PROVA - CATEGORIA GOVERNANÇA DE DADOS

Identificador: GSF879698

Variante A | 35 perguntas

Atenção! Certifique-se de que recebeu uma folha de respostas com o mesmo identificador.

Pergunta 1 | escolha única

De acordo com a Lei Geral de Proteção de Dados (LGPD), em relação à publicação de frequências alélicas oriundas de um estudo populacional em um browser de variantes, é correto afirmar que:

A. O órgão competente deve ser consultado pelos responsáveis pelo estudo, por se tratar da divulgação de dados pessoais sensíveis.

B. Viola diretamente a LGPD, por ser possível a identificação de indivíduos através da frequência alélica.

C. Se estabelecido um número mínimo de indivíduos para cálculo das frequências, não fere a LGPD, pois frequências alélicas são consideradas dados anonimizados devido à agregação estatística.

D. A publicação de frequências alélicas não entra no escopo da LGPD, pelo fato de serem dados oriundos de pesquisa clínica.

E. O dado usado para geração das frequências alélicas deve ser publicado junto às frequências para garantir transparência e replicabilidade.

Pergunta 2 | escolha única

No contexto de segurança da informação, são exemplos de ameaças lógicas:

A. Ataques de negação de serviço, alteração de dados por software não autorizado, alagamento do setor onde se encontra o servidor.

B. Perda de equipamento durante o transporte, escuta na rede, sequestro de dados por criptografia desconhecida.

C. Ausência de sistema de combate a incêndios, alteração de dados por software não autorizado, acesso por usuário não autorizado.

D. Ataques de negação de serviço, alteração de dados por software não autorizado, vazamento de senha de usuário.

E. Roubo de cabo de rede, vazamento de senha de usuário, alteração de dados por software não autorizado.

Pergunta 3 | escolha única

Caso um participante de um estudo científico queira revogar seu consentimento de participação, o procedimento técnico e legal a ser seguido pela equipe de administração dos dados, após notificação pelas instâncias responsáveis, é:

A. Revogar o acesso de toda a equipe aos dados do participante e mantê-los em pasta isolada, uma vez que os dados não poderão ser excluídos devido ao status WORM (Write Once Read Many).

B. Revogar as permissões para análises individuais, mas manter o dado do participante na geração de resultados agregados, uma vez que já foi gerado e pseudoanonimizado.

C. Reter os dados nos equipamentos de storage para fins de prestação de contas sobre sua geração, revogando apenas as permissões dos pesquisadores do projeto para análises científicas posteriores.

D. Revogar o acesso aos dados do participante e mantê-los congelados e com restrição de uso por 10 anos, procedendo à exclusão apenas após nova tentativa de contato com o participante.

E. Revogar o acesso aos dados do participante, excluindo-os de todos os bancos de dados ativos, com o devido registro da exclusão, salvo em domínios WORM, que devem ter o acesso bloqueado e ser excluídos assim que a limitação tecnológica se findar.

Pergunta 4 | escolha única

Assinale a alternativa que indique os riscos de aplicar criptografia simétrica a um sistema multiusuário:

A. O dado fica exposto quando está sendo utilizado por mais de um usuário, por precisar ser descriptografado e não poder ser criptografado enquanto um membro da equipe estiver usando.

B. Quando há o desligamento de um membro da equipe, o dado precisa ser recriptografado para gerar uma nova chave de criptografia.

C. Se mais de um usuário usar o dado simultaneamente, aumenta o risco de quebrar a criptografia e corromper o dado.

D. Se um usuário perder a chave de criptografia, o dado não poderá ser descriptografado novamente por nenhum membro da equipe.

