



Escola de Administração Fazendária



**Prova Objetiva 2 e
Prova Discursiva**

Cargo: Analista Administrativo

**Área: Tecnologia da Informação e Comunicação - Administração
de Redes e Segurança de Informações**

Nome: _____ N. de Inscrição _____

Instruções

1. Escreva seu nome e número de inscrição, de forma legível, nos locais indicados.
2. O CARTÃO DE RESPOSTAS tem, obrigatoriamente, de ser assinado. Esse CARTÃO DE RESPOSTAS não poderá ser substituído, portanto, não o rasure nem o amasse.
3. Transcreva a frase abaixo para o local indicado no seu CARTÃO DE RESPOSTAS em letra *cursiva*, para posterior exame grafológico:
“As ideias e estratégias são importantes, mas o verdadeiro desafio é a execução”.
(Percy Barnevik)
4. DURAÇÃO DAS PROVAS: **4 horas**, incluído o tempo para a elaboração da Prova Discursiva e para o preenchimento do CARTÃO DE RESPOSTAS.
5. Na prova objetiva há **40 questões** de múltipla escolha, com cinco opções: a, b, c, d e e.
6. No CARTÃO DE RESPOSTAS, as questões estão representadas pelos seus respectivos números. Preencha, **FORTEMENTE**, com caneta esferográfica (tinta azul ou preta), toda a área correspondente à opção de sua escolha, sem ultrapassar as bordas.
7. Será anulada a questão cuja resposta contiver emenda ou rasura, ou para a qual for assinalada mais de uma opção. Evite deixar questão sem resposta.
8. Ao receber a ordem do Fiscal de Sala, confira este CADERNO com muita atenção, pois nenhuma reclamação sobre o total de questões e/ou falhas na impressão será aceita depois de iniciadas as provas.
9. Durante as provas, não será admitida qualquer espécie de consulta ou comunicação entre os candidatos, tampouco será permitido o uso de qualquer tipo de equipamento (calculadora, tel. celular etc.).
10. Por motivo de segurança, somente durante os trinta minutos que antecedem o término das provas, poderão ser copiados os seus assinalamentos feitos no CARTÃO DE RESPOSTAS, conforme subitem 6.5 do edital regulador do concurso.
11. A saída da sala só poderá ocorrer depois de decorrida uma hora do início das provas. A não-observância dessa exigência acarretará a sua exclusão do concurso.
12. Ao sair da sala entregue este CADERNO DE PROVAS, juntamente com o CARTÃO DE RESPOSTAS, ao Fiscal de Sala.

Quanto à Prova Discursiva:

1. Identifique-se apenas na capa da prova (**página 7**); sua Prova Discursiva **não** poderá ser assinada ou rubricada nem conter marcas ou sinais identificadores.
2. Use as folhas pautadas deste caderno para desenvolver sua Prova Discursiva.
3. As folhas em branco, no final do caderno, poderão ser usadas para rascunho.
4. Não escreva no espaço à direita “Reservado ao Examinador”.

Boa prova!

