



ISTQB®

# GLOSSÁRIO DE TERMOS

Versão 3.1br

## Advanced Level Technical Tester Analyst

Os termos deste documento são complementares ao Glossário de Termos – Núcleo Base para o exame de certificação CTAL-TTA Technical Tester Analyst.



Tradução realizada pela WG Tradução do BSTQB  
baseada na versão 3.1 do *ISTQB Glossary of  
Testing Terms*

### **Notificação do Detentor dos Direitos Autorais**

Este documento poderá ser copiado na íntegra ou em parte desde que haja menção à sua fonte.  
Copyright ©2014, International Software Testing Qualifications Board (ISTQB®).

**acurácia**

*accuracy*

Capacidade do produto de software em fornecer os resultados ou efeitos, corretos ou acordado com o grau necessário de precisão.

*Ver também:* funcionalidade

*Referência:* ISO 9126

**adaptabilidade**

*adaptability*

Capacidade do produto de software de ser adaptado para diferentes ambientes, sem a necessidade de ações ou meios, além daqueles definidos pelo próprio software considerado.

*Ver também:* portabilidade

*Referência:* ISO 9126

**analísabilidade**

*analyzability*

Capacidade do produto de software de permitir o diagnóstico de deficiências ou causas de falhas no software, ou a identificação de partes a serem modificadas.

*Ver também:* manutenibilidade

*Referência:* ISO 9126

**análise de fluxo de dados**

*data flow analysis*

Forma de análise estática baseada na definição e uso de variáveis

**análise dinâmica**

*dynamic analysis*

Processo de avaliação do comportamento. Por exemplo, o desempenho da memória ou o uso da CPU de um sistema ou componente durante sua execução.

*Referência:* pós IEEE-610

**análise do fluxo de controle**

*control flow analysis*

Forma de análise estática com base em uma representação de caminhos únicos (sequência de eventos) na execução através de um componente ou sistema. A análise de fluxo de controle avalia a integridade das estruturas de controle de fluxo, procurando controlar possíveis anomalias, tais como loops ou etapas do processo logicamente inacessíveis.

**anti-padrão**

*anti-pattern*

Ações repetitivas, solução reutilizável de estrutura ou processo que inicialmente parece ser benéfico e é normalmente utilizada, mas é ineficaz e/ou improdutiva na prática.

## **apreensibilidade**

*learnability*

Capacidade que um produto de software tem de possibilitar ao usuário aprender suas aplicações

*Ver também:* usabilidade

*Referência:* ISO 9126

## **assistente de instalação**

*installation wizard*

Software fornecido em qualquer meio de comunicação adequado que conduz o instalador através do processo de instalação. Ele normalmente é executado em um processo de instalação, pedindo opções e fornecendo feedback sobre os resultados da instalação.

## **atratividade**

*attractiveness*

Capacidade do produto de software de ser atraente ao usuário.

*Ver também:* usabilidade

*Referência:* ISO 9126

## **automação da execução de teste**

*test execution automation*

Utilização de um software, por exemplo, ferramentas de captura/recuperação, para controlar a execução de testes, a comparação entre os resultados reais e os esperados, a criação de condições de teste e outro controle de teste e funções de relatório.

## **buffer**

*buffer*

Dispositivo ou área usado para armazenar dados temporários em diferentes taxas de fluxo de dados, tempo, ocorrência de eventos, quantidades de dados que podem ser tratados pelo dispositivo ou processos envolvidos na transferência ou no uso dos dados.

*Referência:* IEEE-610

## **cobertura da condição de decisão**

*decision condition coverage*

Porcentagem de todos os resultados de condições e de decisões, que foram exercitados por uma suite de teste. 100% de cobertura de condição de decisão implica em ter, ao mesmo tempo, 100% de cobertura de condição e 100% de cobertura de decisão.

