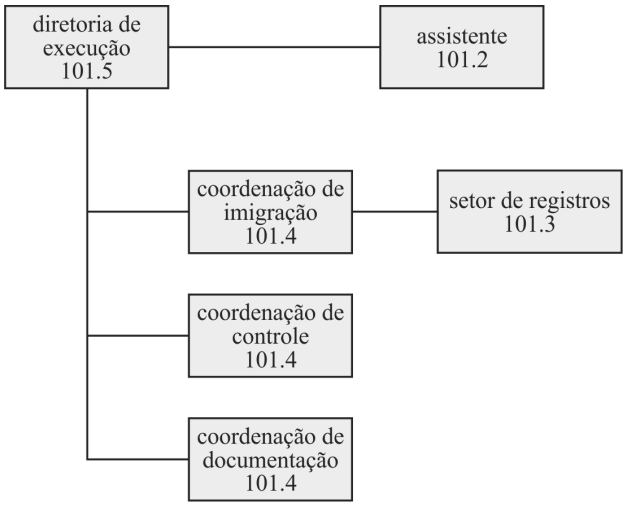
CONHECIMENTOS ESPECÍFICOS



As informações de um departamento e de seus colaboradores devem ser organizadas e armazenadas conforme a estrutura mostrada no diagrama precedente. Para isso, serão utilizados os comandos DDL a seguir.

```
create table organograma (
   id integer primary key,
   descricao varchar(50),
   cargo varchar(50),
   pai integer,
   constraint fk_organograma foreign key (pai)
references organograma
);

create table colaborador (
   cpf bigint primary key,
   nome varchar(50),
   data_nascimento date
);

create table colaborador_organograma
(
   cpf bigint,
   cargo integer,
   data_nomeacao date,
   data_exoneracao date,
   constraint pk_colaborador_organograma primary
key (cpf, cargo),
   constraint     fk_colaborador_organograma_cpf
foreign key (cpf) references colaborador,
   constraint   fk_colaborador_organograma_cargo
foreign key (cargo) references organograma (id)
);
```

Tendo como referência as informações apresentadas, julgue os próximos itens.

51 A tabela `colaborador` está na primeira forma normal.

52 A seguir, é apresentado o diagrama entidade-relacionamento correto para os comandos DDL em questão.

53 A seguir, são apresentadas as expressões SQL corretas para inserir na tabela organograma as informações constantes do diagrama apresentado.

```
insert into organograma (id, descricao, cargo,
pai) values (1, 'assistente', '101.2', 2);

insert into organograma (id, descricao, cargo,
pai) values (2, 'coordenação de imigração',
'101.4', 1);

insert into organograma (id, descricao, cargo,
pai) values (3, 'coordenação de controle',
'101.4', 1);

insert into organograma (id, descricao, cargo,
pai) values (4, 'coordenação de documentação',
'101.4', 1);

insert into organograma (id, descricao, cargo,
pai) values (5, 'setor de registros', '101.3', 3);

insert into organograma (id, descricao, cargo)
values (6, 'diretor de execução', '101.5');
```

54 O comando SQL a seguir permite apagar o conteúdo da tabela `colaborador_organograma`.

```
delete from colaborador_organograma;
```

55 Depois de executados os comandos SQL a seguir, nenhum registro será inserido na tabela `colaborador`.

```
BEGIN TRANSACTION;
   INSERT     into     colaborador     values
('11111111111', 'Clark Stark', '01-03-1963');
   INSERT     into     colaborador     values
('22222222222', 'Antonio Parker', '03-08-1962');
   ROLLBACK;
END TRANSACTION;
```

56 Em uma transação, durabilidade é a propriedade que garante que os dados envolvidos durem por tempo necessário e suficiente até que sejam excluídos.

Acerca de banco de dados, julgue os itens seguintes.

57 Em um banco de dados relacional, os dados são armazenados em tabelas; e as tabelas, organizadas em colunas.

58 NoSQL são bancos de dados que não aceitam expressões SQL e devem ser armazenados na nuvem.

No que se refere aos conceitos de estratégias de distribuição de banco de dados, julgue os itens que se seguem.

59 Na replicação síncrona, recomenda-se que os bancos de dados fiquem armazenados em sítios geograficamente distantes entre si, pois a execução da replicação ocorrerá com um atraso, que varia de poucos minutos a horas.

60 Disponibilidade de um sistema de banco de dados distribuído é, por definição, a característica de o sistema estar sempre disponível para ser utilizado imediatamente.

Julgue os itens seguintes, a respeito de sistema de arquivos.

61 Um disco formatado com sistema de arquivos FAT32 permite armazenar arquivos de tamanho de até 120 gigabaites.

62 NTFS deve ser usado se os arquivos do disco rígido são criptografados no nível de sistema que utilize *encrypting file system*.