CONHECIMENTOS ESPECÍFICOS

- 1 - A camada da arquitetura Internet TCP/IP, responsável pela transferência de dados fim-a-fim, é a
- Física.
 - Enlace.
 - Rede.
 - Transporte.
 - Aplicação.
- 2 - Se um comutador de circuitos opera com N circuitos, o total de entradas e saídas é
- 2N
 - N
 - N/2
 - N + 2
 - 2N + 2
- 3 - O número de conexões necessárias, ao considerar uma topologia de rede em malha para N máquinas, é
- $(N - 1)/2$
 - $N(N - 1)$
 - $N(N - 1)/2$
 - N/2
 - 2N
- 4 - O campo do segmento TCP usado para o controle de fluxo é o(a)
- número de sequência.
 - número de reconhecimento.
 - ponteiro de urgência.
 - flag*.
 - janela de recepção.
- 5 - Quando um usuário acessa *e-mails* por meio de navegadores *Web* (o agente de usuário é o navegador), neste caso, o protocolo utilizado é o
- POP3.
 - Telnet.
 - FTP.
 - IMAP.
 - HTTP.
- 6 - O protocolo de aplicação baseado em duas conexões TCP, cuja conexão de controle opera fora de banda, é denominado
- Protocolo de transferência hiper-texto (HTTP).
 - Protocolo de transferência de mensagens simples (SMTP).
 - Protocolo de serviço de nomes (DNS).
 - Protocolo de transferência de arquivos (FTP).
 - Protocolo de sistema de arquivos de rede (NFS).
- 7 - O campo do quadro Ethernet, cuja função é auxiliar na recepção de nós sincronizados, é o
- endereço de destino.
 - endereço de origem.
 - preâmbulo.
 - tipo.
 - CRC.
- 8 - Para endereçar 16 sub-redes em uma rede cujo endereço é 150.0.0.0, a máscara adequada a ser aplicada é
- 150.0.0.0/20
 - 150.0.0.0/16
 - 150.0.0.0/12
 - 150.0.0.0/8
 - 150.0.0.0/0
- 9 - É exemplo de protocolo que usa UDP na camada de transporte:
- NFS
 - FTP
 - HTTP
 - DHCP
 - SMTP
- 10- Ao fragmentar um fragmento, que não seja o último fragmento de um datagrama, o roteador IP deve
- ativar o bit do *flag* 'mais fragmentos' em todos os sub-fragmentos que produzir, exceto no último deles.
 - ativar o bit do *flag* 'não fragmente'.
 - ficar inativo, pois é impossível ocorrer esta situação em redes IP.
 - ativar o bit do *flag* 'mais fragmentos' apenas do primeiro subfragmento que produzir.
 - ativar o bit do *flag* 'mais fragmentos' em todos os sub-fragmentos que produzir.

- 11- Para resolver o problema de alto tráfego e processamento ARP, em uma rede de grande porte, o equipamento recomendado é
- concentrador.
 - ponte.
 - roteador.
 - sistema de detecção de intrusos (sdi).
 - repetidor.
- 12- Três segmentos de rede que formam um único domínio de colisão são interconectados por
- comutador de comutação acelerada.
 - comutador de armazenamento-e-repasse.
 - roteador.
 - roteador com comutação.
 - concentrador.
- 13- Um registro de recurso DNS é uma tupla composta pelos campos
- Name, Value, TTL.
 - Name, Value, Type.
 - Name, Type, TTL.
 - Name, Value, Type, Cache.
 - Name, Value, Type, TTL.
- 14- O campo da mensagem do servidor DNS que especifica a operação solicitada e um código de resposta associado é denominado
- identificação.
 - parâmetro.
 - seção de perguntas.
 - seção de respostas.
 - seção de autoridades.
- 15- Se um cliente interrompe imediatamente o uso de um endereço IP e retorna ao estado INICIALIZA, ele recebeu do servidor DHCP, a mensagem
- DHCPNACK
 - DHCPREQUEST
 - DHCPPACK
 - DHCPOFFER
 - DHCPDISCOVER
- 16- É função do gerenciamento de falhas:
- medir e analisar o desempenho dos componentes da rede.
 - verificar, a longo prazo, as demandas variáveis de tráfego e falhas ocasionais na rede.
 - tratamento de falhas transitórias da rede.
 - controlar o acesso aos recursos da rede.
 - contabilizar a utilização de recursos da rede.
- 17- Analise as seguintes afirmações relativas aos recursos de segurança providos pelo protocolo SNMPv3:
- O controle de acesso às informações de gerenciamento de redes é baseado em visões.
 - É usado o algoritmo DES no modo de endereçamento de blocos de cifras.
 - Há proteção contra ataques de reprodução, com base em um contador no receptor.
- Indique a opção correta.
- Apenas as afirmações I e II são verdadeiras.
 - Apenas as afirmações I e III são verdadeiras.
 - Apenas as afirmações II e III são verdadeiras.
 - As afirmações I, II e III são verdadeiras.
 - Nenhuma das afirmações é verdadeira.
- 18- Ferramentas clientes de correio eletrônico são capazes de exibir dados não-ASCII via mensagem padrão de correio eletrônico devido
- à flag de sincronização.
 - ao HTML.
 - à MIME.
 - ao metadado.
 - à representação externa de dados (XDR).
- 19- O protocolo capaz de compensar a variação de atraso e a perda de sequência dos pacotes em redes IP é o protocolo
- transporte em tempo real (RTP).
 - reserva de recursos (RSVP).
 - controle de transmissão (TCP).
 - mensagens de controle Internet (ICMP).
 - intercâmbio programado (IP).