## **cobertura de decisão de condição modificada**

*modified condition / decision coverage (MC/DC)*

Porcentagem de todos os resultados de única condição que independentemente afetam um resultado da decisão, que tenham sido testadas por um conjunto de casos de teste. 100% de cobertura de decisão de condição modificada implica em 100% da cobertura de condição de decisão.

*Sinônimos:* cobertura de determinação de condição, cobertura de condição múltipla modificada

**cobertura de desvio**

*branch coverage*

Porcentagem de desvios no código exercitado por uma suíte de teste. Isso significa que 100% de cobertura de desvio implica em 100% de cobertura de decisão e também em 100% de cobertura de sentença.

**cobertura de fluxo de dados**

*data flow coverage*

Porcentagem de pares de definição-utilização exercida por uma suíte de teste

**cobertura de sentença**

*statement coverage*

Porcentagem de sentenças executáveis que tenham sido exercidas por um conjunto de testes.

**coexistência**

*co-existence*

Capacidade do produto de software coexistir com outro software independente em um ambiente comum que compartilhando recursos comuns.

*Ver também:* portabilidade

*Referência:* ISO 9126

**complexidade ciclomática**

*cyclomatic complexity*

O número máximo de caminhos lineares, independentes, através de um programa. A complexidade ciclomática pode ser calculada como:  $L - N + 2P$ , onde: L é o número de arestas/links em um gráfico, N é o número de nós em um gráfico e P é o número de partes desconectadas do gráfico (por exemplo, um gráfico chamado ou sub-rotina).

*Sinônimos:* número ciclomático

*Referência:* pós McCabe

**condição atômica**

*atomic condition*

Uma condição que não pode ser decomposta, isto é, uma condição que não contém duas ou mais condições individuais unidas por um operador lógico (AND, OR, XOR).

**cross-site scripting (XSS)**

*cross-site scripting (XSS)*

Uma vulnerabilidade que permite aos atacantes injetar código malicioso em um site.

*Referência:* NIST.IR.7298

**curto-circuíto**

*short-circuiting*

Técnica de programação para avaliar as condições compostos em que uma condição de um dos lados de um operador lógico não pode ser avaliada, se a condição do outro lado é suficiente para determinar o resultado final.

**denial of service (DOS)**

*denial of service (DOS)*

Um ataque de segurança que se destina a sobrecarregar o sistema com solicitações de tal forma que solicitações legítimas não possam ser atendidas.

**encriptação**

*encryption*

Processo de codificação de informações de modo que somente as partes autorizadas possam recuperar as informações originais, geralmente por meio de uma chave de descriptação específica ou processo.

**entendibilidade**

*understandability*

Capacidade que um produto de software tem de possibilitar ao usuário entender se ele é adequado para uso, e como pode ser utilizado em determinadas tarefas e condições de uso.

*Ver também:* usabilidade

*Referência:* ISO 9126

**escalabilidade**

*scalability*

Capacidade que um produto de software tem para sofrer um upgrade ou para acomodar aumento de cargas.

*Referência:* pós Gerrard

**estouro de buffer**

*buffer overflow*

Falha no acesso de memória, devido ao processo de armazenamento de dados ultrapassar os limites fixos do tamanho da área de armazenamento temporário, resultando em estouro da área de memória adjacente ou levantamento de excessão.

*Ver também:* buffer

**ferramenta de captura e execução**

*capture/playback tool*

Tipo de ferramenta de execução de teste onde os valores de entrada são gravados durante o teste manual a fim de gerar scripts de testes automatizados que possam ser executados mais tarde (ou seja, reproduzidos). Essas ferramentas são frequentemente utilizadas para apoiar testes automatizados de regressão.

*Sinonimos:* ferramenta de captura/reprodução, ferramenta de gravação/reprodução

## **ferramenta de monitoramento**

*monitoring tool*

Ferramenta de software ou dispositivo de hardware que é executado simultaneamente com o componente ou sistema em teste e supervisiona, grava e/ou analisa o comportamento do componente ou sistema.

*Referência:* pós IEEE-610.

