

BACKUP III

HASH

Obs.: O hash possui correlação direta com a cópia forense, sendo necessário como mecanismo de prova, principalmente no âmbito jurídico. No entanto, o hash é utilizado em diversos conceitos dentro da informática, como a assinatura digital, estando diretamente relacionado à garantia de integridade, ou seja, à comprovação de que um dado não foi modificado ao longo do tempo.

Por exemplo, ao se fazer uma cópia forense de um disco rígido de um suspeito, é necessário garantir que essa cópia é idêntica ao original, sem que nenhum caractere tenha sido alterado ou adicionado. Qualquer modificação invalidaria a cópia como prova, tornando-a falsa perante a lei. O hash atua como uma impressão digital para essa verificação.

Hash é um programa que realiza um cálculo matemático sobre um conjunto de dados, gerando um resumo único, representado por uma sequência fixa de letras e números. Esse código é único para cada informação específica. Para ilustrar, considere o texto “Olá, Jefferson.” sem espaços adicionais. Sempre que um hash for gerado para esse texto exato, o resultado será idêntico. Se qualquer alteração for feita, como a remoção da vírgula, resultando em “Olá Jefferson.”, o hash gerado será completamente diferente.

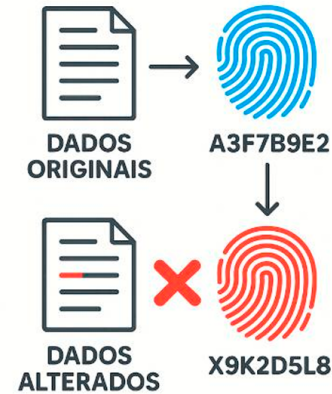
A lógica é que um texto íntegro sempre gerará o mesmo hash, infinitas vezes. É importante mencionar que existem diferentes algoritmos hash, e alguns, considerados defasados, são mais suscetíveis a colisões. Colisão é a possibilidade, matematicamente rara, mas existente, de dois textos diferentes gerarem o mesmo hash. Algoritmos mais antigos apresentam maior probabilidade de colisão, o que é indesejável, pois compromete a confiabilidade do mecanismo.

Retomando a analogia da impressão digital para a cópia forense: a partir dos dados originais, é feita uma cópia. Ao se gerar o hash da cópia, ele deve ser idêntico ao hash do original. Essa igualdade comprova que nenhuma modificação foi realizada durante o processo de cópia. Se qualquer modificação, por mínima que seja (como a adição de um espaço ou a alteração de uma vírgula), for introduzida nos dados, o hash resultante será drasticamente diferente. Isso invalida a cópia para fins forenses, pois sua integridade não pode mais ser garantida.