- 20- A mensagem de requisição do protocolo de inicialização de sessão (SIP), que permite ao cliente conhecer as capacidades do servidor, é denominada
- Invite.
 - Register.
 - Options.
 - ACK.
 - Priority.
- 21- Em redes sem fio, o fenômeno no qual porções de onda eletromagnética que refletem em objetos e no solo, seguindo caminhos de comprimentos variados entre emissor e receptor, é denominado
- redução da força do sinal.
 - interferência de outras fontes.
 - atenuação de percurso.
 - propagação multivias.
 - deslocamento de faixa de alcance.
- 22- O padrão IEEE 802.11, caracterizado por atuar numa faixa de frequências de 2.4 a 2.485 Ghz, com taxa de dados de até 54 Mbps, é o
- 802.11a
 - 802.11b
 - 802.11g
 - 802.11i
 - 802.11q
- 23- O protocolo que fornece autenticação e criptografia de dados entre hospedeiros e um ponto de acesso em redes sem fio, num esquema baseado em chaves simétricas compartilhadas, é o(a)
- algoritmo de troca de chaves na Internet (IKE).
 - privacidade equivalente sem fio (WEP).
 - protocolo de autenticação de cabeçalho (AH).
 - protocolo de segurança de encapsulamento de carga útil (ESP).
 - protocolo extensível de autenticação (EAP).
- 24- Analise as seguintes afirmações sobre o protocolo de reserva de recursos (RSVP):
- Oferece apenas dois tipos de serviços: carga controlada e serviço garantido.
 - O serviço de carga controlada requer largura de banda específica.
 - O serviço garantido requer o estabelecimento de um atraso máximo.
- Assinale a opção correta.
- Apenas as afirmações I e II são verdadeiras.
 - Apenas as afirmações I e III são verdadeiras.
 - Apenas as afirmações II e III são verdadeiras.
 - As afirmações I, II e III são verdadeiras.
 - Nenhuma das afirmações é verdadeira.
- 25- A técnica de enfileiramento que ordena o fluxo de pacotes em diversas filas lógicas, com prioridades associadas, é:
- Primeiro a chegar, primeiro a ser atendido (FCFS).
 - Primeiro a chegar, último a ser atendido (FCLS).
 - Enfileiramento justo (FQ).
 - Enfileiramento baseado em classes (CBQ).
 - Enfileiramento justo balanceado (WFQ).
- 26- No gerenciamento de projetos, as informações de saída da fase de planejamento são entradas para os processos de
- Início.
 - Execução.
 - Controle.
 - Monitoramento.
 - Fechamento.
- 27- A tecnologia utilizada para implementar estruturas de serviço diferenciado (*diffserv*) e redes privadas virtuais (VPNs), baseada em roteadores de comutação de rótulos, é denominada
- Frame Relay.
 - Comutação acelerada.
 - Comutação com roteamento.
 - Comutação de rótulos multiprotocolo (MPLS).
 - ATM.

