COMISSÃO DE VALORES MOBILIÁRIOS

TARDE

ANALISTA CVM - PERFIL 9 - TI - INFRAESTRUTURA E SEGURANÇA

PROVA OBJETIVA DE CONHECIMENTOS ESPECÍFICOS – NÍVEL SUPERIOR

TIPO 1 – BRANCA

SUA PROVA

Além deste caderno de provas contendo setenta questões objetivas, você receberá do fiscal de sala:

- uma folha para a marcação das respostas das questões objetivas

TEMPO

- **4 horas** é o período disponível para a realização da prova, já incluído o tempo para a marcação da folha de respostas da prova objetiva
- **3 horas** após o início da prova é possível retirar-se da sala, sem levar o caderno de provas
- **30 minutos** antes do término do período de prova é possível retirar-se da sala **levando o caderno de provas**

NÃO SERÁ PERMITIDO

- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova
- Usar o sanitário ao término da prova, após deixar a sala

INFORMAÇÕES GERAIS

- As questões objetivas têm cinco alternativas de resposta (A, B, C, D, E) e somente uma delas está correta
- Verifique se este caderno de provas está completo, sem repetição de questões ou falhas. Caso contrário, notifique imediatamente o fiscal da sala, para que sejam tomadas as devidas providências
- Na folha de respostas da prova objetiva, confira seus dados pessoais, especialmente nome, número de inscrição e documento de identidade, e leia atentamente as instruções para preenchimento
- Use somente caneta esferográfica, fabricada em material transparente, com tinta preta ou azul
- Assine seu nome apenas no(s) espaço(s) reservado(s)
- Confira o cargo, a cor e o tipo do seu caderno de provas. Caso tenha recebido caderno de cargo, cor ou tipo diferente do impresso em sua folha de respostas, o fiscal deve ser **obrigatoriamente** informado para o devido registro na ata da sala
- O preenchimento das respostas da prova objetiva é de sua responsabilidade e não será permitida a troca da folha de respostas em caso de erro
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas na folha de respostas da prova objetiva, não sendo permitido anotar informações relativas às respostas em qualquer outro meio que não seja o caderno de provas
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída de sanitários durante a realização das provas

Boa sorte!

PROVA OBJETIVA
CONHECIMENTOS ESPECÍFICOS

Segurança da Informação

1

A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual de cidadãos e de empresas.
Sobre a hierarquia da ICP-Brasil, é correto afirmar que:

(A) a Autoridade Certificadora do Tempo (ACT) tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo, que é o conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere prova da sua existência em determinado período de tempo;
(B) o Prestador de Serviço de Suporte (PSS) é responsável pela interface entre o usuário e a Autoridade Certificadora (AC), tendo por objetivo o recebimento, a validação e o encaminhamento de solicitações de emissão ou revogação de certificados digitais;
(C) uma Autoridade Certificadora (AC) é uma entidade pública, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais;
(D) a Autoridade de Registro (AR) verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;
(E) os Prestadores de Serviço Biométrico (PSBios) gerenciam bancos de dados biométricos e emitem certificados digitais.

2

A norma ISO/IEC 27001 é um padrão internacional que define requisitos a que um Sistema de Gestão de Segurança da Informação (SGSI) deve atender. Ela se divide em duas partes: o texto da norma em si, que descreve os requisitos de forma abrangente, e o Anexo A, mais detalhado e objetivo, que tem por função:

(A) estabelecer a política de certificação digital;
(B) especificar os papéis e responsabilidades da alta administração;
(C) delinear o processo de avaliação de riscos;
(D) fornecer orientação sobre a implementação de controles de segurança da informação;
(E) definir o escopo do Sistema de Gestão de Segurança da Informação.

3

As recomendações de segurança CIS *Critical Security Controls*, estruturadas em camadas, envolvem à implementação de um conjunto de controles de segurança. Em sua versão 8, são compostas por 18 níveis ou controles macro.
Sobre esses controles, aquele que está definido corretamente de acordo com a especificação é o:

(A) controle CIS 5: Gerenciamento de Controle de Acesso - visa a estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicativos);
(B) controle CIS 7: Gerenciamento de Controle de Acesso - usa processos e ferramentas para atribuir e gerenciar a autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, para ativos e software corporativos;
(C) controle CIS 1: Gerenciamento Contínuo de Vulnerabilidades - coleta, alerta, revisão e retenção de logs de auditoria de eventos que podem ajudar a detectar, entender ou se recuperar de um ataque;
(D) controle CIS 11: Teste de Penetração - indica processos e ferramentas para estabelecer e manter monitoramento de rede abrangente e defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuários da empresa;
(E) controle CIS 3: Proteção de dados - desenvolve processos e controles técnicos para identificar, classificar, manipular, reter e descartar dados com segurança.

4

João foi incumbido de implementar criptografia em seus sistemas de informação para aprimorar o nível de segurança na troca de informações sigilosas entre os analistas da CVM. Entre outras decisões, deve definir se e quando empregar os modelos de criptografia simétrica e assimétrica.
Para isso, é necessário levar em consideração que:

(A) a criptografia assimétrica utiliza um par de chaves, em que a chave pública é usada para decriptação de mensagens encriptadas pela chave privada correspondente;
(B) na criptografia assimétrica, a chave pública pode ser utilizada tanto para autenticação de uma mensagem encriptada pela chave privada correspondente, como para encriptação de mensagens, as quais só podem ser decriptadas pela chave privada correspondente;
(C) para autenticação de mensagens na criptografia assimétrica, gera-se um hash da mensagem, que é encriptado com a chave pública, gerando uma assinatura digital;
(D) a criptografia assimétrica veio substituir os algoritmos de criptografia simétrica, principalmente em grandes volumes de dados, em virtude de o esforço computacional envolvido na criptografia assimétrica ser normalmente muito menor;
(E) a criptografia assimétrica e a simétrica coexistem, sendo a simétrica normalmente utilizada para compartilhar as chaves utilizadas na criptografia assimétrica.

5

A equipe de Tecnologia da Informação (TI) de um órgão realizou o processo de hardening nos ativos da organização para minimizar a possibilidade de acessos não autorizados, garantir a disponibilidade do serviço e assegurar a integridade dos dados, mantendo os sistemas estáveis e fidedignos.

Uma boa prática de hardening, baseada em IPV4, adotada pela equipe de TI é:

(A) utilizar usuário comum para todos os administradores do ativo para reduzir a quantidade de usuários no sistema, visando a reduzir o acesso indevido e manter a confidencialidade;
(B) manter o registro dos usuários sem suas respectivas permissões para preservar a confidencialidade;
(C) manter a porta padrão do serviço, garantindo o seu acesso, a fim de preservar a integridade e disponibilidade do ativo;
(D) desabilitar os protocolos de descoberta de vizinhança para impedir a inundação da rede com mensagens desnecessárias, mantendo a disponibilidade;
(E) ativar serviços não utilizados para usá-los como *honey pot* no ambiente de produção, garantindo a disponibilidade do serviço principal.

6

A implementação de um sistema de gestão de segurança da informação (SGSI) baseado na ISO/IEC 27001 envolve diversos processos.

Durante o processo de avaliação de riscos da segurança, deve-se:

(A) priorizar os riscos analisados para o seu tratamento;
(B) determinar os controles para implementar as ações para o tratamento dos riscos;
(C) obter a aprovação dos proprietários dos riscos para definir a aceitação dos riscos residuais;
(D) considerar as interfaces e dependências entre as atividades do órgão;
(E) selecionar as opções de tratamento dos riscos.

