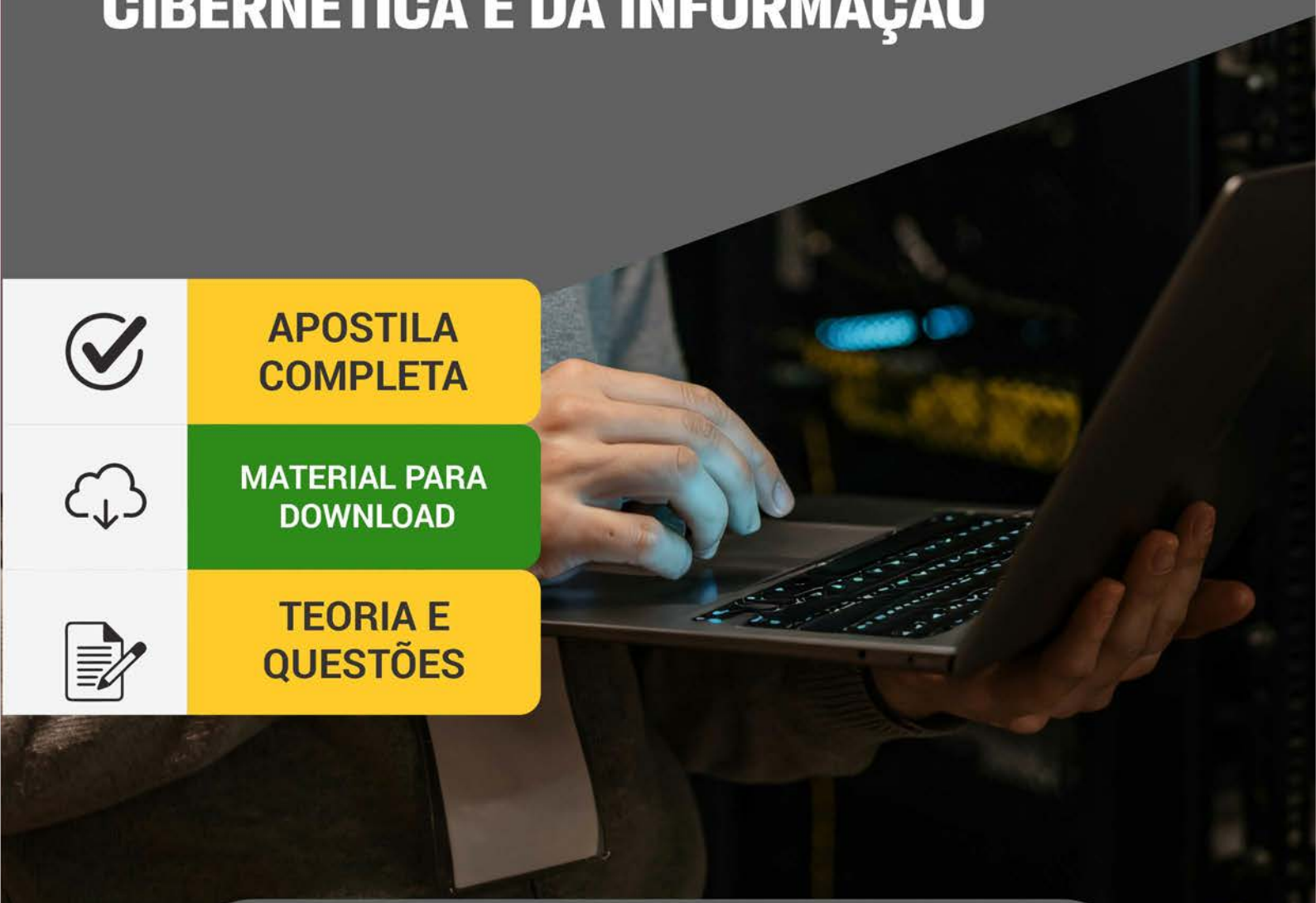
Maxi educa

TRANSPETRO

PETROBRAS TRANSPORTE S.A

ANÁLISE DE SISTEMAS – SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO



- APOSTILA COMPLETA
- MATERIAL PARA DOWNLOAD
- TEORIA E QUESTÕES

EDITAL Nº 4 - TRANSPETRO/PSP/TERRA/NÍVEL SUPERIOR 2026.4, DE 11/08/2026

AVISO IMPORTANTE:

Este é um Material de Demonstração!

