

-- CONHECIMENTOS ESPECÍFICOS --**REDES DE COMPUTADORES****Questão 41**

Na arquitetura TCP/IP, os pacotes na camada de rede são denominados

- A** quadros.
- B** segmentos.
- C** cabeçalhos.
- D** *offsets*.
- E** datagramas.

Questão 42

Assinale a opção na qual é corretamente apresentada a topologia de rede que é usada para definir a ordem em que as estações transmitem seus dados.

- A** estrela
- B** barramento
- C** *multihop*
- D** anel
- E** *ethernet*

Questão 43

A *gigabit ethernet* admite cabeamento UTP de

- A** 16 pares.
- B** 14 pares.
- C** 12 pares.
- D** 10 pares.
- E** 8 pares.

Questão 44

De acordo com o que preconiza a norma EIA/TIA-568 para o padrão de cabos par trançado categoria 5, o comprimento máximo do cabeamento horizontal, da tomada ao *patch panel*, deve ser de

- A** 90 m.
- B** 100 m.
- C** 110 m.
- D** 130 m.
- E** 150 m.

Questão 45

Assinale a opção em que é apresentado o mecanismo que, em *switches fast ethernet*, permite que duas estações ajustem automaticamente a velocidade ideal (10 Mbps ou 100 Mbps) e o tipo de duplex (*half* ou *full*).

- A** direção da transmissão
- B** autonegociação
- C** codificação binária
- D** identificador da porta
- E** taxa de *clock*

Questão 46

Assinale a opção na qual é apresentado o código HTTP que indica que uma requisição do cliente foi recebida, entendida e processada pelo servidor.

- A** 100
- B** 200
- C** 300
- D** 400
- E** 500

Questão 47

Suponha que se utilizem 4 *bits* de um endereço classe C com o intuito de gerar sub-redes considerando-se CIDR. Nesse caso, é correto afirmar que o número máximo de *subnets* que podem ser geradas é igual a

- A** 2.
- B** 4.
- C** 8.
- D** 16.
- E** 32.

Questão 48

A principal função do protocolo IEEE 802.1d (*spanning tree protocol*) é

- A** evitar que o CRC na camada física seja modificado.
- B** evitar *loops*.
- C** permitir o roteamento de pacotes.
- D** evitar pacotes duplicados.
- E** permitir a configuração do atraso do envio do datagrama.

Questão 49

No uso de VLAN com o padrão IEEE 802.1Q, o valor do ID de protocolo de VLAN sempre será de

- A** 0x8100.
- B** 0x1A00.
- C** 0x0081.
- D** 0x0000.
- E** 0xAA00.

Questão 50

Assinale a opção em que são respectivamente apresentados um protocolo criptográfico e uma técnica de autenticação criptográfica utilizados no WPA2.

- A** AES e HMAC
- B** DES e TLS
- C** RC4 e LDAP
- D** DES e LDAP
- E** RC4 e HMAC

Questão 51

Considerando a tolerância das aplicações de voz sobre IP, assinale a opção correta no que se refere a atrasos e variação de atrasos.

- Ⓐ O *jitter* ocorre apenas em redes com comutação de circuitos.
- Ⓑ O *jitter* não afeta aplicações de voz, pois o áudio é reconstruído integralmente no destino.
- Ⓒ O aumento do tamanho do *buffer* reduz simultaneamente o atraso e o *jitter* percebidos.
- Ⓓ *Buffers* de reprodução podem suavizar o *jitter*, ao custo de aumento do atraso fim a fim.
- Ⓔ *Buffers* de reprodução eliminam atrasos e perdas de pacotes em aplicações de voz sobre IP.

Questão 52

```
INVITE sip:destinatario@dominio2.com SIP/2.0
Via: SIP/2.0/UDP 167.180.112.24
From: sip:remetente@dominio1.com
To: sip:destinatario@dominio2.com
Call-ID: a2e3a@pigeon.dominio1.com
Content-Type: application/sdp
Content-Length: 960
```

```
c=IN IP4 167.180.112.24
m=audio 38060 RTP/AVP 0
```

Com base nessa mensagem *invite* do protocolo SIP, assinale a opção correta.

- Ⓐ A última linha da mensagem determina a forma como o remetente quer receber o áudio da ligação SIP.
- Ⓑ O endereço 167.180.112.24 corresponde ao próximo salto que a mensagem deverá fazer para chegar ao destino.
- Ⓒ O endereço a2e3a@pigeon.dominio1.com corresponde ao endereço do servidor SIP.
- Ⓓ A linha *Content-Type* determina os formatos de arquivo que podem ser anexados durante a chamada SIP.
- Ⓔ A linha *Content-Lenght* indica o comprimento, em *bits*, do tamanho da mensagem SIP.

Questão 53

Uma transmissão de dados limitada a ocorrer apenas quando o pacote transmitido tiver comprimento menor ou igual a 120 *bytes*, como forma de se obter qualidade de serviço (QoS) na comunicação, constitui exemplo de

- Ⓐ controle de admissão.
- Ⓑ roteamento proporcional.
- Ⓒ programação de pacotes.
- Ⓓ algoritmo de balde furado.
- Ⓔ reserva de recursos.

Questão 54

A área de gerenciamento de rede cuja meta é controlar o acesso aos recursos da rede de acordo com alguma política bem definida denomina-se

- Ⓐ gerenciamento de segurança.
- Ⓑ gerenciamento de configuração.
- Ⓒ gerenciamento de contabilização.
- Ⓓ gerenciamento de desempenho.
- Ⓔ gerenciamento de falhas.