7

Regularmente, a equipe de gestão de vulnerabilidades realiza auditorias internas nos sistemas operacionais dos ativos escolhidos para verificar a conformidade dos requisitos de segurança estabelecidos para cada ativo.

Conforme a ISO/IEC 27002, convém que a equipe observe a seguinte diretriz para a realização das auditorias internas:

(A) os requisitos de auditoria para acesso aos sistemas devem ser definidos pelo proprietário do risco do ativo;
(B) os testes de auditoria devem possuir acessos de leitura e escrita para validar as ações realizadas nos softwares e nos dados no ambiente de produção;
(C) os testes de auditoria devem ser realizados durante o horário de expediente para refletir o comportamento real do sistema;
(D) os acessos devem ser monitorados e registrados para produzir uma trilha de referência;
(E) um prazo deve ser definido para a reação a notificações de potenciais vulnerabilidades técnicas relevantes.

8

Os gerentes dos departamentos de um órgão público receberam um e-mail com informações específicas sobre suas carreiras, informando-os de que haviam sido selecionados para um evento de mentoria com um especialista em design thinking, que seria totalmente custeado pelo órgão, e que deveriam fazer suas inscrições. No e-mail constava o link para a inscrição, no qual seria necessário se autenticar com as credenciais do sistema de *Single Sign-On* do órgão.

A ETIR (Equipe de Tratamento de Incidentes em Redes) do órgão identificou que os gerentes sofreram um ataque do tipo:

(A) e-mail spoofing;
(B) ransomware;
(C) phishing;
(D) pharming;
(E) spear phishing.

9

Alguns usuários da rede local de um órgão perceberam que, ao tentar acessar um determinado site, eram sempre direcionados para uma página diferente da dos outros usuários do mesmo órgão. O incidente foi relatado para a ETIR (Equipe de Tratamento de Incidentes em Redes), que identificou que o servidor de DNS que esses usuários consultavam estava desviando o tráfego para um site falso, pois o endereço IP que constava na tabela de tradução de nomes havia sido alterado. A ETIR analisou o incidente e detectou que o servidor DNS consultado havia sofrido um ataque devido a uma vulnerabilidade do DNS.

A vulnerabilidade explorada permitiu que o servidor sofresse um ataque do tipo:

(A) IP spoofing;
(B) DNS spoofing;
(C) phishing;
(D) defacement;
(E) sniffing.

10

Um sistema de gestão de segurança da informação (SGSI) deve contemplar os requisitos de segurança necessários para assegurar a confidencialidade, integridade e disponibilidade da informação gerada pela organização. É necessário estabelecer o escopo e limites para a abrangência do SGSI.

Um aspecto que deve ser considerado na determinação do escopo do SGSI é (são):

(A) a liderança e o comprometimento da Alta Direção com o SGSI;
(B) a promoção da melhoria contínua do SGSI;
(C) os critérios para aceitação dos riscos a serem tratados pelo SGSI;
(D) as questões internas e externas que afetam o alcance dos resultados do SGSI;
(E) os recursos para o alcance dos objetivos do SGSI.

11

Um plano de gerenciamento de riscos deve identificar os riscos dos ativos, determinando o seu nível, a probabilidade de sua ocorrência e seu impacto para a organização. Após a avaliação dos riscos, deve-se escolher a opção mais adequada para seu tratamento, considerando o custo para sua implementação e os benefícios esperados.
A opção de tratamento de risco que permite gerenciar o seu nível por meio da inclusão, exclusão ou alteração de controles, a fim de que o risco residual seja aceitável, é o(a):
(A) modificação do risco;
(B) retenção do risco;
(C) ação de evitar o risco;
(D) compartilhamento do risco;
(E) aceitação do risco.

12

A fim de complementar o trabalho de gestão de vulnerabilidades nos ativos da organização, a equipe de segurança implementou uma solução para auxiliar no tratamento das vulnerabilidades residuais que podem colocar a organização em risco de ataques cibernéticos. A solução detecta precocemente as ameaças, correlacionando os eventos de segurança dos ativos, por meio da análise de seus logs, com comportamentos anômalos e ofensivos contra eles, permitindo algumas ações automáticas de resposta ao incidente.
A solução contratada pela equipe de segurança é um:
(A) IDS (*Intrusion Detection System*);
(B) IPS (*Intrusion Prevention System*);
(C) IAM (*Identity Access Management*);
(D) firewall;
(E) SIEM (*Security Information and Event Management*).

13

A fim de incrementar a segurança da rede da organização, a equipe de segurança instalou sistemas de detecção de intrusão (IDS – *Intrusion Detection System*) para monitorar a rede, identificando os eventos que violem suas regras de segurança. O IDS instalado baseia sua detecção na análise do comportamento do tráfego, comparando-o com seu comportamento padrão.
O tipo de IDS instalado foi o:
(A) host-based com detecção de anomalia;
(B) network-based com detecção de anomalia;
(C) host-based com detecção de assinatura;
(D) network-based com detecção de assinatura;
(E) host-based com análise de protocolo.

14

Wallace pertence a um Blue Team da Comissão de Valores Mobiliários (CVM) e tem a função de proteger as infraestruturas, tecnologias e aplicações corporativas. Deve ainda ter a prontidão necessária para prevenir, identificar, conter, mitigar e responder a qualquer tentativa de acesso indevido ou ataque cibernético. Como forma de testar sua equipe, Wallace simulou um ataque de negação de serviço distribuído (DDoS) no DNS por meio de DNS Replay.
Para executar essa simulação, Wallace fez uso da ferramenta:
(A) drool;
(B) manuka;
(C) dyninst;
(D) eztools;
(E) sooty.

15

A Comissão de Valores Mobiliários (CVM) está com um processo licitatório para a aquisição de um Exadata (máquina para uso exclusivo de banco de dados Oracle). Como requisito de segurança, os dados devem estar em uma máquina exclusiva para a CVM. Outro tópico do edital é que a responsabilidade pela infraestrutura continuará com a Oracle, com a CVM no controle do equipamento.
Ao término do processo, a CVM fará um contrato de modelo de implantação de nuvem do tipo:
(A) pública;
(B) privada;
(C) comunitária;
(D) híbrida;
(E) infraestrutura como serviço.

Serviços de Computação em Nuvem

Texto 1
Um órgão público contratou uma solução de computação em nuvem que fica hospedada em seu datacenter para uso exclusivo do órgão. A gerência do hardware é realizada pela empresa contratada. A equipe do órgão é responsável pela gerência do Sistema Gerenciador de Banco de Dados (SGBD) utilizado e pelas tarefas de criação e gestão das bases de dados. Internamente será ofertado o provisionamento de bancos de dados para sistemas corporativos dos clientes internos do órgão.

16

Considerando a situação descrita no texto 1, o tipo de serviço em nuvem ofertado pelo órgão público aos seus clientes internos é o:
(A) IaaS;
(B) DaaS;
(C) SaaS;
(D) PaaS;
(E) NaaS.

17

Considerando a situação descrita no texto 1, a nuvem contratada pelo órgão público é do tipo:
(A) privada;
(B) híbrida;
(C) on premisse;
(D) pública;
(E) edge.

18

Um órgão público contratou serviço de um provedor de computação em nuvem pública no modelo SaaS (*Software as a Service*), mas, por ter dados sigilosos, contratou também uma solução de nuvem privada para manipulá-los, em consonância com a LGPD (Lei Geral de Proteção de Dados). Os requisitos tecnológicos para ambas as soluções são iguais, porém o órgão possui apenas uma conexão com a internet para intercambiar informações entre as soluções contratadas.

