-- CONHECIMENTOS ESPECÍFICOS --

Questão 21

Como política de pessoal, é natural que haja um processo adequado a ser executado no momento em que o funcionário deixa a organização, para garantir que todos os direitos deste sejam revogados e os ativos sob sua custódia sejam devolvidos. Esse processo visa à garantia de

I autenticidade;
II confidencialidade;
III disponibilidade.

Considerando os conceitos de segurança da informação, assinale a opção correta.

A Apenas o item I está certo.
B Apenas o item II está certo.
C Apenas os itens I e III estão certos.
D Apenas os itens II e III estão certos.
E Todos os itens estão certos.

Questão 22

A análise crítica da política de segurança da informação visa assegurar a sua contínua pertinência, adequação e eficácia dentro da organização. Entre suas saídas, deve(m) estar

A a realimentação das partes interessadas.
B o desempenho e a conformidade do processo.
C o relato sobre incidentes de segurança da informação.
D a situação de ações preventivas e corretivas.
E a melhoria dos controles e dos objetivos de controles.

Questão 23

Quando o objetivo for garantir confidencialidade e assinatura digital em uma função de *hash* com redução da carga de processamento, deve-se usar criptografia

A simétrica, para criptografar somente o código de *hash*.
B de chave pública, para criptografar somente o código de *hash*.
C simétrica, para criptografar a mensagem, mais o código de *hash* concatenado.
D assimétrica, para criptografar a mensagem, mais o código de *hash* criptografado com criptografia simétrica.
E simétrica, para criptografar a mensagem, mais o código de *hash* criptografado com chave privada.

Questão 24

Para que a gestão de riscos seja realizada com sucesso, é necessário seguir a norma ISO 31000 – Gestão de riscos – Princípios e Diretrizes. Entre as fases descritas no documento, destaca-se aquela na qual é decidido se o risco será reduzido, evitado ou compartilhado com terceiros. Essa fase é denominada

A estabelecimento do contexto.
B identificação de riscos.
C tratamento de riscos.
D análise de riscos.
E avaliação de riscos.

Questão 25

O OWASP (*Open Web Application Security Project*) criou um conjunto de listas de verificação de práticas de programação segura para as diversas etapas ou tarefas do desenvolvimento de *software*, como a gestão de sessões, com os seguintes itens de verificação:

I não permitir *logins* persistentes;
II não permitir conexões simultâneas com o mesmo identificador de usuário;
III utilizar apenas pedidos POST para transmitir credenciais de autenticação.

Considerando a gestão de sessões, no desenvolvimento seguro de *software*, assinale a opção correta.

A Apenas o item I está certo.
B Apenas o item III está certo.
C Apenas os itens I e II estão certos.
D Apenas os itens II e III estão certos.
E Todos os itens estão certos.

Questão 26

Uma aplicação *web* pode ser atacada por meio da exploração de vulnerabilidades, como, por exemplo, quando os dados fornecidos pelos usuários não são validados, filtrados ou mesmo limpos pela aplicação; pela não renovação dos identificadores de sessão após o processo de autenticação ter sido bem-sucedido; pela elevação de privilégios, atuando como usuário sem autenticação, ou como administrador, mas tendo perfil de usuário regular. Aplicações com essas características são vulneráveis à falha de

I injeção;
II quebra de autenticação;
III quebra de controle de acesso.

Assinale a opção correta.

A Apenas o item I está certo.
B Apenas o item III está certo.
C Apenas os itens I e II estão certos.
D Apenas os itens II e III estão certos.
E Todos os itens estão certos.

Questão 27

Um usuário acessou uma página de Internet e verificou que sua navegação foi redirecionada para um sítio falso, por meio de alterações do DNS (*Domain Name System*).

O exemplo apresentado caracteriza uma situação que envolve um golpe na Internet conhecido como

A *hoax*.
B *pharming*.
C *advence fee fraud*.
D *identity theft*.
E *phishing-scam*.

