

-- CONHECIMENTOS ESPECÍFICOS --**REDES DE COMPUTADORES****Questão 31**

Em relação aos tipos de enlace, um enlace *full-duplex* é aquele que permite

- A** transmissão de sinais digitais somente por fibra óptica.
- B** transmissão nos dois sentidos, mas não simultaneamente.
- C** transmissão simultânea nos dois sentidos.
- D** transmissão em apenas um sentido.
- E** transmissão somente de sinais analógicos.

Questão 32

As redes locais, ou LANs (*local area networks*),

- A** são sempre públicas.
- B** abrangem grandes áreas geográficas.
- C** conectam apenas dispositivos móveis.
- D** operam dentro ou nas proximidades de um único prédio.
- E** funcionam somente em redes corporativas.

Questão 33

O método CSMA no padrão 802.11

- A** aumenta o alcance do sinal.
- B** elimina completamente as colisões.
- C** garante criptografia forte dos dados.
- D** reduz a probabilidade de transmissões simultâneas.
- E** substitui o uso de pontos de acesso.

Questão 34

A utilização da técnica OFDM nos padrões 802.11a e 802.11g contribui para o aumento da taxa de transmissão, porque tal técnica

- A** funciona somente em ambientes sem obstáculos físicos.
- B** divide o canal em múltiplas subportadoras ortogonais transmitidas em paralelo.
- C** reduz a necessidade de codificação de erros.
- D** utiliza apenas uma portadora de alta potência.
- E** elimina completamente o ruído do meio.

Questão 35

Julgue os itens a seguir, em relação às características e ao funcionamento de um *switch*.

- I O *switch* utiliza *buffers* para lidar com situações em que vários quadros precisam sair pela mesma porta ao mesmo tempo.
- II Um *switch* funciona da mesma maneira que um *hub*, replicando todos os quadros recebidos para todas as suas portas, mantendo um único domínio de colisão e exigindo o uso obrigatório do protocolo CSMA/CD em todas as conexões.
- III O *switch* encaminha os quadros apenas para a porta correspondente ao endereço de destino, criando domínios de colisão independentes por porta.

Assinale a opção correta.

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

Questão 36

Acerca de repetidores, *hubs* e roteadores, julgue os itens subsequentes.

- I Os repetidores e os *hubs* operam na camada física.
- II Os repetidores limpam, amplificam e retransmitem sinais, sem reconhecimento de pacotes.
- III Os roteadores operam na camada de rede, interligando redes de diferentes tipos.
- IV O roteador decide a melhor linha de saída com base em informações do cabeçalho do pacote, sem considerar o tipo de rede de origem.

Assinale a opção correta.

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

Questão 37

Julgue os itens seguintes, referentes a noções do modelo de referência OSI.

- I O objetivo principal desse modelo era permitir a interconexão de sistemas abertos.
- II Na concepção do modelo, as funções mais relevantes foram designadas para as camadas de sessão e apresentação, enquanto as camadas de rede e de enlace de dados ficaram desoneradas.
- III O modelo OSI foi associado a iniciativas governamentais e burocráticas, o que reforçou a ideia de que ele era um padrão imposto e complexo.

Assinale a opção correta.

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

Questão 38

Considerando os princípios de projeto do modelo OSI, seus conceitos fundamentais e as críticas históricas à sua adoção, assinale a opção correta.

- A** As camadas de sessão e apresentação do modelo OSI concentraram a maior parte das funcionalidades essenciais de controle de erros e endereçamento, o que tornou o modelo mais eficiente que o TCP/IP.
- B** A principal vantagem do modelo OSI em relação ao TCP/IP foi a simplicidade de suas sete camadas, que evitaram redundâncias funcionais e facilitaram implementações, desde as suas primeiras versões.
- C** O modelo OSI apresentou problemas de aceitação devido a fatores técnicos, históricos e políticos, como desenvolvimento em um momento inadequado, excesso de complexidade e falhas de implementação inicial.
- D** O modelo OSI fracassou principalmente porque foi desenvolvido antes de qualquer pesquisa acadêmica relevante.
- E** O insucesso do modelo OSI deveu-se à superioridade técnica do TCP/IP, uma vez que ambos foram desenvolvidos no mesmo período e possuíam níveis equivalentes de aceitação inicial no meio acadêmico.

