BACKUP

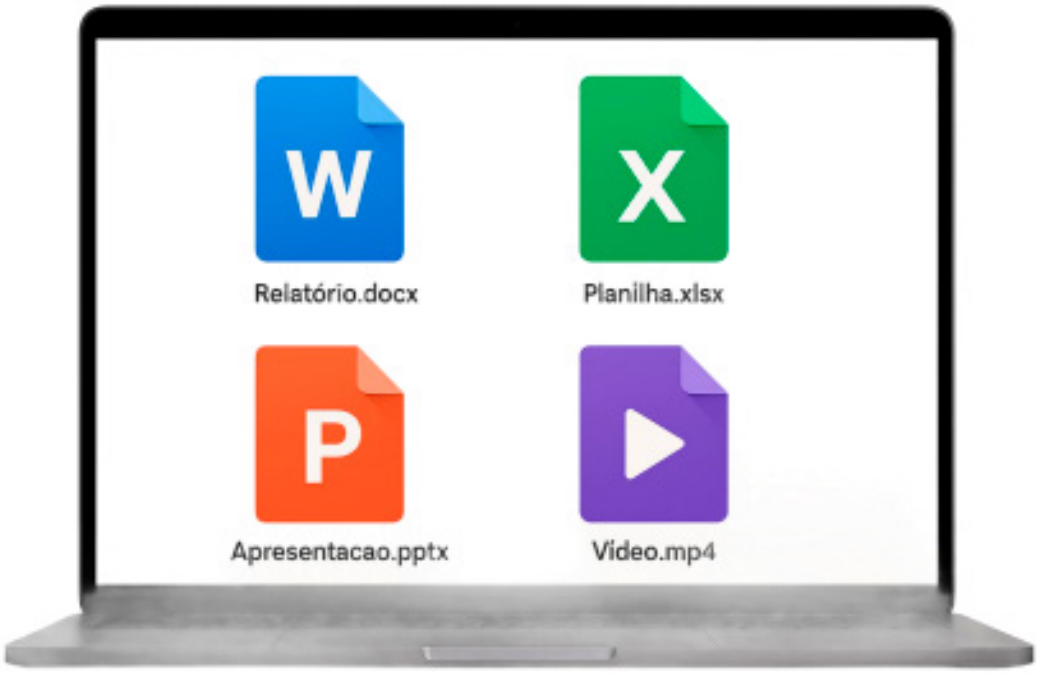
A tradução do termo *backups* ou "becapes" (grafia em português) seria cópia de segurança. Trata-se da cópia de arquivos com o objetivo de garantir a segurança.

O *backup* consiste em fazer uma cópia de segurança que não deve ser mantida no próprio computador de origem. Tal procedimento envolve extrair um arquivo do computador e armazenar sua cópia em um dispositivo externo, como um HD externo.

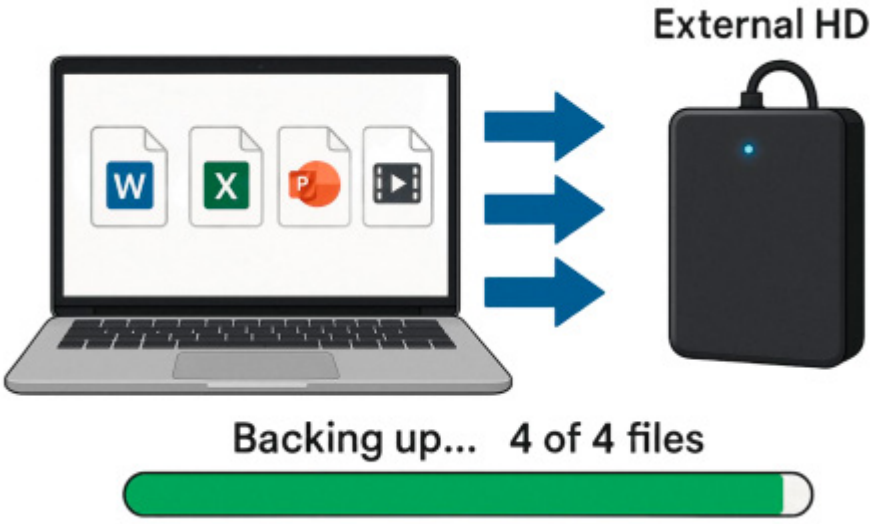
No âmbito dos concursos públicos, considera-se até mesmo o uso de dispositivos simples, como o *pendrive*, como meio para a realização da cópia de segurança.