Uma vantagem da nuvem privada em relação à nuvem pública contratada é o(a):

(A) menor demanda de profissionais do órgão para administrar a solução;
(B) maior controle na administração e configuração da infraestrutura;
(C) maior confiabilidade devido ao maior número de provedores de infraestrutura de comunicação;
(D) maior desempenho devido às configurações dos equipamentos tecnológicos;
(E) maior elasticidade por causa da maior quantidade de equipamentos envolvidos na solução.

19

Para reduzir o recebimento de e-mails falsos de outros domínios, a equipe de Tecnologia da Informação (TI) do órgão configurou o SPF (*Sender Policy Framework*) em seus servidores de domínio que estão hospedados na nuvem. Foi realizada uma configuração no SPF para permitir que uma mensagem não seja rejeitada caso a consulta ao domínio de origem informe que o IP do servidor de e-mail não está cadastrado, implementando-se assim a técnica de greylisting.

A configuração SPF realizada pela equipe de TI foi:

(A) Fail;
(B) SoftFail;
(C) Pass;
(D) Neutral;
(E) TempError.

20

A fim de incrementar a reputação do domínio da organização, a equipe de Tecnologia da Informação (TI) adotou o DMARC (*Domain-based Message Authentication, Reporting & Conformance*) para a autenticação de seus e-mails, implementando uma política que salva e-mails que apresentam falhas de autenticação na pasta de spam.

A política DMARC implementada pela equipe de TI é a:

(A) none;
(B) relaxed mode;
(C) quarantine;
(D) strict mode;
(E) reject.

21

Em uma organização, para garantir a autenticidade do emissor e a integridade do e-mail enviado, foi implementado o processo de autenticação DKIM.

Sobre o DKIM é correto afirmar que:

(A) utiliza criptografia simétrica;
(B) a chave pública para validação da assinatura fica disponível no servidor de DNS;
(C) a chave privada para assinatura do e-mail fica disponível no servidor de e-mail;
(D) seu uso não altera o cabeçalho da mensagem;
(E) criptografa o e-mail inteiro.

22

A analista Vanesa foi designada para configurar um Tenant do Office 365 para uma empresa de médio porte que deseja migrar todos os seus serviços de e-mail para a nuvem. Ela precisa garantir que a configuração esteja otimizada para segurança, desempenho e conformidade.

Considerando as melhores práticas para a configuração de um Tenant do Office 365, a ação que a analista Vanesa deve executar é:

(A) definir políticas de senha fracas para facilitar o acesso dos usuários;
(B) habilitar o *Multi-Factor Authentication* (MFA) para todas as contas de usuário;
(C) configurar todos os usuários para usar apenas o protocolo POP3, pois é o mais antigo e testado;
(D) desativar o acesso ao Exchange Online para evitar possíveis ataques cibernéticos;
(E) permitir o auto-forwarding de e-mails para domínios externos para promover a flexibilidade de comunicação.

23

O analista Gabriel está avaliando a implementação de uma arquitetura serverless para um projeto estratégico na empresa de tecnologia onde atua. Ele sabe que essa arquitetura oferece diversas vantagens, especialmente no que diz respeito à gestão de infraestrutura. No entanto, ele também está ciente dos desafios e limitações.

No que se refere à arquitetura serverless, é correto afirmar que:

(A) ela exige que a equipe de TI gerencie ativamente servidores, sistemas operacionais e redes para assegurar a escalabilidade e a disponibilidade do aplicativo;
(B) em um modelo serverless, o provedor de serviços em nuvem gerencia a alocação e a escala da infraestrutura de backend automaticamente, embora isso possa resultar em custos significativamente mais elevados do que os modelos de computação tradicionais, independentemente do volume de uso;
(C) ela permite que os desenvolvedores se concentrem exclusivamente no desenvolvimento do código e na lógica do aplicativo, sem preocupações com a infraestrutura subjacente, que é totalmente gerenciada pelo provedor de serviços em nuvem;
(D) ela não é adequada para aplicações que exigem processamento em tempo real devido à latência introduzida pelo tempo de inicialização do ambiente de execução;
(E) ela tem como desvantagem a impossibilidade de rodar aplicações em ambientes offline, já que depende estritamente da conexão com o provedor de serviços em nuvem para executar qualquer funcionalidade.

24

O analista Micael está trabalhando em um projeto de automação de infraestrutura para uma grande empresa de tecnologia. Ele decidiu utilizar o Ansible para automatizar a implantação e configuração de servidores na nuvem, visando a melhorar a eficiência e a consistência dos ambientes de computação. Ao configurar seus playbooks no Ansible, ele se deparou com um desafio relacionado à melhor prática para garantir que os scripts sejam idempotentes e reutilizáveis em diferentes ambientes de nuvem.

A melhor prática a ser adotada pelo analista Micael é:

(A) utilizar comandos shell e scripts personalizados dentro dos playbooks para instalação de pacotes e serviços;
(B) utilizar hardcoding de senhas e chaves de API diretamente nos playbooks do Ansible;
(C) evitar o uso de variáveis e templates para configurar os serviços, optando por valores fixos nos playbooks;
(D) utilizar módulos específicos de provedores de nuvem para criar e gerenciar recursos, evitando a abstração;
(E) empregar roles e variáveis para modularizar os playbooks, facilitando a reutilização e a customização em diferentes ambientes.

25

Durante a implementação de uma solução de e-mail corporativo baseada na nuvem, o analista Daniel enfrenta um desafio de segurança complexo. Ele precisa garantir que apenas os funcionários autorizados possam acessar seus e-mails, tanto internamente quanto externamente, de forma segura e eficiente, sem comprometer a facilidade de uso ou a segurança dos dados.

Considerando os mecanismos de autenticação e autorização modernos, a abordagem que ele deve adotar para atender a esses requisitos é:

(A) implementar autenticação baseada em OAuth, pois ela permite que os aplicativos de terceiros acessem os e-mails dos usuários sem exigir suas credenciais diretamente, utilizando tokens de acesso;
(B) utilizar autenticação básica com nome de usuário e senha, por ser uma abordagem simples e direta, fácil de implementar e usar;
(C) adotar SAML (*Security Assertion Markup Language*) para autenticação e autorização, permitindo que os funcionários usem um único conjunto de credenciais para acessar vários serviços, incluindo e-mail;
(D) implementar um sistema de autenticação multifator (MFA) sem nenhuma outra forma de autenticação ou autorização, confiando singularmente na posse de dispositivos físicos pelos usuários;
(E) recorrer exclusivamente ao uso de certificados digitais para autenticação, assegurando que apenas dispositivos com os certificados corretos possam acessar os e-mails.

26

Ao abordar a configuração de um Tenant no Office 365 para uma organização internacional, o analista Aaron enfatiza a importância de adaptar o ambiente às normativas e exigências locais de cada região de forma direta e eficaz.

Nesse contexto, a medida que assegura a conformidade e atende às necessidades específicas de cada localidade é:

(A) estabelecer a mesma zona horária para todos os usuários;
(B) adotar um único idioma para toda a organização;
(C) definir políticas de retenção de dados específicas por região;
(D) restringir o acesso aos aplicativos do Office conforme a localização;
(E) conceder licenças de usuário com base em um único país.

