-- CONHECIMENTOS ESPECÍFICOS --

Questão 26

Em computação em nuvem, quando uma organização monta e fornece serviços para outras empresas, ela está utilizando o modelo de nuvem do tipo

A híbrida.
B pública.
C comunidade.
D proprietária.
E privada.

Questão 27

Quanto ao gerenciamento de memória, o processo em que cada *software* em execução tem seu próprio espaço de endereçamento é o de

A paginação.
B sobreposição.
C segmentação.
D alocação.
E virtualização.

Questão 28

Na autenticação por LDAP, é necessário que o servidor esteja executando o LDAP na rede. Esse item de configuração é denominado

A interface de programação de aplicações (API).
B agente de sistema do diretório (DSA).
C agente de usuário do diretório (DUA).
D nome diferenciado (DN).
E nome diferenciado relativo (RDN).

Questão 29

Na computação em nuvem, quando o gerenciamento do espaço em disco e do sistema operacional é de responsabilidade do provedor, o serviço utilizado é do tipo

A contêiner como serviço (CaaS).
B plataforma como serviço (PaaS).
C *software* como serviço (SaaS).
D infraestrutura como serviço (IaaS).
E dado como serviço (DaaS).

Questão 30

A estratégia para contingência e continuidade de serviços inclui um conjunto de cenários de indisponibilidade e de reações conhecido como

A plano de contingência operacional (PCO).
B plano de gerenciamento de crises (PGC).
C plano de comunicação (PC).
D plano de recuperação de desastres (PRD).
E plano de administração de crises (PAC).

Questão 31

Na virtualização de servidores, a funcionalidade que garante a administração e monitoração centralizada das entidades é a de

A interposição.
B isolamento.
C inspeção.
D eficiência.
E gerenciabilidade.

Questão 32

A métrica das ferramentas de alta disponibilidade que mede por quanto tempo um sistema fica inoperante antes de ser recuperado ou substituído é o

A tempo médio entre falhas (MTBF).
B *downtime* médio.
C objetivo de ponto de recuperação (RPO).
D objetivo de tempo de recuperação (RTO).
E gerenciamento proativo do desempenho.

Questão 33

Na virtualização por contêineres, o mecanismo que engloba recursos do sistema em uma abstração é conhecido como

A *control groups*.
B *union file systems*.
C *namespace*.
D *bare metal*.
E *inter process communication*.

Questão 34

A abertura e o fechamento da comunicação entre dois dispositivos no modelo OSI é de responsabilidade da camada de

A apresentação.
B rede.
C transporte.
D aplicação.
E sessão.

Questão 35

Na arquitetura TCP/IP, é responsável por permitir que os *hosts* enviem pacotes para qualquer rede e garantir que esses dados cheguem ao seu destino final

A o protocolo TCP.
B a camada de aplicação.
C a camada Internet.
D o protocolo UDP.
E a camada de enlace.

Questão 36

A mensagem que um dispositivo envia com o objetivo de receber um endereço IP distribuído por meio de um servidor DHCP é do tipo

A DHCP *request*.
B DHCP *release*.
C DHCP *offer*.
D DHCP *discover*.
E DHCP ACK.

Questão 37

O registro DNS que aponta um nome de domínio (um *alias*) para outro domínio é do tipo

A AAAA.
B NS.
C CNAME.
D MX.
E PTR.

Questão 38

O SSH suporta métodos de autenticação que fornecem um esquema extensível para executar autenticação usando-se mecanismos externos, como Kerberos 5 ou NTLM. Entre esses métodos, inclui-se o

A SFTP.
B SSHFP.
C GSSAPI.
D FASP.
E SCP.

Questão 39

Para dividir uma rede típica classe C em outras duas sub-redes, é correto utilizar uma máscara de redes que, em quantidade de *bits*, seja equivalente a

A \23.
B \24.
C \25.
D \26.
E \27.

Questão 40

No protocolo Spanning Tree, todos os *switches* se comunicam constantemente com seus vizinhos na LAN por meio de

A tabela MAC.
B tabela de *store and forward*.
C ponte *root*.
D mecanismo do tipo estado da porta.
E unidades de dados de protocolo de ponte (BPDU).