Para ilustrar a importância do procedimento, propõe-se seguinte cenário: em caso de um incêndio que destrua o computador original onde os arquivos estavam armazenados, haverá, evidentemente, um prejuízo financeiro. Contudo, se houver uma cópia de segurança em um dispositivo externo (como um HD externo) guardado em local seguro e distinto do computador de origem, os dados permanecem preservados.

Após a aquisição de um novo equipamento, inicia-se o processo de restauração. Este consiste em copiar os dados armazenados no dispositivo de segurança de volta para o computador novo. Ressalta-se que a perda de dados pode ser muito mais prejudicial do que a perda da máquina; há casos em que empresas encerram suas atividades por não conseguirem restaurar informações essenciais perdidas em inundações ou incêndios.



Outra ilustração relevante envolve a proteção de arquivos essenciais como documentos de texto, planilhas, apresentações e vídeos, devidamente copiados para um HD externo, estão protegidos caso o computador principal seja infectado por um vírus, por exemplo.



Embora o termo "vírus" seja utilizado genericamente, um exemplo pertinente seria o ataque de *ransomware*, que sequestra os dados por meio de criptografia, bloqueando o acesso do usuário. Nesse cenário, a ameaça impede o acesso aos dados originais no computador, mas a existência de um *backup* prévio garante que a integridade da informação não seja comprometida, permitindo a recuperação dos arquivos.

Nesse cenário, o prejuízo é menor pela possibilidade de restauração. Diante de uma infecção por *ransomware*, tipo de código malicioso que sequestra e criptografa dados

exigindo o pagamento de resgate, o procedimento adequado consiste na formatação do equipamento (apagando integralmente o conteúdo corrompido) e na subsequente cópia dos dados preservados no dispositivo de segurança de volta para a máquina.

Para fins de estudo para concurso, se trabalha com dois caminhos: o backup (cópia de segurança) e a restauração (processo inverso). Embora o primeiro seja mais frequente em avaliações, a compreensão de ambos é indispensável para o entendimento da integridade da informação.

5m

PLANEJAMENTO DA POLÍTICA DE BACKUP

O estabelecimento de uma política de *backup* é aplicável tanto a ambientes empresariais quanto ao doméstico.

- O que salvar

O primeiro passo desse planejamento é a definição do que deve ser salvo. Nem todos os dados armazenados em um dispositivo são necessários; arquivos temporários ou vídeos recebidos em aplicativos de mensagens, por exemplo, podem ser descartados. Em contrapartida, arquivos pessoais e fotografias familiares possuem valor que justifica o armazenamento de segurança.

Existe o tipo de backup denominado imagem do sistema, que realiza a cópia integral do sistema operacional e de todos os arquivos contidos no disco para uma duplicação futura, caso necessária. Contudo, essa modalidade ocupa muito espaço de armazenamento.

A realização de uma cópia integral do sistema todos os dias se torna inviável caso o usuário altere apenas arquivos pequenos. Para solucionar essa questão, mais adiante serão estudados os tipos específicos de backup.

Neste primeiro passo, é necessário identificar quais pastas e arquivos são vitais e quais, embora menos importantes, ainda devem integrar a política de *backup*. Embora essa seleção seja relativa e subjetiva para fins de prova, a compreensão do critério de relevância é essencial.

- Onde salvar (3-2-1)

A regra 3-2-1 não é explicitamente documentada em normas, mas é muito conhecida e cobrada em provas de concurso.

Esta regra estabelece que devem existir três cópias dos arquivos armazenadas em dois tipos de mídias diferentes, e uma das cópias deve ser guardada em local distinto.

É necessário reiterar que manter uma cópia no mesmo computador não é considerado um backup porquanto não é seguro. Além disso, se o dispositivo de cópia estiver conectado à máquina no momento em que for infectado por *ransomware*, o código malicioso procurará

todos os dispositivos conectados à máquina via rede para também infectá-los e, por conseguinte, perderá o backup (o original e a cópia). No caso de um incêndio, por exemplo, perderia ambos. Por outro lado, em um caso menos drástico como a contaminação por *ransomware* ou vírus que está desconectado, basta formatar e restaurar, sendo a cópia externa a garantia máxima.