Questão 28

Como uma solução temporária para o esgotamento do espaço de endereços IP, a *Request for Comments* 1918 (RFC 1918) adotou o emprego de endereços IP privados, nas classes A, B e C. Assinale a opção que apresenta a notação CIDR para o bloco de endereço IP privado da classe B.

A `172.16.0.0/9`
B `172.16.0.0/10`
C `172.16.0.0/11`
D `172.16.0.0/12`
E `172.16.0.0/13`

Questão 29

O Ettercap é uma ferramenta de segurança de rede livre e de código aberto, que funciona colocando a interface de rede em modo promíscuo com o ARP (*Address Resolution Protocol*), envenenando esse protocolo nas máquinas de destino. Essa ferramenta é utilizada para análise de protocolo de rede e auditoria de segurança, e possui a funcionalidade de um ataque de rede conhecido como

A DoS.
B DDoS.
C HTTP *flood.*
D *man-in-the-middle*.
E DNS *spoofing*.

Questão 30

Após avaliação de segurança da rede de comunicação de determinada empresa, identificou-se que alguns servidores Windows Server 2012 estavam infectados com um vírus não detectável pelo antivírus corporativo; observou-se também que o servidor estava desatualizado, com contas administrativas de ex-funcionários ativas e com a filtragem de pacotes desativada.

Nessa situação hipotética, as configurações adequadas de *hardening* incluem

A desativação de contas não utilizadas, atualização do sistema operacional, ativação de *firewall* e *AppLocker*.
B desativação de contas não utilizadas, atualização do sistema operacional, ativação de *Intrusion Prevention System* (IPS) e *AppLocker.*
C atualização dos sistema operacional e *antimalware*, ativação de *firewall* e *AppLocker*.
D desativação de contas não utilizadas, atualização do sistema operacional, ativação de *Intrusion Prevention System* (IPS) e *firewall.*
E atualização do sistema operacional e *antimalware*, ativação de *Host Intrusion Prevention System* (IPS) e *firewall.*

Questão 31

O sistema de monitoramento de rede de uma organização detectou a utilização total da tabela de endereços de controle de acesso à mídia (MAC) do *switch* de núcleo do *datacenter*, o que o deixou temporariamente com a funcionalidade de um *hub*. A equipe de sustentação e segurança de TIC teve dificuldades para lidar com o ataque, pois eram mais de 1.500 servidores físicos e lógicos, e o *swicth core* possuía alta densidade, com mais de 200 portas físicas para análise.

O tipo de ataque ocorrido na situação apresentada e a contramedida adequada são, respectivamente,

A falsificação de endereço MAC e lista de controle de acesso (ACL) para cada porta do *switch.*
B ataque de negação de serviço (DoS) e lista de controle de acesso (ACL) para cada porta do *switch*.
C estouro de memória de contexto endereçável (CAM) e lista de controle de acesso (ACL) para cada porta do *switch*.
D estouro de memória de contexto endereçável (CAM) e limitação do número máximo de endereços MAC simultâneos que podem ser apreendidos e alocados para cada porta do *switch*.
E ataque de negação de serviço (DoS) e limitação do número máximo de endereços MAC simultâneos que podem ser apreendidos e alocados a cada porta do *switch.*

Questão 32

Considere que determinado tribunal seja conectado às comarcas por meio da Internet, empregando-se a tecnologia de rede privada virtual (VPN) com encriptação a partir da camada de transporte. Nessa situação, a VPN utiliza protocolo de Internet seguro (IPSEC) em modo

A túnel, com encapsulamento seguro de empacotamento (ESP).
B túnel, com cabeçalho de autenticação (AH).
C transparente, com cabeçalho de autenticação (AH) e encapsulamento seguro de empacotamento (ESP).
D transparente, com encapsulamento seguro de empacotamento (ESP).
E túnel, com cabeçalho de autenticação (AH) e encapsulamento seguro de empacotamento (ESP).