63 Para disco rígido utilizado em ambiente Windows 95, recomenda-se adotar o sistema de arquivos HFS+.

64 APFS é uma evolução do sistema de arquivos mais usado no ambiente Linux, a partir da implementação do *journaling* no sistema de arquivos.

Julgue os itens subsecutivos, no tocante a características de computadores e seus componentes.

65 Memória *cache* é o local onde devem estar armazenados os programas e dados a serem manipulados pelo processador.

66 *Seek time* é o tempo que a cabeça de leitura e gravação de um disco rígido leva para ir de uma trilha a outra do disco.

67 Um processador *multicore* permite que o computador execute tarefas gráficas mais complexas, ou seja: quanto mais núcleos, melhor a qualidade dos gráficos.

68 Processadores de 32 bites aproveitam, no máximo, 4 GB de RAM.

Acerca das técnicas de recuperação de arquivos de um computador, julgue os itens subsequentes.

69 *File recovery* é a recuperação de arquivos com base em índice de sistemas de arquivos.

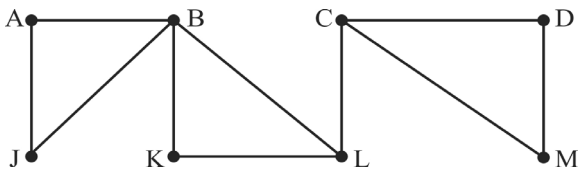
70 O registro do Windows é um arquivo do sistema no qual são guardados todos os usuários dos aplicativos, para o controle do nível de acesso aos respectivos dados.

No que concerne a sistemas operacionais e tecnologias de virtualização, julgue os itens seguintes.

71 Emulador permite a um programa feito para um computador ser executado em outro computador.

72 Um sistema operacional classificado como multitarefa é aquele em que vários processos de utilizador (tarefas) estejam carregados em memória; nesse caso, um pode estar ocupando o processador e outros ficam enfileirados, aguardando a sua vez.

73 *Container* consiste em um conjunto de processos que, isolados do resto do sistema, são executados a partir de uma imagem distinta, que fornece todos os arquivos necessários a eles.



Considerando a terminologia e os conceitos básicos de grafos, julgue os itens a seguir, relativos ao grafo precedente.

74 Os vértices A, B, C, D, J, K, L, M têm graus iguais, respectivamente, a 2, 4, 3, 2, 2, 2, 3, 2.

75 No grafo em apreço, existem três ciclos com comprimento quatro: AJBA, BKLB e CDMC.

76 O grafo em questão tem diâmetro igual a quatro.

Em relação às estruturas de controle e de fluxo de execução, julgue os itens seguintes.

77 Nos laços de repetição *while* e *for*, a condição é verificada no princípio do laço, antes da entrada nesse laço.

78 O laço *do-while* será executado sempre que a condição for falsa e terminará quando esta for verdadeira, ao passo que o laço *repeat-until* será executado sempre que a condição for verdadeira e terminará quando esta for falsa.

79 Nos laços *while* e *repeat-until*, as sentenças serão executadas pelo menos uma vez.

```
1  inteiro pontuacaoFinal (inteiro n)
2     inteiro i, valor;
3     início
4        valor <- 0;
5        para i de 1 até n faça
6          valor <- valor + i * i * i;
7        fim para
8        retorne valor;
9     fim
```

Tendo como referência o algoritmo precedente, julgue os próximos itens.

80 As declarações e a instrução na linha 7 do algoritmo em questão não contribuem para a contagem total de unidades de tempo.

81 A linha 5 do algoritmo em apreço demanda `2n + 2` unidades de tempo.

82 Na linha 6 do algoritmo em pauta, são realizadas cinco unidades de tempo, as quais são executadas `n` vezes, o que totaliza `5n` unidades de tempo.

83 O algoritmo em apreço é `O(n)`, ou seja, um algoritmo de complexidade linear, porque realiza um total de `6n + 4` unidades de tempo.

Para realizar a validação de uma lista com 10 mil endereços de *emails*, será utilizada a seguinte expressão regular.

```
^\w*(\.\w*)?@\w*\.[a-z]+(\.[a-z]+)?$
```

Nessa situação hipotética,

84 a sequência `\w*` reconhecerá todos os caracteres alfanuméricos (letras e números) e o quantificador `*` indicará que há zero ou mais ocorrências do elemento precedente.

85 o quantificador `?`, em `?@`, determinará que o endereço de *email* poderá ter zero ou uma ocorrência do caractere `.` (ponto) antes do símbolo `@`.

86 o metacaractere `$` realizará a soma dos endereços de *emails* validados.