Este arquivo é apenas uma amostra do conteúdo completo da Apostila. Aqui você encontrará algumas páginas selecionadas para que possa conhecer a qualidade, estrutura e metodologia do nosso material. No entanto, esta não é a apostila completa.

POR QUE INVESTIR NA APOSTILA COMPLETA?

- Conteúdo totalmente alinhado ao edital
- Teoria clara, objetiva e sempre atualizada
- Diferentes práticas que otimizam seus estudos

Ter o material certo em mãos transforma sua preparação e aproxima você da APROVAÇÃO.

Garanta agora o acesso completo e aumente suas chances de aprovação: https://www.maxieduca.com.br

Maxi educa

SUMÁRIO

Transpetro

Análise de Sistemas – Segurança Cibernética e da Informação

LÍNGUA PORTUGUESA

Compreensão de textos 1
Ortografia oficial 6
Mecanismos de coesão textual 14
Significação das palavras 22
Emprego de tempos e modos verbais. Emprego das classes de palavras 26
Coordenação e de subordinação 40
Emprego dos sinais de pontuação 46
Concordância verbal e nominal 50
Regência verbal e nominal 57
Emprego do sinal indicativo de crase 63
Colocação dos pronomes átonos 68
Questões 70
Gabarito 83

LÍNGUA INGLESA

Compreensão de texto escrito em língua inglesa 1
Itens gramaticais relevantes para a compreensão dos conteúdos semânticos 3
Questões 59
Gabarito 80

CONHECIMENTOS ESPECÍFICOS

Segurança Ofensiva: Conceitos básicos: vulnerabilidades, ameaças e ataques 1
Ataques Passivos: Escuta Passiva e Inferência 7
Ataques Ativos: Escuta Ativa, Disfarce, Repetição e Negação de Serviço 13
Etapas do Ataque: Footprinting, Varredura, Enumeração, Ganho de acesso, Escalação de privilégios, Criação de Porta dos Fundos, Encobrimento de rastros e Recusas de serviço 20

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

SUMÁRIO

Ataques aos protocolos de comunicação: ARP, IP, ICMP, UDP, TCP, DHCP, SMTP, IMAP, POP3, HTTP, FTP, SMB **26**

Ataques à Rede Wi-Fi: Rogue Access Point, Evil Twin, SSID Tracking, Jamming e Disassociation **32**

Ataques do Man-in-the-Middle: Sniffing e Spoofing **37**

Ataques de Engenharia Social: Ciclo de Ataque e Técnicas **43**

Código Malicioso: Vírus, Worm, Trojan Horse, Backdoor, Screenlogger, Keylogger, Injector, Downloader, Flooder, Rootkit, Bot, Botnet, Exploit, Spyware, Ransomware, Cryptojacking e Formjacking **48**

MITRE ATT&CK: matrizes, táticas, técnicas, procedimentos e mitigações **54**

MITRE CAPEC: Padrões de Ataques Cibernéticos, Mecanismos de Ataque, Domínios de Ataque. **60**

Ferramentas de Hacking: amass, aircrack-ng, airgeddon, arpwatch, beef-xss, burpsuite, ettercap, ghidra, hashcat, hydra, john the ripper, nmap, netcat, maltego, steghide, masscan, mimikatz, metasploit-framework, set, smbmap, sqlmap, theharvester, veil, wireshark **64**

Segurança Defensiva: Defesa em profundidade: Perímetro de segurança (Filtro de Pacotes, Firewall de Estado, Firewall Proxy, IDS, IPS, VPN). **69**