Questão 39

O padrão IEEE 802.3 (LAN)

- Ⓐ utiliza o método de acesso CSMA/CD em redes modernas com *switch*.
- Ⓑ suporta velocidade de até 600 Mbps.
- Ⓒ funciona em frequência de 2,4 GHz e de 5 GHz.
- Ⓓ opera na velocidade de até 1 Gbps no padrão 802.3ab.
- Ⓔ controla e organiza a rede, tornando-a mais segura.

Questão 40

O padrão IEEE 802.11 (*wi-fi*) utiliza bandas de frequência não licenciadas e técnicas específicas para lidar com as limitações do meio sem fio. O motivo para o uso de técnicas de diversidade de caminhos nas redes 802.11 é

- Ⓐ reduzir o consumo de energia dos pontos de acesso e dos clientes.
- Ⓑ evitar completamente colisões de pacotes no meio sem fio.
- Ⓒ eliminar a necessidade de protocolos de controle de acesso ao meio (CSMA).
- Ⓓ contornar os efeitos do enfraquecimento por múltiplos caminhos (*multipath fading*).
- Ⓔ aumentar a potência de transmissão dos dispositivos para superar interferências.

Questão 41

No que diz respeito às características dos protocolos IPv6 e IPsec, assinale a opção correta.

- Ⓐ O IPv6 deixou de usar o protocolo ICMP, tendo-o substituído pelo IPsec.
- Ⓑ O IPv6 não realiza o processo de fragmentação de pacotes na rede, sendo essa uma responsabilidade do *host* de origem.
- Ⓒ O IPsec opera apenas com IPv4, pois o IPv6 possui mecanismos próprios de segurança.
- Ⓓ O IPsec fornece confidencialidade, integridade e autenticação na camada de aplicação.
- Ⓔ O IPv6 utiliza endereços de 64 *bits*, o que permite maior eficiência no roteamento hierárquico.

Questão 42

Acerca do roteamento IP na Internet, assinale a opção correta.

- Ⓐ O encaminhamento de pacotes em redes TCP/IP utiliza agregação de prefixos para maior escalabilidade.
- Ⓑ O roteamento IP depende de conexões previamente estabelecidas.
- Ⓒ As redes TCP/IP utilizam transmissões por difusão para comunicação entre grupos de dispositivos.
- Ⓓ O roteamento IP garante entrega confiável de pacotes.
- Ⓔ O protocolo IP mantém estado das rotas por fluxo.

Questão 43

É correto afirmar que o protocolo TCP

- Ⓐ estabelece túneis criptografados entre nós da rede.
- Ⓑ envia pacotes na rede a uma taxa de transmissão constante.
- Ⓒ ajusta sua taxa de transmissão com base em perdas e atrasos de pacotes percebidos na rede.
- Ⓓ encaminha pacotes entre redes distintas.
- Ⓔ elimina ocorrência de *jitter* em redes TCP/IP.

Questão 44

Em redes TCP/IP, o protocolo UDP

- Ⓐ elimina a perda de pacotes na rede local.
- Ⓑ oferece menor latência que o TCP por não utilizar determinados mecanismos de controle.
- Ⓒ garante entrega ordenada de pacotes transmitidos.
- Ⓓ implementa controle de congestionamento.
- Ⓔ realiza *handshake* para o início da transmissão.

Questão 45

A aplicação DNS

- Ⓐ opera exclusivamente sobre o protocolo TCP.
- Ⓑ garante consistência por não fazer uso de *cache*.
- Ⓒ traduz nomes simbólicos em endereços IP.
- Ⓓ centraliza todas as consultas em um único servidor.
- Ⓔ substitui o protocolo IP em aplicações *web*.

Questão 46

A respeito dos protocolos HTTP e HTTPS, assinale a opção correta.