27

Iniciando a configuração de um Tenant no Office 365, a analista Ana Clara destaca uma etapa crucial para habilitar o uso dos serviços pela organização.

Nesse contexto, a ação essencial para que Ana Clara comece a utilizar os serviços do Office 365 é:

(A) estabelecer um servidor local de Active Directory;
(B) criar ao menos um usuário administrador;
(C) executar a instalação local de todos os aplicativos do Office;
(D) adquirir um certificado SSL;
(E) implementar uma VPN.

28

Andrew, um analista, foi contratado por uma empresa de contabilidade de médio porte, com 50 funcionários, para solucionar problemas com seu sistema de e-mail baseado em servidor local. Devido ao crescimento da empresa e ao aumento do volume de comunicações, o sistema se tornou insuficiente, apresentando falta de espaço de armazenamento, dificuldades de acesso remoto e vulnerabilidades de segurança. Para modernizar sua infraestrutura de comunicação, a empresa optou por migrar para uma solução de hospedagem de e-mail na nuvem.

Nesse contexto, o objetivo de Andrew ao escolher a solução de hospedagem de e-mail na nuvem foi:

(A) impedir a possibilidade de recuperação de dados em caso de desastres;
(B) implementar redundância integrada, o que permitiu a restauração rápida e eficiente dos dados perdidos;
(C) instituir protocolos de backups manuais regulares, apesar da infraestrutura de nuvem já em uso;
(D) prolongar deliberadamente o processo de recuperação de dados para testar a resiliência organizacional;
(E) restringir o acesso aos dados recuperados a locais específicos, visando a aumentar a segurança pós-recuperação.

29

Para implementar uma solução eficaz na empresa onde trabalha, o analista Ted precisa escolher a melhor definição para serviços de e-mail na nuvem.
Um serviço de e-mail na nuvem pode ser corretamente descrito como:
(A) uma plataforma que oferece singularmente armazenamento de e-mails em servidores remotos, acessíveis apenas pela equipe de TI da empresa;
(B) um serviço que permite o envio e recebimento de e-mails usando servidores locais, garantindo maior segurança e controle sobre os dados;
(C) uma solução baseada na Internet que proporciona a empresas e indivíduos a capacidade de enviar, receber, armazenar e gerenciar e-mails, sem a necessidade de manter a infraestrutura de servidores de e-mail internamente;
(D) um tipo de serviço de e-mail que criptografa automaticamente todas as mensagens enviadas e recebidas, tornando-o exclusivo para comunicações governamentais;
(E) uma ferramenta que converte e-mails recebidos em mensagens de texto SMS, facilitando o acesso rápido à comunicação sem a necessidade de Internet.

30

O analista André foi contratado para aprimorar os protocolos de segurança de uma organização. Ele está ciente de que a eficácia do sistema de segurança depende crucialmente da correta implementação e compreensão dos mecanismos de autenticação e autorização.
Nesse contexto, é correto afirmar que:
(A) a importância da autenticação reside em assegurar que os usuários acessem exclusivamente os recursos que lhes são explicitamente permitidos;
(B) a autorização é caracterizada por elementos que apenas os usuários possuem e conhecem, podendo ser implementada através de diversas metodologias;
(C) a expressão "algo que você tem" é aplicável a elementos como senhas, PINs e respostas para perguntas de segurança;
(D) o foco da autenticação está em confirmar a identidade alegada pelo usuário, assegurando que ele é, de fato, quem diz ser;
(E) o objetivo da autenticação é definir as permissões e atividades acessíveis ao usuário após sua identidade ser confirmada.

Infraestrutura de Servidores

31

O LDAP é utilizado como base de autenticação para vários sistemas de uma organização. Para aumentar a disponibilidade, foi criada uma estrutura com dois servidores master que replicam os dados entre si (master x master ou multimaster) e replicam os dados para 2 servidores slaves (master x slave). Foi utilizada a versão 2.4 do OpenLdap.
Sobre a replicação dos dados no LDAP, é correto afirmar que:
(A) os clientes LDAP podem consumir os dados em todos os servidores (master e slave);
(B) durante a replicação master x master, ambos os servidores se comportam como fornecedores dos dados simultaneamente;
(C) a replicação multimaster permite o balanceamento de carga entre os servidores;
(D) na replicação master x slave, os servidores slaves aceitam operações de leitura e escrita;
(E) na replicação master x slave, o servidor slave pode ser tornar master, em caso de indisponibilidade do servidor master.

32

Um órgão adquiriu um novo sistema de circuito fechado de TV (CFTV) para armazenar as imagens das câmeras de monitoramento de seu datacenter. O CFTV é composto por 32 câmeras IP, um servidor e um storage DAS, dedicados ao processamento e armazenamento das imagens.
Sobre o storage DAS, é correto afirmar que:
(A) é acessível por meio de um servidor via conexão SCSI ou USB;
(B) possui sistema operacional próprio, operando como uma unidade de armazenamento em rede autônoma;
(C) pode ser conectado a uma rede por meio de switches ethernet;
(D) pode ser conectado a uma rede SAN via fabric switches;
(E) precisa de zoneamento para que o servidor acesse o storage.

33

Um sistema de gestão de documentos administrativos possui o plano de backup a seguir, com a execução das cópias dos dados, realizadas sempre às 23:00 do dia, com RPO (*Recovery Point Object*) de 24 horas. O backup completo possui duração de 240 minutos e o backup diferencial, de 25 minutos.

- Dia 1 – backup completo
- Dia 2 – backup diferencial
- Dia 3 – backup diferencial
- Dia 4 – backup diferencial

No dia 5, o administrador do sistema identificou uma invasão no servidor que acarretou o comprometimento dos dados a partir de 22:15h do dia 4. Para recuperar o sistema, o administrador instalou um novo servidor e precisou restaurar o backup íntegro e mais atualizado anterior à invasão, que atendesse ao RPO definido.
Para atender aos requisitos de recuperação do sistema, o administrador restaurou sequencialmente os backups dos dias:
(A) Dia 1 + Dia 2 + Dia 3 + Dia 4;
(B) Dia 1 + Dia 2 + Dia 3;
(C) Dia 1 + Dia 2;
(D) Dia 1 + Dia 3;
(E) Dia 1 + Dia 4.

34

Um órgão implementou o Zabbix para monitoramento de sua infraestrutura crítica de Tecnologia da Informação (TI). Para incrementar a segurança, foi implementada criptografia usando o Protocolo *Transport Layer Security* (TLS) v.1.3 na comunicação entre os seus componentes.

A criptografia implementada no Zabbix pela equipe de TI permite:

(A) armazenar as chaves privadas criptografadas em arquivos legíveis pelos componentes do Zabbix durante a inicialização;
(B) proteger as comunicações entre o servidor web rodando o frontend Zabbix e a web do usuário navegador;
(C) usar diferentes configurações de criptografia nos servidores (proxy) para diferentes anfitriões;
(D) abrir uma conexão criptografada com um handshake TLS completo, implementando cache de sessão e tickets;
(E) realizar a descoberta de rede de ativos com criptografia ativada.

35

Camila trabalha na empresa Z, que presta serviços para a Comissão de Valores Mobiliários (CVM). Na busca por uma solução que faça a orquestração de contêineres para automatizar a implantação, dimensionamento e gerenciamento de aplicativos, a CVM escolheu o Kubernetes. De forma a implantar um cluster kubernetes completo e funcional, alguns componentes precisam ser implementados. Trabalhando na camada de gerenciamento e observando os Pods recém-criados e que ainda não foram atribuídos a um nó, Camila seleciona um nó para executá-los.