Texto 13A2-I

No dia 2/11/1988, a história da Internet e a segurança informática mudaram radicalmente. Um *software* malicioso, liberado nesse dia, às 18 horas, parou a Internet e causou um dos maiores prejuízos por *malware* visto até hoje, aproveitando-se das vulnerabilidades de milhões de computadores e paralisando os sistemas. A atividade normal dos equipamentos afetados foi interrompida e as conexões ficaram obstruídas durante vários dias, à medida que o primeiro *malware* para plataformas múltiplas se propagava pela Internet. O *malware* utilizou-se de falhas nas conexões TCP e SMTP para infectar os sistemas e propagar-se automaticamente pelas redes, gerando lentidão na rede e nos computadores devido ao alto consumo de recursos. Por mais que muitos já conhecessem as falhas dos sistemas UNIX, o alcance do ataque pegou todos de surpresa.

Internet: <www.welivesecurity.com.br> (com adaptações).

Questão 33

Atualmente, a prevenção/mitigação mais adequada do *software* malicioso mencionado no texto 13A2-I consiste

A na proteção de perímetro provida por *antispam, firewall* de rede e *Web Application Firewall.*
B na proteção de perímetro provida por *firewall* de rede e de *host, antispam* e filtragem de conteúdo *web.*
C em *hardening* de sistemas operacionais, *Data Loss Prevention* (DLP), *firewall* e *Intrusion Detection System* (IDS) nas máquinas.
D na atualização constante dos sistemas operacionais e dos *softwares*, na utilização de *antimalwares*, *firewalls* e *Data Loss Prevention* (DLP) nas máquinas.
E na atualização constante dos sistemas operacionais e dos *softwares*, na utilização de *antimalwares* e de *firewalls* nas máquinas.

Questão 34

O *software* malicioso utilizado no ataque mencionado no texto 13A2-I foi um

- Ⓐ *worm*, que explorou as vulnerabilidades existentes no UNIX para propagar-se automaticamente, levando ao alto consumo de recursos computacionais.
- Ⓑ vírus, que se espalhou rapidamente na rede, infectando outros computadores devido à existência de vulnerabilidades presentes nos sistemas UNIX, levando ao alto consumo de recursos.
- Ⓒ *bot*, que permitiu a comunicação entre *hackers* e computadores infectados, recebendo instruções remotas para elevar o consumo dos recursos.
- Ⓓ *rootkit*, que alterou as bibliotecas presentes nos sistemas UNIX para propagar-se automaticamente de forma ofuscada e receber comando para aumentar o consumo de recursos.
- Ⓔ *backdoor*, que disponibilizou acesso à rede, passando despercebido pelos controles de segurança existentes, permitindo execução de outros códigos maliciosos.

Questão 35

A proteção de segurança de rede computacional de determinado tribunal é composta por *firewall* de aplicação *Web* (WAF), sistema de detecção e prevenção de intrusão (IDS/IPS), *firewall* e listas de acessos (ACL) utilizadas em *switchs* e roteadores. Um atacante conseguiu, a partir da Internet, ultrapassar a proteção dessa rede e acessar indevidamente informações restritas. A aplicação *web* afetada, E-processos, é utilizada para gestão de processos judiciais, sendo acessada tanto pela Internet quanto pela rede interna por diversos perfis de usuários, como servidores, advogados, juízes. A aplicação conta com alguns recursos de segurança, como bloqueio por tentativa de força bruta e protocolo de transferência de hipertexto seguro (HTTPS). Durante a análise do incidente, identificou-se a utilização da técnica de *SQL Injection* na exploração de uma vulnerabilidade na E-processos, o que permitiu o acesso não autorizado a dados armazenados no servidor de banco de dados.

Nessa situação hipotética, as falhas que podem ser identificadas incluem

- Ⓐ IDS/IPS configurado no modo de detecção e fluxo de comunicação da Internet para o servidor na porta TCP 443 liberado no *firewall.*
- Ⓑ IDS/IPS configurado em modo de detecção e fluxo de comunicação da Internet para o servidor na porta TCP 443 liberado na ACL do roteador de borda.
- Ⓒ WAF com regra de *SQL Injection* desativada no fluxo de comunicação da Internet para o servidor na porta TCP 443 e IDS/IPS configurado em modo de prevenção.
- Ⓓ IDS/IPS configurado em modo de prevenção com regra de *SQL Injection* desativada no fluxo de comunicação da Internet para o servidor na porta TCP 443 e WAF com inspeção desativada para SSL/TLS em HTTP.
- Ⓔ IDS/IPS e WAF com inspeção desativada para SSL/TLS em HTTP e fluxo de comunicação da Internet para o servidor nas portas TCP 80 e 443 liberadas na ACL do roteador de borda e no *firewall*.