- Ⓐ O HTTPS dispensa certificados digitais para seu funcionamento.
- Ⓑ Ambos operam na camada de transporte.
- Ⓒ O HTTP garante a confidencialidade dos dados.
- Ⓓ O HTTPS adiciona criptografia por meio do SSL/TLS.
- Ⓔ Ambos não necessitam do TCP.

Questão 47

É correto afirmar que, em relação ao estabelecimento de conexões e ao controle da transferência de dados, o FTP

- Ⓐ encapsula seus dados diretamente em pacotes IP, dispensando o uso da camada de transporte.
- Ⓑ utiliza UDP para transferência de dados, a fim de reduzir latência.
- Ⓒ implementa o comando RETR para armazenar um arquivo no servidor remoto.
- Ⓓ estabelece uma conexão persistente única, multiplexando comandos de controle e dados no mesmo fluxo TCP.
- Ⓔ utiliza uma conexão de controle que permanece aberta durante a sessão do usuário e cria uma nova conexão de dados para cada arquivo transferido dentro de uma sessão.

Questão 48

No que se refere ao SNMP, assinale a opção correta.

- Ⓐ O protocolo de transporte das mensagens SNMP é o ICMP, sendo utilizadas as portas 161 e 162.
- Ⓑ O SNMP utiliza a linguagem de definição de dados conhecida como MIB.
- Ⓒ O envio, por parte de um agente, de uma mensagem não solicitada à entidade gerenciadora caracteriza o modo comando-resposta.
- Ⓓ A versão SNMPv2 introduziu itens de segurança como criptografia, autenticação e controle de acesso.
- Ⓔ SNMPv3 é a versão mais recente do SNMP, lançada em 1999 e atualizada em 2002.

Questão 49

É correto afirmar que o protocolo RMON

- Ⓐ permite coleta e análise de dados de tráfego de forma remota.
- Ⓑ realiza roteamento dinâmico entre redes.
- Ⓒ substitui o protocolo SNMP.
- Ⓓ define um tipo de dado utilizado pela linguagem SMI.
- Ⓔ opera somente na camada física do modelo OSI.

Questão 50

A respeito das aplicações VoIP, assinale a opção correta.

- Ⓐ O *jitter* é um componente da rede que garante a qualidade das aplicações VoIP.
- Ⓑ Uma comunicação VoIP pode incluir a transmissão de vídeo entre dois dispositivos.
- Ⓒ O protocolo TCP é mais adequado que o UDP em aplicações VoIP.
- Ⓓ O modelo de serviço de melhor esforço do protocolo IP é pouco adequado para aplicações VoIP.
- Ⓔ O encaminhamento não seletivo de pacotes do protocolo IP beneficia as aplicações VoIP.

Questão 51

A transmissão de voz sobre redes IP impõe restrições temporais rigorosas, exigindo mecanismos específicos para lidar com atraso, variação de atraso e perda de pacotes. Para lidar com essas restrições, os sistemas VoIP

- Ⓐ dependem exclusivamente do TCP para garantir ordenação e confiabilidade dos pacotes de áudio.
- Ⓑ eliminam a necessidade de controle do atraso ao operar em redes de alta largura de banda.
- Ⓒ transferem integralmente o controle de qualidade para a camada de aplicação, dispensando mecanismos na rede.
- Ⓓ priorizam retransmissões confiáveis de pacotes perdidos para preservar a integridade da voz.
- Ⓔ utilizam *buffers* de reprodução adaptativos para compensar variações de atraso, aceitando aumento controlado do atraso fim a fim.

Questão 52

É correto afirmar que o protocolo SIP

- Ⓐ é um protocolo monolítico que integra sinalização, transporte e codificação de mídia.
- Ⓑ opera exclusivamente sobre UDP para reduzir a latência associada à sinalização.
- Ⓒ incorpora funcionalidades completas de reserva de recursos de rede, dispensando mecanismos externos de QoS.
- Ⓓ é um protocolo de sinalização que estabelece, modifica e encerra sessões multimídia, enquanto o transporte da mídia é realizado por outros protocolos.
- Ⓔ define mecanismos próprios de transporte de mídia, incluindo controle de atraso e correção de perdas de pacotes.