Questão 41

No Gigabit Ethernet, a transmissão em fibra óptica para distâncias de até 5 km é possível com o uso do padrão

A 1000BASE-LX.
B 1000BASE-SX.
C 1000BASE-CX.
D 1000BASE-TX.
E 1000BASE-T.

Questão 42

No protocolo BGP, uma coleção de prefixos de roteamento IP conectados sob o controle de um ou mais operadores de rede em nome de uma única entidade administrativa ou domínio que apresenta uma política de roteamento comum e claramente definida para a Internet corresponde a

A IANA.
B *autonomous system*.
C *next hop*.
D *atomic aggregate*.
E *multi-exit discriminator*.

Questão 43

A fim de gerar uma chave exclusiva para a autenticação de mensagens no SNMPv3, é correto o uso de

A USM (*user-based security model*).
B *engine* ID.
C VACM (*view-based access control model*).
D CBC com MD5.
E MIB.

Questão 44

De acordo com a norma ISO/IEC 27002, o objetivo da classificação da informação é

A verificar a informação do ponto de vista legal, atribuindo-lhe um valor de acordo com uma escala numérica adequada.
B filtrar o conteúdo da informação acessada pelos colaboradores, com o propósito de manter a produtividade da organização.
C analisar a qualidade da informação, especificamente quanto à sua veracidade, visando-se à prevenção contra a desinformação.
D assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.
E avaliar a utilidade da informação organizacional, descartando-se os conteúdos inúteis à missão corporativa.

Questão 45

Uma função de *hashing*

A apresenta valores de *hash* de saída de tamanho fixo, independentemente dos dados de entrada.
B verifica a disponibilidade de dados em determinada estrutura.
C tem aplicação restrita a porções de dados de entrada de até 1.024 MB de tamanho.
D permite a reconstrução de seus dados de entrada de forma computacionalmente simples, a partir de um valor de *hash* resultante.
E não é aplicável a arquivos executáveis ou a arquivos binários compilados.

Questão 46

No contexto da infraestrutura de chaves públicas ICP-Brasil, homologar, auditar e fiscalizar o sistema ICP-Brasil, inclusive os seus prestadores de serviço, compete

A à autoridade certificadora raiz (AC Raiz).
B ao Comitê Gestor da ICP-Brasil.
C às autoridades certificadoras (AC).
D ao Instituto Nacional de Tecnologia da Informação (ITI).
E às autoridades de registro (AR).

Questão 47

Com base na norma ISO/IEC 27002, assinale a opção correta a respeito de controles de acesso.

A Para evitar sobrecarga no processamento de informações, é recomendado evitar a retenção dos registros de acesso, das identidades dos usuários e dos dados de autenticação.
B É fundamental que o controle de acesso a ativos de uma organização seja estabelecido com base em requisitos políticos e de usabilidade dos recursos.
C Por questões de segurança, é crucial que as informações sobre os requisitos do negócio a serem atendidos pelo controle de acesso sejam restritas ao conselho diretivo da organização.
D Uma política de controle de acesso deve estabelecer a concentração das funções de controle de acesso, tais como pedidos, autorizações e administração de acessos.
E Convém que as regras para controle de acesso sejam apoiadas por procedimentos formais e responsabilidades claramente definidas.

Questão 48

Assinale a opção que apresenta o código malicioso que é projetado para permitir o retorno e o acesso de um invasor a um equipamento comprometido anteriormente, por meio da inclusão de serviços criados ou modificados.

A *backdoor*
B *worm*
C vírus
D cavalo de Troia
E *ransomware*

Questão 49

O protocolo de acesso a redes sem fio que especifica implementações fracas de criptografia RC4 e que, por sua fragilidade característica, não impede que um atacante obtenha a chave usada para cifrar os pacotes a partir do próprio tráfego cifrado é o

A WPA.
B WPA2.
C EAP.
D WEP.
E WPA-PSK.

Questão 50

Assinale a opção que indica um ataque em que um golpista visa obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social.

A DDoS (*distributed denial of service*)
B *brute force*
C *eavesdropping*
D *phishing*
E *port scanning*