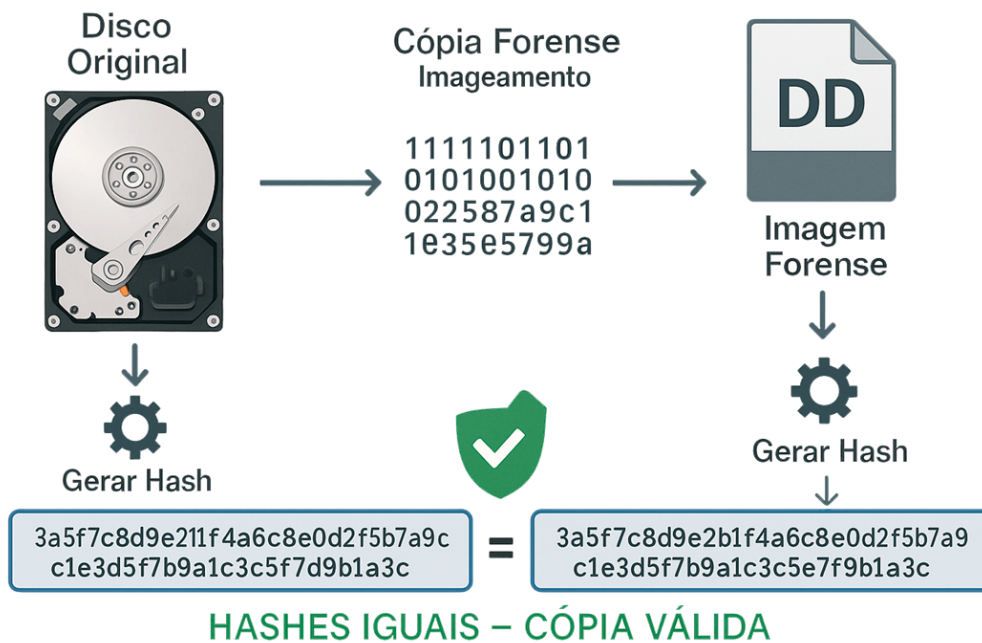
HASH COMO IMPRESSÃO DIGITAL

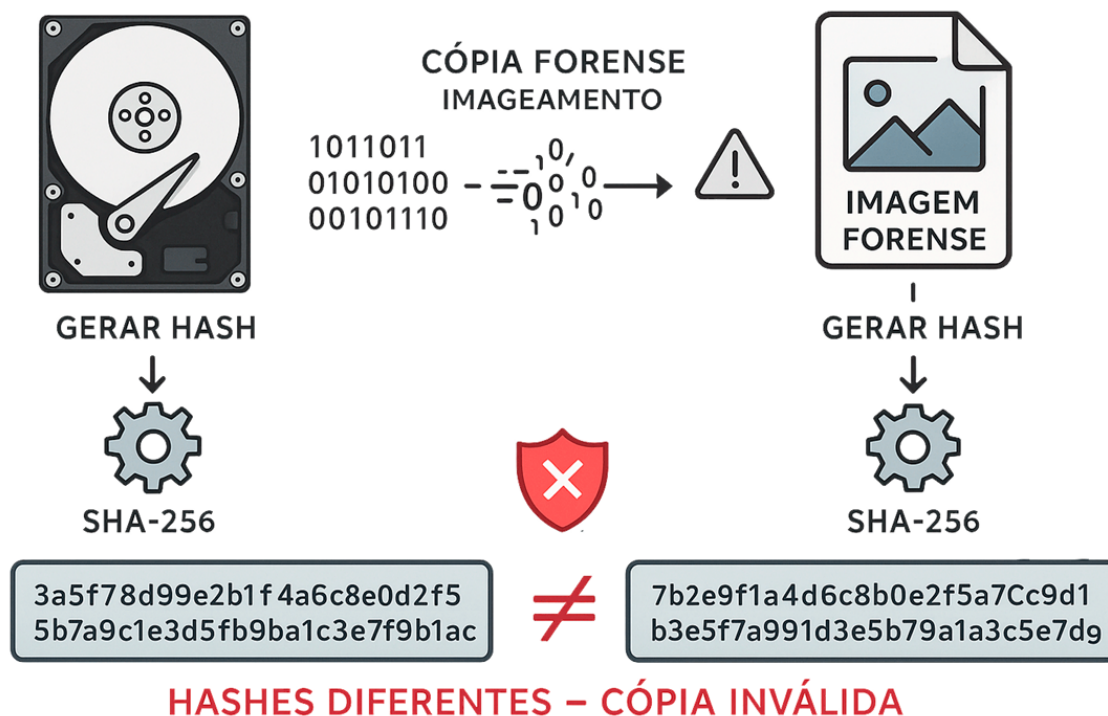


HASH COMO IMPRESSÃO DIGITAL



HASH (MD5 – SHA1 – SHA-256 – SHA-512)





Obs.: Os algoritmos MD5 e SHA-1 são versões de funções hash já consideradas defasadas. Essa classificação se deve principalmente à maior susceptibilidade à colisão, ou seja, à possibilidade de dois conjuntos de dados diferentes produzirem o mesmo valor hash. Embora esses algoritmos possam eventualmente ser citados em questões de prova como exemplos de funções hash, é importante destacar que não são mais considerados seguros para uso prático em contextos que exigem robustez criptográfica.