Camila está trabalhando no componente:

(A) kube-controller-manager;
(B) kube-apiserver;
(C) etcd;
(D) kube-scheduler;
(E) cloud-controller-manager.

36

Renata está buscando uma solução para seu negócio de Tecnologia da Informação de forma a ter informações rápidas, de fácil atualização, alta disponibilidade e principalmente muita segurança. Após um estudo de mercado, ela entendeu que o Active Directory pode oferecer todos esses atributos. Com o objetivo de permitir o acesso com segurança usando apenas um conjunto de credenciais, Renata está habilitando o single sign on.

Para essa habilitação, Renata deverá atuar no seguinte elemento do Active Directory:

(A) *Active Directory Domain Services* (ADDS);
(B) *Active Diretory Certificate Services* (ADCS);
(C) *Active Directory Federation Services* (ADFS);
(D) *Active Directory Lightweight Directry Services* (ADLDS);
(E) *Active Directory Rights Management Services* (ADRMS).

37

Virgínia está fazendo manutenção no servidor de DNS (*Domain Name Server*) da Comissão de Valores Mobiliários. Ela precisa criar um nome alternativo para si, em virtude de sua mudança para um departamento que possui um domínio diferente. Todos, porém, já conhecem seu endereço.

Com o objetivo de orientar pessoas e programas na direção correta da entrega de mensagens, Virgínia deverá criar uma entrada dentro dos conjuntos de registros do tipo:

(A) NS;
(B) CNAME;
(C) MX;
(D) SOA;
(E) SRV.

38

A empresa K está implementando uma solução de autenticação de segurança baseada no protocolo RADIUS com objetivo de melhorar a segurança em sua rede sem fio. Para a execução dessa tarefa, a empresa está buscando um arcabouço de autenticação que forneça autenticação mútua e baseada em certificados do cliente e da rede por meio de um canal criptografado (ou túnel), bem como um meio para derivar chaves WEP dinâmicas, por usuário e por sessão. O arcabouço também deve requerer apenas certificados do lado do servidor.

A empresa K implementará o método de protocolo de autenticação extensível (EAP) denominado:

(A) EAP-MD5;
(B) EAP-TLS;
(C) AP-SIM;
(D) EAP-AKA;
(E) EAP-TTLS.

39

Maria está trabalhando em um contador de desempenho para sua empresa de forma que ele gere relatórios de desempenho e informe caso se chegue a valores limites. Ela está executando essa atividade a partir de um aplicativo de Serviço Windows que escuta os dados do contador de desempenho, implanta o aplicativo e começa a coleta e a análise de dados. Maria fez uma configuração indicando o que deve acontecer quando o serviço continua o funcionamento normal depois de ter sido colocado em pausa.

Para executar essa etapa, Maria fez uso do método:

(A) OnContinue;
(B) OnCustomCommand;
(C) OnPowerEvent;
(D) OnPause;
(E) OnStart.

40

Gomes foi contratado pela Comissão de Valores Mobiliários (CVM) para fazer uma alteração nas diretivas do servidor Apache da CVM. Ele solicitou uma modificação na pasta raiz indicando a partir de qual pasta do servidor os arquivos e pastas contidos na URL solicitada serão pesquisados.

Desse modo, assumindo o caminho como /opt/www, se a URL solicitada for http://www.cvm.com/9.10/index.html, o arquivo index.html será procurado na pasta /opt/www/9.10.

Gomes deverá alterar a configuração na diretiva:

(A) DocumentRoot;
(B) DirectoryIndex;
(C) ServerRoot /etc/apache2;
(D) MaxSpareServers;
(E) UserDir public_html.

Infraestrutura de Redes

41

Considere uma árvore que contém todo e qualquer nó em um grafo, mais formalmente, uma spanning tree de um grafo $G = (N, E)$ e um grafo $G' = (N, E')$ tal que E' *é* um subconjunto de E, G' *é* conectado, G' não contém nenhum ciclo e G' contém todos os nós originais em G.

Se cada enlace tiver um custo associado e o custo de uma árvore for a soma dos custos dos enlaces, é correto afirmar que uma árvore cujo custo seja o mínimo entre todas as spanning trees é denominada:

(A) spanning tree mínima;
(B) spanning tree máxima;
(C) spanning tree de diâmetro mínimo;
(D) spanning tree de diâmetro máximo;
(E) spanning tree geradora de caminho máximo.

42

Analisando um roteador e a política de roteamento, João, analista do CVM, identificou que:

I. o equipamento recebeu duas rotas distintas para o mesmo prefixo e aceitou;
II. a preferência local da rota foi estabelecida por esse roteador ou foi descoberta por outro roteador no mesmo AS;
III. a decisão do item II é política e fica a cargo do administrador de rede do AS.

Para definir a rota escolhida, João identificou que:

(A) apesar de as rotas terem o mesmo valor de preferência local, a rota selecionada tem o comprimento AS-PATH mais longo;
(B) apesar de as rotas terem o mesmo comprimento de AS-PATH, a rota selecionada tem o valor de preferência local mais baixo;
(C) apesar de as rotas terem o mesmo comprimento de AS-PATH, e o mesmo valor de preferência local, a rota selecionada é baseada nos identificadores BGP;
(D) apesar de as rotas terem o mesmo comprimento de AS-PATH e o mesmo valor de preferência local, a rota selecionada será a que tem o roteador next-hop com menor custo;
(E) apesar de as rotas terem o mesmo comprimento de AS-PATH, o mesmo valor de preferência local e o mesmo custo de caminho do roteador next-hop, a rota selecionada será aleatória.

43

Claudio, analista de TI, ao identificar um problema na camada de enlace, pediu apoio ao técnico Luís para efetuar diversos testes com os equipamentos a fim de analisar todo o funcionamento dos equipamentos envolvidos.

No que se refere ao funcionamento da camada de enlace, é correto afirmar que:

(A) códigos de CRC também são conhecidos como códigos polinomiais, já que é possível considerar a cadeia de bits a ser enviada como um polinômio cujos coeficientes são os valores 0 e 1 na cadeia;
(B) técnicas de detecção e correção permitem que o receptor sempre descubra a ocorrência de erros de bits, enquanto técnicas mais sofisticadas de detecção e correção de erros ficam sujeitas a uma sobrecarga maior;
(C) cada padrão de CRC pode detectar erros de rajada de menos do que $r + 1$ bits. Além disso, em hipóteses apropriadas, uma rajada de comprimento maior do que $r + 1$ bits é detectada com probabilidade de $2 - 0{,}5r$;
(D) todos os cálculos de CRC são feitos por aritmética de módulo 2 sem "vai 1" nas adições nem "empresta 1" nas subtrações. Isso significa que a adição e a subtração são idênticas e ambas são equivalentes à operação *OU(OR)*bit a bit dos operandos;
(E) um método simples de soma de verificação é multiplicar inteiros de k bits e somar o total resultante com bits de detecção de erros. A soma de verificação da Internet é baseada nessa técnica, em que bytes de dados são tratados como inteiros de 16 bits.

