-- CONHECIMENTOS ESPECÍFICOS –

Julgue os itens a seguir, a respeito de organização e arquitetura de computadores, gerenciamento de memórias e de arquivos, bem como de tecnologias de virtualização.

51 Quando se usa a paravirtualização, o sistema operacional convidado é modificado para chamar diretamente o hipervisor por meio de hiperchamadas, o que melhora o desempenho do ambiente virtualizado por meio da redução do *overhead*.

52 A memória *flash* é do tipo volátil, a exemplo da RAM, sendo muito utilizada em diversos dispositivos computacionais por sua capacidade de reter dados apenas durante a execução do sistema.

53 No modelo de paginação, o espaço de endereçamento lógico de um processo é dividido em páginas (blocos de tamanho fixo) e o espaço de memória físico é dividido em molduras (*frames*) de tamanhos iguais.

54 Em sistemas de arquivos com *journaling*, tais como Ext4 e ReiserFS, as alterações realizadas são aplicadas diretamente ao sistema de arquivos, e o *journal* funciona como uma cópia completa dos arquivos, destinada à recuperação em caso de falhas.

Em relação às características do RAID e do NTFS, julgue os seguintes itens.

55 Diferentemente do XFS, o sistema de arquivos NTFS não suporta estrutura de dados especializada para tratamento de blocos defeituosos (*bad clusters*).

56 RAID 0 (*striping*) distribui dados em blocos de mesmo tamanho entre múltiplos discos para melhorar o desempenho; esse nível de RAID, no entanto, não oferece redundância.

Acerca de bancos de dados, julgue os seguintes itens.

57 A técnica de agregação em bancos de dados multidimensionais permite pré-computar somatórios e médias, o que otimiza o tempo de resposta nas consultas analíticas.

58 Nos sistemas de gerenciamento de banco de dados relacionais, o modelo lógico descreve como os dados são organizados em tabelas, relacionamentos e restrições, independentemente da forma como são fisicamente armazenados no disco.

59 O SQLite exige configuração prévia de usuários e permissões de acesso nativas para garantir controle de acesso a dados.

Julgue os itens subsecutivos, a respeito de bancos de dados.

60 Durante uma recuperação após falha, o sistema aplica apenas os registros presentes no log de transações já confirmadas (*commit*), ignorando qualquer operação registrada após o último *checkpoint*.

61 Em SQL, as junções externas (`LEFT OUTER JOIN`, `RIGHT OUTER JOIN` e `FULL OUTER JOIN`) permitem incluir registros de uma ou de ambas as tabelas, mesmo quando não há correspondência entre as chaves de junção.

No que se refere a NoSQL, julgue os itens subsequentes.

62 A escalabilidade horizontal, uma característica comum em bancos de dados NoSQL, permite a distribuição de dados por múltiplos servidores.

63 Os bancos de dados NoSQL garantem atomicidade, consistência, isolamento e durabilidade em todas as operações realizadas em arquiteturas distribuídas.

64 Sistemas NoSQL de grafos armazenam dados sem explorar conexões e relacionamentos entre as informações.

A fim de identificar vulnerabilidades e entender o algoritmo criptográfico, foi realizada a análise de um *firmware* embarcado proprietário, compilado para uma arquitetura customizada RISC com instruções não padrão (ISA *extension*), que implementa rotinas criptográficas e anti-depuração avançadas, incluindo *anti-tampering* e *control flow flattening*, além de otimizações de compilador de tempo de ligação.

A partir da situação hipotética precedente, julgue os itens que se seguem.

65 O *control flow flattening* implementado no *firmware* pode ser eficientemente revertido por meio de técnicas de análise estática de descompiladores que utilizam algoritmos de reconhecimento de padrões baseados em grafos de fluxo de controle, restaurando o fluxo de execução original sem a necessidade de *taint analysis* ou execução simbólica.

66 A utilização de uma ISA *extension* customizada requer que o descompilador possua um processador específico (ou uma extensão) que compreenda as novas instruções; desse modo, deve-se criar ou adaptar o processador do descompilador, para evitar que a descompilação resulte em pseudocódigo incoerente ou em erros na interpretação de blocos inteiros.

Em relação à análise de código malicioso e às técnicas de *sandboxing*, julgue os itens a seguir.

67 Uma *sandbox* é um ambiente de segurança isolado que permite a execução de programas ou códigos potencialmente perigosos sem que eles afetem diretamente o sistema operacional principal ou outros arquivos importantes da máquina.

68 A análise estática de um vírus se concentra na execução do código malicioso em um ambiente controlado, como uma *sandbox*, a fim de se observar seu comportamento dinâmico no que concerne, por exemplo, a chamadas de sistema, modificações no registro e comunicações de rede.

