

## Gabarito

### 1ª Questão: (20 pontos)

--	--

#### 1) DEFINIÇÕES:

**Teste:** execução de um programa com a intenção de descobrir erros.

**Verificação:** tentativa de achar defeitos através de revisões e testes.

**Validação:** tentativa de achar defeitos; não conformidade com os requisitos.

**Depuração:** diagnóstico preciso de um defeito; seguido de sua correção.

**Método da Caixa Branca (Estrutural)** – tem por objetivo determinar defeitos na estrutura interna ou no código do software. Os Testes de Unidade, geralmente realizados pelos programadores nos seus códigos, são normalmente classificados em Testes da Caixa Branca.

**Método da Caixa Preta (Funcional)** – tem por objetivo determinar se os requisitos foram total ou parcialmente satisfeitos pelo software. Verifica apenas os resultados produzidos e não requer conhecimento interno do sistema, apenas conhecimento dos requisitos do negócio.

**A figura a seguir apresenta uma visão geral da classificação dos testes presentes no Método da Caixa Preta:**

**(foi solicitada a apresentação de pelo menos três testes)**

<i>Categoria</i>	<i>Tipos de Teste</i>	<i>Requisitos</i>
Funcionalidade	<a href="#">Teste Funcional</a> <a href="#">Teste de Volume</a> <a href="#">Teste de Segurança</a> <a href="#">Teste de Acessibilidade</a>	Conjunto de características; Capacidade; Segurança.
Usabilidade	<a href="#">Teste de Usabilidade</a>	Fator humano e Estética; Consistência da Interface do usuário; Help online e assistentes.
Confiabilidade	<a href="#">Teste de Estresse</a> <a href="#">Teste de Regressão</a> <a href="#">Teste de Integridade</a> <a href="#">Teste de Estrutura</a>	Frequência e severidade de falhas; Confiança nos resultados; Recuperação de falhas; Tempo entre falhas (MTBF).
Desempenho	<a href="#">Teste de Desempenho</a> <a href="#">Teste de Carga</a> <a href="#">Teste de Contenção</a> <a href="#">Teste de Perfil de Desempenho</a>	Vazão; Eficiência; Tempo de Resposta; Consumo de recursos.
Suportabilidade	<a href="#">Teste de Instalação</a> <a href="#">Teste de Configuração</a>	Facilidade de instalação; Requisitos de configuração; Requisitos de adaptabilidade; Requisitos de Compatibilidade.

2ª Questão: (20 pontos)

--	--

**Spoofing identity**

As ameaças de spoofing permitem a um invasor fazer passar-se por outro usuário ou permitem a um servidor trapaceiro (rogue server) fazer passar-se por um servidor válido. Um exemplo de spoofing de identidade do usuário é acessar ilegalmente e depois utilizar outras informações de autenticação, como o nome e a senha do usuário.

**Tampering with data**

A adulteração de dados envolve modificação mal-intencionada dos dados. Os exemplos incluem alterações não-autorizadas feitas em dados persistentes, como aqueles mantidos em um banco de dados, e a alteração de dados à medida que fluem entre dois computadores em uma rede aberta, como a Internet. Frequência e severidade  
=altas;

**Repudiation**

As ameaças de repúdio estão associadas a usuários que negam a realização de uma ação sem que outras partes tenham alguma maneira de provar o contrário - por exemplo, um usuário que realiza uma operação ilegal em um sistema que não tem a capacidade de rastrear as operações proibidas. O não-repúdio é a capacidade de um sistema de opor-se a ameaças de repúdio.

**Information disclosure**

As ameaças de revelação de informações envolvem a exposição de informações para indivíduos que supostamente não devem ter acesso a elas - por exemplo, a capacidade de um usuário de ler um arquivo ao qual não lhe foi concedido acesso e a capacidade de um invasor de ler dados em trânsito entre dois computadores.

**Denial of service**

Ataques de negação de serviço (DoS - Denial of Service) negam um serviço a usuários válidos - por exemplo, tornando um servidor da Web temporariamente indisponível ou inutilizável.

**Elevation of privilege**

Nesse tipo de ameaça, um usuário não-privilegiado ganha acesso privilegiado e assim tem acesso suficiente para comprometer ou destruir todo o sistema. As ameaças de elevação de privilégio incluem aquelas situações em que um invasor efetivamente penetrou em todas as defesas do sistema e tornou-se parte do próprio sistema confiável, uma situação realmente perigosa.

3ª Questão: (20 pontos)

--	--

**Backups totais**

Um backup total captura todos os dados, incluindo arquivos de todas as unidades de disco rígido. Cada arquivo é marcado como tendo sido submetido a backup; ou seja, o atributo de arquivamento é desmarcado ou redefinido. Uma fita atualizada de backup total pode ser usada para restaurar um servidor completamente em um determinado momento.

**Vantagens:**

**Cópia total dos dados.** Um backup total significa que é obtida uma cópia completa de todos os dados permitindo a necessária recuperação do sistema.

**Acesso rápido aos dados de backup.** Não é preciso pesquisar em várias fitas para localizar o arquivo que se deseja restaurar, porque os backups totais incluem todos os dados contidos nos discos rígidos em um determinado momento.

**Desvantagens:**

**Dados redundantes.** Backups totais mantêm dados redundantes, porque os dados alterados e não alterados são copiados para fitas sempre que um backup total é executado.

**Tempo.** Backups totais levam mais tempo para serem executados e podem ser muito demorados.

**Backups incrementais**

Um backup incremental captura todos os dados que foram alterados desde o backup total ou o incremental mais recente. Deve-se usar uma fita de backup total (não importa há quanto tempo ela tenha sido criada) e todos os conjuntos de backups incrementais subseqüentes para restaurar um servidor. Um backup incremental marca todos os arquivos como tendo sido submetidos a backup; ou seja, o atributo de arquivamento é desmarcado ou redefinido.

**Vantagens:**

**Uso eficiente do tempo.** O processo de backup leva menos tempo porque apenas os dados que foram modificados ou criados desde o último backup total ou incremental são copiados para a fita.

**Uso eficiente da mídia de backup.** O backup incremental usa menos fita porque apenas os dados que foram modificados ou criados desde o último backup total ou incremental são copiados para a fita.

**Desvantagens:**

**Restauração completa complexa.** Pode ser preciso restaurar os dados de um conjunto incremental de várias fitas para obter uma restauração completa do sistema.

**Restaurações parciais demoradas.** Pode ter que pesquisar em várias fitas para localizar os dados necessários para uma restauração parcial.

**Backups diferenciais.**

Um backup diferencial captura os dados que foram alterados desde o último backup total. É preciso uma fita de backup total e da fita diferencial mais recente para executar uma restauração completa do sistema. Ele não marca os arquivos como tendo sido submetidos a backup (ou seja, o atributo de arquivamento não é desmarcado).

**Vantagens:**

**Restauração rápida.** A vantagem dos backups diferenciais é que eles são mais rápidos do que os backups incrementais, porque há menos fitas envolvidas. Uma restauração completa exige no máximo dois conjuntos de fitas — a fita do último backup total e a do último backup diferencial.

**Desvantagens:**

**Backups mais demorados e maiores.** Backups diferenciais exigem mais espaço em fita e mais tempo do que backups incrementais porque quanto mais tempo tiver se passado desde o backup total, mais dados haverá para copiar para a fita diferencial.

**Aumento do tempo de backup.** A quantidade de dados dos quais é feito backup aumenta a cada dia depois de um backup total.