44

No que se refere ao funcionamento de uma conexão TCP, é correto afirmar que:

(A) durante a apresentação de três vias, o processo cliente bate na porta de entrada do processo servidor. Quando o servidor "ouve" a batida, aloca uma porta (mais precisamente, um socket) compartilhada entre diversos clientes;
(B) ao criar a conexão TCP, associamos a ela o endereço de socket (apenas o número de porta) do cliente e do servidor. Com a conexão estabelecida, quando um lado quer enviar dados para o outro, basta deixá-los na conexão TCP por meio de seu socket;
(C) com o processo servidor em execução, ele pode iniciar uma conexão TCP com o cliente, o que é feito no programa cliente pela criação de um socket TCP. Quando cria seu socket TCP, o servidor especifica o endereço do socket receptivo do cliente;
(D) como acontece no UDP, o programa servidor TCP precisa rodar como um processo antes de o cliente tentar iniciar contato, e o programa servidor tem de ter algum socket especial que acolha algum contato inicial de um processo cliente que esteja rodando em um hospedeiro qualquer;
(E) do ponto de vista da aplicação, o socket do cliente e o de conexão do servidor estão conectados diretamente, e o processo servidor pode enviar bytes para seu socket de modo arbitrário; entretanto, o TCP não garante que o processo servidor receberá cada byte na ordem em que foram enviados.

45

Após uma determinada rede receber ataques de DNS spoofing, foi sugerida a implantação do DNSsec.
Acerca desse assunto, é correto afirmar que:
(A) sigilo é um serviço oferecido, pois todas as informações no DNS são consideradas privadas;
(B) o DNSsec também admite alguns tipos de registros. O registro CERT pode ser usado para armazenar certificados;
(C) DNSsec oferece três serviços, que são a prova onde os dados se originaram, distribuição de chave privada e autenticação de transação e solicitação;
(D) o segundo entre os novos tipos de registros é o registro *SIG*. Ele contém o hash assinado de acordo com o algoritmo especificado no registro *ALG;*
(E) *o*s registros DNS são agrupados, em conjuntos chamados RRreg, com todos aqueles que têm o mesmo nome e o mesmo tipo.

46

Foi configurado o Snort com a seguinte regra:

Alert tcp $BINARIO any - > $HEXA any\
(msg: "SCAN SYN FIN" flags: SF, 12;\
reference: arachnids, 198: classtype: attempted

Analisando a regra acima, é correto afirmar que:
(A) está sendo especificada a porta 12 como origem;
(B) está sendo especificada a porta 198 como destino;
(C) está sendo verificado apenas se os bits SYN e FIN estão com valor 1;
(D) a "\" é reservada no Snort e está sendo usada para escrever instruções em uma única linha;
(E) os nomes $BINARIO e $HEXA são nomes de variáveis predefinidos para especificar tipos de arquivos.

47

Luís, analista da CVM, recebeu do encarregado de segurança a demanda de especificar um equipamento que seja capaz de fazer o controle de serviço, de direção, de usuário e de comportamento.
Luís especificou um:
(A) ids;
(B) snort;
(C) dnssec;
(D) firewall;
(E) proxy de aplicação.

48

No que se refere ao funcionamento do protocolo SIP, é correto afirmar que:
(A) o chamador, para estabelecer uma sessão, cria uma conexão TCP com o chamado e envia uma mensagem INVITE sobre ela, ou então envia a mensagem INVITE em um pacote UDP;
(B) os números de telefones no SIP são representados como URLs que utilizam o esquema SIP. Os URLs do SIP também podem conter endereços IPv4 e endereços IPv6, mas não números de telefone reais;
(C) ele é um protocolo de texto modelado sobre o HTTP. Uma parte envia uma mensagem em texto binário que consiste em nome do método na primeira linha, seguido por linhas adicionais contendo cabeçalhos para passar parâmetros;
(D) o método OPTIONS se relaciona com a habilidade do SIP de localizar um usuário que está longe de casa e se conectar a ele. Essa mensagem é enviada a um servidor de localização do SIP que controla a localização de cada usuário;
(E) o método REGISTER é usado para consultar uma máquina sobre seus próprios recursos. Em geral, ele é usado antes de uma sessão ser iniciada, a fim de descobrir se essa máquina é capaz de se comunicar usando voz sobre IP ou se está sendo utilizado qualquer outro tipo de sessão.

49

Jorge recebeu a demanda de fazer a distribuição de IP para novos departamentos da CVM, baseado nas informações a seguir.
I. o range 172.16.0.0/20 é o único que está disponível para esse projeto;
II. o departamento de material terá 255 notebooks;
III. o departamento de TI terá 200 máquinas e 200 telefones IP conectados;
IV. cada telefone será conectado ao switch por um cabo de rede;
V. cada máquina será conectada à rede por um cabo de rede conectado ao telefone, onde houver telefone;
VI. o departamento de inteligência terá 15 máquinas, sendo somente 4 delas conectadas à rede, por questões de segurança.
Atendendo às premissas acima, é correto afirmar que Jorge deve configurar:
(A) o gateway do departamento de inteligência com o IP 172.16.14.1, máscara 255.255.255.252 e as máquinas no bloco 172.16.14.248/30, excluindo o IP do gateway, para que as devidas máquinas se conectem à rede;
(B) o gateway do departamento de inteligência com o IP 172.16.14.249, máscara 255.255.255.248 e as máquinas no bloco 172.16.14.248/29, excluindo o IP do gateway, para que as devidas máquinas se conectem à rede;
(C) o gateway do departamento de material com o IP 172.16.0.1, máscara 255.255.255.0 e os notebooks no bloco 172.16.0.0/24, excluindo o IP do gateway, para que todas as máquinas do departamento citado se conectem à rede;
(D) o gateway do departamento de TI com o IP 172.17.16.1, máscara 255.255.254.0 e as máquinas no bloco 172.17.16.0/23, excluindo o IP do gateway, para que todas as máquinas e telefones do departamento citado se conectem à rede;
(E) o gateway do departamento de TI com o IP 172.16.0.1, máscara 255.255.255.0 e as máquinas e os telefones IP no bloco 172.16.0.0/24, excluindo o IP do gateway, para que todas as máquinas e telefones do departamento citado se conectem à rede.

50

Analise os registros a seguir.

```
cvm.com  86400  IN  A    35.1.4.5
cvm.com  86400  IN  KEY  36367503A8B848F527225B7EF…
cvm.com  86400  IN  SIG  86947503A8B848F527225850C6…
```

Em relação a esses registros, é correto afirmar que o:
(A) registro KEY é a chave privada de cvm;
(B) registro do tipo A contém um endereço IPv4 ou IPv6;
(C) registro SIG contém o hash assinado do servidor *com* de nível superior dos registros A e KEY;
(D) tempo de vida fornece uma indicação de estabilidade do registro, que, no caso acima, é de 60 dias;
(E) tempo de vida fornece uma indicação de estabilidade do registro, que, no caso acima, é de 60 horas.

Banco de Dados

51

João trabalha na filial de uma multinacional no Rio de Janeiro (GMT-3) e recebeu alguns relatórios da sede da empresa localizada na Califórnia (GMT-8). Durante a verificação, João identificou uma tabela com uma coluna que trazia informações de timestamp e timezone da sua filial e não da sede onde o relatório havia sido gerado. João entrou em contato com a sede para relatar o ocorrido, pois, se o relatório foi feito na Califórnia, deveria estar com as configurações de timestamp e timezone da sede. Entretanto, a sede da empresa informou que tabela anexada ao relatório teve seu campo definido como:
(A) localtimestamp;
(B) current_timestamp;
(C) timestamp;
(D) timestamp with timezone;
(E) timestamp with local timezone.

