restabelecido e ainda pode incentivar o crime e levar a novos pedidos de extorsão. Por isso é importante que você proteja seus *backups*:

- ✓ **Mantenha os *backups* desconectados dos seus equipamentos.**
- ✓ **Desabilite o compartilhamento de arquivos, se ele não for necessário.**
- ✓ **Escolha serviços de nuvem que ofereçam proteção *anti-ransomware* e habilite a verificação em duas etapas, sempre que possível.**

Proteja seus *equipamentos*

Lembre-se: O *backup* é a última linha de defesa para proteção dos seus arquivos, aquela que só deverá ser usada quando todas as demais falharem. Por isso é importante que você tome alguns cuidados para proteger seus arquivos e equipamentos.

- ✓ **Mantenha seus equipamentos seguros:**
  - instale a versão mais nova do sistema operacional e dos aplicativos usados;
  - aplique todas as atualizações e não se esqueça de reiniciar o equipamento sempre que solicitado;
  - desabilite os serviços desnecessários;
  - instale mecanismos de segurança, como antivírus, *anti-ransomware* e *firewall* pessoal, e mantenha-os atualizados.

- ✓ **Proteja suas contas de acesso:**
  - crie senhas bem elaboradas;
  - não reutilize suas senhas;
  - ative a verificação em duas etapas.

- ✓ **Adote uma postura preventiva:**
  - seja cuidadoso ao abrir arquivos anexos e ao clicar em *links*;
  - não repasse correntes e nem mensagens contendo ofertas e promoções, pois 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, pois 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.

Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre *backup* e outros mecanismos de segurança:

https://cartilha.cert.br/mecanismos/

INTERNET SEGURA.BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!
http://internetsegura.br/

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

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em www.cert.br.

nic.br
Núcleo de Informação e Coordenação do Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (www.nic.br) é uma entidade civil, sem fins lucrativos, que, entre outras atribuições, implementa as decisões e projetos do CGI.br. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (www.registro.br), estudar e tratar incidentes de segurança no Brasil - CERT.br (www.cert.br), produzir indicadores sobre as tecnologias da informação e da comunicação - Cetic.br (www.cetic.br), promover a interconexão direta entre redes por meio de pontos de troca de tráfego Internet - IX.br (www.ix.br), estudar e pesquisar tecnologias de redes e operações - Ceptro.br (www.ceptro.br), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web - Ceweb.br (www.ceweb.br) e abrigar o escritório do W3C no Brasil (www.w3c.br).

cgi.br
Comitê Gestor da Internet no Brasil

O Comitê Gestor 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. Com base nos princípios de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (www.cgi.br/principios). Mais informações em www.cgi.br.

dezembro / 2017