Segurança da Informação: Integridade, Autenticidade, Confidencialidade, Autorização de Acesso, Disponibilidade e Irretratabilidade **80**

Mecanismos de Segurança: Resumo de Mensagem, Cifragem de Dados, Assinatura Digital, Envelope Digital, Certificado Digital, Autenticação Multifator, Carimbo do Tempo e Técnicas de Redundância e Tolerância a Falhas **86**

ICP-Brasil: Autoridade Certificadora, Autoridade de Carimbo do Tempo, Organização, Normas e Padrões **92**

Comunicação Segura: TLS, SSL, IPsec **96**

Segurança no Endpoint: Antimalware e Firewall Pessoal **102**

Segurança em Sistemas Operacionais: CIS Benchmarks, Linux e Windows **109**

Segurança em Sistemas de Controle e Automação Industrial: ameaças e vulnerabilidades, ICS Advisory Project, Série ISA/IEC 62443 e NIST SP 800-82 ..... **115**

Forense Digital: Evidência Digital, Processo de Análise Forense, Análise Forense de Dispositivos de Armazenamento, Sites e E-mails e Open Source Intelligence (OSINT) **121**

Compliance de Segurança e Privacidade: Normas: ABNT NBR ISO/IEC 27001:2022 (Versão Corrigida: 2023), ABNT NBR ISO/IEC 27002:2022, ABNT NBR ISO/IEC 27005:2023, ABNT ISO/IEC 27035-1:2023, ABNT NBR ISO 22301:2020, ABNT NBR ISO 22313:2020, ABNT NBR ISO/IEC 29100:2024, ABNT NBR ISO/IEC 29134:2024, ABNT NBR ISO/IEC 27701:2019 (Versão corrigida: 2020) **126**

Frameworks e Controles: The NIST Cybersecurity Framework (CSF) 2.0, CIS Critical Security Controls Version 8.1 ..... **135**

Leis e Regulamentações: Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014, e suas alterações) **140**

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

SUMÁRIO

LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018, e suas alterações) **148**

Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações – ANATEL (Resolução nº 740, de 21 de dezembro de 2020, e suas alterações) **171**

QUESTÕES **180**

GABARITO **185**

SUMÁRIO

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

Língua Portuguesa

A compreensão e a interpretação de textos são habilidades essenciais para que a comunicação alcance seu objetivo de forma eficaz. Em diversos contextos, como na leitura de livros, artigos, propagandas ou imagens, é necessário que o leitor seja capaz de entender o conteúdo proposto e, além disso, atribuir significados mais amplos ao que foi lido ou visto.

Para isso, é importante distinguir os conceitos de compreensão e interpretação, bem como reconhecer que um texto pode ser verbal (composto por palavras) ou não-verbal (constituído por imagens, símbolos ou outros elementos visuais).

Compreender um texto implica decodificar sua mensagem explícita, ou seja, captar o que está diretamente apresentado. Já a interpretação vai além da compreensão, exigindo que o leitor utilize seu repertório pessoal e conhecimentos prévios para gerar um sentido mais profundo do texto. Dessa forma, dominar esses dois processos é essencial não apenas para a leitura cotidiana, mas também para o desempenho em provas e concursos, onde a análise de textos e imagens é frequentemente exigida.

Essa distinção entre compreensão e interpretação é crucial, pois permite ao leitor ir além do que está explícito, alcançando uma leitura mais crítica e reflexiva.

Conceito de Compreensão

A compreensão de um texto é o ponto de partida para qualquer análise textual. Ela representa o processo de decodificação da mensagem explícita , ou seja, a habilidade de extrair informações diretamente do conteúdo apresentado pelo autor, sem a necessidade de agregar inferências ou significados subjetivos. Quando compreendemos um texto, estamos simplesmente absorvendo o que está dito de maneira clara, reconhecendo os elementos essenciais da comunicação, como o tema , os fatos e os argumentos centrais.