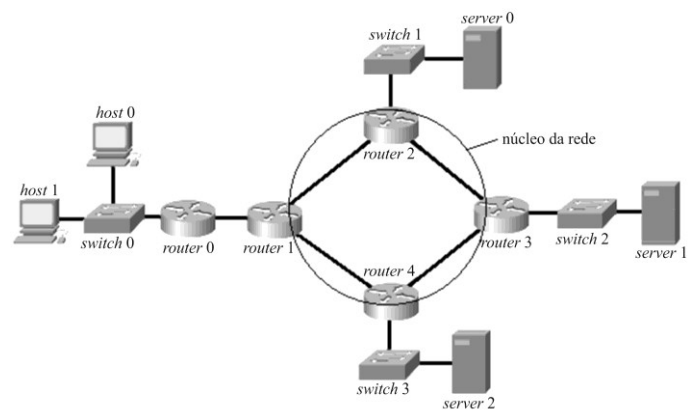
Questão 55

Em uma rede corporativa, o administrador pretende reduzir o tráfego de gerenciamento entre os dispositivos e o sistema central, mantendo informações detalhadas sobre desempenho, erros e padrões de tráfego.

Nessa situação hipotética, considerados os conceitos de SNMP, MIB, NMS, agentes e RMON,

- Ⓐ a combinação de SNMP e RMON exige que o protocolo SNMP utilize TCP para suportar grandes volumes de dados.
- Ⓑ a utilização de sondas RMON permite que os agentes colem e armazenem estatísticas localmente, expondo-as ao NMS por meio de objetos definidos em MIB.
- Ⓒ o RMON substitui o papel do NMS, pois realiza análise, decisão e visualização dos dados de gerenciamento.
- Ⓓ o SNMP opera de forma totalmente distribuída, sem entidade central, dispensando o uso de agentes.
- Ⓔ o administrador deve configurar o NMS para realizar *polling* contínuo dos agentes SNMP.

Texto 2A2



Na rede exemplificada acima, os *hosts* acessam serviços disponíveis em todos os servidores representados e o *router* 0, o *router* 1, o *router* 2 e o *router* 3 estão localizados em cidades diferentes.

Questão 56

Com base na rede exemplificada no texto 2A2, considerando que, para se garantirem níveis de qualidade de serviço no acesso aos servidores, uma reserva de recursos tenha sido configurada por meio do protocolo RSVP entre o *router* 0 e o *router* 1, e que tenham sido configuradas classes de serviço entre o *router* 1, o *router* 2, o *router* 3 e o *router* 4, com encaminhamento garantido, assinale a opção correta.

- Ⓐ Entre o *router* 0 e o *router* 1 foi configurado serviço diferenciado, e configurado serviço integrado no *router* 1, no *router* 2, no *router* 3 e no *router* 4.
- Ⓑ Entre o *router* 0 e o *router* 1 foi configurado serviço integrado, e configurado serviço diferenciado no *router* 1, no *router* 2, no *router* 3 e no *router* 4.
- Ⓒ Não foram configurados nem serviços integrados, nem serviços diferenciados nos roteadores da rede em questão.
- Ⓓ Entre o *router* 0 e o *router* 1 foi configurado serviço diferenciado, assim como no *router* 1, no *router* 2, no *router* 3 e no *router* 4.
- Ⓔ Entre o *router* 0 e o *router* 1 foi configurado serviço integrado, assim como no *router* 1, no *router* 2, no *router* 3 e no *router* 4.

Questão 57

Ainda com base na rede exemplificada no texto 2A2, assinale a opção correta em relação aos conceitos de redes de computadores e aos elementos de interconexão de redes de computadores.

- A** Caso o *server* 1 e o *server* 2 estejam localizados em cidades diferentes, então eles deverão ser configurados em VLAN diferentes.
- B** A topologia da zona delimitada como núcleo da rede é estrela.
- C** O protocolo MPLS é uma alternativa para o encaminhamento de informação no núcleo da rede.
- D** A solução mais viável para realizar a conexão entre os *hosts* 0 e 1 ao *switch* 0 são os cabos coaxiais.
- E** Um protocolo de roteamento é necessário para a realização da comunicação entre o *server* 2 e o *router* 4.

Questão 58

Na comunicação entre dois *hosts*, o gerenciamento de *token*, uma das facilidades existentes no modelo OSI, ocorre na camada

- A** de apresentação.
- B** de transporte.
- C** de sessão.
- D** física.
- E** de enlace de dados.

Questão 59

Assinale a opção correta no que se refere às bandas de operação dos padrões IEEE 802.11.

- A** O padrão 802.11n opera apenas na banda de 2,4 GHz.
- B** O padrão 802.11ac funciona em uma faixa de frequências que não sofre interferências por micro-ondas.
- C** O padrão 802.11g funciona em uma faixa de frequências que não sofre interferências por micro-ondas.
- D** Os padrões 802.11b e 802.11g operam na banda de 5 GHz.
- E** Os padrões 802.11a e 802.11ac operam apenas na banda de 5 GHz.

Questão 60

Assinale a opção correta acerca dos protocolos do modelo TCP/IP.

- A** Em uma conexão HTTPS, a resolução de nomes via DNS acontece depois no estabelecimento da conexão TCP.
- B** O DNS e o DHCP são protocolos da camada de transporte.
- C** A resolução iterativa de nomes, no DNS, ocorre apenas no cliente final.
- D** A utilização preferencial do protocolo UDP pelo DNS deve-se à redução de latência que aquele protocolo propicia.
- E** Enquanto o DHCP fornece o endereço IP a um *host*, o DNS fornece os demais parâmetros de rede.

GOVERNANÇA DE TI**Questão 61**

Um dos objetivos da governança de I&T, conforme o COBIT 2019, é assegurar que o uso da informação e da tecnologia esteja alinhado à estratégia organizacional. Esse alinhamento contribui para a geração de valor e para a tomada de decisões mais eficazes, devendo a governança atuar como elo entre estratégia e execução. De acordo com a literatura especializada de Jean Ribeiro a respeito do COBIT 2019, a governança de I&T deve

- A** assegurar que a I&T suporte e amplifique a estratégia organizacional.
- B** centralizar decisões técnicas da organização na área de I&T.
- C** priorizar principalmente iniciativas de I&T de curto prazo.
- D** garantir padronização total das tecnologias da organização.
- E** reduzir o número de projetos de I&T no âmbito da organização.