Questão 53

É correto afirmar que o protocolo H.323

- Ⓐ tem foco exclusivo em redes IP sem garantia de qualidade de serviço.
- Ⓑ é um padrão típico da indústria de telefonia com pilha completa de protocolos responsáveis por diferentes funções de controle e mídia.
- Ⓒ adota uma abordagem minimalista, evitando a definição de entidades intermediárias de controle.
- Ⓓ é um protocolo leve de sinalização, inspirado diretamente no modelo do HTTP.
- Ⓔ delega a sinalização e o controle de chamadas a protocolos externos independentes.

Questão 54

É correto afirmar que os mecanismos de qualidade de serviço (QoS) em redes TCP/IP

- Ⓐ são destinados especialmente a aplicações orientadas à transferência de arquivos.
- Ⓑ garantem confiabilidade de entrega por meio de retransmissões automáticas na rede.
- Ⓒ eliminam a necessidade de adaptação das aplicações multimídia às condições da rede.
- Ⓓ buscam fornecer limites previsíveis de atraso, variação de atraso e perda de pacotes para aplicações sensíveis ao tempo.
- Ⓔ substituem as técnicas de compressão e codificação de mídia.

Questão 55

É correto afirmar que os sistemas de videoconferência

- Ⓐ apresentam requisitos idênticos aos de aplicações de transferência de arquivos.
- Ⓑ operam tipicamente sobre protocolos orientados à conexão confiável.
- Ⓒ dispensam métodos de adaptação dinâmica da taxa de transmissão.
- Ⓓ priorizam a entrega confiável de dados, em detrimento do atraso.
- Ⓔ exigem limites rígidos de atraso e utilizam mecanismos para lidar com *jitter* e perda de pacotes.

SEGURANÇA DA INFORMAÇÃO**Questão 56**

Suponha que, em um centro de operações de segurança, tenham sido implantadas soluções para detectar tentativas de intrusão, bloquear ataques automaticamente e correlacionar eventos de múltiplas fontes. Considerando esse caso hipotético, assinale a opção em que estão corretamente descritas as associações entre as tecnologias necessárias para a implantação das soluções em apreço e suas funções.

- Ⓐ Antivírus centraliza *logs*, IDS protege túneis e IPS valida certificados.
- Ⓑ IDS detecta intrusões, IPS atua na prevenção e SIEM realiza correlação de eventos.
- Ⓒ IPS correlaciona eventos, SIEM bloqueia tráfego e IDS autentica usuários.
- Ⓓ VPN detecta ataques, *firewall* correlaciona eventos e SIEM previne intrusões.
- Ⓔ *Firewall* detecta intrusões, IDS bloqueia ataques e SIEM cifra *logs*.

Questão 57

Em uma rede corporativa, a equipe de TI implementou antivírus nas estações de trabalho, filtros de *email* no *gateway* corporativo e mecanismos de inspeção de tráfego na rede interna, com o objetivo de reduzir o impacto de códigos maliciosos.

A estratégia adotada pela equipe de TI na situação hipotética precedente está fundamentada no conceito de

- Ⓐ segregação lógica de redes, que visa ao isolamento completo de serviços.
- Ⓑ defesa em profundidade, que consiste no uso de múltiplos mecanismos de segurança em diferentes camadas.
- Ⓒ autenticação forte, que funciona com base em múltiplos fatores de identificação do usuário.
- Ⓓ criptografia fim a fim, que assegura a confidencialidade dos dados trafegados.
- Ⓔ controle de acesso obrigatório, que é baseado em políticas centralizadas de autorização.

Questão 58

Considere que, para a transmissão de grandes volumes de dados sensíveis entre servidores de um tribunal, tenha-se optado por utilizar um algoritmo criptográfico que oferecesse alta eficiência computacional e baixo custo de processamento. Nessa situação, o tipo de criptografia mais adequado para atender à finalidade pretendida é a

- Ⓐ esteganografia, que oculta a existência da informação.
- Ⓑ assinatura digital, que protege o conteúdo contra acesso indevido.
- Ⓒ função de *hash* criptográfica, que assegura confidencialidade dos dados.
- Ⓓ criptografia simétrica, em razão do uso de uma única chave compartilhada.
- Ⓔ criptografia assimétrica, devido à inexistência de chaves secretas.