E. Os membros da equipe não poderão trabalhar no mesmo ambiente, por risco de vazamento.

Pergunta 5 | escolha única

Quando um sistema é invadido e há o impedimento de que os usuários autorizados façam o login para suas atividades normais, o aspecto da informação afetado é:

A. Integridade

B. Autenticidade

C. Confidencialidade

D. Disponibilidade

E. Não repúdio

Pergunta 6 | escolha única

Durante a avaliação de riscos de segurança da informação de uma instituição de ciência e tecnologia (ICT), a equipe de segurança identificou que a indisponibilidade de um repositório de dados públicos, usado apenas como apoio a consultas, tem probabilidade e impacto baixos. O nível de risco está abaixo do critério de aceitação definido pela ICT, e o custo de implantar redundância seria superior ao impacto esperado. De acordo com a ABNT NBR ISO/IEC 27005, a ação mais adequada para esse risco é:

A. Reter o risco, documentando a decisão e monitorando-o periodicamente.

B. Evitar o risco, desativando o repositório.

C. Modificar o risco, implantando redundância no repositório.

D. Compartilhar o risco, contratando um seguro para o repositório.

E. Ignorar o risco, sem registro, por estar abaixo do critério de aceitação.

Pergunta 7 | escolha única

A criptografia é um dos principais mecanismos para proteger dados armazenados ou em trânsito. Considere as sentenças abaixo, relativas às criptografias simétrica e assimétrica.

(01) Na criptografia simétrica, são utilizadas duas chaves distintas, uma para cifrar e outra para decifrar os dados.
(02) A criptografia assimétrica utiliza um par de chaves, sendo uma chave pública e uma chave privada mantida em sigilo.
(04) Na criptografia simétrica, o emissor da mensagem criptografada deve compartilhar sua chave com o receptor.
(08) Na criptografia assimétrica, o emissor da mensagem criptografada deve gerar uma chave secreta e o receptor, outra.

Assinale a alternativa que representa a soma dos números dos itens corretos:

A. 3
B. 5
C. 6
D. 10
E. 12

Pergunta 8 | escolha única

O firewall de uma universidade bloqueia conexões consideradas inseguras, como as feitas sem TLS ou as que usam certificado cuja confiança não pode ser verificada. Um sistema web hospedado em um servidor externo, utiliza HTTPS com certificado digital autoassinado e não pode ser acessado a partir da universidade. A medida mais adequada para resolver o problema, sem reduzir o nível de segurança da universidade, é:

A. Aumentar o tamanho da chave do certificado autoassinado, para fortalecer a cifragem do canal.
B. Liberar o acesso ao sistema por HTTP, já que o bloqueio ocorre apenas em conexões cifradas.
C. Desativar a validação de certificados no firewall, para que a conexão seja aceita.
D. Trocar o algoritmo simétrico negociado na sessão TLS, mantendo o certificado atual.
E. Substituir o certificado por outro emitido por uma autoridade certificadora (AC) confiável, instalando a cadeia de certificação no servidor.

Pergunta 9 | escolha única

Uma instituiçao de pesquisa segmentou sua rede local em sub-redes para isolar seu servidores de pesquisa. Dois servidores foram configurados conforme abaixo: Servidor A: IP 172.16.30.45, rede 172.16.30.32/27, gateway 172.16.30.33. Servidor B: IP 172.16.30.100, rede 172.16.30.96/27, gateway 172.16.30.97. Os dois gateways correspondem a interfaces de um mesmo roteador, que não possui regras de filtragem entre elas. Em relação à comunicação entre os servidores A e B, é correto afirmar que:

A. Os servidores se comunicam diretamente na camada de enlace, pois pertencem à mesma rede 172.16.30.0/24.
B. Os servidores não podem se comunicar, pois endereços de sub-redes distintas não trocam tráfego.
C. Os servidores podem se comunicar, desde que o tráfego seja encaminhado pelo roteador entre as sub-redes.
D. Um switch de camada 2 posicionado entre os segmentos é suficiente para a comunicação, sem necessidade de roteamento.
E. A comunicação exige a tradução de endereços por NAT entre as duas sub-redes.

Pergunta 10 | escolha única

Um bioinformata de um hospital universitário foi transferido do projeto de oncologia para o de cardiologia. Após a transferência, ele continuou com acesso às bases de dados do projeto anterior e passou a precisar de acesso às bases do novo projeto, onde realizará apenas consultas e análises. Para aplicar o princípio do privilégio mínimo, a ação mais adequada do gestor de acessos é:

A. Revogar o acesso às bases do projeto anterior e conceder, nas novas bases, apenas as permissões necessárias às atividades atuais.