O hash é exemplificado no contexto da cópia forense. Considera-se um disco original do qual é feita uma cópia forense (imageamento). Para ambas as mídias, é gerado um valor hash. Se os hashes forem idênticos, comprova-se que a cópia é válida e integral, ou seja, não houve alteração nos dados durante o processo de duplicação.

No exemplo inverso, se houver qualquer modificação na cópia, mesmo que em um único bit, o hash gerado será diferente. Se o hash da cópia não for idêntico ao hash do disco original, a cópia é considerada inválida, pois sua integridade não pode ser garantida.



5m



DIRETO DO CONCURSO

01. (Q3698143/LEGATUS/PREFEITURA DE BURITI BRAVO/PROFESSOR DO 1º AO 5º ANO/2025)
Sobre o uso de backup na nuvem, analise as afirmações abaixo:

I – Backup na nuvem permite que os dados sejam armazenados de forma segura em servidores remotos, acessíveis pela internet.

II – Embora o backup na nuvem elimine a necessidade de cópias físicas, a velocidade de restauração dos dados não é influenciada pela qualidade da conexão à internet.

III – A realização de backups na nuvem não oferece proteção contra a perda de dados causada por falhas de hardware no dispositivo do usuário.

IV – A escalabilidade é uma das vantagens do backup na nuvem, permitindo que a capacidade de armazenamento seja facilmente ajustada conforme a necessidade.

Pode-se afirmar que:

- a) Apenas as afirmações I e II estão corretas.
- b) Apenas as afirmações I e IV estão corretas.
- c) Apenas as afirmações II e III estão corretas.
- d) Apenas as afirmações I, II e IV estão corretas.
- e) Apenas as afirmações II, III e IV estão corretas.



I – Isso se deve ao fato de que os provedores de nuvem implementam medidas de segurança para a proteção dos dados.

II – A velocidade de restauração de dados armazenados na nuvem é diretamente influenciada pela largura de banda e qualidade da conexão de internet do usuário. Restaurações que envolvem grandes volumes de dados exigem uma conexão robusta e podem levar um tempo considerável, geralmente maior do que uma restauração a partir de uma mídia local.

III – Um dos propósitos fundamentais do backup na nuvem é justamente proteger os dados contra falhas locais, como a quebra de um disco rígido. Se os dados estão armazenados remotamente na nuvem, eles podem ser recuperados para um novo dispositivo em caso de falha no hardware original.

IV – A escalabilidade é uma característica essencial dos serviços em nuvem. Diferentemente de soluções locais, que exigem a compra e instalação física de novos dispositivos de armazenamento, na nuvem é possível aumentar (ou diminuir) a capacidade de forma ágil, normalmente por meio de ajustes no plano de serviço contratado. Isso se aplica tanto a contextos domésticos, como no exemplo de armazenamento crescente de fotos, quanto a ambientes empresariais, que demandam flexibilidade para gerenciar grandes volumes de dados.

02. (Q3654862/EDUCA/PREFEITURA DE PEDRAS DE FOGO/ENCANADOR/2025) “De forma simples, o backup é uma espécie de cópia de segurança. Caso tenha algum problema com o original, você poderá acionar a cópia (ou seja, o backup) para fazer os procedimentos de restauração. O backup pode ser realizado sobre os arquivos da rede ou sobre os dados armazenados no banco.” Considerando os tipos de backup e seus meios de armazenamento, assinale a alternativa CORRETA:

- a) Backup Completo: copia todos os arquivos, sem distinção. Pelo fato de copiar tudo, o processo de backup é mais rápido.
- b) Backup Incremental: copia somente os arquivos modificados desde o último backup, independente do seu tipo. Pelo fato de não copiar tudo, o processo de backup é mais devagar.
- c) Nuvem: tendência do momento. A nuvem transfere a responsabilidade do armazenamento para a empresa provedora do serviço.
- d) Disco: O disco não permite acesso direto aos dados, que facilita e traz agilidade ao processo de gravação e recuperação.
- e) Backup Diferencial: copia somente os dados não modificados dos primeiros backups completos.