Questão 59

Considere um sistema de troca segura de informações em que um usuário utiliza a chave pública do destinatário para cifrar uma mensagem enviada pela rede. Nesse modelo de criptografia,

- Ⓐ a confidencialidade é garantida porque apenas o destinatário possui a chave privada correspondente.
- Ⓑ o mesmo par de chaves é utilizado para cifrar grandes volumes de dados.
- Ⓒ a necessidade de algoritmos simétricos é eliminada.
- Ⓓ a chave pública deve ser mantida em sigilo absoluto.
- Ⓔ a integridade da mensagem é assegurada automaticamente pela criptografia.

Questão 60

Se um documento eletrônico for assinado digitalmente e validado por meio de um certificado emitido por uma autoridade certificadora confiável, esse procedimento assegurará que o documento

- Ⓐ impeça qualquer forma de acesso não autorizado ao sistema.
- Ⓑ esteja protegido contra a hipótese de indisponibilidade do sistema.
- Ⓒ utilize exclusivamente criptografia simétrica.
- Ⓓ permaneça confidencial durante todo o seu ciclo de vida.
- Ⓔ mantenha os atributos de integridade, autenticidade do autor e não repúdio.

Questão 61

Uma autarquia federal decidiu alinhar suas práticas de segurança da informação às normas internacionais, adotando controles técnicos e administrativos descritos em uma norma de referência, sem, contudo, instituir formalmente um sistema de gestão da segurança da informação (SGSI).

Com base na situação hipotética precedente e nas normas NBR ISO/IEC 27001 e 27002, é correto afirmar que a decisão da autarquia caracteriza

- Ⓐ implementação exclusiva de requisitos legais, sem relação com boas práticas internacionais.
- Ⓑ implementação parcial da ISO 27001, com possibilidade imediata de certificação.
- Ⓒ adoção de um *framework* de controles, conforme a ISO 27002, sem gestão sistêmica.
- Ⓓ inconformidade com ambas as normas, por ausência de auditoria externa.
- Ⓔ atendimento integral às exigências de governança da segurança da informação de ambas as normas.

Questão 62

No âmbito de um processo de auditoria de sistemas e *compliance* digital, verificou-se que uma organização implementou, com sucesso, controles de criptografia assimétrica, mecanismos de MFA (*multi-factor authentication*) e processos de CSIRT (*computer security incident response team*). Contudo, a análise do fluxo de dados revelou que o *dataset* processado para fins de *marketing* direto incluía metadados de geolocalização e histórico de saúde dos titulares, sem que tais dados fossem essenciais para a execução do serviço proposto.

À luz da literatura especializada de Sêmola e da Lei Geral de Proteção de Dados (LGPD), é correto concluir que, na situação hipotética precedente, a dicotomia entre a eficácia dos controles e a governança dos dados revela que

- Ⓐ o cenário caracteriza um incidente de segurança positivo, em que a abundância de dados coletados visa à resiliência do negócio.
- Ⓑ a organização atingiu a segurança formal, mas incorre em desvio de finalidade por inobservância ao princípio da necessidade.
- Ⓒ a implementação de criptografia e gestão de incidentes invalida a hipótese de violação à privacidade, pois os dados estão protegidos contra terceiros.
- Ⓓ a organização apresenta um alto nível de maturidade em segurança, o que supre as lacunas éticas do tratamento de dados.
- Ⓔ existe uma falha na integridade (pilar da segurança), uma vez que o dado está sendo tratado para propósito diverso da sua finalidade original.