Questão 62

A norma NBR ISO/IEC 38500:2018 adota o modelo “avaliar, dirigir e monitorar” (ADM) como base para a governança de TI. Esse modelo fornece uma estrutura para orientar decisões estratégicas e acompanhar o desempenho da TI em relação aos objetivos organizacionais. De acordo com o modelo ADM, a atividade “dirigir” corresponde a

- A** definir e implementar soluções tecnológicas.
- B** executar serviços de TI.
- C** monitorar e avaliar indicadores operacionais de TI.
- D** resolver problemas técnicos e identificar sua causa-raiz.
- E** definir políticas e direcionamentos para orientar o uso da TI.

Questão 63

A norma NBR ISO 31000:2018 apresenta uma definição ampliada de risco. Assinale a opção em que é corretamente apresentado o conceito de risco adotado pela referida norma.

- A** situação que deve ser sempre evitada
- B** evento indesejado que causa prejuízo financeiro
- C** probabilidade de ocorrência de falhas operacionais
- D** efeito da incerteza sobre os objetivos da organização
- E** ameaça externa que pode gerar incidentes

Questão 64

Um dos mecanismos do Kanban é a limitação do trabalho em progresso (WIP – *work in progress*), mecanismo amplamente utilizado por times de tecnologia. O principal objetivo do estabelecimento de limites de WIP é

- A** possibilitar que todos trabalhem simultaneamente em várias atividades.
- B** aumentar a quantidade de tarefas iniciadas em determinado período.
- C** otimizar o fluxo das atividades e reduzir acúmulo de trabalho.
- D** reduzir o número total de demandas recebidas em determinado período.
- E** controlar o desempenho individual dos membros da equipe.

Questão 65

A visualização é um dos pilares do Kanban, e seu principal benefício resulta do fato de que ela

- Ⓐ elimina a necessidade de reuniões de acompanhamento.
- Ⓑ torna explícito o fluxo de trabalho e possibilita a identificação de gargalos.
- Ⓒ controla o tempo individual que cada colaborador leva para concluir determinada tarefa.
- Ⓓ substitui a necessidade de elaboração de relatórios gerenciais formais.
- Ⓔ automatiza o controle do trabalho, prescindindo-se da gestão humana.

Questão 66

O Guia PMBOK organiza o gerenciamento de projetos em domínios de desempenho que interagem entre si. Esses domínios não representam fases sequenciais, mas áreas de foco que devem ser gerenciadas ao longo do ciclo de vida do projeto. Com base na 7.^a edição do referido guia, assinale a opção em que é corretamente apresentado um dos domínios de desempenho do PMBOK.

- Ⓐ gerenciamento do cronograma
- Ⓑ aquisições
- Ⓒ gerenciamento do escopo
- Ⓓ equipe
- Ⓔ custos

Questão 67

De acordo com o Guia PMBOK 7.^a edição, a prática denominada *tailoring* corresponde a

- Ⓐ realizar processos que reduzam a necessidade de controles formais em projetos ágeis.
- Ⓑ aplicar de forma padronizada a mesma metodologia em todas as etapas do gerenciamento de projetos.
- Ⓒ selecionar e ajustar as práticas de gerenciamento conforme o contexto do projeto e da organização.
- Ⓓ eliminar processos considerados burocráticos e dispensáveis para o andamento do projeto.
- Ⓔ aplicar processos que substituam a estrutura de governança da organização.

Questão 68

Conforme o Scrum, o *scrum team* é composto por três papéis, com responsabilidades claramente definidas. Assinale a opção em que esses três papéis são corretamente apresentados.

- Ⓐ gerente de projeto, analista e desenvolvedor
- Ⓑ *product owner*, *stakeholder* e *scrum master*
- Ⓒ desenvolvedor, líder técnico e *scrum master*
- Ⓓ *product owner*, *scrum master* e gerente de projeto
- Ⓔ *product owner*, *scrum master* e desenvolvedores

Questão 69

Certo *scrum team* está conduzindo sua 5.^a *sprint*. Durante o *sprint review*, *stakeholders* identificam a necessidade de ajustes relevantes em funcionalidades recém-entregues. Diante disso, foi tomada a decisão de se reorganizar o *product backlog*, incluindo-se novos itens derivados do *feedback*. Paralelamente, parte dos itens originalmente planejados para a *sprint* não atingiu a *definition of done*. A equipe questiona como tratar os itens incompletos e como o *feedback* recebido deve impactar o planejamento futuro, considerando o papel do refinamento contínuo.

Na situação hipotética apresentada, a conduta que a equipe deve adotar é

- Ⓐ bloquear alterações no *product backlog* até o encerramento do ciclo do produto.
- Ⓑ incluir o *feedback* no *product backlog*, reordenar o *backlog* conforme valor e tratar itens não concluídos como não entregues.
- Ⓒ considerar os itens parcialmente concluídos como parte do incremento, se tiverem sido testados.
- Ⓓ prorrogar a *sprint* até que todos os itens atinjam a *definition of done*.
- Ⓔ transferir automaticamente os itens incompletos para a próxima *sprint*.

Questão 70

Uma organização pública decidiu reformular sua central de serviços após recorrentes reclamações sobre lentidão na resolução de incidentes. A alta gestão da organização determinou que qualquer mudança deveria priorizar valor ao usuário final, evitar desperdícios de esforço e considerar as capacidades já existentes na equipe antes de adquirir novas ferramentas. Durante o planejamento da melhoria, a equipe de TI propôs: revisar fluxos de atendimento, redefinir acordos de nível de serviço e analisar causas recorrentes de incidentes, sem alterar inicialmente a estrutura organizacional.