- Frequência

A frequência com que os dados devem ser salvos, seja diariamente, de hora em hora, semanalmente ou mensalmente, depende da análise do volume de alterações realizadas. No ambiente doméstico, se as modificações forem eventuais, uma periodicidade mensal ou semanal pode ser suficiente.

- Testes de Restauração

O teste de restauração consiste em fazer uma cópia de volta verificando a integridade dos dados copiados. Não basta possuir a cópia armazenada; é preciso verificar se os dados estão íntegros e se podem ser recuperados caso ocorra a perda dos originais.

10m

- Criptografia

A depender do caso, os dados necessitarão ser criptografados, isto é, codificar usando algoritmos. Isso implica tempo e a capacidade computacional necessária, visto que criptografar muitos dados demanda muito tempo.

A necessidade de criptografia justifica-se quando a confidencialidade é prioritária. Em órgãos governamentais, empresas ou mesmo no âmbito privado, dados sensíveis não devem ficar expostos. Caso o dispositivo de armazenamento seja extraviado ou acessado por terceiros, a criptografia garante que a intimidade ou os segredos institucionais não sejam expostos.

- Período de Retenção

O período de retenção refere-se ao ciclo de vida dos dados, ou seja, ao tempo em que a informação deve ser mantida armazenada. Em determinados contextos, estabelece-se uma validade específica; por exemplo, os dados podem ser mantidos por um ano e, após esse prazo, são descartados ou deletados para liberar espaço.

Um exemplo prático ocorre com sistemas de monitoramento por vídeo. As gravações são mantidas por um período determinado por precaução. Caso não haja incidentes ou reclamações nesse intervalo, os dados são apagados para que novas gravações ocupem o dispositivo. A disponibilidade de informações antigas, como registros de quatro ou cinco anos atrás, dependerá estritamente da logística e da política de retenção adotada pela instituição.

MÍDIAS

Para a execução dessas políticas de backups, utilizam-se diversos tipos de mídias. Dentre as mídias utilizadas para a realização de cópias de segurança, destacam-se:

- Fitas Magnéticas: Embora ainda utilizadas, possuem como desvantagem o acesso sequencial aos dados, o que torna a localização de informações específicas um pouco mais difícil.

- Disco Rígido (HD) e SSD: O HD (disco rígido) é frequentemente citado em exames e possui componentes mecânicos. Já o SSD é um dispositivo inteiramente eletrônico. Em termos de velocidade, o SSD é significativamente mais rápido que o HD, tanto na gravação quanto na recuperação de dados.

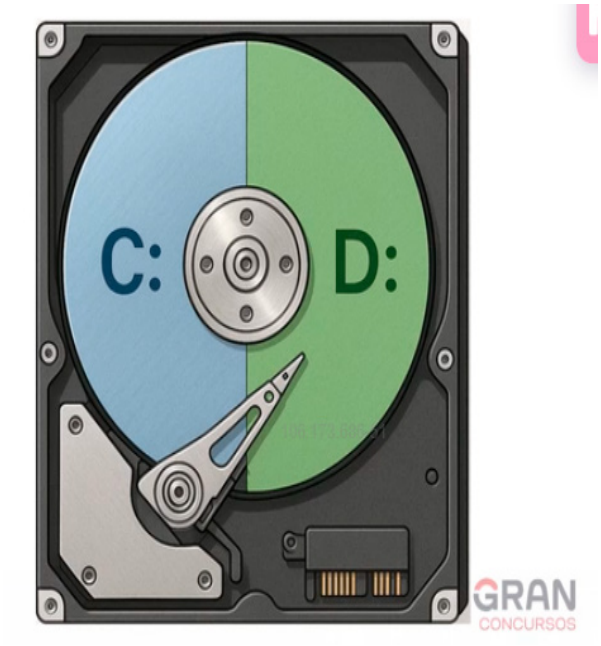
- Mídias Ópticas: Incluem o CD (capacidade média de 700 MB), o DVD (4,7 GB) e o Blu-ray (25 GB). Embora mencionadas em provas, não são as mais indicadas para segurança devido à vulnerabilidade a danos físicos e à ação do tempo; um risco na superfície pode resultar na perda total dos dados.