## **ferramenta de sementeamento de falhas**

*fault seeding tool*

Ferramenta para a semear (isto é, inserir intencionalmente) falhas em um componente ou sistema.

*Sinônimos:* ferramenta de sementeamento de erro

## **ferramenta de teste de hyperlink**

*hyperlink test tool*

Ferramenta utilizada para verificar se existem hyperlinks desfeitos (quebrados) presentes em uma página da web.

## **gerenciamento de defeito**

*defect management*

Processo de reconhecimento, investigação, tomada de medidas e eliminação de defeitos. Trata-se de gravação de defeitos, classificação e identificação do impacto.

*Sinônimos:* gerenciamento de problema

*Referência:* pós IEEE-1044

## **gráfico de chamada**

*call graph*

Representação abstrata dos relacionamentos de chamadas entre as subrotinas de um programa

## **gráfico do fluxo de controle**

*control flow graph*

Representação abstrata de todas as possíveis sequências de eventos (caminhos) na execução de um componente ou sistema.

## **homem no meio ataque**

*man in the middle attack*

A interceptação, imitação, e/ou alteração e posteriormente de afinação de comunicações (por exemplo, transações de cartão de crédito) por um terceiro, de tal forma que um usuário permaneça sem ser notado na presença que de terceiros.

## **hyperlink**

*hyperlink*

Ponteiro dentro de uma página web que leva a outras páginas da web.

## **identificação de risco**

*risk identification*

Processo que identifica os riscos por meio de técnicas como brainstorming, listas de verificação ou histórico de falhas.

## **injeção de falha**

*fault injection*

Processo de adição de defeitos intencionalmente a um sistema com o objetivo de descobrir se o mesmo pode detectar e, possivelmente, recuperar-se a partir de um defeito. A injeção de falhas é destinada a imitar as falhas que podem ocorrer no campo.

*Ver também:* tolerância a falha

## **instalabilidade**

*installability*

Capacidade que um produto de software tem para ser instalado em um ambiente específico.

*Ver também:* portabilidade

*Referência:* ISO 9126

## **integração funcional**

*functional integration*

Abordagem de integração que combina os componentes ou sistemas com a finalidade de fazer com que a funcionalidade básica funcione o mais rápido possível.

*Ver também:* teste de integração

## **máquina de estado finito**

*finite state machine*

Modelo computacional que consiste em um número finito de estados e de transições entre esses estados, possivelmente com ações de acompanhamento.

*Referência:* IEEE-610

## **modificabilidade**

*changeability*

Capacidade de um produto de software em permitir modificações específicas sejam implementadas.

*Ver também:* manutenibilidade

*Referência:* ISO 9126

## **modo de falha**

*failure mode*

Manifestação física ou funcional de uma falha. Por exemplo, um sistema em modo de falha pode ser caracterizado pelo funcionamento lento, saídas incorretas, ou a paralização completa da execução.

*Referência:* IEEE-610

**operabilidade**

*operability*

Capacidade do produto de software em habilitar o usuário a operá-lo e controlá-lo.

*Ver também:* usabilidade

*Referência:* ISO 9126

**par definição-utilização**

*definition-use pair*

Associação da definição de uma variável com sua utilização. Uma variável pode ser utilizada de forma computacional (por exemplo, multiplicação) ou para direcionar a execução de um caminho (uso de predicado).

**perfil de carga**

*load profile*

Especificação da atividade que um componente ou sistema a ser testado pode ter na produção. Um perfil de carga consiste em um determinado número de usuários virtuais que transformam um conjunto definido de operações em um período de tempo especificado e de acordo com um perfil pré-operacional.

*Ver também:* perfil operacional

**política de segurança**

*security policy*

Documento de alto nível que descreve os princípios, a abordagem e os principais objetivos da organização em matéria de segurança.

**ponteiro**

*pointer*

Item de dados que especifica o local de um outro item de dados, por exemplo, um item de dados que especifica o endereço do registro do funcionário próximo a ser processado.