87 o *email* `joao-silva@email.com` será considerado como inválido.

Julgue os itens subsequentes, relativos às características da computação em nuvem (*cloud computing*).

88 No modelo IaaS *(infrastructure as a service*), é de responsabilidade do provedor proteger a infraestrutura básica de rede e as camadas de abstração.

89 O modelo PaaS (*platform as a service*) oferece menos recursos e funcionalidades integradas de segurança, necessitando que o cliente projete e gerencie os sistemas operacionais, aplicativos e dados.

Com relação a redes *peer-to-peer* (P2P), julgue os itens subsecutivos.

90 Em uma rede P2P centralizada, o paradigma cliente-servidor é usado pelo sistema de diretórios (lista de *peers* disponíveis) e para o armazenamento e o *download* de arquivos.

91 Uma busca de um arquivo em uma rede P2P descentralizada e não estruturada produz uma quantidade significativa de tráfego, haja vista que a mensagem é difundida por meio de técnicas de inundação.

92 O principal objetivo de se usar DHT (*distributed hash table*) em redes P2P descentralizadas e estruturadas é permitir que cada *peer* tenha informação total sobre seus vizinhos.

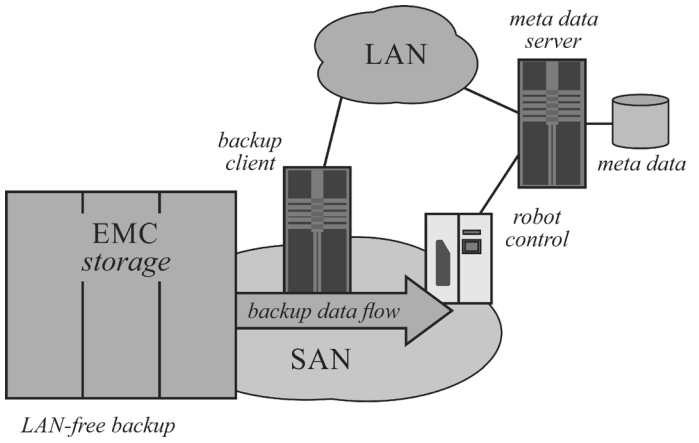
Julgue os itens que se seguem, a respeito de DNS (*domain name service*).

93 O registro DNS do tipo NS resolve um apelido para o *hostname*, sendo, portanto, uma forma de endereçamento.

94 As atualizações entre servidores DNS utilizam o UDP, enquanto as consultas feitas a servidores DNS utilizam o TCP (ou, opcionalmente, o SCTP).

95 Um tipo de ataque contra o serviço DNS é o *pharming*, que envolve o redirecionamento do navegador do usuário para sítios falsos por meio da técnica conhecida como envenenamento de *cache* DNS.

96 Ao obter êxito e conseguir resolver uma consulta de resolução de nome, o servidor DNS armazenará a resposta no *cache* do cliente e a encaminhará para a aplicação que tiver realizado a solicitação.



Backup and recovery in a SAN. *Version* 1.2. Internet: <japan.emc.com> (com adaptações).

A arquitetura para becape em ambiente SAN (*storage area network*) na figura precedente leva em consideração conceitos de becape que não precisam necessariamente da rede local para a cópia dos dados. Considerando essas informações e a figura apresentada, julgue os itens a seguir.

97 Esse tipo de arquitetura exige o uso de *software* de becape que não suporte agrupamento de fitas (*tape pooling*) para implementação, já que usa SAN.

98 Dada a capacidade de desempenho de *fibre channel*, a tecnologia de becape em SAN apresenta como vantagem permitir que a aplicação de becape mova os dados em altas velocidades, já que, normalmente, são requeridas janelas curtas para a realização de cópias de segurança em determinados tipos de sistemas em tempo real.

99 Em uma SAN, o *switched fabric* tem capacidade de se conectar com vários clientes de becape acessando as bibliotecas de fitas.

Existem diversas técnicas para descompilar programas maliciosos. Conforme a característica de um *malware*, essas técnicas podem ou não ser utilizadas. A respeito desse assunto, julgue os seguintes itens.

100 É possível verificar a entropia de *malware* por meio do cálculo de entropia de Shannon: se um *malware* usar criptografia para ofuscação, a entropia tende a 0, o que caracteriza alta entropia.

101 Normalmente, quando se verifica que um binário possui alta entropia, é possível que o *malware* utilize técnicas de compactação, o que torna a análise mais complexa.

102 Existem três técnicas chaves para a análise de *malware*: análise binária, análise de entropia e análise de *strings.*

Softwares desenvolvidos para a Web podem ter diversas vulnerabilidades e cada uma delas pode ser explorada com uma técnica específica. Sendo o ataque bem-sucedido, o atacante tem o controle do sistema. A respeito de características de ataques em *software web*, julgue os próximos itens.