- Pendrive: Tecnicamente, não é o dispositivo mais recomendado para segurança profissional, mas é aceito em contextos domésticos e frequentemente abordado em questões de prova como um meio de backup por utilizar memória *flash* (similar ao SSD).

PARTICIONAMENTO DE DISCO

PARTIÇÕES

O particionamento consiste na divisão lógica de um disco rígido em duas ou mais unidades (como C: e D:, no padrão Windows). É fundamental compreender que se trata de uma divisão lógica e não física; o hardware continua sendo um só.



Portanto, realizar a cópia de um arquivo da unidade C: para a unidade D: dentro do mesmo disco não é considerado um backup seguro. Em caso de falha física do hardware, incêndio ou furto do equipamento, ambas as unidades seriam perdidas simultaneamente. O particionamento pode ser útil em situações menos drásticas, como a formatação seletiva do sistema operacional, mas não substitui a necessidade de armazenamento em um dispositivo externo.

Como exemplo prático de manutenção preventiva, cita-se o monitoramento da vida útil do hardware. Ao identificar ruídos anômalos ou alertas em programas de diagnóstico, deve-se proceder à migração imediata dos dados para uma nova unidade física a fim de evitar a perda por falha mecânica.

15m

SISTEMAS DE ARQUIVOS

- Windows – NTFS e Linux – EXT4

A organização dos dados nas unidades depende do sistema de arquivos adotado pelo sistema operacional. No Windows e no Linux, as estruturas de gerenciamento apresentam características distintas que influenciam a forma como o backup é processado.

Os sistemas de arquivos operam como uma estrutura organizacional para os dados. No ambiente Windows, utiliza-se predominantemente o NTFS, enquanto na maioria das distribuições Linux, adota-se o EXT4. De maneira simplificada, o sistema de arquivos equivale à divisão de vagas em um estacionamento físico; ele determina como o espaço será distribuído e quais recursos de segurança serão aplicados.

Tanto o NTFS quanto o EXT4 oferecem funcionalidades avançadas, como a criptografia de dados e tabelas de alocação que auxiliam na recuperação de informações em tabelas de alocação e minimizam erros durante o processo de gravação.

Outro sistema relevante, embora mais obsoleto, é o FAT32, comumente utilizado em *pendrives*. Este possui limitações importantes, como a ausência de suporte à criptografia nativa e a restrição de tamanho máximo de 4 GB para arquivos individuais.

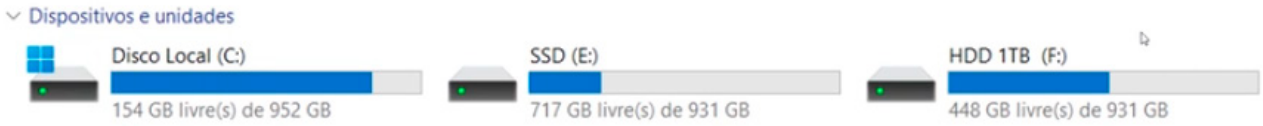
PARTICIONAMENTO DE DISCO

O disco rígido (HD) é um componente selado que protege discos magnéticos internos. Para fins educacionais, ilustra-se a configuração de um computador com dois HDs físicos distintos:

Embora a realização de uma cópia de um disco para outro dentro da mesma máquina seja uma prática comum, ela não é plenamente segura contra sinistros graves, como incêndios ou danos elétricos que afetem todo o gabinete.

A vida útil dos dispositivos de armazenamento é variável. Enquanto a média de funcionamento de um HD costuma ultrapassar 40.000 horas, falhas mecânicas ou danos elétricos podem reduzir drasticamente esse período. No caso de SSDs, a ausência de partes móveis não os isenta de falhas, que geralmente ocorrem por problemas elétricos.

PARTIÇÕES



Visualmente, no sistema operacional, diferentes partições de disco podem parecer unidades independentes. No entanto, é fundamental discernir se essas partições pertencem ao mesmo *hardware* físico ou a dispositivos distintos. Reforça-se que manter cópias em uma mesma máquina não constitui um sistema de backup resiliente.