Questão 63

Considere que, em determinado órgão público, tenha-se identificado que os servidores utilizavam senhas fracas, sem que houvesse registro de acesso indevido ou dano às informações. Essa situação, segundo os conceitos de segurança da informação, caracteriza

- Ⓐ um risco inexistente, por ausência de dano.
- Ⓑ um incidente de segurança da informação.
- Ⓒ um impacto operacional já materializado.
- Ⓓ uma ameaça externa concretizada.
- Ⓔ uma vulnerabilidade ainda não explorada.

Questão 64

Determinada organização tem documentação completa de políticas de segurança, alinhadas às normas ISO e à LGPD, mas não realiza treinamento, monitoramento contínuo nem testes de controles.

Essa situação hipotética, segundo a abordagem de Sêmola, evidencia

- Ⓐ eliminação das vulnerabilidades humanas.
- Ⓑ nível elevado de maturidade em segurança da informação.
- Ⓒ abordagem de segurança da informação baseada apenas em conformidade formal.
- Ⓓ atendimento pleno ao princípio da *accountability* da LGPD.
- Ⓔ redução automática do risco organizacional.

Questão 65

Se, ao estruturar seu programa de segurança da informação, uma empresa decidir integrar gestão de riscos, controles técnicos, políticas internas e requisitos da LGPD, essa decisão reforçará a

- Ⓐ eliminação da dependência de pessoas nos processos de segurança.
- Ⓑ abordagem da segurança como processo contínuo, multidisciplinar e alinhado ao negócio.
- Ⓒ substituição da governança corporativa por normas técnicas.
- Ⓓ centralização da segurança exclusivamente na área de TI.
- Ⓔ abordagem da segurança como ciência exata e previsível.

Questão 66

Uma organização pública enfrenta recorrentes eventos de indisponibilidade em um sistema crítico de atendimento ao cidadão. As falhas são restauradas rapidamente pela equipe técnica, porém voltam a ocorrer em momentos distintos.

Nessa situação hipotética, conforme as boas práticas de gestão de infraestrutura de TI, segundo o ITIL v3 e o COBIT, a ação correta a ser adotada para sanar o problema consiste em

- Ⓐ migrar o sistema para ambiente terceirizado, transferindo a responsabilidade operacional por meio de contrato de suporte especializado.
- Ⓑ ampliar a capacidade de processamento e armazenamento da infraestrutura, tratando a indisponibilidade como limitação de recursos físicos.
- Ⓒ intensificar o gerenciamento de incidentes, com foco exclusivo na redução do tempo médio de restauração do serviço.
- Ⓓ renegociar os acordos de nível de serviço, adequando os níveis de disponibilidade às condições atuais da infraestrutura.
- Ⓔ implementar o gerenciamento de problemas, com análise de causa-raiz, manutenção de base de erros conhecidos e uso de registros históricos de incidentes.

Questão 67

Durante a implantação de um novo sistema corporativo, a área de TI de uma organização pretende estabelecer um mecanismo formal para avaliar, decidir e autorizar solicitações de alteração no ambiente produtivo, com vistas à redução de riscos à estabilidade dos serviços em produção.

Nessa situação hipotética, segundo as boas práticas do ITIL v3, o único processo que atende integralmente ao objetivo da área de TI é o gerenciamento de

- Ⓐ capacidade.
- Ⓑ mudanças.
- Ⓒ incidentes.
- Ⓓ liberação e implantação.
- Ⓔ configuração e ativos de serviço.

Questão 68

Uma organização pública visa fortalecer sua governança de TI, assegurando alinhamento entre TI e objetivos institucionais, tratamento adequado dos riscos e mecanismos claros de acompanhamento do desempenho da área de TI.

Nessa situação, o único domínio do COBIT que atende aos propósitos da organização é o que compreende as ações de

- Ⓐ planejar, avaliar, implementar.
- Ⓑ avaliar, dirigir e monitorar.
- Ⓒ entregar, servir e suportar.
- Ⓓ construir, adquirir e implementar.
- Ⓔ monitorar, avaliar e analisar.

Questão 69

As iniciativas de TI de uma organização são executadas de forma tecnicamente adequada, porém sem priorização clara, com decisões pouco alinhadas às metas institucionais e sem critérios consistentes para balancear valor, risco e recursos.