- a) O backup completo é o tipo mais lento e que mais consome recursos, pois realiza a cópia integral de todos os dados selecionados, independentemente de alterações anteriores.
- b) O backup incremental é justamente mais rápido do que o completo e também do que o diferencial, pois copia um volume menor de dados, limitando-se às alterações ocorridas desde o último backup de qualquer tipo.
- c) Ao utilizar um serviço de backup em nuvem, o usuário ou empresa delega ao provedor a infraestrutura física e a gestão do armazenamento remoto dos dados.
- d) Discos, como os discos rígidos, permitem acesso direto aos dados, o que de fato contribui para a agilidade nos processos de leitura e escrita.
- e) O backup diferencial copia todos os dados alterados desde o último backup completo, não desde os “primeiros” backups. É um método cumulativo que, a cada execução, inclui todas as modificações ocorridas desde a última cópia integral.



03. (Q3828051/QUADRIX/CRM-MS/ASSISTENTE ADMINISTRATIVO/2025) Uma boa prática que deve ser adotada tanto por usuários domésticos quanto pelas empresas é realizar o backup de seus arquivos importantes no mesmo HD em que seu sistema operacional está instalado. Tal prática visa a uma maior segurança das informações, em caso de necessidade de recuperação.



Não é considerado seguro manter a cópia de segurança no mesmo dispositivo físico do sistema e dos dados originais. Isso porque, em caso de falha física do disco rígido, como danos mecânicos, corrupção de setores ou falha eletrônica, tanto o sistema operacional quanto o backup seriam perdidos simultaneamente.

A mesma lógica se aplica mesmo que o disco seja particionado, com o sistema em uma partição e o backup em outra. Como as partições residem no mesmo dispositivo físico, uma falha nesse único disco comprometeria todos os dados, incluindo a cópia de segurança.

04. (Q3810655/INSTITUTO IBEST/CRMV-ES/AGENTE FISCAL/2025) No contexto de proteção de dados, a estratégia de backup conhecida como 3-2-1 recomenda

- a) realizar três backups completos por semana em dois dispositivos diferentes.
- b) utilizar três servidores em nuvem, dois locais e um internacional, para replicação de dados.
- c) fazer três backups incrementais e dois diferenciais por mês.
- d) manter duas cópias locais e uma cópia parcial dos dados em uma mídia removível.
- e) manter três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia armazenada fora do local.



A estratégia de backup conhecida como 3-2-1 recomenda manter três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia armazenada fora do local (também chamada de off-site).

05. (Q3949241/AMEOSC/PREFEITURA/PROFESSOR DE INFORMÁTICA/2025) A segurança e a continuidade dos negócios em qualquer organização dependem diretamente da implementação de robustas políticas e técnicas de backup e recuperação de dados. A escolha da estratégia de backup adequada influencia criticamente o tempo de restauração, o uso do espaço de armazenamento e a janela de backup. Diferentes tipos de backup se distinguem pela maneira como os dados são copiados e pela complexidade do processo de restauração. Sobre o tema, relacione corretamente os termos da Coluna A com as descrições da Coluna B.

Coluna A (Tipos de Backup):

- 1. Backup Completo (Full Backup).
- 2. Backup Incremental.
- 3. Backup Diferencial.

Coluna B (Descrições):

() Copia apenas os dados que foram alterados desde o último backup de qualquer tipo (completo ou incremental anterior); a restauração requer o backup completo mais recente e todas as sequências de backups incrementais subsequentes.

() Realiza uma cópia de todos os dados selecionados, independentemente de terem sido alterados desde a última operação de backup; cada operação é uma cópia independente, simplificando a restauração, mas consumindo mais tempo e espaço.

() Copia apenas os dados que foram alterados desde o último backup completo; é um método cumulativo que requer apenas o último backup completo e o último backup diferencial para restauração.