B. Manter o acesso às bases do projeto anterior, por poderem ser úteis em colaborações futuras.

C. Revogar o acesso às bases do projeto anterior e conceder perfil de administrador nas novas, evitando solicitações adicionais.

D. Criar uma conta compartilhada entre os membros do novo projeto, para simplificar a gestão de acessos.

E. Manter as permissões atuais e substituir a revisão de acessos por monitoramento dos registros de uso.

Pergunta 11 | escolha única

Um centro de bioinformática identificou um ransomware que criptografou servidores de arquivos com dados de projetos. A equipe de resposta isolou os servidores afetados da rede, confirmando que o ataque não se propagou mais pela rede. Os registros indicam que a intrusão inicial ocorreu há 10 dias, e o backup mais recente foi feito há 3 dias. Segundo as boas práticas de resposta a incidentes, a ação mais adequada neste momento é:

A. Restaurar o backup mais recente, para reduzir a indisponibilidade, e investigar a causa raiz depois.

B. Formatar os servidores e restaurar um backup anterior à intrusão, deixando a análise forense para depois.

C. Restaurar o backup mais recente se o antivírus não detectar malware nele, dispensando a análise da causa raiz.

D. Preservar as evidências, eliminar a causa raiz e os mecanismos de persistência e restaurar um backup anterior à intrusão, após verificar sua integridade.

E. Pagar o resgate para obter a chave de decifração, evitando a restauração e a investigação.

Pergunta 12 | escolha única

De acordo com a Lei Geral de Proteção de Dados (LGPD), uma organização que trata dados pessoais precisa definir claramente os papéis de controlador, operador e encarregado (DPO). Sobre as atribuições de cada um, é correto afirmar que:

A. O operador é responsável pelas decisões referentes ao tratamento de dados pessoais, definindo suas finalidades.

B. O controlador pode delegar ao encarregado a responsabilidade pelo cumprimento da LGPD, ficando isento de responder por ela.

C. O operador realiza o tratamento de dados pessoais em nome do controlador, podendo contrariar as instruções deste quando julgar mais adequado.

D. O encarregado atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

E. O encarregado realiza o tratamento de dados pessoais em nome do controlador, seguindo as instruções fornecidas por este.

Pergunta 13 | escolha única

Uma universidade pública brasileira pretende compartilhar dados pessoais de participantes de uma pesquisa com um centro de pesquisa localizado no exterior. De acordo com a Lei Geral de Proteção de Dados (LGPD), em relação à transferência internacional de dados pessoais, é correto afirmar que:

A. A transferência é vedada quando o destinatário for um organismo internacional, sendo permitida apenas para países.

B. A transferência somente pode ocorrer mediante consentimento do titular, pois a lei não prevê outras hipóteses.

C. A transferência pode ser realizada para país que proporcione grau de proteção de dados pessoais adequado ao previsto na lei, conforme reconhecido pela ANPD.

D. O controlador pode decidir, por conta própria, que o país de destino possui legislação semelhante à brasileira, dispensando o reconhecimento pela ANPD.

E. Por ser um órgão público, a universidade está dispensada de observar as hipóteses do art. 33 ao transferir dados a instituições estrangeiras.

Pergunta 14 | escolha única

Um instituto de pesquisa, que atua como controlador de dados pessoais, identificou um incidente de segurança que afetou os dados de seus titulares. Em relação à comunicação do incidente à Autoridade Nacional de Proteção de Dados (ANPD), de acordo com a Lei Geral de Proteção de Dados (LGPD) e a regulamentação da ANPD, é correto afirmar que:

A. A comunicação é de responsabilidade exclusiva do operador, por ser ele quem executa o tratamento dos dados.

B. A comunicação deve ser realizada em até 72 horas, contadas da ocorrência do incidente.

C. A comunicação é facultativa, ficando a critério do controlador comunicar ou não, mesmo que haja risco relevante aos titulares.

D. Todo incidente de segurança deve ser comunicado, independentemente do risco ou dano que possa causar aos titulares.

E. O controlador deve comunicar à ANPD e ao titular o incidente que possa acarretar risco ou dano relevante, no prazo de três dias úteis.