As necessidades de melhoria da organização da situação hipotética precedente podem ser atendidas por meio de uma combinação entre um princípio orientador do ITIL v4 e práticas nele previstas. Assinale a opção em que esse princípio e essas práticas são corretamente apresentados.

- Ⓐ princípio “pensar e trabalhar holisticamente” e práticas de gerenciamento de fornecedores
- Ⓑ princípio “progredir iterativamente com *feedback*” e práticas de gerenciamento de mudança
- Ⓒ princípio “focar no valor” e práticas de central de serviços e gerenciamento de incidentes
- Ⓓ princípio “focar no valor” e práticas de gerenciamento de capacidade
- Ⓔ princípio “colaborar e promover visibilidade” e práticas de central de serviços e gerenciamento de incidentes

Questão 71

Um gestor de TIC do SEMA/AM deve elaborar um instrumento de planejamento voltado para a área de TI do órgão. No patamar estratégico do documento, deve ser descrito como realizar a transição da situação atual para a futura, por meio de metas e ações, com base na definição de objetivos específicos de longo prazo.

Nessa situação hipotética, de acordo com o **Guia de Elaboração de PDTI**, produzido pela Secretaria de Governo Digital, o documento a ser elaborado pelo gestor é

- Ⓐ o planejamento estratégico institucional (PEI).
- Ⓑ o plano plurianual (PPA).
- Ⓒ o plano diretor de tecnologia da informação e comunicação (PDTIC).
- Ⓓ o plano estratégico de tecnologia da informação e comunicação (PETIC).
- Ⓔ a estratégia de governo digital (EGD).

Questão 72

De acordo com o **Guia de elaboração de PDTI**, produzido pela Secretaria de Governo Digital, o subprocesso denominado planejamento, parte do ciclo de elaboração do PDTIC, contempla atividades relacionadas à priorização das necessidades e metas, sob o ponto de vista de pessoal, orçamento e riscos. Acerca da atividade “definir metas e ações” desse subprocesso, assinale a opção correta.

- Ⓐ Devem-se estimar, nesse subprocesso, os prazos e os recursos humanos necessários ao desenvolvimento das ações planejadas, incluindo-se data provável de início e conclusão das ações; os recursos orçamentários para o desenvolvimento das ações só devem ser estimados no subprocesso seguinte.
- Ⓑ No relacionamento entre as necessidades, metas e ações, é possível que uma necessidade possa ser satisfeita com o alcance de uma ou mais metas, assim como uma meta pode ser alcançada com a execução de uma ou mais ações.
- Ⓒ Devem ser estabelecidos indicadores com prazos estimativos, de modo que se possam alcançar as metas estabelecidas, sem a necessidade de elencar, nesse subprocesso, os respectivos responsáveis principais.
- Ⓓ No âmbito do planejamento, a necessidade deve ser considerada mais concreta que a meta, uma vez que, para se satisfazer uma necessidade, as metas devem ser utilizadas como referências para a identificação de ações e indicadores.
- Ⓔ A descrição de todas as características importantes para a resolução das necessidades de TIC inventariadas dispensa a definição das soluções tecnológicas dessa resolução, uma vez que estas serão detalhadas no próximo subprocesso.

Espaço livre

Questão 73

Assinale a opção correta com base na Instrução Normativa SGD/ME n.º 94, que rege o processo de contratação de soluções de TIC.

- Ⓐ Na contratação de infraestrutura de centro de dados, os órgãos que necessitem criar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços *on-premises*, salvo nos casos de expansão de sua estrutura em *cloud computing*, em que poderão seguir a mesma arquitetura, exigindo-se, em quaisquer casos, a demonstração de viabilidade em estudo técnico preliminar da contratação.
- Ⓑ Pertencente à equipe de fiscalização do contrato, o fiscal requisitante do contrato é servidor representante das unidades desconcentradas de um órgão, devendo ser indicado pela autoridade competente da área administrativa para o acompanhamento da execução do contrato na esfera de negócio e na esfera funcional da solução de TIC.
- Ⓒ Na contratação de licenciamento de *software* e serviços agregados, deve-se incluir cláusula que, direta ou indiretamente, exija a contratação conjugada de serviços de suporte técnico e de atualização de versões, quando não houver a necessidade de ambos.
- Ⓓ Durante o monitoramento da execução do contrato, o fiscal técnico deve confeccionar, com base na avaliação da qualidade dos serviços realizados e na conformidade e aderência aos termos contratuais, com o apoio do fiscal requisitante do contrato, o termo de recebimento definitivo (TRD), que deverá ser assinado pelo fiscal administrativo.
- Ⓔ Na contratação de solução de autenticação para serviços públicos digitais, é permitida a contratação de soluções de autenticação em aplicações destinadas a serviços públicos digitais, desde que prevista no PDTIC do órgão e observadas, em quaisquer circunstâncias, as normas publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

Questão 74

Ainda à luz da Instrução Normativa SGD/ME n.º 94, assinale a opção correta.

- Ⓐ O termo de referência deve garantir, por meio de cláusulas vinculantes, que, após a assinatura do contrato e durante toda sua vigência, o gestor do contrato exerça vínculo de subordinação com funcionário da empresa prestadora de serviço, não sendo esse fato considerado intervenção da administração em sua gestão interna.
- Ⓑ O termo de referência deverá ser assinado pela autoridade máxima da área de TIC, sendo obrigatória a definição precisa do objeto da contratação, vedadas especificações que limitem a competição, exigindo-se também que se assegure sua prorrogação por meio de cláusulas contratuais, as quais devem conter a indicação do prazo da prorrogação e da duração do contrato.
- Ⓒ O contrato que prever a operação continuada de sistemas estruturantes de tecnologia da informação — sistemas de informação desenvolvidos para sustentar atividades como orçamento ou administração financeira comuns a todos os órgãos da administração que, a critério do Poder Executivo, necessitem de coordenação central — poderá ter vigência máxima de 15 anos.
- Ⓓ O apoio técnico aos processos de gestão das soluções de TIC não pode ser objeto de contratação, salvo quando a contratada que provê a solução de TIC seja a mesma que mensura a fiscalização.
- Ⓔ Para fins de prorrogação contratual, fica a critério do gestor do contrato, desde que neste previsto, realizar ou não pesquisa de preços que venha a compor a documentação e vise subsidiar a decisão da administração de renovar a contratação.