Considerando os princípios da programação orientada a objetos, bem como os conceitos de linguagens de programação procedurais, julgue os itens subsequentes.

69 Inteiro (`int`) e caractere (`char`) são dados do tipo elementar, ou seja, que armazenam valores únicos e indivisíveis, enquanto um registro (`struct`, em C) é um dado do tipo estruturado, que permite agrupar variáveis de diferentes tipos sob um único nome.

70 Em linguagens de programação como Java e C#, a herança múltipla de classes é um recurso amplamente suportado e incentivado para maximizar a reutilização de código.

71 Em linguagens procedurais, um *array* (`vetor`) é um tipo de dado estruturado que, tipicamente, permite armazenar uma coleção de elementos de tipos de dados variados, como um inteiro, um texto e um valor booleano, sob um único nome de variável, acessível por meio de um índice.

Julgue os próximos itens, a respeito das características e das aplicações básicas das linguagens Java e JavaScript.

72 Devido à compilação do código-fonte em *bytecode*, que é executado pela máquina virtual Java (JVM), os programas Java podem ser executados em diversos sistemas operacionais, sem a necessidade de recompilação.

73 A linguagem JavaScript é executada principalmente no lado do servidor (*back-end*) para construir a lógica de banco de dados e APIs, sendo incapaz de interagir com o navegador *web* do cliente.

Julgue os itens seguintes, em relação às tecnologias e aos conceitos do desenvolvimento *web*.

74 A principal desvantagem da GraphQL, que é uma linguagem de consulta para APIs, é que ela não suporta consultas complexas que envolvam a combinação de dados de múltiplos recursos em uma única requisição.

75 Uma característica fundamental de uma API RESTful é que as requisições entre cliente e servidor devem ser *stateless* (sem estado), não devendo o servidor armazenar informações sobre o estado do cliente entre as requisições.

No que se refere ao SonarQube, às estruturas de dados e à complexidade de algoritmos, julgue os itens subsecutivos.

76 Para gerenciar a ordem de execução de chamadas de função em um programa recursivo, a estrutura de dados mais adequada é a pilha (*stack*), pois sua característica LIFO (*last-in*, *first-out*) espelha o fluxo de execução em que a última função chamada é a primeira a finalizar sua execução e retornar.

77 No SonarQube, um QualityGate representa um conjunto de condições que um projeto deve satisfazer a fim de que seu código seja considerado aceitável para prosseguir no *pipeline* de desenvolvimento ou para ser liberado.

78 Para grandes volumes de dados, um algoritmo com complexidade de tempo O(n) (linear) é considerado menos eficiente que um algoritmo com complexidade de tempo O($n \log n$), uma vez que o crescimento linear é mais acentuado que o crescimento logarítmico.

Acerca dos protocolos SSH e HTTPS, julgue os itens a seguir.

79 De acordo com o modelo TCP/IP, o HTTPS opera na camada de transporte.

80 O SSHv2 não limita o número de sessões de *shell* em uma única conexão SSH.

Certa aplicação *web* tem uma funcionalidade de busca de usuários por nome, realizada em PHP, conforme os parâmetros a seguir.

```
$ username = $ _GET['username'];
$ query = "SELECT * FROM users WHERE
username = '$ username'";
$ result = mysqli_query($ connection, $ query);
```

A partir dessas informações, julgue os itens subsequentes, considerando o que é definido pelo OWASP Top 10 de 2021 no que diz respeito a falhas de aplicação.

81 Na URL a seguir, o uso de `--` indica o início de um comentário em SQL, de modo que o restante da consulta é ignorado.

```
http://prova.com/busca?username=admin'--
```

82 Considere que um atacante tenha acesso à aplicação em apreço e realize a seguinte chamada.

```
http://prova.com/busca?username=admin'--
```

Nesse caso, essa chamada equivale à consulta SQL a seguir.

```
SELECT * FROM users WHERE username = 'admin'-
-'
```

A respeito do OAuth 2.0 e do OpenId Connect (OIDC), julgue os itens subsequentes.

83 O OIDC é uma camada de autorização construída sobre o OAuth 2.0 que permite que os clientes usem a identidade do usuário final com base na autorização realizada pelo servidor de autenticação.

84 OAuth 2.0 permite que serviços de terceiros acessem os dados de um usuário em determinado serviço, mas essa ação expõe a senha do usuário.

Julgue os próximos itens, no que se refere à esteganografia.

85 Na área de informática forense digital, os peritos usam técnicas de esteganografia para realizar a alteração da assinatura digital de arquivos.

