INSTITUTO FEDERAL
Rio Grande do Norte
Campus Natal-Central

CADERNO DE PROVAS

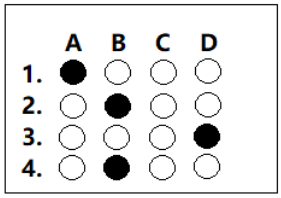
PROVA ESCRITA
PROFESSOR SUBSTITUTO – REDES DE COMPUTADORES

Edital Nº 04/2025 - DIAPE/DG/CNAT/RE/IFRN

11 DE MARÇO DE 2025

INSTRUÇÕES GERAIS PARA A REALIZAÇÃO DA PROVA

- ☑ Use apenas caneta esferográfica azul ou preta.
- ☑ Escreva o seu nome completo e o número do seu documento de identificação no espaço indicado nesta capa.
- ☑ A prova terá duração máxima de 3 (três) horas, incluindo o tempo para responder a **Folha de Resposta.**
- ☑ O **Caderno de Provas** somente poderá ser levado depois de transcorrida 1 (uma) hora do início da aplicação da prova.
- ☑ Confira, com máxima atenção, o **Caderno de Provas**, observando se há defeito(s) de encadernação e/ou de impressão que dificultem a leitura.
- ☑ Confira, com máxima atenção, se os dados (nome do candidato, inscrição, número do documento de identidade, matéria/disciplina e opção de *campus*) constantes na **Folha de Resposta** estão corretos.
- ☑ Em havendo falhas na **Folha de Resposta**, comunique imediatamente ao fiscal de sala.
- ☑ A **Folha de Resposta** não poderá ser dobrada, amassada ou danificada. Em hipótese alguma, será substituída.
- ☑ Assine a **Folha de Resposta** no espaço apropriado.
- ☑ Transfira as respostas para a **Folha de Resposta** somente quando não mais pretender fazer modificações.
- ☑ Cada questão de múltipla escolha apresenta apenas **uma** resposta correta. Para a marcação da alternativa escolhida na **Folha de Respostas,** pinte completamente o campo correspondente conforme figura a seguir:



- ☑ Ao retirar-se definitivamente da sala, entregue a **Folha de Resposta** ao fiscal.

NOME COMPLETO:	DOCUMENTO DE IDENTIFICAÇÃO:

QUESTÕES DE MÚLTIPLA ESCOLHA – REDES DE COMPUTADORES

QUESTÃO N° 01

Um protocolo consiste em um conjunto de regras que regem a comunicação de dados, determinando o que é comunicado, como é comunicado e quando. Assinale a alternativa que apresenta os principais elementos de um protocolo.

A) Ordem, Coordenação e Controle.

B) Sintaxe, Semântica e Sincronismo.

C) Estrutura, Fluxo e Concorrência.

D) Concorrência, Continuidade e Progressão.

QUESTÃO N° 02

A respeito do conjunto de protocolos TCP/IP, que estabelece a comunicação confiável entre dispositivos em redes de computadores, assinale a opção correta:

A) A camada de transporte do modelo TCP/IP realiza o endereçamento lógico, o controle de congestionamento e a fragmentação dos pacotes a serem transmitidos.

B) O IP é responsável por estabelecer e gerenciar a conexão entre dois dispositivos, garantindo a entrega confiável e ordenada de pacotes de dados; ele divide os dados em pacotes e os reagrupa no destino, verificando se todos os pacotes foram entregues corretamente.

C) A camada de transporte do modelo TCP/IP utiliza três protocolos: TCP, UDP e SCTP.

D) O TCP é responsável pelo roteamento e endereçamento dos pacotes de dados na rede; ele fornece a possibilidade de enviar pacotes de dados entre diferentes redes e determinar o melhor caminho para a entrega.

QUESTÃO N° 03

Na arquitetura TCP/IP, qual camada é responsável por permitir que um par de dispositivos de origem e destino mantenha uma conversação?

A) Camada de transporte, que estabelece, mantém e finaliza conexões entre processos em dispositivos distintos.

B) Camada física, que assegura a troca contínua de dados e implementa mecanismos de controle para garantir a integridade da comunicação.

C) Camada de aplicação, que gerencia a interface entre os serviços de rede e os aplicativos do usuário, garantindo a comunicação eficiente entre dispositivos por meio de técnicas de controle de fluxo.