Questão 75

À luz do disposto no **Guia Prático de Gestão de Processos**, elaborado pela Secretaria de Gestão do Ministério da Economia, assinale a opção correta.

- Ⓐ De acordo com as diretrizes metodológicas para a gestão de processos, ao se analisar um processo, é preciso realizar o levantamento das apresentações gráficas dos processos de negócio existentes (AS IS) e realizar o desenho do novo processo, com a visão melhorada (TO BE) do processo, inclusive com o plano inicial de ação para sua implantação.
- Ⓑ A utilização de indicadores é importante no fluxo de melhoria de processos, pois evidencia o grau de sucesso alcançado, sendo, portanto, necessário que todos os processos sejam acompanhados por indicadores, incluindo-se a implantação das rotinas de coleta de dados e a análise desses indicadores.
- Ⓒ O planejamento do projeto de melhoria de um processo engloba atividades de estudo preliminar, plano de trabalho e cronograma, bem como a definição de escopo e reuniões de sensibilização para garantir o engajamento dos responsáveis pelo processo.
- Ⓓ A governança de processos estabelece papéis e responsabilidades, cabendo ao gestor do processo, dada a sua função central, com responsabilidade geral pelo processo de ponta a ponta, patrocinar as iniciativas em gerenciamento de processos de forma a disponibilizar os recursos necessários para sua implantação.
- Ⓔ Espera-se que haja ciclo virtuoso de melhoria contínua por meio da gestão de processos desde que a modelagem do processo se restrinja à documentação de manuais e fluxos, e não enseje transformação de processos de trabalho que elevem custos financeiros para o órgão.

Questão 76

Assinale a opção em que é corretamente citado o princípio estabelecido pela ABNT NBR ISO/IEC 38500:2018, segundo o qual TI é adequada à finalidade de suporte da organização, fornecendo os serviços, os níveis de serviço e a qualidade dos serviços necessários para o atendimento dos requisitos do negócio, tanto atuais quanto futuros.

- Ⓐ estratégia
- Ⓑ desempenho
- Ⓒ responsabilidade
- Ⓓ conformidade
- Ⓔ capacidade

Questão 77

O BSC (*balanced scorecard*), técnica de planejamento empresarial, propicia o alinhamento das iniciativas de TI aos objetivos estratégicos do negócio. Especificamente, a satisfação do cliente é, no BSC, considerada resultado diretamente associado à perspectiva

- Ⓐ financeira.
- Ⓑ de fator crítico de sucesso.
- Ⓒ de aprendizado e crescimento.
- Ⓓ de processo interno.
- Ⓔ de conhecimento.

Questão 78

De acordo com as etapas de construção de um BSC, deve-se

- I estabelecer a visão da empresa sobre o futuro que ela deseja atingir.
- II definir tanto os indicadores de resultado quanto os indicadores de desempenho para cada objetivo estratégico.
- III determinar relações de causa e efeito, descrevendo-se como os objetivos se relacionam entre si.
- IV determinar metas quantitativas para cada um dos indicadores de resultado.

Assinale a opção correta.

- Ⓐ Apenas os itens I, II e III estão certos.
- Ⓑ Apenas os itens I, II e IV estão certos.
- Ⓒ Apenas os itens I, III e IV estão certos.
- Ⓓ Apenas os itens II, III e IV estão certos.
- Ⓔ Todos os itens estão certos.

Questão 79

De acordo com a ABNT NBR ISO/IEC 27001:2022, ao planejar o sistema de gestão da segurança da informação (SGSI) a organização deve

- Ⓐ fazer apenas o levantamento de riscos, sem avaliações ou tratamento, pois, no caso de um SGSI, a gestão de riscos é executada assim que o sistema é aprovado pela alta direção.
- Ⓑ manter critérios para avaliação de riscos, mas não de tratamento nem de aceitação de riscos.
- Ⓒ estabelecer critérios de aceitação de riscos para as avaliações de riscos, assim como estabelecer e aplicar processo de tratamento de riscos.
- Ⓓ manter critérios para tratamento de riscos, mas não sobre avaliação de riscos.
- Ⓔ utilizar norma complementar, pois a norma 27001:2022 não sugere ações afetas a riscos na fase de planejamento.

Questão 80

Assinale a opção correta em relação ao disposto na ABNT NBR ISO/IEC 27002:2022 acerca de itens afetos ao uso de serviços em nuvem, à privacidade e proteção de dados pessoais (*personally identifiable information*), e ao trabalho remoto.

- Ⓐ Não há previsão de controles específicos para nenhum dos itens mencionados, em que se pese a existência de tratamento indireto de todos eles, por meio de outros controles.
- Ⓑ Os processos de uso e gestão de serviços em nuvem devem ser estabelecidos de acordo com os requisitos de segurança da informação da organização, não havendo controles específicos para os itens afetos ao uso de serviços em nuvem e à privacidade e proteção de dados pessoais (*personally identifiable information*).
- Ⓒ São previstos controles específicos para todos os itens mencionados.
- Ⓓ As medidas de segurança devem ser implementadas durante o trabalho remoto para a proteção das informações acessadas ou armazenadas fora das instalações da organização, não sendo previstos controles específicos para os itens afetos ao uso de serviços em nuvem e à privacidade e proteção de dados pessoais (*personally identifiable information*).
- Ⓔ A organização deve atender aos requisitos relativos à preservação da privacidade de dados pessoais, não sendo previstos controles específicos para os itens afetos ao uso de serviços em nuvem e ao trabalho remoto.