86 A técnica do LSB (*least significant bit*) altera o *bit* menos significativo de *pixels* em imagens para codificar dados, mantendo a alteração visual imperceptível.

Considerando que, em uma rede local interna, um computador use o IP 192.168.1.10 e que a rede local acessa a Internet usando o IP 203.0.113.12 público, julgue os itens subsecutivos.

87 O dispositivo responsável por fazer o NAT importa uma tabela de endereços do servidor DHCP, que, por sua vez, é o responsável por associar endereços internos com conexões externas.

88 Se o computador em questão enviar uma solicitação para um *site* na Internet, o dispositivo que faz o NAT na rede local deverá traduzir o endereço privado para o endereço 203.0.113.12 e manter o controle dessa tradução para a solicitação.

Em relação ao DNSSEC e às suas chaves, julgue os itens que se seguem.

89 A *key signing key* é usada para assinar as chaves *zone signing keys* e não deve ser compartilhada com nenhuma entidade.

90 A *zone signing key* é usada para assinar os registros DNS de uma zona de domínio.

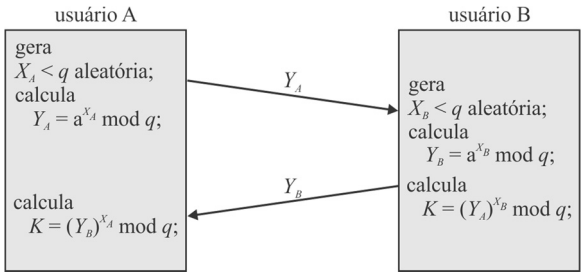
Julgue os itens seguintes, relativos ao WPA3.

91 A técnica denominada *simultaneous authentication of equals* torna o WPA3 resistente a ataques de dicionário e força bruta em tentativas de senha.

92 A técnica denominada *opportunistic wireless encryption*, utilizada em WPA3, é destinada para uso em dispositivos que possuem senha compartilhada.

Julgue os próximos itens, a respeito do algoritmo Twofish e da técnica MITM (*man-in-the-middle*).

93 Considerando-se que a figura a seguir descreve um acordo de chave Diffie-Hellman, é correto afirmar que, nesse cenário, o protocolo de acordo de chave é vulnerável ao ataque MITM porque não autentica os participantes, vulnerabilidade que pode ser superada com a utilização de assinaturas digitais e certificados de chave pública.



94 Twofish é uma cifra simétrica com um tamanho de bloco de 128 *bits* e uma chave de até 256 *bits* que, semelhante aos algoritmos AES e DES, depende da estrutura de *Feistel* — especificamente 16 rodadas na rede *Feistel* (16-*round Feistel network*).

Julgue os itens subsequentes, relativos ao sistema operacional Windows Server 2022.

95 No Windows Server 2022, quando o DoH (DNS-*over*-HTTPS) está habilitado, as consultas DNS entre o cliente DNS do Windows Server e o servidor DNS passam por uma conexão HTTPS segura, de modo que a consulta fica protegida contra interceptação por terceiros não confiáveis.

96 No Windows Server 2022, o servidor *secured-core* é projetado para fornecer maior segurança por meio de três pilares: raiz de confiança apoiada por *hardware*; defesa contra ataques de nível de *firmware*; e proteção do sistema operacional contra a execução de código não verificado.

No que diz respeito ao sistema operacional Linux, julgue os seguintes itens.

97 No Linux, os arquivos de *log* do sistema contêm informações sobre as atividades do sistema operacional (SO); como exemplo, o arquivo `/var/log/dmesg` contém mensagens internas do SO, inclusive notificações de serviços do sistema e erros de aplicativos.

98 Considere que a sequência de comandos a seguir tenha sido executada no Linux por certo usuário com permissão de *root* no arquivo em comento.

```
touch testepf
chmod 664 testepf
chmod o+x testepf
```

Nesse caso, é correto afirmar que o arquivo `testepf` terá as permissões `-rwx-rw-r--` se o comando `ls -la testepf` for executado.

99 No Linux, `systemd` é um sistema de registro centralizado que coleta e armazena dados de *log* de várias fontes, incluindo serviços do sistema, eventos do *kernel* e aplicativos do usuário, e cujo conteúdo pode ser consultado com o uso do comando `journalctl`.

A respeito dos sistemas operacionais Android e iOS, julgue os itens que se seguem.

100 No Android, a UID (*user identifier*) é utilizada para configurar um *sandbox* de aplicativo, no entanto, por questão de segurança, o *sandbox* não se estende ao código nativo e aos *apps* e bibliotecas do Android, os quais são executados em área de memória protegida, com acesso somente pelo *kernel*.