Além do risco físico, deve-se considerar a vulnerabilidade em ambiente de rede. Conforme mencionado, ameaças como o *ransomware* são capazes de se propagar por todos os dispositivos e unidades mapeadas na rede. Se o backup estiver conectado à máquina ou acessível via rede no momento da infecção, tanto os dados originais quanto as cópias de segurança serão comprometidos. Portanto, a desconexão física e o armazenamento externo permanecem como as práticas mais eficazes de proteção.

Um caso relevante ocorrido em um tribunal de Brasília exemplifica os riscos da conectividade: durante um ataque de *ransomware*, as cópias de segurança que estavam conectadas à rede foram igualmente criptografadas pelo invasor. Embora o armazenamento em nuvem possua ferramentas para detectar alterações suspeitas, a sincronização permanente pode permitir a propagação da ameaça. Por essa razão, a manutenção de um backup *offline* (armazenado fisicamente fora da rede e em local distinto) é uma medida de segurança necessária em cenários críticos.

20m

Os Backups Quente (*Hot Backup*) e Backup Frio (*Cold Backup*) não são tipos de backup, mas sim a maneira como ele pode ser feito.

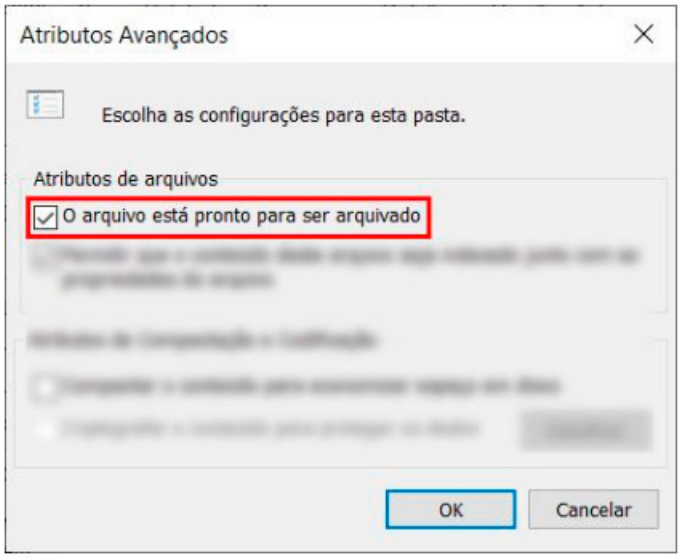
O Backup Quente (*Hot Backup*) é realizado com o sistema em pleno funcionamento. A principal vantagem é a continuidade do trabalho, sem interrupções. Contudo, arquivos que estejam sendo modificados no exato momento da cópia podem não ser salvos em sua versão mais recente, e falhas no sistema durante o processo podem resultar na perda dessas modificações pontuais.

Backup Frio (*Cold Backup* ou *Cold*) é realizado com o sistema desligado ou processos interrompidos. Embora a disponibilidade constante dos serviços atuais torne essa prática menos comum, ela é programada para horários específicos, como o período noturno ou fora do expediente. O ponto de atenção nesta modalidade é que quaisquer alterações feitas após o encerramento do processo de backup só serão protegidas na execução seguinte.

ATRIBUTO DE ARQUIVAMENTO

Um conceito fundamental para a compreensão dos tipos de backup é o atributo de arquivamento (ou atributo de backup). Funciona como uma marcação ou sinalizador no arquivo que indica se ele foi copiado ou se sofreu alterações recentes. As luzes do estacionamento dos shoppings para sinalizar se a vaga está livre ou ocupada é um exemplo, por analogia.

Analogamente a uma lista de compras, onde um item é marcado após ser adquirido, o sistema utiliza esse atributo para identificar o estado do arquivo.



A presença da marcação na ilustração acima indica basicamente duas hipóteses: i) o arquivo nunca foi submetido a um backup; e ii) o arquivo foi alterado após a última cópia realizada, significando que a versão armazenada está desatualizada.

É importante ressaltar que a utilidade de um backup diminui proporcionalmente ao tempo decorrido desde a última atualização. Uma cópia realizada há um ano terá pouco valor prático caso o arquivo original tenha sofrido modificações substanciais nesse período.

.