52

Lara trabalha em uma empresa aérea e todos os dias, às 17:00, é gerado por ela um relatório com o número total de reservas em todos os voos de sua companhia. Porém, ao apresentar o relatório ao seu encarregado, ela vem notando que o número total tem mostrado inconsistências. O relatório calculava incorretamente a quantidade de reservas, pois pegava alguns dados de antes do cálculo do número total e outros de depois desse cálculo.
Lara pesquisou o problema na transação e o identificou como:
(A) atualização temporária;
(B) atualização perdida;
(C) resumo incorreto;
(D) leitura não repetitiva;
(E) bloqueio exclusivo.

53

Karen está atuando junto à Comissão de Valores Mobiliários (CVM) para a melhoria da performance das consultas aos bancos de dados. Após algumas verificações, ela chegou à conclusão de que o banco deveria executar sua indexação das linhas de uma tabela com base no resultado da chamada de alguma função especificada sobre os valores das linhas, em vez de indexar com base nos valores em si.
Isso significa que os índices criados por Karen deverão ser índices:
(A) multitabelas;
(B) bitmap;
(C) funcionais;
(D) multiníveis dinâmicos;
(E) em árvore B.

54

Anualmente, a Comissão de Valores Mobiliários (CVM) efetua a contratação da empresa X para executar uma auditoria em sua base de dados, de forma a manter a segurança e conformidade. Entretanto, a CVM efetuou a contratação da empresa Y apenas seis meses após a última auditoria. Essa empresa terá uma abordagem mais direcionada, concentrando-se em áreas críticas do banco de dados.
Logo, a empresa Y deverá assinar com a CVM um contrato de execução de uma auditoria do tipo:
(A) tradicional;
(B) exclusão de riscos;
(C) alterações;
(D) análise de desempenho;
(E) integridade.

55

Davi, um *Database Administrator* (DBA) que trabalha na Comissão de Valores Mobiliários, identificou, em sua base de dados SQL Server, que muitas operações efetuadas no banco não tinham rastreamento. Com o objetivo de identificá-las, ele iniciou a configuração de auditoria dos dados iniciando com as operações CREATE, ALTER e DROP para qualquer objeto de servidor.
Os itens de auditoria a serem configurados por Davi formam um grupo de ações chamadas:
(A) server_object_change_group;
(B) server_object_ownership_change;
(C) server_operation_group;
(D) server_principal_impersonation_group;
(E) server_state_change_group.

56

Durante uma manutenção de rotina, a equipe de banco de dados Oracle da Comissão de Valores Mobiliários identificou que uma tablespace de sistema estava com um crescimento descontrolado. Ao refinar a pesquisa, observou que os registros de auditoria ainda estavam com a sua tablespace default.
Conforme a documentação de melhores práticas da Oracle, é recomendado que seja criada uma tablespace específica para os dados de auditoria e que estes sejam removidos da tablespace:
(A) system;
(B) users;
(C) temp;
(D) sysaux;
(E) undo.

57

Gabriela é a administradora dos bancos de dados gerenciados pelo PostgreSQL de uma instituição. Ela está monitorando o espaço em disco utilizado por algumas tabelas dos bancos de dados por meio da inspeção do catálogo do sistema, que foi recentemente atualizado por outra operação.
Gabriela está usando o seguinte comando SQL:

(A) SELECT relpages
FROM pg_class
WHERE relname = 'mytable';

(B) SELECT relsize
FROM pg_database
WHERE relname = 'mytable';

(C) SELECT tabsize
FROM pg_relations
WHERE tabname = 'mytable';

(D) SELECT *
FROM pg_table_size
WHERE tabname = 'mytable';

(E) SELECT relation
FROM pg_data
WHERE relname = 'mytable'.

58

Existem diferentes tipos de privilégios aplicáveis aos objetos de um banco de dados. O comando SQL abaixo será executado em uma instância de banco de dados mantida pelo PostgreSQL:

GRANT USASE ON SCHEMA objeto1 TO objeto2;

O resultado da execução do comando acima resultará na concessão de privilégios para que a role:
(A) procure e acesse objetos contidos no esquema;
(B) utilize as funções dos esquemas currval e nextval;
(C) crie funções em esquemas de uma determinada linguagem;
(D) defina tipos e domínios na criação de esquemas de tabelas;
(E) leia os nomes dos objetos do esquema no catálogo do sistema.

59

A aplicação JUNTAWeb usa um banco de dados NoSQL para armazenar as relações entre documentos de interesse, tais como: legislações federais e estaduais, normas de comitês internacionais, normas internas e procedimentos de nível operacional, juntamente com seus conjuntos de metadados. O JUNTAWeb possibilita que seus usuários tenham ampla rastreabilidade do ciclo de vida e das relações entre os documentos de interesse.
Considerando a necessidade de rastreabilidade entre os documentos de interesse, a estrutura do banco de dados NoSQL, aderente à demanda, deve estar baseada em:
(A) conjuntos de links organizados em esquemas semânticos de modo estruturado;
(B) células agrupadas em colunas organizadas por tipo de documento;
(C) associações de dados das coleções a registros identificados com chaves exclusivas;
(D) matrizes associativas utilizadas como um banco de dados semiestruturado na qual uma chave individual é vinculada a um valor em uma coleção;
(E) modelos que não tenham esquema mas que possibilitem que as associações sejam armazenadas direta e explicitamente na base de dados.

60

BDFree é um banco de dados distribuído que utiliza uma estrutura de armazenamento NoSQL. No BDFree quaisquer solicitações retornam respostas válidas em um intervalo de tempo razoável, independentemente da aplicação que o utiliza, devido ao cumprimento da propriedade que:
(A) viabiliza que cada cliente tenha a mesma visão dos dados;
(B) mantém cópias de itens de dados visíveis para várias transações;
(C) assegura que cada requisição receba a informação mais recente ou um erro;
(D) garante que partes da estrutura do banco de dados que estejam desativadas sejam ignoradas;
(E) replica dados entre as estruturas do banco de dados antes que a gravação seja considerada bem-sucedida.

Projetos e Governança TI

61

Ao assumir nova função na CVM, o analista Pedro ficou responsável por acompanhar todos os projetos de seu departamento. Sua primeira iniciativa foi solicitar que todos os gerentes de projeto acompanhassem de perto a execução orçamentária dos seus projetos. Além disso, ele determinou que, devido a cortes orçamentários, todos os projetos tivessem seu orçamento previsto diminuído em 10%.
Na gerência do ciclo de vida do projeto, a determinação do corte orçamentário, solicitada por Pedro, é classificada como:
(A) tendência;
(B) restrição;
(C) limitação;
(D) requisito;
(E) critério.

62

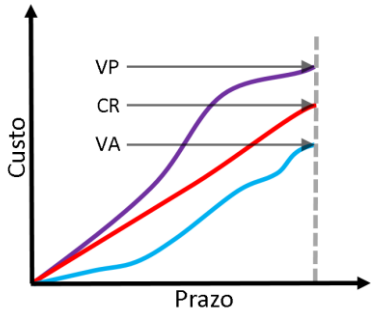
Ao assumir seu cargo na CVM, a analista Maria ficou responsável por fiscalizar o contrato do Projeto ABC, de responsabilidade da empresa Y. Esse contrato possui baixo valor, se comparado aos demais projetos da CVM. Na primeira reunião, a empresa Y apresentou os principais pontos do projeto, mas não apresentou o documento gerencial que define a Estrutura Analítica do Projeto (EAP). Maria solicitou, então, que a empresa confeccionasse a EAP, mas esta argumentou que o projeto era "pequeno" e, portanto, a EAP não era necessária. Ainda, a empresa afirmou que a confecção da EAP acarretaria perda de tempo e alegou que essa tarefa não era de sua responsabilidade, dado que não estava prevista em contrato.

