-- CONHECIMENTOS ESPECÍFICOS --

SEGURANÇA DA INFORMAÇÃO

Questão 31

A classificação de informações fornece às pessoas que lidam com a informação organizacional

- A uma indicação concisa de como manusear e proteger a informação organizacional.
- B um arcabouço jurídico completo para lidar com incidentes de segurança da informação.
- C uma relação de pessoas da organização capazes de prover as informações necessárias aos processos.
- D uma estrutura organizacional apropriada para lidar com a tecnologia e a segurança da informação.
- E um método de classes sobre como decriptar informações sensíveis da organização previamente criptografadas.

Questão 32

De acordo com normatização internacional de referência, o controle de entrada física de pessoas em instalações da organização nas quais sejam manuseadas e processadas informações organizacionais tem como principal propósito

- A elaborar medidas de segurança física que possam ser reforçadas quando a probabilidade de incidentes físicos aumentar.
- B implantar uma área de recepção monitorada pelo pessoal ou outros meios para controlar o acesso físico ao local ou edifício.
- C inspecionar e examinar pertences pessoais do pessoal e partes interessadas em momentos de entrada e saída.
- D viabilizar a operacionalização do uso de algum tipo visível de identificação para colaboradores e visitantes das instalações.
- E assegurar que ocorra apenas acesso físico autorizado a informações da organização e outros ativos associados.

Questão 33

A respeito de algoritmos de criptografia simétrica e criptografia assimétrica, assinale a opção correta.

- A Uma das principais vantagens dos algoritmos assimétricos, como RSA e ECC, é o desempenho de processamento superior em relação aos algoritmos simétricos para cifragem de grandes volumes de dados.
- B O AES (*Advanced Encryption Standard*) é considerado um algoritmo de chave pública por utilizar blocos de 128 *bits* e chaves de até 256 *bits*.
- C Os algoritmos de criptografia assimétrica, por utilizarem pares de chaves distintas, são menos suscetíveis a ataques de força bruta que os de criptografia simétrica, independentemente do tamanho da chave.
- D Algoritmos de criptografia simétrica, como DES e 3DES, baseiam-se em aritmética de curvas elípticas para garantirem segurança contra fatoração de inteiros em larga escala.
- E O algoritmo RSA permite tanto a confidencialidade quanto a autenticação de mensagens, podendo ser usado para criptografar dados e assinar digitalmente documentos.

Questão 34

Considerando os algoritmos de *hash* criptográfico e suas aplicações em segurança da informação, assinale a opção correta.

- A Em sistemas de deduplicação de dados, utiliza-se a função de *hash* para maximizar colisões, identificar conteúdos similares e reduzir o volume de armazenamento.
- B Em transmissões com protocolos TLS, a função de *hash* substitui a criptografia simétrica ao tornar os dados transmitidos autênticos e invioláveis.
- C Em verificação de integridade de arquivos, é recomendável utilizar funções de *hash* reversíveis para permitir a reconstrução dos dados originais em caso de corrupção.
- D Em assinaturas digitais, a função de *hash* produz um resumo criptográfico da mensagem, que é assinado com a chave privada do emissor, garantindo integridade e autenticidade.
- E Em sistemas de *blockchain*, a função de *hash* é usada para criptografar os dados da transação e, assim, garantir a confidencialidade entre os nós da rede.

Questão 35

De acordo com normatização internacional de referência, dispositivos, pessoas e mecanismos que não atuem ativamente em busca de incidentes de segurança da informação, mas que, no decorrer de suas atividades, produzam sinal de possível incidente que deva ser relatado ao CSIRT, compõem a

- A observação de tecnologia.
- B detecção proativa.
- C detecção reativa.
- D monitoração de fontes públicas.
- E validação de fontes externas.

Questão 36

Assinale a opção correta a respeito do NAT (*Network Address Translator*).