Questão 36

São exemplos de autenticação por

- Ⓐ *tokens*: chaves de sessão de aplicações *web* e senhas pessoais.
- Ⓑ geolocalização: nome de dispositivos, endereços IPs públicos e geolocalização.
- Ⓒ biométrica: reconhecimento de íris, voz, cor do cabelo, digital, maneira de andar e maneira de escrever.
- Ⓓ *tokens*: senha descartável com base em eventos (HOTP) e senha de uso único com base em tempo (TOTP).
- Ⓔ biométrica: reconhecimento de peso, altura, circunferência abdominal e tamanho das mãos.

Questão 37

O uso do *syslog* em servidores Linux é comum para registrar eventos do sistema operacional. A fim de enviar os *logs* para um servidor externo ao que está gerando os eventos, é necessário informar essa configuração ao *syslog*. Assinale a opção que apresenta a configuração que deve estar presente no arquivo `syslog.conf`, caso seja necessário enviar os *logs* do serviço de *email* para um servidor externo com endereço `192.168.1.5`, com somente mensagens críticas.

- Ⓐ `smtp.crit @192.168.1.5`
- Ⓑ `mail.!crit @192.168.1.5`
- Ⓒ `smtp.!crit @192.168.1.5`
- Ⓓ `smtp.!err @192.168.1.5`
- Ⓔ `mail.crit @192.168.1.5`

Questão 38

O DNS é responsável por resolver endereços IPs, nomes, apelidos, entre outros recursos referentes à localização de serviços na Internet. Além disso, é um serviço que possui visibilidade elevada para ações maliciosas. Assinale a opção que apresenta o registro de recurso de DNS responsável por informar a assinatura de correio para autenticar o domínio do remetente.

- Ⓐ `A`
- Ⓑ `PTR`
- Ⓒ `DNSKEY`
- Ⓓ `SRV`
- Ⓔ `SPF`

Questão 39

As organizações normalmente validam seus controles de segurança da informação em intervalos regulares por meio de testes de penetração. Assinale a opção que apresenta o tipo de validação cujo objetivo é verificar se o sistema operacional está vulnerável a ações maliciosas de ataques que consigam exceder de forma proposital o uso de memória designado aos programas, para elevar privilégios de acesso dos atacantes.

- Ⓐ `Denial of Service`
- Ⓑ `Error Handling`
- Ⓒ `Data protection`
- Ⓓ `Buffer Overflow`
- Ⓔ `Input Validation`

Questão 40

O e-PING é um documento de referência sobre os padrões de interoperabilidade de governo eletrônico, que, em uma das suas segmentações, descreve padrões de segurança. Para a transferência de dados em redes inseguras, o padrão recomendado é o

- Ⓐ TLS (*Transport Layer Security*).
- Ⓑ SHA512.
- Ⓒ AES.
- Ⓓ MD5.
- Ⓔ 3DES.

Questão 41

Para acessar o sistema operacional Linux remotamente ou para transferir arquivos de forma que o tráfego de rede não passe o *login* e a senha em texto plano, deve ser usado o

- Ⓐ Telnet.
- Ⓑ FTP (*File Transfer Protocol*).
- Ⓒ SSH (*Secure Shell*).
- Ⓓ RCP (*Remote Copy Protocol*).
- Ⓔ Vsftp.

Questão 42

Na norma ISO/IEC 27002, existe um controle cujo escopo é manter a segurança na troca de informações e *softwares* na organização, de forma interna ou externa, tendo como diretriz de implementação assegurar que o endereçamento e o transporte da mensagem estejam corretos. Essa diretriz de implementação faz parte do controle denominado

A mídias em trânsito.
B mensagens eletrônicas.
C acordos para troca de informações.
D políticas e procedimentos para troca de informações.
E sistemas de informações do negócio.