- 28- A quantidade de canais virtuais permanentes necessários para conectar N pontos de entrada a N pontos de saída em redes ATM é
- N
 - $N(N - 1)$
 - 2N
 - $N - 1$
 - $2N - 1$
- 29- Se a variável de ambiente PATH, considerando o *Bash Shell*, contém inicialmente `/bin:/usr/bin:/usr/X11R6/bin`, após a execução do comando `$ export PATH = $PATH:/usr/local/bin`, o valor da variável PATH será
- `/bin:/usr/bin:/usr/X11R6/bin`
 - `/bin:/usr/bin:/usr/X11R6/bin:/usr/local/bin`
 - `/bin:/usr/local/bin`
 - `/usr/local/bin`
 - `/bin:/usr/bin:/usr/local/bin`
- 30- São critérios a serem considerados para a classificação da informação:
- Os requisitos legais associados à informação.
 - O valor da informação.
 - Criticidade da informação para o negócio.
- Assinale a opção correta.
- Apenas as afirmações I e II são verdadeiras.
 - Apenas as afirmações I e III são verdadeiras.
 - Apenas as afirmações II e III são verdadeiras.
 - As afirmações I, II e III são verdadeiras.
 - Nenhuma das afirmações é verdadeira.
- 31- Um risco de segurança pode ser considerado uma função da ameaça em relação a
- impacto, apenas.
 - probabilidade de ocorrência, apenas.
 - ocorrência ou não da ameaça.
 - ocorrência ou não da ameaça, num intervalo de tempo pré-especificado.
 - impacto e probabilidade de ocorrência.
- 32- Os procedimentos para a recuperação de operações, na escala de tempo estipulada, após a ocorrência de falhas de processos críticos do negócio, devem constar do(a)
- Plano de continuidade.
 - Política de segurança.
 - Auditoria de segurança.
 - Acordo de confidencialidade.
 - Política de senhas.
- 33- A política de segurança de uma organização pressupõe, primordialmente,
- a publicação do documento em meios de comunicação variados.
 - a análise crítica regularmente, em intervalos planejados.
 - a aprovação da direção e a conformidade com requisitos de negócio.
 - a declaração de responsabilidades para a segurança da informação.
 - a identificação dos riscos relacionados com partes externas.
- 34- Os algoritmos MD5 e SHA-1 são amplamente utilizados em
- assinatura digital.
 - criptografia simétrica.
 - criptografia assimétrica.
 - planos de contingência.
 - planos de *backup*.
- 35- No contexto de detecção de intrusos, a ausência de alerta quanto à ocorrência de um evento real representa
- falso positivo.
 - falso negativo.
 - inundação de alertas.
 - ação de *sniffers*.
 - ação de *proxies*.
- 36- O mecanismo de controle de acesso adequado para bloquear segmentos UDP e conexões FTP, em uma rede, é o(a)
- sistema de detecção de intrusos (SDI).
 - firewall de filtragem de pacotes.
 - rede privada virtual (VPN).
 - gateway de aplicação.
 - rede local virtual (VLAN).

37- O(A) _____ representa um ataque que compromete diretamente a disponibilidade.

Assinale a opção que completa corretamente a frase acima.

- a) cavalo de tróia
- b) falsificação
- c) negação de serviço
- d) *phishing*
- e) *sniffing*

38- O código malicioso caracterizado por ser executado independentemente, consumindo recursos do hospedeiro para a sua própria manutenção, podendo propagar versões completas de si mesmo para outros hospedeiros, é denominado

- a) vírus.
- b) *backdoor*.
- c) *cookie*.
- d) verme.
- e) *spyware*.

39- O pacote inteiro em uma extremidade VPN é criptografado – cabeçalho e dados. Nesse caso, os roteadores identificam o endereço-destino

- a) por meio de um circuito virtual permanente, criado previamente.
- b) através de um circuito virtual temporário entre os envolvidos, previamente estabelecido.
- c) por meio de pacotes não são criptografados em VPNs.
- d) através de um túnel P estabelecido após a criptografia dos pacotes.
- e) por meio de um cabeçalho não-criptografado contendo as informações de endereço adicionado aos pacotes criptografados.

40- Considere um grupo de N usuários em um esquema de criptografia assimétrica. O número total de encriptações/decriptações para o envio/recepção de uma mensagem confidencial M de um usuário para os outros (N – 1) usuários do mesmo grupo é

- a) N
- b) 2N
- c) 2(N – 1)
- d) 2N – 1
- e) 2N + 1