Quanto ao cenário descrito, no que se refere à EAP e à responsabilidade por sua confecção, é correto afirmar que a EAP:

(A) é uma decomposição hierárquica do escopo total do trabalho a ser realizado pela equipe do projeto para cumprir seus objetivos e criar as entregas necessárias, assim sendo de responsabilidade da empresa a sua confecção;
(B) não é necessária em projetos de pequeno porte, dada a necessidade de otimizar o tempo e recursos alocados, sendo de responsabilidade do fiscal, caso deseje, a sua confecção;
(C) tem a finalidade de consolidar o projeto em um organograma, facilitando a sua apresentação para as partes envolvidas, não sendo de importância gerencial, e não tendo, portanto, responsável pela sua confecção;
(D) é a ferramenta que mostra as interdependências entre os pacotes de trabalho do projeto, assim sendo de responsabilidade da empresa a sua confecção;
(E) é ferramenta essencial para a realização do projeto e não pode ser substituída por outro instrumento gerencial, de modo que o projeto deve ser parado até a sua confecção.

63

O gerente de um projeto apresentou o seguinte extrato da curva de gerenciamento do valor agregado até o presente momento, onde VP, CR e VA são, respectivamente: valor planejado, custo real e valor agregado.



A partir do gráfico apresentado pelo gerente, conclui-se que o projeto está:

(A) no prazo e mais barato que o orçado inicialmente;
(B) adiantado e mais barato que o estimado inicialmente;
(C) atrasado, porém mais barato que o orçado inicialmente;
(D) mais barato, porém não está agregando valor;
(E) atrasado e mais caro que o orçado inicialmente.

64

A área de TI da CVM irá iniciar um novo projeto com as seguintes características:

- há baixo grau de inovação, tendo em vista que projetos similares já foram realizados na Administração Pública;
- os requisitos estão muito bem definidos;
- é muito improvável que o escopo mude;
- há uma grande entrega a ser feita, somente ao final do projeto;
- os requisitos de segurança são rigorosos; e
- a estrutura organizacional do órgão é hierarquizada.

A partir das características apresentadas, o projeto deve ser desenvolvido com o emprego da abordagem:

(A) ágil;
(B) adaptativa;
(C) híbrida;
(D) preditiva;
(E) hierárquica.

65

Um analista da CVM reforçou para sua equipe que os fatores de desempenho impactam de diferentes maneiras a adaptação do sistema de governança de uma organização.

O COBIT 2019 distingue três tipos diferentes de impacto, que são:

(A) conformidade, prioridade e necessidade de áreas de foco específicas;
(B) prioridade, componentes variantes e necessidade de áreas de foco específicas;
(C) prioridade, serviços de segurança gerenciados e componentes variantes;
(D) conformidade, componentes variantes e serviços de segurança gerenciados;
(E) serviços de segurança gerenciados, conformidade e necessidade de áreas de foco específicas.

66

A gestão de riscos relacionados à TI deve ser realizada de forma integrada à gestão corporativa de riscos, com uma abordagem de balanceamento de custos e benefícios.

Diante do contexto apresentado, é correto afirmar que:

(A) o investimento necessário para a mitigação do risco deverá ser balizado pelo desejo do gerente de TI. É importante comunicar a tolerância e as probabilidades de ocorrência do risco correspondente;
(B) em organizações com qualquer nível de governança corporativa, é estabelecido um sistema de gestão de riscos operacionais já com metodologias estabelecidas e com mapas de risco por processo de negócio ou por serviços;
(C) a avaliação de riscos implica coletar dados e identificar eventos (importantes ameaças reais que exploram significativas vulnerabilidades) com potenciais impactos negativos nos objetivos ou nas operações da organização;
(D) a manutenção e monitoramento do plano de ação de risco envolvem também a obtenção de aprovações para ações recomendadas, a aceitação de quaisquer riscos residuais e a garantia de que as ações aprovadas sejam assumidas pelos donos dos processos afetados;
(E) qualquer impacto em potencial, independente de afetar ou não os objetivos da empresa, causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis.

67

A CVM necessita desenvolver o Plano de Tecnologia da Informação. Esse plano deverá, também, contemplar as informações de:

(A) escopo de negócios, competências requeridas, investimentos e custeio;
(B) organização das operações de serviços de TI, arquitetura de TI e balanced scorecard;
(C) necessidade de aplicações, estratégia para fornecedores de serviços e relacionamento com o cliente;
(D) princípios de TI, Roadmap de TI e capacidade requerida de atendimento em relação a RH e infraestrutura;
(E) estratégia para fornecedores de serviço, gestão de negócios e políticas de segurança da informação.

68

A Comissão de Valores Mobiliários iniciou um processo licitatório para a implantação de um sistema de callcenter. A empresa X foi a vencedora e, conforme edital publicado, deverá seguir o modelo ITIL v4 na implementação do serviço. De forma a seguir a cadeia de valor preconizada no ITIL, a empresa elaborou um conjunto de atividades interconectadas para a entrega do serviço. Durante uma reunião de acompanhamento, a empresa identificou problemas em seu conjunto de atividades e, com isso, concluiu que não poderia entregar o serviço em funcionamento na data prevista. Tal fato poderia acarretar perda de *timing* de mercado.

Com o objetivo de adequar o conjunto de atividades e manter a entrega no prazo, a empresa X deverá atuar na atividade de:

(A) engajamento;
(B) desenho e transição;
(C) obtenção e construção;
(D) entrega e suporte;
(E) planejamento.

69

Amanda é funcionária da Comissão de Valores Mobiliários (CVM) e está criando um novo produto por ordem da chefia. A CVM preconiza a utilização do ITIL V4 em seus projetos. Amanda notou que, dentro da prática de gerenciamento de serviços, precisava efetuar o gerenciamento do catálogo de serviços.

Dentre as atividades das práticas existentes, Amanda deverá:

(A) garantir que informações precisas e confiáveis sobre a configuração de serviços estejam disponíveis quando e onde forem necessárias;
(B) assegurar que a disponibilidade e o desempenho de um serviço sejam mantidos em níveis suficientes no caso de um desastre;
(C) definir metas claras de negócios para níveis de serviço e garantir que a entrega de serviços seja avaliada, monitorada e gerenciada adequadamente em relação a essas metas;
(D) oferecer suporte à qualidade acordada de um serviço, manipulando todas as requisições de serviço predefinidas e iniciadas pelo usuário de maneira eficaz e amigável;
(E) fornecer uma única fonte de informações consistentes sobre todos os serviços e ofertas de serviços e garantir que eles estejam disponíveis para o público relevante.

70

Na empresa T, Davi está implementando o gerenciamento de serviços com base no ITIL versão 4. O Sistema de Valor de Serviços (SVS) representa o modo como os vários componentes e atividades da organização trabalham juntos para facilitar a criação de valor através dos serviços de TI implementados. Davi está executando práticas gerais de gestão adotadas e adaptadas para atendimento à gestão de domínios gerais. Ele busca garantir que a organização tenha a combinação certa de programas, projetos, produtos e serviços para executar a estratégia da organização dentro de suas restrições de recursos.

Davi está implementando a prática de gerenciamento de:

(A) portfólio;
(B) projeto;
(C) relacionamento;
(D) risco;
(E) estratégia.

RASCUNHO

RASCUNHO

RASCUNHO

RASCUNHO

Realização