D) Camada de rede, que organiza a fragmentação e remontagem de pacotes, além de realizar o controle de erros e evitar congestionamento durante a transmissão.

QUESTÃO N° 04

Na arquitetura TCP/IP, o enquadramento é uma função essencial da camada de enlace. Ele tem como objetivo:

A) Permitir a transmissão contínua de dados ao estabelecer sincronização entre os dispositivos de origem e destino, garantindo que os quadros sejam corretamente interpretados e reorganizados na camada física.

B) Garantir que os dados sejam transmitidos de maneira confiável, corrigindo erros e controlando o fluxo de pacotes na comunicação fim-a-fim entre dispositivos finais.

C) Adicionar cabeçalhos e *trailers* aos dados recebidos da camada de rede, delimitando os quadros para que o receptor consiga identificar corretamente o início e o fim de cada unidade de transmissão.

D) Realizar a conversão dos pacotes de dados em sinais elétricos, ópticos ou de rádio, permitindo sua transmissão pelo meio físico da rede.

QUESTÃO N° 05

Um analista de tecnologia foi encarregado de projetar uma arquitetura de infraestrutura em nuvem computacional capaz de hospedar uma aplicação escalável e de alta demanda, baseada em microsserviços, constituída por:

- ✓ **Uma aplicação web para acesso dos clientes.**
- ✓ **Um servidor de API RESTful para processar requisições dos clientes.**
- ✓ **Um sistema gerenciador de banco de dados para armazenar as informações da aplicação.**

Diante desses requisitos, qual das alternativas a seguir melhor atende às necessidades do cliente?

A) Uma solução viável para esse arranjo é utilizar contêineres Docker para encapsular cada componente da aplicação. Um proxy reverso como Nginx pode ser configurado para direcionar o tráfego entre a aplicação web e o servidor de API. Além disso, um banco de dados como MySQL ou PostgreSQL pode ser hospedado em um contêiner separado. Para orquestração e gerenciamento dos contêineres, pode-se utilizar Docker Compose para ambientes menores ou Kubernetes para ambientes mais complexos e escaláveis.

B) Uma arquitetura de infraestrutura em nuvem para hospedar uma aplicação escalável baseada em microsserviços pode ser implementada utilizando apenas máquinas virtuais (VMs) sem a necessidade de contêineres atendendo aos requisitos do arranjo. Cada componente da aplicação (web, API e banco de dados) seria hospedado em uma VM separada. O balanceamento de carga pode ser feito manualmente configurando regras em um *firewall*, e o banco de dados pode ser acessado diretamente pelas outras VMs para fornecer mais velocidade.

C) Para hospedar uma aplicação escalável baseada em microsserviços em nuvem, a melhor abordagem seria utilizar um único servidor físico para hospedar todos os componentes da aplicação, incluindo a aplicação web, o servidor de API e o banco de dados. Isso simplificaria a administração e reduziria os custos de infraestrutura. O servidor poderia ser configurado com um sistema operacional como Ubuntu ou CentOS, e todos os serviços seriam executados diretamente no sistema operacional para ter melhor desempenho.

D) Esse arranjo pode ser implementado utilizando serviços *serverless* de provedores de nuvem para

todos os componentes. A aplicação web pode ser hospedada em um serviço como AWS Lambda, o servidor de API pode ser implementado usando Google Cloud Functions, e o banco de dados pode ser substituído por um serviço de armazenamento de objetos como Amazon S3. Essa abordagem elimina a necessidade de gerenciar servidores ou contêineres.

QUESTÃO N° 06

O serviço de DNS (*Domain Name System*) é fundamental para o bom funcionamento das redes baseadas na arquitetura da Internet. O BIND9 (*Berkeley Internet Name Domain*) é um dos servidores DNS mais utilizados no mundo e possui um conjunto de arquivos de configuração e instruções próprias para implementar o bom funcionamento do serviço de resolução de nomes. Sobre o funcionamento e configuração do BIND9, analise as afirmativas abaixo:

I. O BIND9 permite a configuração de zonas de pesquisa direta (*forward zones*) e zonas de pesquisa reversa (*reverse zones*), sendo que as zonas de pesquisa reversa são utilizadas para mapear endereços IP para nomes de domínio.

II. O arquivo `named.conf` é o arquivo de configuração principal do BIND9, onde são definidas as zonas e as opções globais do servidor DNS.