Pergunta 15 | escolha única

Um instituto de pesquisa em saúde mantém um repositório com dados científicos que incluem dados pessoais sensíveis de participantes de estudos clínicos. Ao estruturar a governança desse repositório, a organização decidiu adotar as boas práticas previstas na Lei Geral de Proteção de Dados (LGPD). Nesse contexto, é correto afirmar que:

A. O programa de governança em privacidade deve ser adaptado à estrutura, à escala e ao volume das operações e à sensibilidade dos dados tratados, com salvaguardas baseadas em avaliação sistemática de impactos e riscos.

B. A pseudonimização dos dados da pesquisa os torna dados anonimizados, de modo que deixam de ser considerados dados pessoais.

C. As regras de boas práticas devem ser uniformes para todos os projetos, independentemente da natureza, do escopo e dos riscos de cada tratamento.

D. O consentimento dos participantes dispensa a adoção de medidas de segurança e de mecanismos internos de supervisão, pois legitima o tratamento.

E. A implementação de programa de governança em privacidade é obrigatória para todo controlador que trate dados pessoais sensíveis.

Pergunta 16 | escolha única

Segundo a Lei Geral de Proteção de Dados (LGPD), em relação à realização de estudos por órgãos de pesquisa, é correto afirmar que:

A. O órgão de pesquisa sempre deve eliminar os dados pessoais após o término do seu tratamento.

B. O órgão de pesquisa poderá ter acesso a bases de dados pessoais, na realização de estudos em saúde pública.

C. O tratamento de dados pessoais poderá ser realizado, sem necessidade de se buscarem meios de anonimização.

D. O tratamento de dados pessoais sensíveis poderá ser realizado somente nos casos em que seja garantida a anonimização.

E. O órgão de pesquisa será o responsável pela segurança da informação quando desejar realizar a transferência dos dados a terceiro.

Pergunta 17 | escolha única

A rede de um departamento de uma universidade utiliza o bloco de endereços 192.168.40.0/24. O departamento divide a rede em sub-redes com máscara 255.255.255.240. Um servidor desse departamento possui o endereço IP 192.168.40.150. Os endereços de rede e de broadcast da sub-rede à qual esse servidor pertence são, respectivamente:

A. 192.168.40.128 e 192.168.40.143.

B. 192.168.40.144 e 192.168.40.255.

C. 192.168.40.0 e 192.168.40.255.

D. 192.168.40.145 e 192.168.40.158.

E. 192.168.40.144 e 192.168.40.159.

Pergunta 18 | escolha única

Sobre as características de serviços essenciais de infraestrutura, como DNS, DHCP, HTTP, SSH e SMTP, é correto afirmar que:

A. Os roteadores encaminham, por padrão, as mensagens DHCPDISCOVER entre sub-redes, dispensando o agente de retransmissão (relay).

B. O DNS utiliza o TCP, além do UDP, em situações como respostas truncadas e transferências de zona entre servidores.

C. Os métodos GET e POST do HTTP são idempotentes, o que permite repeti-los sem efeitos adicionais no servidor.

D. Na primeira conexão a um servidor, o SSH dispensa a verificação da chave do host, pois a autenticação do usuário garante a identidade do servidor.

E. No SMTP, a porta 25 é destinada à submissão de mensagens por clientes autenticados, e a 587, à transferência entre servidores.

Pergunta 19 | escolha única

Um sistema de browser de variantes genômicas de um projeto de pesquisa é executado em três servidores idênticos, posicionados atrás de um balanceador de carga que distribui as requisições pelo algoritmo round robin. Após a falha de um dos servidores, os usuários passaram a receber erros em cerca de uma a cada três requisições, embora os outros dois servidores estejam operando normalmente. Para resolver o problema, mantendo o balanceamento entre os servidores restantes, a configuração mais adequada no balanceador é:

