



TRIBUNAL DE CONTAS DO ESTADO DO PARÁ

CONCURSO PÚBLICO – EDITAL Nº 01/2024

TARDE

AUDITOR DE CONTROLE EXTERNO – ÁREA DE INFORMÁTICA

ANALISTA DE SEGURANÇA

NÍVEL SUPERIOR TIPO 1 – BRANCA



SUA PROVA

- Além deste caderno contendo **5 (cinco)** questões discursivas você receberá do fiscal de sala as folhas de textos definitivos;
- Cada questão discursiva deverá ser redigida em até **25 (vinte e cinco)** linhas.



TEMPO

- Você dispõe de **4 (quatro) horas** para a realização da prova, já incluído o tempo para a marcação do cartão de respostas e o preenchimento das folhas de textos definitivos;
- **1 (uma) hora e 30 (trinta) minutos** após o início da prova, é possível retirar-se da sala, sem levar o caderno de questões;
- A partir dos **30 (trinta) minutos** anteriores ao término da prova é possível retirar-se da sala **levando o caderno de questões**.



NÃO SERÁ PERMITIDO

- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova;
- Anotar informações relativas às respostas em qualquer outro meio que não seja o caderno de questões;
- Levantar da cadeira sem autorização do fiscal de sala;
- Usar o sanitário ao término da prova, após deixar a sala.



INFORMAÇÕES GERAIS

- Verifique se seu caderno de questões está completo, sem repetição de questões ou falhas. Caso contrário, **notifique imediatamente o fiscal da sala**, para que sejam tomadas as devidas providências;
- Confira seus dados pessoais, especialmente nome, número de inscrição e documento de identidade e leia atentamente as instruções para preencher as folhas de textos definitivos;
- Para o preenchimento das folhas de textos definitivos, use somente caneta esferográfica, fabricada em material transparente, com tinta preta ou azul;
- Assine seu nome apenas no(s) espaço(s) reservado(s) na folha de textos definitivos;
- Confira seu cargo, cor e tipo do caderno de questões. Caso tenha recebido caderno de cargo ou cor ou tipo **diferente** do impresso em sua folha de textos definitivos, o fiscal de sala deve ser **obrigatoriamente** informado para o devido registro na ata da sala;
- Reserve tempo suficiente para o preenchimento das suas folhas de textos definitivos. O preenchimento é de sua responsabilidade e **não será permitida a troca de folha de texto definitivo em caso de erro cometido pelo candidato**;
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas nas folhas de textos definitivos;
- A FGV coletará as impressões digitais dos candidatos na lista de presença;
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída de sanitários durante a realização das provas.
- **Boa prova!**

Questão 1

O Tribunal de Contas do Estado do Pará (TCE-PA) está implementando uma série de medidas para garantir a segurança da informação em seus sistemas e processos. O uso de criptografia, protocolos criptográficos, assinaturas digitais e certificados digitais são componentes essenciais dessa estratégia.

Considerando o cenário acima, responda ao que se pede a seguir sobre criptografia e assinatura digital.

- a) Explique a diferença entre criptografia simétrica e criptografia assimétrica com relação ao emprego das chaves criptográficas.**
- b) Cite um exemplo de algoritmos utilizados para criptografia simétrica e um exemplo para criptografia assimétrica.**
- c) Explique o processo para assinar digitalmente um documento a ser transmitido.**

Obs.: descreva o processo de verificação de uma assinatura digital em um documento que foi recebido.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