Assinale a alternativa que apresenta a sequência da associação correta dos itens acima, de cima para baixo:

a) 2 – 3 – 1.

b) 3 – 2 – 1.

c) 1 – 3 – 2.

d) 2 – 1 – 3.



2. (BACKUP INCREMENTAL) Copia apenas os dados que foram alterados desde o último backup de qualquer tipo (completo ou incremental anterior); a restauração requer o backup completo mais recente e todas as sequências de backups incrementais subsequentes.

1. (BACKUP COMPLETO – FULL BACKUP) Realiza uma cópia de todos os dados selecionados, independentemente de terem sido alterados desde a última operação de backup; cada operação é uma cópia independente, simplificando a restauração, mas consumindo mais tempo e espaço.

3. (BACKUP DIFERENCIAL) Copia apenas os dados que foram alterados desde o último backup completo; é um método cumulativo que requer apenas o último backup completo e o último backup diferencial para restauração.

06. (Q3861994/EDUCA/PREFEITURA DE UMBUZEIRO/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2025) Organizações que operam com grandes volumes de dados precisam adotar estratégias eficientes de backup para garantir a recuperação das informações em caso de falhas. Considerando os principais tipos de backup, analise as alternativas abaixo e assinale a CORRETA:

a) O backup incremental copia todos os dados existentes, substituindo o backup completo diariamente.

b) O backup diferencial registra apenas as alterações feitas desde o último backup incremental.

- c) O backup completo é o mais econômico em termos de tempo e armazenamento, pois não depende de backups anteriores.
- d) O backup incremental requer, para restauração completa, o último backup completo e todos os incrementais realizados posteriormente.
- e) O backup espelhado mantém cópias de segurança em mídias diferentes, sem replicar alterações deletadas nos arquivos originais.



- a) O backup incremental não copia todos os dados; ele copia apenas os dados que foram criados ou modificados desde o último backup de qualquer tipo (completo ou incremental).
- b) O backup diferencial registra todas as alterações feitas desde o último backup completo, não desde o último incremental.
- c) O backup completo é o mais demorado para executar e o que mais consome espaço de armazenamento, pois realiza uma cópia integral de todos os dados selecionados. A independência de backups anteriores é uma característica, mas não o torna econômico nesses aspectos.
- d) Para restaurar um sistema a partir de backups incrementais, é necessário aplicar, sobre o último backup completo, todos os backups incrementais subsequentes, na ordem correta, para se obter o estado mais recente dos dados.



- e) Embora técnicas de espelhamento, como certos níveis de RAID, existam para redundância, o termo “backup espelhado” não é um tipo padrão de estratégia de backup. Além disso, o espelhamento RAID tem a função primária de fornecer alta disponibilidade e proteção contra falhas de disco, mas não substitui um plano de backup convencional, pois não protege contra cenários como exclusão acidental, corrupção de software ou desastres que afetem o local físico.

07. (Q3789044/FGV/MPU/ANALISTA DO MPU/PERITO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO/2025) A utilização de funções de resumo (hash) consiste na aplicação de algoritmos matemáticos que, dada uma entrada de dados de qualquer tamanho, produzem um único valor de tamanho fixo correspondente, com diversos empregos na computação. Em relação ao uso de funções de hash em evidências digitais, é correto afirmar que:

- a) o cálculo de hashes de evidências digitais é fundamental para a preservação da cadeia de custódia, pois permite a verificação de integridade dos dados e a exatidão das cópias;
- b) o uso de hashes é extremamente útil em procedimentos forenses, pois permite a recuperação dos dados em casos de erros de gravação;
- c) deve-se priorizar o emprego dos hashes MD5 ou SHA1, pois são seguros e de cálculo mais rápido;

- d) o uso de hashes permite a busca e identificação de arquivos suspeitos, dispensando a necessidade de verificação visual, mesmo no caso de imagens e vídeos;
- e) no caso de cópias integrais de conteúdos de dispositivos de armazenamento, um único valor de hash total é suficiente, visto que os dispositivos modernos raramente apresentam erros de acesso.