- A O NAT permite que múltiplos dispositivos compartilhem um único endereço IP público ao mapear conexões com base em endereços e portas, o que pode afetar a rastreabilidade individual das sessões.
- B Em termos de segurança, o uso do NAT dispensa a adoção de sistemas de *firewall*, uma vez que já impede conexões externas diretas, sendo capaz, portanto, de filtrar plenamente qualquer tráfego malicioso.
- C O NAT dinâmico define um mapeamento ativo fixo e pré-configurado entre um IP interno e um IP externo, independentemente da existência de tráfego.
- D O NAT impede a comunicação entre dispositivos de redes distintas ao eliminar cabeçalhos IP originais e, assim, inviabilizar o roteamento entre domínios diferentes.
- E A arquitetura NAT aplica-se à tradução de endereços IPv4 para endereços IPv6, dada a escassez de endereços públicos nativos da tecnologia IPv4.

Questão 37

Durante a análise de um incidente de segurança em um ambiente corporativo, identificou-se que diversos sistemas internos começaram a apresentar lentidão súbita, acompanhada de consumo elevado de banda de saída para a Internet e envio simultâneo de milhares de requisições a endereços IP externos à organização. Também foi observado que usuários dos equipamentos comprometidos receberam previamente *e-mail* com tema relacionado a importante comunicado interno da empresa, no qual estava anexado um arquivo executável que vários usuários admitiram ter executado.

Com base na situação hipotética precedente, assinale a opção em que é apresentada a única classificação compatível para o tipo de ataque ou ameaça envolvido, considerando sua origem e seu comportamento subsequente.

- **A** A descrição sugere uma infecção por *botnet* usada em ataque DDoS, sendo o *e-mail* malicioso o vetor inicial, e os sistemas internos os agentes distribuídos no ataque.
- **B** O cenário enquadra-se como a propagação de um *worm* clássico direcionado para a rede interna, cujo tráfego elevado indica replicação descontrolada entre os equipamentos infectados.
- **C** O incidente está alinhado a um ataque de *ransomware* padrão em estágio de cifragem ativa simultânea nas máquinas infectadas, quando é percebida a lentidão dos sistemas.
- **D** O incidente propõe um ataque de *phishing* com *adware*, pois o *e-mail* induz ao clique e o aumento de tráfego está associado à exibição massiva de propagandas.
- **E** A descrição corresponde a um ataque de *flood* tradicional gerado por *spoofing*, dado que o tráfego massivo e a lentidão são sintomas típicos de pacotes forjados em grandes quantidades.

INFRAESTRUTURA DE REDES

Questão 38

A respeito dos protocolos das redes TCP/IP, assinale a opção correta.

- **A** O endereço IP 200.123.24.255 nunca pode ser atribuído a um equipamento, pois representa o endereço de *broadcast* da rede.
- **B** O ARP serve para identificar pacotes TCP de acordo com a VLAN da sub-rede de determinado equipamento.
- **C** As mensagens ICMP Tipo 3 significam destino inacessível, ou seja, indicam que um pacote não pôde chegar até seu destino final.
- **D** Os endereços IP identificam os dispositivos conectados a uma rede TCP/IP e nunca se repetem, mesmo que os equipamentos estejam em redes distintas.
- **E** Os endereços MAC identificam as interfaces de rede dos equipamentos e podem ser duplicados em uma mesma rede, sem afetar seu correto funcionamento.

Questão 39

Assinale a opção em que é citado o nome ou o termo usado para descrever a organização e distribuição padronizada dos cabos empregados em redes de computadores e telefonia.

- **A** estrutura de rede
- **B** arquitetura de rede
- **C** topologia de rede
- **D** cabeamento estruturado
- **E** engenharia de redes

Questão 40

O gerenciamento de redes TCP/IP

- **A** envolve supervisão, monitoramento, configuração e manutenção dos dispositivos e recursos da rede.
- **B** visa à detecção de falhas físicas, não abrangendo aspectos de desempenho e segurança de redes.
- **C** deve ser executado regularmente e de forma manual para garantir maior controle e evitar falhas de sistemas automatizados.
- **D** resume-se à boa configuração inicial dos dispositivos, de forma a evitar necessidade de manutenções futuras.
- **E** é restrito aos ambientes de servidores dedicados, não se aplicando a redes de equipamentos de usuários finais.