*Referência:* IEEE-610

**ponteiro perdido**

*wild pointer*

Ponteiro que referencia um local que está fora do escopo desse ponteiro ou que não existe.

*Ver também:* ponteiro

**ponto de entrada**

*entry point*

Sentença executável ou etapa do processo que define um ponto em que um determinado processo destina-se a começar.



**predicado**

*predicate*

Uma declaração avaliada se verdadeira ou falsa, usada para determinar o fluxo de controle de lógica de decisão posterior.

*Ver também:* decisão

**pseudo-aleatório**

*pseudo-random*

Série que parece ser aleatória, mas que, de fato, foi gerada de acordo com alguma sequência preestabelecida.

**recuperabilidade**

*recoverability*

Capacidade de um produto de software para estabelecer novamente um nível específico de desempenho e de recuperar os dados diretamente afetados em caso de falha.

*Ver também:* confiabilidade

*Referência:* ISO 9126

**relatório de defeito**

*defect report*

Documento que relata qualquer falha em um componente ou sistema que possa fazer com este componente ou sistema deixe de desempenhar sua função requisitada.

*Sinônimos:* relatório de erro, relatório de problema

*Referência:* pós IEEE-829

**revisão formal**

*formal review*

Revisão caracterizada por procedimentos e requisitos documentados, por exemplo, inspeção.

**semeamento de falhas**

*fault seeding*

Processo de adição intencional de defeitos conhecidos que já estão no componente ou sistema para efeito de controle da taxa de detecção e remoção, e estimar o número de defeitos restantes. Semeamento de falha é tipicamente parte do teste de desenvolvimento (pre-release) e pode ser realizado em qualquer nível do teste (componente, integração, ou do sistema).

*Sinônimos:* depuração, semear erros

*Referência:* pós IEEE-610

**sensibilização de caminho**

*path sensitizing*

Escolha de um conjunto de valores de entrada para forçar a execução de um dado caminho.

**substitutibilidade**

*replaceability*

Capacidade que um produto de software tem para ser utilizado no lugar de outro produto de software específico para os mesmos fins e no mesmo ambiente.

*Ver também:* portabilidade

*Referência:* ISO 9126

**tempo médio de reparo (MTTR)**

*mean time to repair (MTTR)*

Média aritmética (média) do tempo que um sistema levará para se recuperar de eventuais falhas. Isso normalmente inclui testes para garantir que o defeito foi resolvido.

**tempo médio entre falhas (MTBF)**

*mean time between failures (MTBF)*

A média aritmética (média) de tempo entre falhas de um sistema. O MTBF é normalmente parte de um modelo de crescimento da confiabilidade que supõe que o sistema não é imediatamente reparado como parte de um processo de correção de defeitos.

*Ver também:* modelo de crescimento da confiabilidade

**teste analítico**

*analytical testing*

Teste baseado em uma análise sistemática, por exemplo, dos riscos de produtos ou requisitos.

**teste baseado no modelo (MBT)**

*model-based testing (MBT)*

Testes baseados ou envolvendo modelos.

**teste combinatório**

*combinatorial testing*

Técnica de modelagem de teste caixa preta na qual os casos de teste são escritos para executar combinações específicas de valores de vários parâmetros.

*Ver também:* método de classificação por árvore, teste n-wise, teste de pares, teste de arranjo ortogonal

**teste de caminho**

*path testing*

Técnica de modelagem de teste caixa-branca na qual os casos de teste são modelados para executar caminhos.

**teste de carga**

*load testing*

Tipo de teste de desempenho realizado para avaliar o comportamento de um componente ou sistema com carga crescente, por exemplo, número de usuários paralelo e/ou o número de transações, para determinar qual a carga pode ser manipulada por um componente ou sistema.

*Ver também:* teste de performance, teste de stress

**teste de condição**

*condition testing*

Técnica para modelagem de testes caixa-branca onde os casos de teste são modelados para executar o resultado de uma condição.