Questão 43

A Lei n.º 13.709/2018 formaliza uma série de condutas e ações relacionadas ao uso dos dados. Para que seja retirada de um dado a possibilidade de associação direta a um indivíduo, a lei considera o uso de meio técnico do tipo

A bloqueio.
B anonimização.
C tratamento.
D transferência.
E consentimento.

Text 9A3-I

If you were to judge 2018's most important legal technology by looking at conference agendas and media coverage, you'd probably say it was the continuing development of artificial intelligence. But if you judge the most important technology by its direct impact on the practice of law, then it would have to be analytics. As I suggested in a recent column, we could be nearing the point where it would be malpractice for a lawyer *not* to use analytics.

Internet: <lawsitesblog.com> (adapted).

Questão 44

According to the author of text 9A3-I, 2018's most impactful legal technology was

A higher salaries for judges.
B digital calendars.
C artificial intelligence.
D malpractice for lawyers.
E analytics.

Questão 45

In the first sentence of text 9A3-I, the word "it" refers to

A "judge".
B "media coverage".
C "artificial intelligence".
D "2018's most important legal technology".
E "conference agendas".

Questão 46

In the first sentence of text 9A3-I, the word "judge" is synonymous with

A justice.
B consider.
C court.
D examiner.
E try.

Questão 47

The author of text 9A3-I mentions conference agendas and media coverage in order to

A demonstrate that their focus did not reflect the most impactful trend in the field of legal technology in 2018.
B show that they focused suficient attention on analytics in the field of legal technology in 2018.
C demonstrate that these events and institutions establish priorities for the field of legal technology.
D suggest that conferences related to legal technology should not be venues for discussions about analytics.
E advertise future events of interst in the field of legal technology.

Questão 48

O entendimento de que o ato administrativo é considerado válido até que se prove em contrário corresponde ao atributo da

A presunção de legitimidade.
B tipicidade.
C exigibilidade.
D imperatividade.
E autoexecutoriedade.

Questão 49

Considerando o disposto na Lei n.º 8.666/1993 (Lei de Licitações e Contratos), julgue os seguintes itens.

I Embora tenha sido editada pela União, a Lei de Licitações e Contratos é considerada lei nacional, aplicando-se a todos os Poderes da União, dos estados, do Distrito Federal e dos municípios.
II Quando a administração pública efetua compra de um produto não comum cujo valor é superior a um milhão, quatrocentos e trinta mil reais, deve-se utilizar a modalidade de licitação concorrência.
III No caso de aquisição de material que só possa ser fornecido por empresa exclusiva, a administração pública deverá realizar contratação direta mediante dispensa de licitação.

Assinale a opção correta.

A Apenas o item I está certo.
B Apenas o item II está certo.
C Apenas os itens I e II estão certos.
D Apenas os itens II e III estão certos.
E Todos os itens estão certos.

Questão 50

Suponha que Ana, servidora do Tribunal de Justiça, agindo no exercício de suas funções administrativas, tenha causado dano a João.

Nessa situação hipotética, caso João pretenda ajuizar ação judicial requerendo indenização em face do Estado, a responsabilidade civil

A será subjetiva, por meio de ação de regresso.
B será objetiva, independentemente de dolo ou culpa.
C não será possível, porque o Estado não responde pelos atos de seus agentes, devendo João ajuizar ação diretamente contra Ana.
D será subsidiária, se comprovado dolo ou culpa.
E não será possível, porque o Brasil adota a teoria da irresponsabilidade estatal.

Questão 51

O Sistema de Registro de Preços poderá ser adotado nos casos em que

- Ⓐ a aquisição de bens vier a atender mais de um programa de governo, podendo ser acrescida a quantidade prevista na ata de registro de preços.
- Ⓑ houver necessidade de aquisição de bens com uma única entrega.
- Ⓒ houver quantitativo exato do produto demandado pela administração.
- Ⓓ a aquisição de bens vier a atender exclusivamente um órgão público.
- Ⓔ houver necessidade de contratações frequentes, em razão das características do serviço.