SEGURANÇA DA INFORMAÇÃO**Questão 81**

Uma organização pública avalia a adoção da ABNT NBR ISO/IEC 27001 como referência para estruturar a gestão da segurança da informação, com o intuito de proteger seus ativos informacionais, apoiar seus objetivos institucionais e tratar adequadamente os riscos associados ao uso da informação. No diagnóstico preliminar, verificou-se que existem iniciativas pontuais de segurança, porém sem integração formal entre políticas, processos e responsabilidades organizacionais.

Na situação hipotética precedente, a escolha pela adoção da NBR ISO/IEC 27001:2013 seria benéfica para a organização em questão, considerando-se que tal norma

- A** estabelece um modelo de gestão baseado em política formal, liderança da alta administração e abordagem sistemática e preventiva de gestão de riscos no contexto da segurança da informação.
- B** orienta a implementação de controles de segurança apenas como resposta a incidentes já ocorridos, priorizando uma abordagem corretiva e reativa.
- C** restringe a responsabilidade pela segurança da informação às áreas de TI, concentrando a tomada de decisão em equipes com especialização técnica.
- D** prioriza exclusivamente a implementação de controles técnicos de segurança, como *firewalls* e antivírus, reduzindo a necessidade de controles administrativos.
- E** define um conjunto fixo e obrigatório de controles de segurança que devem ser aplicados de forma uniforme, independentemente do contexto e dos riscos da organização.

Questão 82

Durante a implantação de um sistema de gestão da segurança da informação (SGSI) na secretaria de meio ambiente de certo estado da Federação, a equipe responsável identificou que já existiam controles técnicos de segurança em operação, porém sem diretrizes formais documentadas, sem definição clara de responsabilidades e sem um processo estruturado de análise de riscos. Diante desse cenário, a alta administração solicitou a adoção de práticas que permitissem integrar governança, gestão de riscos e controles de segurança da informação, de forma consistente e alinhada às boas práticas de gestão da segurança da informação.

Nessa situação, de acordo com as disposições da NBR ISO/IEC 27001:2013 relativas à gestão da segurança da informação, a medida prioritária que a secretaria deve adotar para atender à solicitação da alta administração é

- A** definir os controles de segurança da informação adotando uma abordagem puramente reativa, baseada apenas nos incidentes de segurança que já ocorreram na organização.
- B** delegar a responsabilidade pela segurança da informação exclusivamente às equipes de TI, a fim de não sobrecarregar a alta administração, cujo envolvimento direto poderá ser dispensado.
- C** estabelecer uma política de segurança aprovada pela alta administração e baseada em análise sistemática de riscos para a seleção coerente de controles organizacionais.
- D** implantar novos controles técnicos de forma imediata, com foco em tecnologias avançadas, mas sem a devida formalização de políticas ou uma prévia análise de riscos institucionais.
- E** focar a elaboração de procedimentos operacionais para as áreas técnicas, postergando a definição da política de segurança da informação, que é o documento norteador.

Questão 83

Uma organização pública, após decidir pela adoção da norma NBR ISO/IEC 27001:2013, iniciou a implementação de um SGSI. Durante esse processo, a organização buscou estruturar suas ações de modo a garantir que a segurança da informação fosse mantida e aprimorada ao longo do tempo.

Considerando a situação hipotética precedente e as disposições da NBR ISO/IEC 27001:2013, assinale a opção em que é apresentada prática necessária à efetividade do SGSI no caso.

- A** adoção de controles de segurança focados predominantemente no atendimento a exigências formais de auditoria e conformidade
- B** implementação inicial de controles de segurança, dispensando-se revisões posteriores do SGSI após sua formalização
- C** centralização das decisões relativas à segurança da informação no âmbito exclusivo da área de tecnologia da informação
- D** definição de controles de segurança estáveis, mantidos independentemente de mudanças no contexto organizacional
- E** realização periódica de avaliações e ajustes no SGSI em função de alterações nos riscos e nos objetivos institucionais

Questão 84

Conforme os fundamentos da NBR ISO/IEC 27001:2013, a política de segurança da informação cumpre adequadamente seu papel quando

- A** estabelece diretrizes gerais alinhadas aos objetivos organizacionais e define responsabilidades relacionadas à segurança da informação.
- B** é elaborada exclusivamente para atender exigências formais de auditoria, dispensando ampla divulgação interna.
- C** permanece inalterada ao longo do tempo, independentemente de mudanças no contexto organizacional ou nos riscos associados à informação.
- D** define regras técnicas de segurança, sendo sua aplicação delegada exclusivamente à área de tecnologia da informação.
- E** descreve de forma detalhada procedimentos operacionais e controles técnicos específicos para todos os sistemas da organização.

Espaço livre

Questão 85

De acordo com a NBR ISO/IEC 27001:2013, com a literatura especializada de Sêmola e Stallings e com as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD), é compatível com a estruturação adequada de um SGSI e com o regime legal aplicável à proteção de dados pessoais a ação de

- I definir e divulgar uma política formal de segurança da informação, devidamente aprovada pela alta administração da organização, estabelecendo-se diretrizes para controle de acesso, classificação da informação, tratamento de incidentes e uso aceitável de recursos.
- II realizar processo sistemático de avaliação e tratamento de riscos de segurança da informação, contemplando ameaças e vulnerabilidades associadas ao tratamento de dados pessoais, com seleção e documentação de controles técnicos e administrativos.
- III instituir mecanismos formais de registro e gestão de incidentes de segurança da informação que envolvam dados pessoais, com procedimentos para detecção, resposta, comunicação às partes interessadas e registro de evidências.
- IV assegurar que o uso de criptografia em trânsito e em repouso seja adotado de forma isolada, dispensando-se monitoramento contínuo e revisões periódicas de sua efetividade.