Questão 41

No contexto de gerenciamento de redes TCP/IP, diversos protocolos são usados para monitoramento e controle de dispositivos. Entre eles, o SNMP

- **A** utiliza, a partir da versão 1, criptografia de dados para garantir que eles não sejam lidos por agentes não autorizados.
- **B** usa, por padrão, a porta TCP 22, com criptografia de dados para maior garantia de segurança.
- **C** opera na camada de enlace do modelo TCP/IP e pode ser usado para controle de acesso ao meio físico.
- **D** tem sido substituído pelo HTTPS em redes de grande porte, por suas deficiências de segurança e desempenho.
- **E** permite a coleta de informações dos dispositivos gerenciados por meio da estrutura MIB (*Management Information Base*).

Questão 42

As redes locais (LANs) e as redes de longa distância (WANs) são os principais tipos de redes de computadores, cada uma com características e aplicações distintas. A esse respeito, assinale a opção correta.

- **A** As principais características e vantagens de uma WAN são sua alta velocidade e baixa latência em comparação a uma LAN.
- **B** As LANs exigem a contratação de provedores de serviços de comunicação para seu funcionamento, enquanto as WANs podem operar de forma local e independente.
- **C** As WANs são formadas basicamente por fios e cabos ópticos, sem necessidade de uso de roteadores ou *switches*.
- **D** As LANs operam exclusivamente com tecnologia sem fio, enquanto as WANs utilizam conexões cabeadas.
- **E** Uma LAN é limitada a uma área geográfica restrita, como salas e prédios, enquanto uma WAN interliga redes localizadas em locais distantes, como cidades e países diferentes.

Questão 43

Considerando os protocolos de segurança empregados nas redes sem fio que utilizam o padrão IEEE 802.11, assinale a opção correta.

- **A** As redes cabeadas não utilizam mecanismos de autenticação e criptografia em seus dispositivos, pois são naturalmente seguras.
- **B** O WEP é mais seguro que o WPA2, pois utiliza chaves criptográficas estáticas que não se alteram durante a conexão.
- **C** O protocolo IEEE 802.1x é utilizado exclusivamente em redes cabeadas, não se aplicando a redes sem fio.
- **D** O EAP é um método de criptografia usado exclusivamente para proteger dados transmitidos via rede sem fio.
- **E** O WPA2, ao contrário do WEP, oferece autenticação robusta e criptografia forte baseada no protocolo AES.

Questão 44

Assinale a opção correta, considerando que as redes cabeadas, como as redes Ethernet, e as redes sem fio padrão IEEE 802.11 apresentam características distintas em termos de desempenho, segurança, mobilidade e confiabilidade.

- A Em comparação às redes sem fio, as redes cabeadas, apesar de terem mobilidade limitada, oferecem maior alcance, maior largura de banda, menor interferência do ambiente e maior confiabilidade para transmissão de dados.
- B Em ambientes corporativos, o uso das redes sem fio (Wi-Fi) elimina a necessidade de políticas de segurança, uma vez que os dados são criptografados automaticamente.
- C As redes cabeadas são sempre a opção mais barata e mais simples em relação às redes sem fio, qualquer que seja o ambiente físico e geográfico.
- D As redes sem fio oferecem maior estabilidade de conexão e menor latência se comparadas às redes cabeadas, sendo preferidas para aplicações críticas em *datacenters*.
- E A mobilidade oferecida pelas redes cabeadas é superior à das redes sem fio, pois as conexões via cabo permitem conectar múltiplos dispositivos simultaneamente.

Questão 45

O protocolo IEEE 802.1x, empregado para controle de acesso à rede de comunicação, especialmente em redes sem fio,

- A é um protocolo proprietário da Cisco, sendo utilizado apenas em redes com equipamentos dessa marca.
- B realiza autenticação de dispositivos na camada de aplicação, utilizando exclusivamente senhas pré-compartilhadas (PSK).
- C usa o ICMP para negociar chaves de criptografia entre o cliente e o servidor de autenticação.
- D depende de um servidor de autenticação chamado *supplicant*, o qual valida os dispositivos que solicitam acesso à rede.
- E utiliza um modelo com três entidades: *supplicant*, *authenticator* e *authentication server*; este último é geralmente implementado via servidor Radius.