- a) O hash serve como uma impressão digital; se uma cópia for idêntica ao original, os hashes serão idênticos, comprovando que nenhuma alteração ocorreu e fortalecendo a cadeia de custódia.
- b) A função primária de um hash é a verificação da integridade, não a recuperação de dados corrompidos ou perdidos.
- c) Ambos os algoritmos, MD5 e SHA-1, são considerados criptograficamente quebrados e inseguros para uso em contextos que exigem garantia de integridade, devido à sua suscetibilidade a colisões.
- d) Embora um hash possa identificar um arquivo específico (por exemplo, comparando-o com uma base de dados de hashes conhecidos de malware), ele não analisa o conteúdo semântico do arquivo. Para determinar se uma imagem ou vídeo é relevante como prova, é necessária uma análise visual ou contextual do seu conteúdo, que o hash por si só não fornece.
- e) Na prática forense, é comum gerar múltiplos hashes: um hash para a imagem forense completa (hash total) e hashes individuais para arquivos específicos dentro dela. Essa prática fornece camadas adicionais de verificação e ajuda a isolar e identificar possíveis problemas de integridade, não dependendo apenas da suposta confiabilidade do hardware.

08. (Q3838322/CESPE/CEBRASPE/MPO/ANALISTA DE PLANEJAMENTO E ORÇAMENTO/2024)

Em relação a conceitos e fundamentos da forense computacional, julgue os itens a seguir. Imagem e espelhamento consistem em técnicas de duplicação/cópia que são utilizadas na fase de análise e que, ao serem realizadas por meio de softwares e equipamentos forenses, garantem uma cópia fiel dos dados e, consequentemente, a preservação correta do material apreendido.



Na forense computacional, as técnicas de criação de imagem e de espelhamento são realizadas principalmente na fase de aquisição de evidências, sendo a etapa inicial do processo. A fase de análise, por sua vez, ocorre posteriormente.

09. (Q3884909/INSTITUTO CONSULPLAN/NITERÓI PREV/ANALISTA DE SISTEMAS/2025)

No âmbito da Niterói Prev, um analista de sistema assumiu a responsabilidade pela estruturação de um banco de dados voltado ao gerenciamento de informações previdenciárias. Dada a sensibilidade e o volume dos dados envolvidos, a adoção de políticas de proteção e

recuperação torna-se um requisito crítico para garantir a continuidade das operações. Nesse cenário, é necessário que o profissional considere não apenas o projeto físico e lógico da base de dados, mas também os mecanismos que assegurem a disponibilidade e a integridade das informações diante de falhas inesperadas. Entre as práticas adotadas, destacam-se as estratégias de cópia de segurança, que variam quanto à abrangência, frequência e complexidade da restauração. O planejamento da rotina de cópias envolve decisões sobre a periodicidade das operações, os critérios de seleção dos dados a serem replicados e os dispositivos mais apropriados para o armazenamento, respeitando a relação entre custo, velocidade de acesso e resiliência. Cada escolha impacta diretamente o tempo de resposta frente a incidentes e a capacidade de manter os serviços em funcionamento. Considerando as informações anteriores sobre estratégias de backup no contexto da modelagem de banco de dados para sistemas previdenciários da Niterói Prev, analise as afirmativas a seguir.

I – Backups incrementais exigem cuidado na manutenção da sequência, pois uma falha em qualquer ponto pode comprometer a restauração completa.

II – A restauração a partir de backups diferenciais requer o último backup completo e apenas o último diferencial, reduzindo o esforço em comparação ao incremental.

III – Fitos magnéticas oferecem boa capacidade de armazenamento, mas geralmente têm tempo de acesso mais lento que discos rígidos ou soluções em nuvem.

IV – Para sistemas com alto volume de dados, recomenda-se priorizar apenas backups completos para simplificar o processo e evitar riscos de falha.

V – Definir ciclos de backup diários, semanais ou mensais deve considerar o volume de transações e a criticidade dos dados, além do custo-benefício das mídias utilizadas.