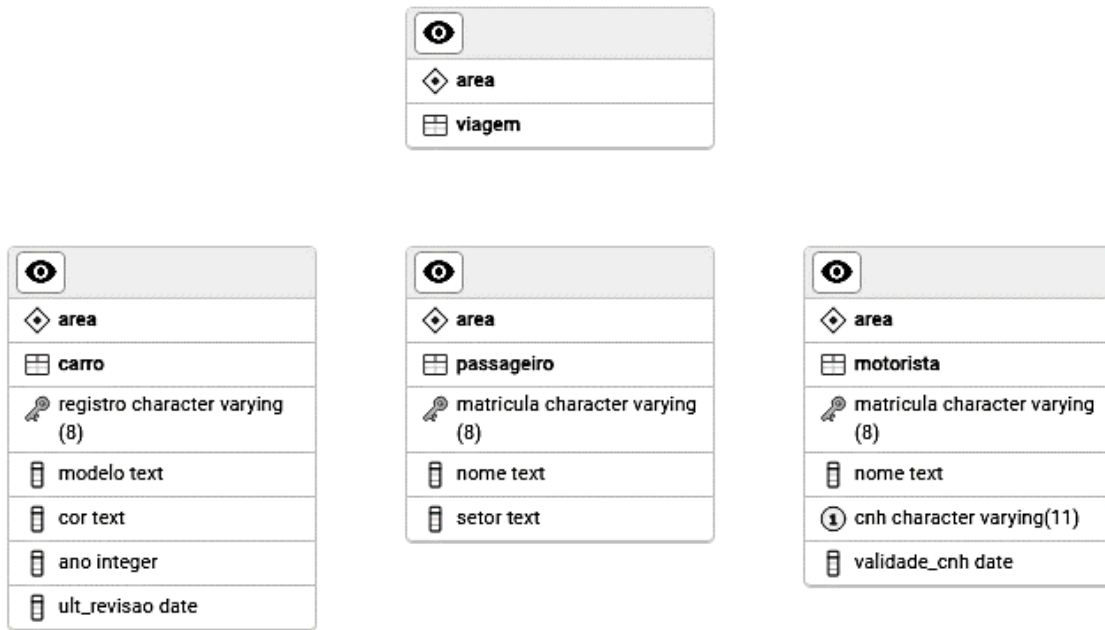
22

23

24

25

Questão 2



No modelo relacional ilustrado na figura acima, a tabela viagem deverá armazenar informações sobre as viagens realizadas a serviço, incluindo o carro utilizado, o motorista responsável e a pessoa a ser transportada. Devem ser ainda registrados detalhes como o destino, data e hora do início e do fim da viagem, preservando a consistência temporal dos valores referentes ao início e ao fim da viagem.

Diante do exposto, pede-se:

- especifique atributos, tipos e restrições da tabela viagem;
- especifique restrições no relacionamento entre as tabelas;
- Elabore consulta SQL para inserir valores ao iniciar a viagem.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Questão 3

Em uma análise para aumentar a segurança da rede de sua empresa, um projetista resolveu implementar os seguintes elementos de segurança:

1 firewall X conectado à Internet e a um segmento de rede A.

1 firewall Y conectado aos segmentos de redes A, B e C.

1 servidor de VPN na rede B para conexões tipo client-to-site.

Na rede A foi posicionado um servidor web que visa a atender requisições vindas da Internet.

Na rede B foram colocados os computadores dos funcionários da empresa

Na rede C foram colocados os servidores para o funcionamento do negócio da empresa.

Diante do exposto, pede-se:

- a) **Indique como é chamada a solução de segurança implementada pelo segmento de rede A, e como ela ajuda na segurança da rede.**
- b) **Compare as políticas de segurança que devem ser implementadas nos firewalls X e Y e identifique qual deve ser mais restritivo e por quê.**
- c) **Sob o viés de segurança, os segmentos de rede B e C devem ser segregadas? Por quê?**
- d) **Qual o objetivo do servidor VPN instalado? Explique se ele foi colocado no segmento correto (ou não) para atingir tal objetivo.**

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Questão 4

Em um cenário corporativo, uma grande empresa de tecnologia implementou recentemente uma solução de EDR (*Endpoint Detection and Response*) para melhorar sua conduta relacionada à segurança cibernética. Essa implementação foi motivada por uma série de tentativas de ataques que foram identificadas e neutralizadas graças à nova solução. A empresa agora busca compreender melhor os benefícios e desafios associados ao EDR, além de explorar o futuro dessa tecnologia.

Diante da situação descrita, pede-se:

- a) explique o que é EDR e citar três exemplos de endpoints.
- b) Cite e detalhe três principais funcionalidades de uma solução de EDR.
- c) Explique a diferença entre EDR e antivírus tradicional.
- d) Explique a principal diferença entre EDR e XDR em termos de visibilidade e alcance.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Questão 5

Em uma aplicação de troca de mensagens corporativo utilizado por uma empresa, não eram empregados protocolos para garantir a segurança das mensagens transmitidas. Com a intenção de melhorar a segurança na troca de mensagens, foi proposta uma nova versão da aplicação, que utiliza criptografia capaz de prover a confidencialidade e autenticidade das mensagens trocadas pelos integrantes da empresa. Entretanto, há uma preocupação grande com a eficiência da aplicação, devido ao alto tráfego de mensagens.

Diante do exposto, pede-se:

- a) À luz da preocupação com eficiência da cifração e decifração das mensagens, qual tipo de criptografia deve ser empregado para garantir a confidencialidade das mensagens? Explique por que escolheu esse tipo de criptografia.
- b) Cite um exemplo de implementação do tipo de criptografia escolhido no item a).
- c) Qual tipo de criptografia deve ser empregado para garantir a autenticidade das mensagens? Explique o porquê de tal necessidade.
- d) Cite um exemplo de implementação do tipo de criptografia escolhido no item c).
- e) É possível utilizar os dois tipos de criptografia em uma única solução? Explique ou esquematize a solução completa, mostrando como ela provê autenticidade e confidencialidade.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Realização