Questão 46

Assinale a opção correta, considerando que o funcionamento de uma rede de computadores depende dos mecanismos de comutação de pacotes (*switching*) e de roteamento (*routing*), que operam de forma distinta e em diferentes camadas do modelo OSI.

- A O *switching* encaminha pacotes com base nos endereços de rede, como os endereços IP, já o *routing* usa os endereços MAC para a identificação dos pacotes.
- B O *switching* cria domínios de *broadcast* para a comunicação em massa, enquanto o *routing* divide os domínios de *broadcast* em subdomínios de colisão.
- C O *routing* é mais eficiente que o *switching* em redes locais, pois exige menos processamento e possui menor latência.
- D *Switching* é o encaminhamento de quadros com base no endereço MAC e opera na camada 2 do modelo OSI, enquanto o *routing* opera na camada 3, com base nos endereços de rede, como o IP.
- E O *switching* opera na camada 3 de rede, enquanto o *routing* opera na camada física, ou camada 1 do modelo OSI.

Questão 47

Assinale a opção correta, a respeito do processo de roteamento (*routing*) em redes TCP/IP.

- A No roteamento dinâmico, os dispositivos atualizam automaticamente suas tabelas com base em protocolos como OSPF e BGP.
- B O *routing* é responsável por encaminhar pacotes dentro de uma mesma LAN, com uso de endereços MAC para a escolha do caminho a seguir.
- C No processo de roteamento, a decisão de encaminhamento é tomada com base nos endereços IP de origem dos pacotes.
- D Os protocolos de roteamento dinâmico, como o OSPF e o BGP, funcionam apenas em redes sem fio.
- E O roteamento é executado na camada de aplicação do modelo OSI e sua principal função é executar o processo NAT.

SISTEMAS OPERACIONAIS

Questão 48

Sistemas operacionais fazem o gerenciamento de recursos do sistema, o que inclui a abstração de *hardware* para os aplicativos. A responsabilidade direta de um sistema operacional consiste em

- A codificar algoritmos de compressão em arquivos `.zip`.
- B compilar códigos-fonte de aplicações do usuário.
- C gerenciar o acesso concorrente à RAM.
- D traduzir linguagens de programação para linguagem de máquina.
- E atualizar automaticamente os aplicativos do usuário.

Questão 49

Em sistemas Linux, cada processo é identificado por um número único chamado PID, sendo esse identificador utilizado para monitorar e controlar a execução de processos. Assinale a opção em que é apresentado o comando usado para visualizar todos os processos em execução e seus respectivos usuários no sistema operacional Linux.

- A `ls -p`
- B `ps aux`
- C `exec -list`
- D `lsof /proc`
- E `cat /proc`

Questão 50

O gerenciamento de memória em servidores Windows inclui mecanismos como a paginação e o *cache* de disco, visando ao melhor desempenho do sistema. Assinale a opção em que é apresentada ferramenta integrada ao Windows Server que permite monitorar em tempo real o uso das memórias RAM e virtual.

- A Resource Monitor
- B Task Scheduler
- C Disk Cleanup
- D Group Policy Editor
- E PowerShell ISE

Questão 51

O Linux trata dispositivos de entrada e saída como arquivos, sendo comum o uso de arquivos especiais em `/dev` para interagir com esses dispositivos. Nesse contexto, assinale a opção em que é apresentado comando utilizado para verificar estatísticas de discos e operações de entrada e saída no Linux.

- A `journalctl`
- B `ifconfig`
- C `lsblk`
- D `iostat`
- E `traceroute`

Questão 52

Durante a instalação do RHEL 8, é possível escolher ambientes de sistema, como servidor com GUI ou servidor mínimo. A vantagem principal do ambiente servidor mínimo durante a instalação do RHEL 8 é

A carregar *drivers* adicionais para dispositivos legados.
B oferecer interface gráfica com suporte a recursos multimídia.
C reduzir a superfície de ataque e o consumo de recursos.
D permitir a execução de aplicações Windows sem configurações adicionais.
E incluir automaticamente o GNOME como gerenciador de *desktop*.

Questão 53

Tendo em vista que o gerenciamento de volumes no Linux é facilitado pelo uso do LVM (*Logical Volume Manager*), que permite redimensionamento e movimentação de volumes, assinale a opção em que é apresentado o comando utilizado para criar um volume físico no LVM.