Questão 52

É considerado direito social previsto na Constituição Federal de 1988

- Ⓐ o décimo terceiro salário com base no salário básico.
- Ⓑ o salário-família pago em razão do dependente do trabalhador, independentemente da renda auferida.
- Ⓒ a assistência aos desamparados, na forma da Constituição.
- Ⓓ o salário mínimo, sendo permitida sua vinculação para qualquer fim.
- Ⓔ o seguro-desemprego, em caso de desemprego voluntário ou involuntário.

Questão 53

Conforme a Constituição Federal de 1988, as pessoas

- Ⓐ estão, em princípio, proibidas a fazer tudo, podendo um decreto regulamentar presidencial permitir a atuação individual.
- Ⓑ estão autorizadas a fazer tudo desde que a lei não proíba.
- Ⓒ só estão autorizadas a fazer aquilo que está previsto em lei.
- Ⓓ só podem fazer algo quando ato normativo legal ou infralegal expressamente permitir.
- Ⓔ não podem ser obrigadas a fazer ou deixar de fazer algo senão em virtude de ato normativo legal ou infralegal.

Questão 54

Ao Conselho Nacional de Justiça compete apreciar, de ofício ou mediante provocação,

- Ⓐ o mérito dos atos administrativos praticados por membros do Poder Judiciário.
- Ⓑ a legalidade e o mérito dos atos administrativos praticados por servidores ou membros do Poder Judiciário.
- Ⓒ o mérito dos atos administrativos praticados por servidores ou membros do Poder Judiciário.
- Ⓓ a legalidade dos atos administrativos praticados por servidores do Poder Judiciário.
- Ⓔ a legalidade dos atos administrativos praticados por membros do Poder Judiciário.

Questão 55

Maria, que possui emprego público privativo de profissionais de saúde em empresa pública estadual, foi aprovada em outro concurso público para cargo público federal privativo de profissionais de saúde.

Nessa situação hipotética, Maria

- Ⓐ não poderá acumular as funções, porque uma é estadual e a outra é federal.
- Ⓑ não poderá acumular as funções, porque apenas um dos vínculos é oriundo do regime estatutário.
- Ⓒ não poderá acumular as funções, porque não há previsão constitucional expressa que permita cumulações de funções públicas remuneradas.
- Ⓓ poderá assumir o cargo e acumular as duas funções públicas, não se aplicando a esse caso o teto remuneratório da administração pública.
- Ⓔ poderá assumir o cargo e acumular as duas funções públicas, se os horários forem compatíveis e as profissões forem regulamentadas.

Questão 56

De acordo com as resoluções do CNJ,

- Ⓐ no caso de emissão de certidão judicial, a ausência de alguns dos dados impede a expedição da certidão negativa, ainda que não haja dúvida quanto à identificação física da pessoa.
- Ⓑ os planos estratégicos dos órgãos do Poder Judiciário devem ser alinhados à Estratégia Judiciário e ter abrangência máxima de seis anos.
- Ⓒ o modelo de requisitos para sistemas informatizados de gestão de processos e documentos do Poder Judiciário brasileiro, no que concerne à segurança, é requisito imprescindível para garantir a origem e a integridade dos documentos com assinatura digital.
- Ⓓ a gestão da segurança da informação somente pode ser objeto de contratação caso a empresa contratada que provê a solução de TIC não seja a mesma que avalia ou fiscaliza o objeto da contratação.
- Ⓔ a administração do sistema Processo Judicial Eletrônico cabe exclusivamente ao CNJ, garantida a participação de representantes dos tribunais superiores, cujas atribuições serão definidas por ato do presidente do CNJ.