A. Habilitar verificações de integridade (health checks), para retirar do conjunto os servidores que não respondem.

B. Trocar o algoritmo para menor número de conexões, para que o servidor com falha receba menos requisições.

C. Habilitar a persistência de sessão, para que cada usuário permaneça sempre no mesmo servidor.

D. Substituir o balanceador por DNS round robin com TTL elevado, para distribuir as requisições entre os servidores.

E. Atribuir pesos maiores aos servidores saudáveis, mantendo o servidor com falha no conjunto.

Pergunta 20 | escolha única

Na rede local de um laboratório de pesquisa, todos os computadores e um servidor de armazenamento em rede (Network Attached Storage, NAS) estão conectados, cada um por um cabo individual, a um switch central. Sobre a topologia dessa rede, é correto afirmar que:

A. A falha no cabo de um computador interrompe a comunicação de toda a rede.

B. Todos os dispositivos compartilham um único cabo como meio de comunicação.

C. A falha do switch central interrompe a comunicação entre todos os dispositivos da rede.

D. Cada dispositivo possui uma conexão direta com todos os outros dispositivos da rede.

E. Os dados circulam em um único sentido, passando por todos os dispositivos em sequência.

Pergunta 21 | escolha única

Um administrador de um servidor com sistema operacional Ubuntu 22.04 LTS precisa verificar a configuração do serviço de acesso remoto SSH. De acordo com o Filesystem Hierarchy Standard (FHS), o diretório padrão em que ficam armazenados os arquivos de configuração do sistema e dos serviços instalados é:

A. /bin

B. /opt

C. /usr

D. /var

E. /etc

Pergunta 22 | escolha única

Em um servidor com sistema operacional Ubuntu 22.04 LTS, o diretório projeto é compartilhado por um grupo de pesquisa. Ao ser executado o comando ls -ld projeto, foi apresentado na tela o seguinte resultado: drwx------ 2 user_ti grupo_ti 4096 nov 04 09:15 projeto O administrador executou, então, com sucesso e nesta ordem, os comandos abaixo: sudo chgrp grupo_bio projeto sudo chmod 2755 projeto sudo chmod o-x projeto Considerando que nenhuma outra alteração foi aplicada ao diretório, o resultado exibido após uma nova execução do comando ls -ld projeto é:

A. drwxr-xr-- user_ti grupo_bio

B. drwxr-sr-- user_ti grupo_bio

C. drwxr-sr-- user_ti grupo_ti

D. drwxr-Sr-- user_ti grupo_bio

E. drwxr-sr-x user_ti grupo_bio

Pergunta 23 | escolha única

Em um servidor com sistema operacional Ubuntu 22.04 LTS, o administrador precisa configurar, com o systemd, o comportamento de dois serviços. O serviço analise.service não deve ser iniciado automaticamente na inicialização do sistema, mas pode ser iniciado manualmente quando necessário. Já o serviço download.service não deve ser iniciado de forma alguma, nem manualmente nem como dependência de outros serviços, mesmo após reinicializações. Os subcomandos do systemctl mais adequados para configurar analise.service e download.service são, respectivamente:

A. stop e disable.

B. mask e disable.

C. stop e mask.

D. disable e mask.

E. disable e stop.

Pergunta 24 | escolha única

Considere que você é o administrador de um servidor com sistema operacional Ubuntu 22.04 LTS e acessou o servidor pelo console local. Partindo de cadeias do iptables vazias, com política padrão ACCEPT, executa com sucesso os comandos abaixo na ordem apresentada: sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT sudo iptables -A INPUT -p tcp --dport 22 -j DROP Desconsiderando o tráfego da interface de loopback e considerando que nenhuma outra regra foi criada, é correto afirmar que:

A. As conexões SSH são aceitas, pois a política padrão da cadeia é ACCEPT.

B. Todo o tráfego, exceto o HTTP, é descartado, pois a regra DROP se aplica a todas as portas além da 80.

C. As conexões HTTPS (porta 443) são descartadas, pois não há regra que as aceite explicitamente.

D. As conexões HTTP são aceitas e as conexões SSH são descartadas, e o tráfego que não casa com nenhuma regra é aceito pela política padrão.