A Compreensão em Textos Verbais

Nos textos verbais , que utilizam a linguagem escrita ou falada como principal meio de comunicação, a compreensão passa pela habilidade de ler com atenção e reconhecer as estruturas linguísticas. Isso inclui:

- **Vocabulário :** O entendimento das palavras usadas no texto é fundamental. Palavras desconhecidas podem comprometer a compreensão, tornando necessário o uso de dicionários ou ferramentas de pesquisa para esclarecer o significado.
- **Sintaxe:** A maneira como as palavras estão organizadas em frases e parágrafos também influencia o processo de compreensão. Sentenças complexas, inversões sintáticas ou o uso de conectores como conjunções e preposições requerem atenção redobrada para garantir que o leitor compreenda as relações entre as ideias.
- **Coesão e coerência:** são dois pilares essenciais da compreensão. Um texto coeso é aquele cujas ideias estão bem conectadas, e a coerência se refere à lógica interna do texto, onde as ideias se articulam de maneira fluida e compreensível.

Ao realizar a leitura de um texto verbal, a compreensão exige a decodificação de todas essas estruturas. É a partir dessa leitura atenta e detalhada que o leitor poderá garantir que absorveu o conteúdo proposto pelo autor de forma plena.

A Compreensão em Textos Não-Verbais

Além dos textos verbais, a compreensão se estende aos textosnão-verbais , que utilizam símbolos, imagens, gráficos ou outras representações visuais para transmitir uma mensagem. Exemplos de textos não-verbais incluem obras de arte, fotografias, infográficos e até gestos em uma linguagem de sinais.

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

Língua Inglesa

A compreensão e interpretação de textos em língua inglesa vão muito além da simples tradução de palavras. Esse processo envolve a capacidade de entender o significado global do texto, reconhecer relações entre suas partes e identificar como ele dialoga com outros textos e contextos. Para que isso ocorra de forma eficiente, é fundamental desenvolver tanto o domínio do vocabulário e da estrutura da língua quanto a habilidade de perceber relações intratextuais e intertextuais.

O processo de leitura em inglês requer não apenas o reconhecimento de palavras isoladas, mas a capacidade de entender como essas palavras se organizam para construir significados complexos. Além disso, é essencial que o leitor consiga identificar relações internas no texto, como a coesão entre parágrafos e a progressão de ideias, bem como conexões externas, que envolvem referências a outros textos, contextos históricos, culturais ou literários.

A seguir, o tema será explorado em três partes: o domínio do vocabulário e da estrutura da língua, as relações intratextuais e a intertextualidade no processo de leitura.

Domínio do vocabulário e da estrutura da língua

O primeiro passo para uma compreensão eficaz de textos em inglês é o domínio do vocabulário. O vocabulário pode ser dividido em dois tipos principais:

- **Active vocabulary (vocabulário ativo):** composto por palavras que o leitor é capaz de usar em sua própria produção oral e escrita.
- **Passive vocabulary (vocabulário passivo):** formado por palavras que o leitor reconhece e compreende quando encontra em um texto, mas que pode não usar com frequência em suas próprias falas ou escritas.

Para interpretar textos com precisão, é necessário ampliar o vocabulário passivo, pois ele representa uma grande parte das palavras encontradas em leituras acadêmicas, jornalísticas, literárias e técnicas. Estratégias como a leitura regular de diferentes tipos de textos, o uso de flashcards, a prática de contextos de uso e o estudo de sinônimos e antônimos ajudam a expandir esse repertório.

Além do vocabulário isolado, é fundamental compreender o uso de expressões idiomáticas (idiomatic expressions), phrasal verbs, collocations (combinações de palavras que ocorrem naturalmente) e false cognates (falsos cognatos), que podem levar a interpretações equivocadas se não forem bem conhecidos. Por exemplo, o termo “actually” em inglês significa “na verdade” e não “atualmente”, o que é um erro comum entre estudantes de inglês.

O domínio da estrutura da língua (grammar structures) também é essencial. Isso inclui o conhecimento de tempos verbais (verb tenses), vozes ativa e passiva (active and passive voice), uso de modais (modal verbs), estruturas condicionais (conditional sentences) e conjunções (conjunctions) que conectam ideias. A compreensão da gramática permite que o leitor identifique o papel de cada elemento no texto, facilitando a interpretação de informações implícitas e explícitas.