Questão 57

A Resolução n.º 211/2015 do CNJ trata sobre a estratégia nacional de tecnologia da informação e comunicação (TIC) do Poder Judiciário. De acordo com essa resolução,

- Ⓐ cabe exclusivamente à área de TIC estabelecer estratégias, indicadores e metas institucionais, bem como pela orientação das iniciativas e dos investimentos tecnológicos no âmbito institucional.
- Ⓑ é vedada a participação de magistrados no comitê de governança de TIC.
- Ⓒ cabe ao CNJ classificar os sistemas de informação de cada órgão, identificando os que são estratégicos por meio de inspeção ou a pedido do órgão.
- Ⓓ o comitê de governança de TIC é responsável pela elaboração de planos táticos e a área de TIC os planos operacionais e pelo estabelecimento de indicadores operacionais do órgão.
- Ⓔ cada órgão deverá elaborar o plano estratégico de TIC e o plano diretor de TIC, em harmonia com as diretrizes estratégicas institucionais e nacionais.

Questão 58

A Resolução n.º 192/2014 do CNJ descreve a Política Nacional de Formação e Aperfeiçoamento dos Servidores do Poder Judiciário. Segundo essa resolução,

- **A** as ações de formação e aperfeiçoamento deverão ser oferecidas, preferencialmente, fora da jornada de trabalho do servidor, de modo a não atrapalhar o andamento do setor ou área no qual ele esteja lotado.
- **B** as horas da ação de formação e aperfeiçoamento que excederem a jornada diária deverão ser compensadas como horas extraordinárias e pagas em pecúnia ou inseridas em bancos de horas.
- **C** ainda que a ação de formação e aperfeiçoamento tenha carga horária inferior à jornada diária, o servidor não necessita cumprir as horas faltantes.
- **D** a frequência em eventos presenciais de capacitação oferecidos pelo órgão será computada como hora trabalhada, exceto as horas de estudo realizadas pelo servidor fora das dependências do Poder Judiciário, na metodologia à distância.
- **E** os servidores inscritos em ações de educação a distância oferecidas pelo órgão podem dedicar até duas horas diárias de trabalho para participação nas atividades, desde que seja de interesse da administração.

Questão 59

De acordo com a Instrução Normativa n.º 01/2019 do Ministério da Economia, na fase de planejamento da contratação, é obrigatório

- **A** prever em edital a remuneração média dos funcionários da contratada.
- **B** prever reembolso de despesas com transporte e hospedagem, desde que afetos ao objeto da contratação e justificados pela contratada.
- **C** prever em edital exigência que os fornecedores apresentem, em seus quadros, funcionários certificados para o fornecimento da solução, antes da contratação.
- **D** elaborar o termo de referência, inclusive nos casos de inexigibilidade ou dispensa de licitação.
- **E** adotar a métrica homem-hora nos casos de contratação de serviços de desenvolvimento de *software*.

Questão 60

De acordo com a Instrução Normativa n.º 01/2019 do Ministério da Economia, o estudo técnico preliminar da contratação é o documento que descreve as análises realizadas em relação às condições da contratação, em termos de necessidades, alternativas e escolhas que demonstrem a viabilidade técnica e econômica da contratação. Esse documento

- **A** será aprovado e assinado pelos integrantes técnico e requisitante da equipe de planejamento da contratação e pela autoridade máxima da área de TIC ou, caso esta componha a equipe, pela autoridade superior à ela.
- **B** será especificado com base em requisitos necessários e suficientes e conterá o quantitativo de bens e serviços, ressalvado à forma de cálculo para a sua composição que deve ser inserida no termo de referência ou projeto básico.
- **C** considera estritamente os aspectos econômicos da solução, com descrição detalhada, motivada e justificada.
- **D** exclui aspectos qualitativos em termos de benefícios, sob pena de tornar inválida a imparcialidade exigida no estudo da contratação, ainda que haja necessidades de adequação do ambiente do órgão para viabilizar a execução contratual.
- **E** compreende a análise comparativa de soluções e de custos para as soluções técnicas, ainda que não sejam funcionalmente viáveis, desde que haja a possibilidade de contratação como serviço e o *Total Cost Ownership* seja vantajoso para o órgão.

Espaço livre