A `pvcreate`
B `vgcreate`
C `lvcreate`
D `mkfs.ext4`
E `fdisk -lE`

Questão 54

Considerando que, no Red Hat Enterprise Linux, são utilizadas permissões `POSIX` para controlar acesso a arquivos e diretórios, assinale a opção em que é apresentado o comando empregado para alterar o dono e o grupo de um arquivo no Linux.

A `usermod`
B `chown`
C `chmod`
D `chgrp`
E `setfacl`

Questão 55

No Windows Server 2019, a função principal do Active Directory Domain Services é

A fornecer autenticação e gerenciamento centralizado de identidades.
B gerenciar configurações de rede de forma dinâmica.
C sincronizar arquivos em servidores remotos.
D monitorar o consumo de energia dos *hosts*.
E armazenar dados relacionais para aplicações empresariais.

Questão 56

Os AD DS (*Active Directory Domain Services*) organizam seus dados em partições de diretório, também conhecidas como contextos de nomenclatura. Estas partições são partes contíguas do diretório com escopo de replicação independente. Cada controlador de domínio em uma floresta AD armazena diferentes partições, responsáveis por funções específicas na estrutura do diretório. Acerca dos contextos de nomenclatura (partições de diretório) no AD DS, assinale a opção correta.

A As partições de esquema e configuração são replicadas para todos os controladores de domínio da floresta.
B A partição de esquema armazena contas de usuários e grupos de segurança.
C Controladores de domínio replicam partições de domínio de todos os domínios da floresta.
D A partição de configuração armazena os dados de auditoria e *logs* de eventos dos controladores de domínio.
E Um controlador de domínio não armazena a partição de esquema quando está configurado como servidor secundário.

Questão 57

Uma das principais funções dos AD DS em uma rede corporativa Windows é

A compactar e criptografar automaticamente os arquivos armazenados nos servidores.
B criar páginas *web* dinâmicas para a *intranet* da empresa.
C prover um serviço centralizado que inclui a autenticação e autorização de computadores e recursos.
D monitorar o desempenho dos computadores e servidores da rede.
E gerenciar e aplicar políticas de *firewall* para controlar o tráfego da rede.

Questão 58

Acerca do LDAP versão 3 ou superior, utilizado pelo *Active Directory* e outros serviços de diretório, assinale a opção correta.

A As consultas LDAP não permitem a seleção de atributos específicos, o que provoca o retorno dos atributos disponíveis nas entradas encontradas.
B As entradas LDAP são organizadas em uma estrutura linear, não sendo possível estabelecer relações hierárquicas entre objetos.
C O LDAP permite operações de autenticação, consulta, comparação, adição, remoção e modificação de entradas no diretório.
D O LDAP utiliza o formato XML para representação de dados e comunicação entre cliente e servidor.
E Em uma consulta LDAP, o caractere asterisco (*) é utilizado para representar exatamente um caractere em buscas com curingas.

Questão 59

Em ambientes corporativos com sistemas heterogêneos, a interoperabilidade entre serviços de diretório é fundamental para a garantia da autenticação única e do gerenciamento centralizado de usuários. Para que haja essa interoperabilidade entre diferentes sistemas, é essencial

A a limitação do acesso a recursos compartilhados apenas aos usuários do sistema operacional predominante na rede.
B o isolamento completo das bases de usuários para garantir a segurança entre plataformas distintas.
C a implementação de protocolos proprietários exclusivos para cada sistema presente na rede corporativa.
D a duplicação manual de todas as contas de usuário em cada um dos diferentes serviços de diretório.
E a implementação de um protocolo comum de comunicação que permita a troca padronizada de informações de autenticação.

Questão 60

No AD (*Active Directory*), a implementação de uma nova infraestrutura de diretório completamente independente, com seu próprio esquema, configurações globais e limites de segurança isolados, requer que o administrador de sistemas configure um novo contêiner lógico de nível mais alto na hierarquia. Nesse caso, o elemento do AD a ser criado é

A a floresta.
B o grupo.
C a unidade organizacional.
D a árvore.
E o domínio.