Está correto o que se afirma em

- a) I, II, III, IV e V.
- b) I e II, apenas.
- c) III e V, apenas.
- d) I, II, III e V, apenas.



I – Como a restauração a partir de incrementais requer a aplicação ordenada de todos os backups desde o último completo, a corrupção ou perda de um único backup incremental na cadeia pode impedir a recuperação bem-sucedida dos dados.

II – O backup diferencial é cumulativo; cada execução copia todas as alterações desde o último backup completo. Portanto, para restaurar o estado mais recente, são necessários



20m

apenas dois conjuntos: a última cópia completa e o último backup diferencial, simplificando o processo em relação ao incremental.

III – As fitas magnéticas são uma mídia de armazenamento sequencial com alta capacidade e baixo custo por gigabyte, mas o acesso aos dados é tipicamente mais lento do que em mídias de acesso aleatório, como discos (HDDs/SSDs) ou serviços em nuvem, que permitem recuperação mais ágil.

IV – Realizar exclusivamente backups completos em ambientes com grandes volumes de dados é geralmente inviável devido ao longo tempo de execução, ao consumo significativo de largura de banda (em backups remotos) e ao alto uso de espaço de armazenamento. Estratégias combinadas, utilizando backups completos periódicos intercalados com backups incrementais ou diferenciais, são padrão para equilibrar eficiência e confiabilidade.

V – A definição de uma política de backup, incluindo sua frequência, é um processo de planejamento que deve levar em conta fatores como a taxa de alteração dos dados (volume de transações), o impacto da perda de dados (criticidade) e os trade-offs entre custo, velocidade e capacidade das soluções de armazenamento escolhidas.

10. (Q3605775/QUADRIX/CORE-RJ/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2025) Assinale a opção que apresenta uma vantagem dos backups incrementais em comparação com os backups completos.

- a) Maior segurança de dados.
- b) Menor tempo de restauração.
- c) Utilizam mais espaço de armazenamento.
- d) São mais rápidos e utilizam menos espaço, pois só armazenam alterações desde o último backup.
- e) São mais fáceis de configurar.



- a) Não se trata de uma vantagem comparativa direta.
- b) A restauração a partir de incrementais geralmente leva mais tempo, exigindo a aplicação sequencial de múltiplos conjuntos de backup.
- c) É o oposto da realidade, backups incrementais utilizam menos espaço.
- d) O backup incremental é cumulativo e sempre referenciado ao último backup completo.
- e) Não é uma vantagem técnica definidora.

11. (Q3617272/FURG/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/ÁREA REDE/2025) Com relação aos tipos de backup, assinale a afirmativa correta quanto aos backups full, incremental e diferencial.

- a) O backup full copia apenas os arquivos que foram alterados desde o último backup incremental.
- b) O backup incremental copia todos os arquivos do sistema, independentemente de terem sido alterados ou não.
- c) O backup diferencial copia todos os arquivos que foram alterados desde o último backup completo.
- d) O backup incremental é executado mais rapidamente e consome menos espaço de armazenamento porque copia apenas os dados que foram criados ou modificados desde o último backup de qualquer tipo (completo ou incremental anterior).
- e) O backup incremental mantém uma cópia completa de todos os dados, o que resulta em um arquivo de backup maior a cada execução.



- a) O backup full (completo) copia todos os arquivos selecionados, não apenas os alterados desde um incremental.
- b) O incremental copia apenas os arquivos alterados desde o último backup, não todos os arquivos do sistema.
- c) O diferencial é cumulativo e sempre referenciado ao último backup completo.
- d) O backup full é mais lento que o incremental, pois copia um volume muito maior de dados, independentemente de verificar modificações.
- e) O backup incremental não mantém uma cópia completa de todos os dados a cada execução, isso seria característica do backup completo. Cada incremental contém apenas as alterações desde o backup anterior.



25m

GABARITO

01. b**02. c****03. E****04. e****05. d****06. d****07. a****08. E****09. d****10. d****11. c**

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jeferson Bogo Severino.

A presente gravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.