Estão certos apenas os itens

- A I e IV.
- B II e III.
- C II e IV.
- D I, II e III.
- E I, III e IV.

Questão 86

Uma organização pública adota um mecanismo no qual, após a validação inicial das credenciais do usuário, é emitido um artefato digital assinado que passa a acompanhar as requisições subsequentes ao sistema, permitindo que o servidor valide a identidade e os atributos do usuário sem a necessidade de nova autenticação a cada solicitação.

A partir da descrição do mecanismo adotado na situação hipotética precedente, é correto concluir que a referida organização faz o uso de

- A autenticação baseada em certificado digital.
- B autenticação por *token* físico.
- C autenticação de dois fatores (2FA).
- D OAuth 2.0.
- E JWT (JSON *web token*).

Questão 87

Em um ambiente de aplicações distribuídas, uma organização adota um modelo no qual o usuário realiza autenticação junto a um provedor de identidade e, a partir desse processo, passa a acessar diferentes aplicações sem necessidade de novas autenticações diretas em cada serviço. Nesse contexto, são utilizados mecanismos distintos para autenticar o usuário, delegar autorização de acesso a recursos e transportar informações de identidade entre os sistemas envolvidos.

Considerando esse cenário, assinale a opção em que é apresentada a combinação adequada de tecnologias para autenticação do usuário, delegação de autorização e transporte de informações de identidade, respectivamente.

- A OpenID Connect; JWT; OAuth 2.0
- B OAuth 2.0; JWT; OpenID Connect
- C JWT; OAuth 2.0; OpenID Connect
- D OpenID Connect; OAuth 2.0; JWT
- E OAuth 2.0; OpenID Connect; JWT

Questão 88

Uma equipe de TI da SEMA/AM está projetando a arquitetura de autenticação de um conjunto de APIs internas acessadas por aplicações *web* e móveis. A solução deverá: (i) permitir que aplicativos clientes obtenham acesso a recursos protegidos em nome do usuário, sem expor a senha ao serviço consumidor; (ii) padronizar a autenticação única (SSO) entre múltiplas aplicações, com entrega de informações de identidade em formato de *token*; (iii) suportar autenticação forte com segundo fator (2FA) baseada em aplicativo autenticador ou *token* físico, integrada ao fluxo de *login*. Considerando os requisitos de governança definidos no SGSI da organização, alinhado à NBR ISO/IEC 27001, bem como as recomendações de segurança sobre autenticação robusta e controle de acesso, a equipe deve avaliar algumas opções de desenho.

Na situação hipotética precedente, a solução de autenticação que melhor atende, em conjunto, às três necessidades apresentadas consiste na arquitetura em que

- A cada microsserviço possua seu próprio banco de senhas e *tokens* proprietários, combinando autenticação por senha com 2FA por SMS, sem um provedor de identidade central.
- B um provedor de identidade central aplique 2FA e exponha fluxos OAuth 2.0 com OpenID Connect, emitindo *tokens* de identidade em formato JWT para viabilizar o SSO.
- C as APIs exijam certificados digitais de cliente para autenticação mútua TLS, dispensando *tokens*, e o segundo fator de autenticação seja aplicado apenas na emissão dos certificados.
- D a autenticação combine biometria local em dispositivos móveis e sessões por *cookies* na Web, sem usar protocolos de delegação ou *tokens* de identidade padronizados.
- E um servidor de autorização central com OAuth 2.0 emita *tokens* de acesso, mas a autenticação de usuários permaneça descentralizada e independente em cada aplicação.

Questão 89

Uma equipe de TI da SEMA/AM está desenvolvendo um novo sistema de licenciamento ambiental, que será acessado por servidores internos e por cidadãos. A arquitetura proposta prevê: (i) uso de autenticação de dois fatores (2FA) para os servidores internos, combinando-se senha e aplicativo gerador de códigos temporários (OTP); (ii) autenticação baseada em biometria facial em aplicativo móvel para cidadãos, associada a um PIN cadastrado; (iii) utilização de um provedor de identidade que emite JWT assinados, contendo informações de identidade (*claims*), que serão apresentados às APIs após o processo de autenticação. No desenvolvimento da solução, a equipe deve aplicar corretamente conceitos de autenticação multifator, classificação de fatores de autenticação (conhecimento, posse e inerência) e uso de *tokens* em protocolos modernos, bem como deve observar as boas práticas de controle de acesso em sistemas de gestão da segurança da informação.

A respeito da aplicação de métodos de autenticação e uso de *tokens* na arquitetura descrita na situação hipotética precedente, assinale a opção correta.

- Ⓐ A biometria facial impede o uso de 2FA, pois esse fator (inerência) não pode ser combinado com PIN ou senha em uma mesma arquitetura, por restrições técnicas.
- Ⓑ A autenticação dos servidores é de fator único, pois senha e OTP pertencem à mesma categoria (conhecimento), enquanto a biometria dos cidadãos constitui fator independente.
- Ⓒ O uso de senha com OTP para servidores, bem como a biometria com PIN para cidadãos, caracteriza 2FA (conhecimento e posse), enquanto os JWT são *tokens* pós-autenticação.
- Ⓓ Os JWT assinados substituem integralmente os fatores de autenticação, de modo que senha, biometria e PIN passam a ser mecanismos de conveniência para o usuário.
- Ⓔ A biometria com PIN dos cidadãos fornece dois fatores (inerência e conhecimento), mas o uso de JWT assinados elimina a necessidade de 2FA para servidores internos.