Questão 61

Em tecnologias de serviços de diretório, de acordo com as principais implementações e fornecedores (Microsoft, OpenLDAP, RedHat, Oracle, IBM, por exemplo), o elemento utilizado para a identificação, de forma única, do caminho completo e da posição exata de um objeto dentro da estrutura hierárquica do diretório é o

- A UUID (*universally unique identifier*).
- B DN (*distinguished name*).
- C GUID (*globally unique identifier*).
- D OID (*object identifier*).
- E SID (*security identifier*).

Questão 62

Assinale a opção em que é citado, de acordo com o LDAP versão 3 ou superior, o controle específico utilizado para retornar resultados em páginas sequenciais, organizando os resultados de pesquisas extensas e permitindo que o cliente receba os resultados em blocos gerenciáveis, em vez de uma única resposta grande.

- A `subentries`
- B `entryChange`
- C `permissiveModify`
- D `pagedResults`
- E `matchedValues`

SERVIDORES

Questão 63

O papel de um servidor de aplicação, componente responsável por processar requisições HTTP e HTTPS e que conecta as camadas na arquitetura em três camadas, é

- A hospedar a lógica de negócios e intermediar a comunicação com o banco de dados.
- B armazenar e distribuir arquivos estáticos como HTML e imagens.
- C controlar dispositivos de rede e rotear pacotes entre sub-redes.
- D oferecer serviços de autenticação via LDAP.
- E gerenciar o acesso aos discos físicos do sistema operacional.

Questão 64

Uma prática comum de alta disponibilidade em servidores de aplicação consiste em

- A utilizar múltiplas instâncias de servidores de aplicação atrás de um balanceador de carga.
- B utilizar um servidor com alta capacidade de processamento para evitar redundância.
- C executar a aplicação em modo *standalone*, sem dependências externas.
- D adotar *logs* síncronos no banco de dados para rastreabilidade total.
- E implementar sessões de usuários em arquivos locais temporários.

Questão 65

Assinale a opção em que é apresentada uma técnica de balanceamento de carga em servidores de aplicação.

- A compactação de pacotes de rede para a redução do tempo de resposta
- B uso exclusivo de *round-robin* no DNS, sem avaliação do estado de disponibilidade de instâncias
- C aplicação do algoritmo LRU (*least recentrly used*) ao gerenciamento de memória do sistema
- D balanceamento na camada de aplicação com a utilização de algoritmos como *round-robin* ou *least connections*
- E análise de *logs* do sistema operacional para a redistribuição de conexões

Questão 66

Assinale a opção em que é citado o procedimento que, em ambientes distribuídos, permite a replicação de sessão entre múltiplos servidores de aplicação.

- A registro da sessão em arquivos de *log*
- B inclusão de todas as informações de sessão em *cookies* do cliente
- C armazenamento de sessões na RAM local de cada instância
- D clusterização com replicação de sessão via *middleware* ou *engine* do servidor
- E encaminhamento de todas as requisições do usuário ao mesmo servidor

ARMAZENAMENTO

Questão 67

A respeito dos tipos de armazenamento na nuvem, assinale a opção correta.

- A O armazenamento em bloco segue rígidos protocolos de arquivos, como SMB, NFS ou Lustre, e tem acesso direto aos blocos de disco brutos.
- B O armazenamento de arquivos é organizado hierarquicamente em diretórios e pastas, sendo mais indicado para bancos de dados ou sistemas de ERP.
- C No armazenamento de objetos, é utilizada uma estrutura simples com dados, metadados e um identificador exclusivo para cada objeto.
- D No armazenamento em bloco, priorizam-se metadados e escalabilidade, por isso ele é mais indicado para grandes volumes de dados não estruturados.
- E O armazenamento de objetos fornece valores de baixa latência e alto desempenho, sendo útil principalmente para armazenamento de dados estruturados.

Questão 68

No armazenamento de computador, várias interfaces facilitam a conexão entre unidades de disco rígido (HDD), unidades de estado sólido (SSD) e a placa-mãe do computador. Acerca das características dessas interfaces, assinale a opção correta.