III. O BIND9 suporta apenas a configuração de servidores DNS primários (*masters*), não sendo possível configurar servidores DNS secundários (*slaves*).

IV. A diretiva `allow-transfer` no BIND9 é usada para especificar quais servidores têm permissão para realizar transferências de zona, aumentando a segurança do servidor DNS.

Assinale a alternativa que contém todas as afirmativas corretas.

A) I e II.

B) II e IV.

C) I, II e IV.

D) I, II, III e IV.

QUESTÃO N° 07

O protocolo HTTP (*Hypertext Transfer Protocol*) utiliza códigos de status para indicar o resultado de uma requisição. Esses códigos são divididos em cinco classes, conforme o primeiro dígito do código. Sobre os códigos de status HTTP, analise as afirmativas abaixo:

I. O código `200 OK` indica que a requisição foi bem-sucedida e o recurso solicitado foi encontrado e retornado na resposta.

II. O código `301 Moved Permanently` indica que o recurso solicitado foi movido permanentemente para uma nova URL, e o cliente deve usar a nova URL fornecida no cabeçalho `Location` para futuras requisições.

III. O código `404 Not Found` indica que o servidor não conseguiu encontrar o recurso solicitado, mas que ele pode estar disponível no futuro.

IV. O código `500 Internal Server Error` indica que o servidor encontrou uma situação com a qual não sabe lidar, geralmente devido a um erro no código do servidor.

Assinale a alternativa que contém todas as afirmativas corretas.

A) I e II.

B) II e III.

C) I, II e IV.

D) I, II, III e IV.

QUESTÃO N° 08

O que são MIB (*Management Information Base*) e OID (*Object Identifier*) no contexto do SNMP (*Simple Network Management Protocol*), e qual a relação entre eles?

A) A MIB é um banco de dados hierárquico que armazena informações sobre os dispositivos gerenciados, e os OIDs são identificadores únicos que representam objetos dentro dessa estrutura.

B) A MIB é um protocolo de comunicação que substitui o SNMP, e os OIDs são pacotes de dados trocados entre agentes e gerentes SNMP.

C) A MIB é uma tabela de configuração usada apenas no SNMPv3, e os OIDs são números aleatórios gerados para identificar dispositivos na rede.

D) A MIB é um software utilizado para monitorar redes, e os OIDs são endereços IP atribuídos automaticamente aos dispositivos SNMP.

QUESTÃO N° 09

Qual das seguintes afirmações descreve corretamente a diferença entre SNMPv1, SNMPv2c e SNMPv3?

A) O SNMPv1 e o SNMPv2c são idênticos em termos de funcionalidade e segurança.

B) O SNMPv3 remove o suporte para a MIB e utiliza um novo modelo de gerenciamento.

C) O SNMPv2c é mais lento do que o SNMPv1 devido à sobrecarga de pacotes adicionais.

D) O SNMPv3 introduz mecanismos de autenticação e criptografia, enquanto SNMPv1 e SNMPv2c não possuem segurança avançada.

QUESTÃO N° 10

No SNMPv3, o objeto `snmpEngineBoots` é um contador importante dentro da estrutura da SNMP *engine*. O que esse contador representa?

A) A quantidade de mensagens SNMP processadas pela *engine* desde sua última reinicialização.

B) O tempo total de operação da SNMP *engine* desde sua ativação, medido em segundos.

C) O número de vezes que uma SNMP *engine* foi reinicializada desde que a `snmpEngineID` foi definida, começando com um valor inicial de zero.

D) O número de falhas de autenticação detectadas pela SNMP *engine* em tentativas de comunicação.

QUESTÃO N° 11

O protocolo de roteamento OSPF (*Open Shortest Path First*) é amplamente utilizado para a troca dinâmica de informações dentro de um sistema autônomo (AS). Considerando suas características, assinale a alternativa correta:

A) O OSPF permite organizar conjuntos de redes em áreas, ocultando sua topologia para os demais ASs, contribuindo para otimizar a distribuição das informações de roteamento, sem necessariamente diminuir o volume dessas atualizações.

B) O OSPF possibilita uma configuração flexível de endereços IP, permitindo que cada rota divulgada inclua um destino e uma máscara de sub-rede.

C) No OSPF, sub-redes que compartilham o mesmo número de rede IP podem apresentar topologias distintas ou serem identificadas de maneira independente.