**teste de condição de decisão**

*decision condition testing*

Técnica de modelagem de teste caixa-branca na qual os casos de teste são modelados para executar resultados de condição e resultados de decisão.

**teste de condição múltipla**

*multiple condition testing*

Técnica caixa-branca de modelagem de teste no qual os casos de teste são modelados para executar combinações de resultados de condição simples (dentro de uma instrução).

*Sinonimos:* teste de combinação de condição de ramificação, teste de combinação de condição

**teste de decisão de condição modificada**

*modified condition / decision testing*

Técnica de teste caixa-branca em que os casos de teste são projetados para ao serem executados obter resultados de única condição que independentemente afetam um resultado da decisão.

*Sinonimos:* teste de determinação de condição, teste de condição múltipla modificado

**teste de escalabilidade**

*scalability testing*

Teste que determina a escalabilidade de um produto de software.

**teste de fluxo de dados**

*data flow testing*

Técnica de modelagem de teste caixa-branca na qual casos de teste são projetados para definir-utilizar a execução de pares de variáveis.

**teste de funcionalidade**

*functionality testing*

Realizado para determinar a funcionalidade de um produto de software.

**teste de instalabilidade**

*installability testing*

Processo de testar a instalabilidade de um produto de software.

*Ver também:* teste de portabilidade

**teste de integração de pares**

*pairwise integration testing*

Uma forma de teste de integração que visa pares de componentes que trabalham em conjunto, como mostrado em um gráfico de chamadas.

**teste de integração de vizinhança**

*neighborhood integration testing*

Uma forma de teste de integração onde todos os nós que se ligam a um determinado nó são a base para o teste de integração.

**teste de pares**

*pairwise testing*

Teste caixa-preta de um projeto no qual os casos de teste são projetados para executar todas as possíveis combinações distintas de cada par de parâmetros de entrada.

*Ver também:* teste combinatório, teste n-wise, teste de arranjo ortogonal

**teste de portabilidade**

*portability testing*

Processo que determina a portabilidade de um produto de software.

*Sinônimos:* teste de configuração

**teste de recuperabilidade**

*recoverability testing*

Processo que determina a recuperabilidade de um produto de software.

*Ver também:* teste de confiabilidade

*Sinônimos:* teste de recuperação

**teste de sistema**

*system testing*

Testa um sistema integrado para verificar se ele atende aos requisitos especificados.

*Referência:* Hetzel

**teste de utilização de recurso**

*resource utilization testing*

Processo que determina a utilização de recursos por um dado produto de software.

*Ver também:* teste de eficiência

*Sinônimos:* teste de armazenamento

**teste negativo**

*negative testing*

Visa mostrar que um componente ou sistema não funciona. O teste negativo se refere mais à atitude do testador do que a uma abordagem de teste específica ou uma técnica de modelagem de teste, por exemplo, o teste com valores de entrada inválidos ou com exceções.

*Sinônimos:* teste sujo

*Referência:* pós Beizer.

**teste sobre falha**

*failover testing*

Teste simulando modos de falha ou causados por falhas conhecidas em um ambiente controlado. Após uma falha, o mecanismo é testado para garantir que os dados não são perdidos ou danificados e que os níveis de serviço acordados sejam mantidos, por exemplo, a disponibilidade de função ou tempos de resposta.

*Ver também:* teste de recuperabilidade

**tolerância a falha**

*fault tolerance*

Capacidade que um produto de software tem para manter um nível específico de desempenho em casos de faltas (defeitos) de software ou de infração de sua interface específica.

*Ver também:* confiabilidade, robustez

*Referência:* ISO 9126

**varredura de vulnerabilidades**

*vulnerability scanner*

Analisador estático que é usado para detectar vulnerabilidades de segurança específicas no código.

**vulnerabilidade de segurança**

*security vulnerability*

Fraqueza no sistema que poderia permitir um ataque de segurança bem-sucedido.