- A Dispositivos USB 3.2 Gen 2 × 2 operam a uma velocidade de 5 Gbps quando conectados a portas USB 4, devido a incompatibilidades elétricas entre os padrões.
- B A velocidade SATA é definida pelo padrão — I, II ou III —, sendo imune a fatores como o controlador da placa-mãe, o tamanho do cabo ou o tipo do protocolo.
- C No PATA, a velocidade é definida pelo padrão ATA, mas varia conforme a qualidade do cabo, o controlador da placa-mãe e as especificações da unidade.
- D As interfaces SCSI operam na mesma velocidade, independentemente do padrão, pois todas usam o mesmo protocolo de comunicação baseado no SCSI-1 original.
- E A configuração de *wide port* em SAS reduz a largura de banda para 6 Gbps totais, pois as pistas operam em modo *half-duplex* compartilhado.

Questão 69

Em um servidor com RAID 5 que utiliza quatro HDD, cada um deles de 10 TB, um disco falhou e foi substituído. Durante o *rebuild* — processo lento em discos grandes —, um segundo disco falhou, o que resultou em perda total de dados. O *backup*, armazenado no mesmo *array*, tornou-se inacessível.

Com base nessa situação hipotética, é correto inferir que o problema principal foi causado por

A falta de alertas para a substituição de discos degradados previamente.
B uso de HDD de alta capacidade, que aumenta o risco durante *rebuild*.
C interrupção do *rebuild* devido ao tempo excessivo em HDD de 10 TB.
D limitação inerente ao RAID 5, que suporta apenas uma falha.
E armazenamento do *backup* no mesmo *array*, o que inviabilizou a recuperação de dados.

Questão 70

A respeito do NAS (armazenamento conectado à rede), julgue os seguintes itens.

I O NAS funciona como um sistema de arquivo e lida com solicitações de arquivos individuais.
II O aumento de escala horizontal consiste em comprar mais unidades de armazenamento.
III Um arquivo `.txt` armazenado no NAS é enviado como `.txt` via SMB para um Windows ou via NFS para um Linux.

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.

COMPUTAÇÃO EM NUVEM

Questão 71

Assinale a opção em que é citada uma das características do modelo de computação em nuvem.

A impossibilidade de acesso remoto a arquivos e aplicativos
B capacidade de adaptação dinâmica, que possibilita a expansão ou redução dos recursos conforme a necessidade do usuário
C restrição ao uso de apenas um provedor de serviços em nuvem
D dependência de servidores físicos locais para processar os dados
E necessidade de aquisição de *hardware* próprio, o que implica elevação de custos

Questão 72

Na computação em nuvem, diferentes modelos de serviço oferecem níveis variados de controle e responsabilidade ao usuário. Um dos principais modelos é o PaaS (plataforma como serviço), que se caracteriza por

A restringir a implementação de aplicações apenas a servidores físicos próprios da empresa.
B fornecer *hardware* e armazenamento ao usuário, sem interface de desenvolvimento.
C proporcionar total controle sobre *hardware* e *software*, o que permite a configuração personalizada do sistema operacional.
D limitar o acesso remoto à plataforma, o que exige instalação local das ferramentas de desenvolvimento.
E disponibilizar um ambiente completo para desenvolvimento e execução de aplicações, sem necessidade de gerenciamento de infraestrutura.

Questão 73

Um dos principais desafios para empresas que utilizam serviços baseados na nuvem é a segurança dos dados. Uma estratégia eficaz para a mitigação de riscos consiste em

A implementar autenticação multifator, criptografia de dados e monitoramento contínuo, para a proteção contra acessos não autorizados.
B utilizar eventualmente um único fator de autenticação, para facilitar o acesso dos usuários.
C manter os dados em servidores locais, para evitar a necessidade de criptografia na nuvem.
D compartilhar credenciais administrativas entre múltiplos usuários, para garantir rapidez ao gerenciamento.
E evitar ferramentas de monitoramento de segurança, pois sua utilização pode impactar o desempenho da infraestrutura em nuvem.