Com base nessa situação hipotética, assinale a opção em que é corretamente apresentado, conforme as boas práticas do COBIT, o conjunto de objetivos de gestão que trata diretamente do planejamento estratégico da TI, em conformidade com as diretrizes definidas pela governança, para fortalecer o papel da TI no apoio à estratégia organizacional.

- Ⓐ monitorar, corrigir e validar
- Ⓑ avaliar, corrigir e implementar
- Ⓒ analisar, adquirir e entregar
- Ⓓ alinhar, planejar e organizar
- Ⓔ planejar, validar e apoiar

Questão 70

Durante a operação de um serviço crítico, a equipe de TI de uma organização passou a receber alertas automáticos que indicavam variações fora do padrão em componentes da infraestrutura, sem que tenha ocorrido, contudo, interrupção ou degradação do serviço.

Com base nessa situação hipotética e no ITIL v3, é correto afirmar que o processo responsável por registrar, classificar e acompanhar o tipo de ocorrência mencionado é o gerenciamento

- Ⓐ de eventos.
- Ⓑ de suporte.
- Ⓒ técnico.
- Ⓓ de atualizações.
- Ⓔ de problemas.

Questão 71

Supondo que uma organização identifique acesso não autorizado a informações sensíveis, com indícios de comprometimento de credenciais e possível exfiltração de dados, assinale a opção em que é corretamente apresentado, de acordo com as boas práticas internacionais de gestão de segurança da informação estabelecidas na NBR ISO/IEC 27001:2022, o controle organizacional de segurança da informação a ser aplicado para estabelecer e implementar procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas ao referido evento.

- Ⓐ coleta de evidências
- Ⓑ planejamento e preparação da gestão de incidentes da segurança da informação
- Ⓒ resposta a incidentes da segurança da informação
- Ⓓ segurança da informação durante a interrupção
- Ⓔ avaliação e decisão sobre eventos da segurança da informação

Questão 72

No âmbito da gestão de incidentes de segurança da informação, o conhecimento adquirido pela organização com incidentes de segurança da informação, segundo a norma NBR ISO/IEC 27001:2022, deve ser usado para

- Ⓐ fortalecer e melhorar os controles da segurança da informação.
- Ⓑ orientar o processo de sucessão das chefias na área de segurança da informação.
- Ⓒ responsabilizar o pessoal interno envolvido nos incidentes.
- Ⓓ estabelecer critérios para o aprimoramento dos processos de seleção de recursos humanos.
- Ⓔ definir os novos tipos de ferramentas e sistemas de segurança a serem adquiridos.

Questão 73

De acordo com a NBR ISO/IEC 27002:2022, os prazos de tratamento e resolução de incidentes devem ser estabelecidos pela organização conforme níveis de prioridade definidos no plano de gestão de incidentes, com base

- Ⓐ na disponibilidade da equipe técnica responsável.
- Ⓑ na ordem cronológica de registro dos incidentes.
- Ⓒ na severidade e nas consequências potenciais do incidente.
- Ⓓ no relato do colaborador que reportou o incidente.
- Ⓔ na complexidade técnica do incidente.

Questão 74

Conforme a NBR ISO/IEC 27002:2022, no contexto da definição de papéis e responsabilidades na gestão de incidentes de segurança da informação, convém que a organização estabeleça um processo para identificar

- Ⓐ as obrigações legais e regulatórias relacionadas a incidentes aplicáveis ao pessoal de resposta a incidentes.
- Ⓑ os indicadores de desempenho requeridos para a equipe de resposta a incidentes.
- Ⓒ o treinamento, a certificação e o desenvolvimento profissional continuado requeridos para o pessoal de resposta a incidentes.
- Ⓓ os níveis de autoridade e as competências decisórias requeridos para o pessoal de resposta a incidentes.
- Ⓔ os procedimentos operacionais e os fluxos de comunicação internos requeridos para o pessoal de resposta a incidentes.