101 No iOS, a aleatorização de espaço de endereço ajuda a proteger o sistema contra a exploração de erros de corrupção da memória, sendo usada pelos *apps* integrados para aleatorizar as regiões da memória na inicialização.

Com base nas legislações aplicáveis à governança de TI, julgue os itens seguintes.

102 Considere que o comando da Polícia Federal tenha solicitado ao Ministério da Justiça e Segurança Pública (MJSP) a aquisição urgente de um sistema avançado para quebrar senhas e descriptografia de dispositivos eletrônicos para comunicação em operações estratégicas e fronteiriças do Brasil. Considere, ainda, que a aquisição se ampara em uma ameaça iminente de ciberataques identificada pela PF que poderia comprometer a segurança nacional, de acordo como o estabelecido pelo Ministro de Estado da Defesa. Nessa situação hipotética, conforme a Lei n.º 14.133/2021, a PF poderia realizar a aquisição em apreço por meio de contratação direta por inexigibilidade de licitação.

103 De acordo com o Marco Civil da Internet, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial ou notificação extrajudicial, não tomar as providências, no prazo assinalado, para tornar indisponível o conteúdo apontado como infringente.

Julgue os itens a seguir, relativos à inteligência artificial (IA).

104 *Deepfakes* são vídeos gerados por IA para produzir conteúdo altamente realista e podem ser criados por meio de rede adversária generativa (GAN), a qual corresponde a uma arquitetura de aprendizado profundo que treina duas redes neurais para competirem entre si.

105 LLM (*Large Language Models*) são modelos de aprendizado profundo pré-treinados em grandes quantidades de dados que podem ser utilizados para gerar texto e outros conteúdos, além de executar outras tarefas de processamento de linguagem natural.

Julgue os itens a seguir, considerando que uma equipe forense tenha sido acionada para investigar possíveis crimes cibernéticos relacionados a um incidente de segurança que comprometeu o servidor de arquivos de uma instituição.

106 A criptografia ponta a ponta inviabiliza completamente a extração de qualquer vestígio útil em uma análise forense.

107 A coleta de vestígios digitais deve ser precedida pela identificação e pelo isolamento do ambiente comprometido, como forma de preservar a integridade da evidência.

108 A mera visualização de arquivos realizada por perito diretamente no material suspeito e antes de uma cópia pericial não interfere na cadeia de custódia da evidência.

109 Na análise do incidente, o perito deve buscar vestígios nos metadados de arquivos em diferentes formatos, tais como PDF e JPG, além de *logs* do sistema e artefatos armazenados em memória.

Supondo que dados sigilosos de clientes de uma empresa tenham vazado por meio de uma aplicação hospedada em nuvem, julgue os itens que se seguem.

110 Se documentos tiverem sido impressos em uma impressora da rede, será possível resgatar informações como usuário que solicitou a impressão, data da impressão, nome do arquivo impresso e quantidade de folhas impressas.

111 Arquivos de configuração são irrelevantes para a análise de incidentes em nuvem.

112 A coleta de vestígios em ambiente de nuvem requer atenção especial à legislação vigente e aos acordos com os provedores.

113 Em ambientes de nuvem, a coleta de evidências pode ser feita diretamente nos arquivos hospedados, mesmo sem autorização judicial.

Julgue os próximos itens, considerando que, em uma operação contra crimes financeiros, haja suspeita de que um aparelho celular apreendido contenha provas relevantes.

114 A análise de arquivos temporários, de *caches* e de histórico de navegação pode revelar informações importantes, mesmo após a exclusão intencional do conteúdo feita pelo usuário.

115 Metadados EXIF são encontrados em arquivos separados do arquivo original analisado.

116 A correta identificação da versão do sistema operacional é fundamental para a escolha das ferramentas e técnicas de extração forense aplicáveis ao dispositivo.

Considerando que um suspeito de ataques de *ransomware* utilize máquinas virtuais para encobrir sua identidade durante esses ataques, julgue os itens subsequentes.

117 A identificação de vestígios cibernéticos pode envolver a análise de arquivos temporários, tarefas agendadas e entradas de registro do sistema operacional analisado.

118 A aplicação do princípio da proporcionalidade justifica a omissão de etapas do processo pericial para acelerar a obtenção da prova.

119 A duplicação forense de um disco virtual pode ser feita sem necessidade de validação por *hash*, uma vez que a imagem original está preservada.

120 A análise forense em ambientes virtualizados deve considerar *logs* de *hypervisor*, *snapshots* e arquivos do tipo .vmdk.

Espaço livre