Questão 74

A virtualização é uma tecnologia essencial para a computação em nuvem, pois permite a criação de ambientes isolados dentro de um único servidor físico. Um dos principais componentes responsáveis por essa funcionalidade é o

A *firewall*, que protege as máquinas virtuais contra acessos não autorizados.
B balanceador de carga, que distribui os recursos entre as máquinas virtuais.
C hipervisor, que gerencia e aloca recursos para as máquinas virtuais dentro do servidor físico.
D sistema operacional do *host*, que gerencia diretamente todas as máquinas virtuais.
E armazenamento em nuvem, que permite a execução de múltiplas instâncias simultâneas.

Questão 75

A virtualização de servidor

A consolida múltiplos dispositivos físicos em um único sistema lógico.
B permite o acesso remoto a ambientes de trabalho personalizados.
C isola programas para a execução independente do sistema operacional.
D permite a criação de várias máquinas virtuais independentes dentro de um único *hardware* físico.
E segmenta e gerencia conexões de tráfego.

Questão 76

A conteinerização de aplicações permite que se empacote uma aplicação junto com todas as suas dependências, garantindo que ela funcione de maneira consistente em diferentes ambientes. Uma das características dessa abordagem é a

A redução da escalabilidade devido ao isolamento dos contêineres.
B portabilidade, que permite que a aplicação seja executada em diferentes sistemas operacionais sem necessidade de ajustes.
C dependência de um único sistema operacional para garantir compatibilidade.
D necessidade de máquinas virtuais para rodar aplicações conteinerizadas.
E restrição ao uso de apenas um tipo de infraestrutura de nuvem.

Questão 77

Na computação em nuvem, a coordenação automatizada de contêineres é um processo essencial para gerenciá-los em larga escala. Uma das ferramentas mais utilizadas para essa finalidade é o

A Kubernetes, que administra e orquestra múltiplos contêineres em ambientes distribuídos.
B Terraform, que automatiza a criação de infraestrutura em nuvem.
C Jenkins, que facilita a integração contínua de aplicações conteinerizadas.
D VirtualBox, que permite a criação de máquinas virtuais para rodar contêineres.
E Apache Kafka, que gerencia fluxos de dados entre aplicações conteinerizadas.

Questão 78

DevSecOps é uma abordagem que integra segurança ao ciclo de vida do desenvolvimento de *software*, garantindo que vulnerabilidades sejam identificadas e corrigidas desde as primeiras etapas do processo. Uma das características dessa abordagem é a

A dependência exclusiva de ferramentas externas para a garantia da segurança do *software*.
B separação total entre desenvolvimento e segurança, que permite que cada equipe trabalhe de forma independente.
C eliminação da necessidade de monitoramento contínuo, pois os testes são realizados apenas antes da implantação.
D restrição do acesso ao código-fonte apenas para a equipe de segurança, o que garante maior proteção.
E automação de testes de segurança, que reduz o tempo necessário para identificação e correção de vulnerabilidades.

Questão 79

No DevSecOps, diversas ferramentas são utilizadas para a segurança do *software* durante todo o ciclo de desenvolvimento. Uma das práticas dessa abordagem consiste na

A eliminação da necessidade de auditorias de segurança, pois os testes automatizados garantem a proteção do *software*.
B separação entre desenvolvimento e segurança, que permite que cada equipe trabalhe de forma independente.
C integração de testes de segurança automatizados no *pipeline* de CI/CD, para garantir a detecção precoce de vulnerabilidades.
D realização de testes de segurança restrita à fase final do desenvolvimento para evitar impacto na produtividade.
E implementação de segurança manual, sem o uso de automação, para garantir maior controle sobre os processos.

Questão 80

Uma das estratégias avançadas do DevSecOps para a garantia da segurança do *software* em ambientes de nuvem é a implementação de

A testes de segurança limitados à fase de implantação, para que o *software* esteja protegido antes de ser disponibilizado.
B monitoramento de segurança em servidores locais, que torna desnecessária a análise em ambientes de nuvem.
C segurança como código (*security as code*), que permite que políticas de segurança sejam definidas e aplicadas automaticamente no ambiente de desenvolvimento.
D restrição do acesso ao código-fonte para a equipe de segurança, para maior proteção contra ataques externos.
E *firewalls* para proteger as aplicações em nuvem, que torna desnecessárias outras medidas de segurança.

Espaço livre