103 O ataque conhecido por *blind* SQL *injection* tem por característica a exploração de perguntas ao banco de dados, as quais retornam verdadeiro ou falso; conforme a resposta da aplicação, o atacante consegue identificar de onde os dados podem ser extraídos do banco, por falhas de programação na aplicação.

104 O ataque de sequestro de sessão tem por característica o comprometimento do *token* de autenticação de um usuário, podendo esse *token* ser obtido interceptando-se a comunicação ou predizendo-se um *token* válido.

105 O ataque de CSRF (*cross site request forgery*) ocorre quando um usuário executa um conteúdo malicioso sem se dar conta, sendo sua principal característica a desnecessidade de o usuário estar autenticado, além da resistência da aplicação com CSRF a XSS (*cross site script*).

Certificação digital é amplamente utilizada na Internet e em diversos sistemas. No Brasil, a ICP-Brasil, sob a responsabilidade do ITI, é quem regulamenta e mantém a autoridade certificadora brasileira. A respeito da certificação digital e suas características, julgue os itens subsequentes.

106 O uso de HSM (*hardware security module*) para a geração e a manipulação das chaves utilizadas em autoridades certificadoras é prática não recomendada pelo ITI, já que impossibilita a recuperação da chave pública.

107 Certificados digitais possuem campos específicos, os quais podem ser de preenchimento obrigatório ou facultativo, de acordo com a necessidade ou a finalidade de uso do certificado digital.

108 Assinatura digital é uma técnica que utiliza um certificado digital para assinar determinada informação, sendo possível apenas ao detentor da chave privada a verificação da assinatura.

A respeito dos tipos de RAID e suas principais características, julgue os itens que se seguem.

109 RAID 0, também conhecido como *disk striping*, requer no mínimo dois discos rígidos: se um disco falhar, os demais garantem o acesso e a recuperação dos dados.

110 RAID 1, também conhecido como *disk mirroring*, requer pelo menos dois discos rígidos e permite a recuperação dos dados em caso de falha de um dos discos.

111 RAID 6, que requer no mínimo três discos e é também conhecido como *striping with double parity*, não permite a recuperação dos dados em caso de falha de dois dos seus discos.

Julgue os itens a seguir, em relação às características de *software* malicioso.

112 *Keyloggers* em estações Windows 10 podem ser implementados em modo usuário ou em modo *kernel*.

113 Formatos comuns de arquivos, como, por exemplo, `.docx` ou `.xlsx`, são utilizados como vetor de infecção por *ransomware*, um tipo de *software* malicioso que encripta os dados do usuário e solicita resgate.

114 *Exploit kits* não podem ser usados como vetor de propagação de *worms*, uma vez que a principal característica de um *worm* consiste na possibilidade de propagação sem a intervenção direta do usuário.

Redes sem fio são amplamente utilizadas para a conexão de usuários em ambientes que permitam alta mobilidade ou onde não seja possível prover infraestrutura cabeada. Devido a sua arquitetura, redes sem fio possuem diversos problemas de segurança. No que se refere a segurança de redes sem fio e alguns dos ataques conhecidos a esse tipo de redes, julgue os itens que se seguem.

115 *Krack* (*key reinstallation attack*) é um tipo de ataque que funciona contra o Wi-Fi *protected access* II (WPA2) sob determinadas condições. Satisfeitas essas condições, sistemas Android e Linux podem ser enganados por esse ataque para reinstalar uma chave de criptografia toda composta por zeros.

116 O WPS (Wi-Fi *protected setup*) pode ser atacado por uma técnica conhecida por *pixie dust attack* em alguns tipos de ponto de acesso. Nesse ataque, a senha WPA2 é modificada em tempo real no ponto de acesso atacado para uma senha que o atacante determinar.

117 O ataque em redes Wi-Fi conhecido por *evil twin* cria um ponto de acesso não autorizado na rede, o que permite interceptar a comunicação da vítima que se conecta nesse ponto de acesso malicioso.

Julgue os seguintes itens, a respeito dos algoritmos RSA e AES e de noções de criptografia.

118 O RSA é suscetível a um ataque conhecido como ataque de Wiener, que pode expor a chave privada de um sistema criptográfico RSA se os parâmetros utilizados para definir a chave privada forem considerados pequenos, e consequentemente, tido como matematicamente inseguros.

119 O AES trabalha com o conceito de cifra de fluxo ou *stream cipher.*

120 O AES e o RSA são sistemas assimétricos e simétricos, respectivamente; o RSA suporta chaves de no máximo 4.096 bites, enquanto o AES trabalha com chaves de no máximo 256 bites.

Espaço livre