D) A troca de informações de roteamento entre os roteadores de um AS pode ocorrer de maneira mais flexível, uma vez que nem todas as mensagens do OSPF exigem autenticação.

QUESTÃO N° 12

O BGP (*Border Gateway Protocol*) é um protocolo de roteamento responsável por permitir a comunicação entre ASs (Sistemas Autônomos) na Internet. Ele possibilita que os ASs anunciem e aprendam rotas para alcançar diferentes redes. Com base nesse protocolo, julgue as afirmativas abaixo, marcando V para verdadeiro e F para falso.

( ) Roteadores vizinhos estabelecem conexões TCP semipermanentes utilizando a porta 179 para a troca de informações de roteamento.

( ) Os destinos no BGP são prefixos IP expressos em notação CIDR (*Classless Inter-Domain Routing*), podendo representar uma única sub-rede ou um conjunto delas.

( ) Cada AS é identificado por um número único e globalmente reconhecido, atribuído por uma entidade reguladora.

( ) O atributo `AS-PATH` registra os ASs percorridos pelo anúncio de um prefixo, enquanto o atributo `NEXTHOP` define a interface de origem desse anúncio.

A) F, F, F, F.

B) V, V, F, F.

C) V, V, V, F.

D) F, F, F, V.

QUESTÃO N° 13

Os protocolos de roteamento RIPv2 (*Routing Information Protocol version 2*) e RIPng (*RIP Next Generation*) são variações do RIP projetadas para diferentes cenários de rede. Considerando

suas características, assinale a alternativa correta:

A) Ambos utilizam TCP como protocolo de transporte para envio de atualizações de roteamento, garantindo uma comunicação confiável entre os dispositivos da rede.

B) O protocolo RIPng é compatível com IPv6, enquanto o RIPv2 foi desenvolvido para operar exclusivamente com IPv4.

C) Tanto o RIPv2 quanto o RIPng utilizam a porta UDP 520, independentemente do tipo de endereço IP empregado na comunicação.

D) O protocolo RIPng adota a abordagem de estado de enlace (*link-state*) para cálculo de rotas, enquanto o RIPv2 segue o modelo vetor de distância (*distance-vector*).

QUESTÃO N° 14

Sobre os *firewalls* é correto afirmar que:

A) Os do tipo *stateful inspection* mantêm o controle do estado das conexões ativas, podendo permitir ou negar o tráfego com base nestas informações de estado.

B) Uma das características dos *firewalls* de próxima geração para o protocolo IPv4 é trabalhar sempre com a política padrão de descarte de pacotes.

C) Com a adoção do protocolo IPv6, perderão grande parte de sua aplicabilidade, dada as funcionalidades de filtragem intrínsecas a este protocolo.

D) Possuem como característica a incapacidade de analisar informações da camada de aplicação. Quando necessário esta análise é delegada a outros tipos de ferramentas.

QUESTÃO N° 15

Sobre criptografia e as tecnologias dela derivada é correto afirmar que:

A) Assinaturas digitais podem ser emitidas por qualquer usuário da criptografia assimétrica, usando para tanto uma chave compartilhada com o destino.

B) Um certificado digital é um documento emitido por uma autoridade certificadora; para tanto ela assina digitalmente um conjunto de informações com sua chave privada.

C) Quando comparamos um algoritmo assimétrico, como o RSA, com um simétrico, como o AES, o RSA terá menor peso computacional nas operações de cifragem.

D) Uma das propriedades básicas de uma função de HASH criptográfico, como o SHA, é que deve ser computacionalmente viável encontrar duas informações “X” e “Y”, que sejam diferentes, mas que possuam o mesmo HASH.

QUESTÃO N° 16

Por meio de um *pentest* podemos simular ataques e identificar/explorar vulnerabilidades em um sistema, rede ou aplicação. Para sua realização existe uma série de metodologias formais

definidas. Uma atividade da etapa inicial de um *pentest* é:

A) A análise estática do código fonte das aplicações utilizadas nos sistemas alvos para encontrar erros de programação.

B) A exploração de vulnerabilidades conhecidas utilizando *exploits* já existentes e utilizados.

C) A realização de uma varredura de portas para mapear os serviços em execução nos sistemas alvos.

D) A realização de ataques direcionados a aplicações web, dado que esses comumente são utilizados para a obtenção de persistência.