Por exemplo, ao ler a frase “If I had known about the meeting, I would have attended,” o leitor deve reconhecer que se trata de uma third conditional sentence, que expressa uma situação hipotética no passado, indicando que o falante não sabia da reunião e, portanto, não compareceu. Esse entendimento é crucial para interpretar o significado além das palavras individuais.

O conhecimento gramatical também contribui para a identificação de referências anafóricas e catafóricas (quando um pronome ou termo faz referência a algo já mencionado ou que será mencionado no texto), o que é fundamental para manter a coesão e entender como as ideias se relacionam.

Assim, o domínio do vocabulário e da estrutura gramatical da língua inglesa é o alicerce para uma leitura eficiente, permitindo que o leitor vá além da decodificação de palavras para compreender o significado completo do texto.

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

Segurança ofensiva é o conjunto de práticas destinadas a avaliar sistemas, aplicações, redes, identidades e processos a partir da perspectiva de um possível atacante. Seu objetivo não é provocar danos, mas identificar antecipadamente condições que poderiam ser utilizadas em um incidente real. Dessa forma, a organização consegue compreender sua exposição, validar controles de segurança e corrigir fragilidades antes que sejam exploradas por agentes maliciosos.

Relação entre segurança ofensiva e defensiva

A segurança ofensiva e a segurança defensiva atuam sobre o mesmo problema por perspectivas diferentes. Enquanto a abordagem defensiva busca impedir, detectar e responder a atividades maliciosas, a abordagem ofensiva procura verificar se essas proteções realmente resistem a cenários plausíveis de ataque.

Essa relação pode ser compreendida pelos seguintes papéis complementares:

- **Segurança ofensiva:** identifica fragilidades, simula comportamentos adversários e testa a efetividade dos controles existentes.
- **Segurança defensiva:** monitora ambientes, reduz superfícies de ataque, detecta atividades suspeitas e responde a incidentes.
- **Gestão de riscos:** transforma os resultados técnicos dessas atividades em decisões sobre prioridade, tratamento e investimento.

Um programa maduro de segurança combina essas perspectivas. Encontrar uma vulnerabilidade possui valor limitado se a organização não conseguir compreender seu impacto, definir prioridade e implementar medidas de redução de risco.

Ativos, exposição e superfície de ataque

O conceito de ativo

Um ativo é qualquer recurso que possua valor para uma organização e que, por esse motivo, necessite de proteção. Servidores, estações de trabalho, aplicações, bancos de dados, contas de usuários, informações confidenciais, equipamentos de rede e serviços em nuvem são exemplos comuns.

A análise ofensiva precisa compreender quais ativos existem, como estão conectados e quais consequências podem resultar de seu comprometimento.

Superfície de ataque

A superfície de ataque corresponde ao conjunto de pontos pelos quais um sistema ou organização pode ser alcançado ou influenciado por um possível atacante. Quanto maior e mais complexa essa superfície, maior tende a ser a quantidade de condições que precisam ser protegidas.

Alguns componentes frequentemente presentes nessa superfície incluem:

- Serviços de rede expostos à Internet ou a redes internas.
- Aplicações web, APIs e interfaces administrativas.
- Contas, credenciais, permissões e mecanismos de autenticação.
- Estações de trabalho, dispositivos móveis e equipamentos conectados.
- Usuários suscetíveis a engenharia social ou manipulação.
- Integrações com fornecedores, parceiros e serviços externos.

Esta é apenas uma amostra gratuita. Adquira a apostila completa com desconto clicando aqui.

Maxi educa

GOSTOU DESSE

MATERIAL?

A versão **COMPLETA** é o passo decisivo para você finalmente alcançar a aprovação e mudar sua vida. Ative agora seu DESCONTO ESPECIAL!

QUERO MINHA APROVAÇÃO!