Questão 90

Durante análise de uma aplicação *web* utilizada por certa secretaria estadual de meio ambiente para gerenciamento de autos de infração, a equipe de segurança identificou que campos de formulário não tinham validação adequada no servidor. Foi possível enviar dados contendo comandos de banco de dados por meio de um campo de pesquisa, o que resultou em alteração indevida de registros. Em outro teste, verificou-se que o aplicativo refletia, na resposta HTML, trechos de entrada do usuário sem filtragem, permitindo a inserção de *scripts* que eram executados no navegador de quem acessava a página. Esses dois achados foram registrados no processo de gestão de vulnerabilidades previsto no SGSI da organização, em conformidade com a NBR ISO/IEC 27001:2013.

Considerando ameaças e vulnerabilidades em aplicações *web*, assinale a opção correta a respeito da classificação das duas falhas descritas na situação hipotética apresentada.

- Ⓐ A primeira falha é um *cross-site request forgery*, e a segunda, um armazenamento inseguro de dados.
- Ⓑ A primeira falha é uma quebra de autenticação, e a segunda, um *injection* em diretório LDAP.
- Ⓒ A primeira falha é um armazenamento inseguro de dados, e a segunda, um *cross-site request forgery*.
- Ⓓ A primeira falha é um *cross-site scripting*, e a segunda, uma referência insegura a objetos.
- Ⓔ A primeira falha é um *SQL injection*, e a segunda, um *cross-site scripting*.

Questão 91

Considerando que, na infraestrutura de chaves públicas brasileira, o certificado digital funciona como uma identidade virtual, assinale a opção em que é apresentada a tecnologia que permite vincular uma chave pública a uma pessoa, assegurando que uma mensagem eletrônica provém de um remetente específico e que o seu conteúdo permanece íntegro desde a sua emissão.

- Ⓐ herança de permissões
- Ⓑ barramento de serviços
- Ⓒ tunelamento de dados
- Ⓓ espelhamento de disco
- Ⓔ assinatura digital

Questão 92

Um analista de segurança da informação de certa organização identificou um ataque em que um indivíduo enviou mensagens eletrônicas em massa para colaboradores da organização. Tais mensagens direcionavam os colaboradores a um sítio eletrônico fraudulento que simulava o portal corporativo, com o intuito de capturar suas credenciais de acesso.

A técnica maliciosa descrita na situação hipotética precedente é classificada, quanto ao seu tipo, como

- Ⓐ *brute force*.
- Ⓑ *eavesdropping*.
- Ⓒ *phishing*.
- Ⓓ *port scanning*.
- Ⓔ *DNS spoofing*.

Questão 93

Um servidor *web* de uma instituição pública recebeu um fluxo massivo e coordenado de dados, proveniente de milhares de computadores infectados geograficamente distribuídos, o que resultou na indisponibilidade total do serviço.

A modalidade de ataque descrita na situação hipotética apresentada é denominada

- Ⓐ *brute force*.
- Ⓑ *port scanning*.
- Ⓒ DDoS.
- Ⓓ *phishing*.
- Ⓔ *eavesdropping*.

Questão 94

Na criptografia de chave pública, as entidades utilizam pares de chaves matematicamente relacionados. Para que um remetente consiga enviar uma mensagem cifrada garantindo que apenas o destinatário pretendido possa realizar a leitura do conteúdo original, o remetente deve realizar a cifragem utilizando a chave

- Ⓐ pública do destinatário.
- Ⓑ privada do destinatário.
- Ⓒ pública do remetente.
- Ⓓ privada do remetente.
- Ⓔ simétrica de sessão.

Questão 95

O protocolo TLS (*transport layer security*) é fundamental para a segurança das comunicações na camada de transporte. Durante o estabelecimento de uma conexão segura entre cliente e servidor, o protocolo TLS utiliza

- I algoritmos assimétricos para a autenticação inicial das partes e troca segura de chaves.
- II algoritmos simétricos para a cifragem do tráfego de dados após o estabelecimento da sessão.
- III funções de *hash* para assegurar a integridade das mensagens trocadas durante a comunicação.

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 96

De acordo com o que dispõe a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), dados pessoais relativos a convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter político, bem como dados referentes à saúde ou à vida sexual da pessoa natural, são denominados

- A dados de relatório de impacto.
- B dados pessoais sensíveis.
- C dados de banco de dados.
- D dados de uso compartilhado.
- E dados anonimizados.

Questão 97

Conforme a LGPD, é direito do titular de dados pessoais obter do controlador, a qualquer momento e mediante requisição, a correção de dados que

- A estejam bloqueados.
- B estejam incompletos, desatualizados ou inexatos.
- C tenham sido compartilhados com entes privados.
- D tenham sido anonimizados.
- E tenham sido eliminados.

Questão 98

Com base na norma ABNT NBR ISO/IEC 27005, assinale a opção na qual é corretamente apresentada a atividade de gestão de segurança da informação em que, a partir de uma lista de riscos com níveis de valores designados, o nível dos riscos é comparado com os critérios de avaliação e de aceitação do risco.

- A monitoramento de riscos
- B identificação de riscos
- C avaliação de riscos
- D tratamento de riscos
- E estimativa de riscos

Questão 99

A metodologia OWASP categoriza as falhas mais críticas em aplicações *web*. Quando uma aplicação permite que um usuário autenticado altere o identificador de um objeto em uma URL para acessar dados de outro usuário sem que haja uma verificação de autorização adequada, ocorre uma vulnerabilidade denominada

- A *insecure design*.
- B *injection*.
- C *cryptographic failure*.
- D *broken access control*.
- E *security misconfiguration*.

Questão 100

Na análise de vulnerabilidades de *software*, as técnicas de análise estática de segurança de aplicações (SAST)

- A realizam testes de invasão com a aplicação em pleno funcionamento no ambiente de produção.
- B avaliam a segurança física do local onde os servidores da aplicação estão hospedados.
- C interceptam requisições HTTP entre o navegador e o servidor para manipular parâmetros de entrada.
- D simulam ataques de negação de serviço para verificar a resiliência da infraestrutura de rede.
- E examinam o código-fonte ou binário da aplicação sem que haja a execução do *software*.

Espaço livre