Questão 75

De acordo com a NBR ISO/IEC 27002:2022, no âmbito da gestão de incidentes de segurança da informação, a coordenação da resposta e o compartilhamento de informações com organizações externas são particularmente apropriados no contexto de ocorrência de incidentes

- Ⓐ decorrentes de vulnerabilidades técnicas identificadas internamente.
- Ⓑ cuja análise possa ser conduzida integralmente pela equipe interna.
- Ⓒ restritos a ativos isolados sem impacto sobre terceiros.
- Ⓓ classificados como de baixa severidade operacional.
- Ⓔ que transcendam fronteiras organizacionais e nacionais.

Questão 76

De acordo com os controles estabelecidos na NBR ISO/IEC 27001:2022, a prontidão de TIC deve ser planejada, implementada, mantida e testada com base

- Ⓐ nos requisitos de conformidade regulatória aplicáveis aos serviços de TIC.
- Ⓑ nos requisitos de segurança da informação definidos na análise de riscos.
- Ⓒ nas políticas internas de tecnologia e nos níveis de serviço acordados com fornecedores.
- Ⓓ nos objetivos de continuidade do negócio e nos requisitos de continuidade da TIC.
- Ⓔ nos objetivos estratégicos corporativos e nas metas financeiras da organização.

Questão 77

A NBR ISO/IEC 27002:2022 recomenda que a organização determine requisitos para adaptar os controles de segurança da informação a serem aplicados durante uma interrupção. De acordo com a referida norma, convém que esses requisitos sejam incluídos

- Ⓐ nas decisões operacionais tomadas pela alta direção da organização durante a crise.
- Ⓑ nas políticas internas de tecnologia da informação aplicáveis aos serviços críticos.
- Ⓒ nos requisitos regulatórios aplicáveis ao setor de atuação da organização.
- Ⓓ nos resultados atualizados da análise de riscos de segurança da informação.
- Ⓔ nos processos de gestão de continuidade de negócios.

Questão 78

Conforme disposto na NBR ISO/IEC 27002:2022, entre as informações de continuidade de TIC dos planos de continuidade de TIC incluem-se

- Ⓐ os critérios de classificação da informação e níveis de confidencialidade atribuídos aos ativos essenciais da organização.
- Ⓑ as especificações de desempenho e capacidade para atender aos requisitos e objetivos de continuidade de negócios especificados na análise de impacto nos negócios.
- Ⓒ os requisitos regulatórios setoriais aplicáveis à proteção de dados e à segurança cibernética dos sistemas de informação corporativos.
- Ⓓ os resultados consolidados da análise de riscos de segurança da informação aplicáveis aos serviços críticos de TIC identificados pela organização.
- Ⓔ os indicadores financeiros e as projeções orçamentárias destinados à manutenção da infraestrutura tecnológica durante períodos de interrupção operacional.

Questão 79

De acordo com a NBR ISO/IEC 27002:2022, o gerenciamento da continuidade de TIC, parte fundamental dos requisitos de continuidade de negócios em relação à disponibilidade, deve ser capaz de

- Ⓐ reduzir o impacto financeiro decorrente de falhas operacionais nos serviços de TIC.
- Ⓑ garantir a confidencialidade das informações críticas em condições normais de operação.
- Ⓒ manter a conformidade dos controles internos com as políticas corporativas de governança tecnológica.
- Ⓓ assegurar que a continuidade das atividades priorizadas seja apoiada pelos serviços de TIC necessários.
- Ⓔ assegurar o cumprimento integral de requisitos regulatórios setoriais relacionados à segurança cibernética.

Questão 80

De acordo com a NBR ISO/IEC 27002:2022, convém que as medidas de *backup* e restauração de dados para sistemas e serviços individuais sejam

- Ⓐ realizadas em ambientes de produção de modo a preservar a consistência operacional dos sistemas.
- Ⓑ armazenadas em mídias físicas mantidas nas dependências da organização.
- Ⓒ executadas após a ocorrência de incidentes que resultem em perda ou corrupção de dados.
- Ⓓ configuradas de maneira uniforme entre os diferentes sistemas e serviços da organização.
- Ⓔ testadas regularmente para assegurar que atendam aos objetivos do plano de continuidade de negócios da organização.