E. As regras só passam a valer após a reinicialização do servidor.

Pergunta 25 | escolha única

Um laboratório de pesquisa utiliza hipervisores do tipo 1 nos servidores de seu centro de dados e hipervisores do tipo 2 nos notebooks dos seus pesquisadores, para testes. Sobre as diferenças entre esses dois tipos de hipervisores, é correto afirmar que:

A. O tipo 1 depende de um sistema operacional hospedeiro, ao passo que o tipo 2 é executado diretamente sobre o hardware.

B. No tipo 2, a falha do sistema operacional hospedeiro não afeta as máquinas virtuais em execução, pois o hipervisor as isola do hospedeiro.

C. A criação de snapshots de máquinas virtuais só é possível em hipervisores tipo 1, por exigirem acesso direto ao hardware.

D. O tipo 2 exige que as máquinas virtuais executem o mesmo sistema operacional do notebook em que está instalado.

E. O tipo 1 é executado diretamente sobre o hardware, sem depender de um sistema operacional hospedeiro de uso geral, ao contrário do tipo 2.

Pergunta 26 | escolha única

Um projeto de pesquisa precisa executar dezenas de instâncias isoladas de uma mesma aplicação de análise genômica em um servidor Linux e avalia usar contêineres (p.ex., Docker) ou máquinas virtuais (VMs). Em relação às diferenças entre essas duas tecnologias, é correto afirmar que:

A. Os contêineres compartilham o kernel do sistema operacional hospedeiro, ao passo que cada VM executa seu próprio sistema operacional convidado.

B. Cada contêiner executa um sistema operacional convidado completo, o que o torna mais pesado que uma VM.

C. As VMs compartilham o kernel do hospedeiro e, por isso, iniciam mais rapidamente que os contêineres.

D. Os contêineres oferecem isolamento mais forte que as VMs, pois cada um possui hardware virtualizado próprio.

E. Os contêineres exigem um hipervisor tipo 1 para serem executados, enquanto as VMs dispensam hipervisor.

Pergunta 27 | escolha única

O departamento de bioinformática de uma universidade contratou um serviço de e-mail e edição colaborativa de documentos, acessado pelos pesquisadores por meio do navegador, sem instalação de programas nos computadores. Esse serviço é um exemplo de Software como Serviço (Software as a Service, SaaS). Sobre as características desse modelo, é correto afirmar que:

A. O instituto gerencia o sistema operacional e o armazenamento em que a aplicação é executada.

B. O provedor gerencia a infraestrutura e a aplicação, cabendo ao instituto, em geral, a gestão dos usuários, dos acessos e dos dados inseridos.

C. O instituto desenvolve e implanta suas próprias aplicações sobre a plataforma, sem gerenciar a infraestrutura.

D. A aplicação precisa ser instalada em cada computador do instituto, que fica responsável por atualizá-la.

E. O provedor é integralmente responsável pela segurança, inclusive por definir quem pode acessar os dados do instituto.

Pergunta 28 | escolha única

Um projeto de pesquisa definiu, para o seu repositório de dados, um objetivo de ponto de recuperação (RPO) de 4 horas e um objetivo de tempo de recuperação (RTO) de 2 horas. A política de backup atual realiza um backup completo todos os domingos e um backup incremental diário às 22h, ambos armazenados em local externo. Em relação à situação descrita, é correto afirmar que:

A. A política atende ao RPO, pois o backup incremental diário garante a recuperação com perda máxima de 4 horas de dados.

B. O RTO indica a quantidade máxima de dados que pode ser perdida, e a política o atende por manter cópias em local externo.

C. A substituição do backup incremental pelo diferencial resolveria o descumprimento do RPO, pois reduz a perda de dados.

D. A política não atende ao RPO, pois, em caso de falha, até cerca de 24 horas de dados podem ser perdidas.

E. O RPO indica o tempo máximo para restabelecer o serviço, e a política o atende por usar backups incrementais.

Pergunta 29 | escolha única

Um analista de governança de dados escreveu o script em Python abaixo para identificar usuários com número de acessos acima de um limite em uma base de pesquisa.

```
registros = [
{"usuario": "ana", "acessos": 3},
{"usuario": "bruno", "acessos": 12},
{"usuario": "carla", "acessos": 10},
{"usuario": "diego", "acessos": 15},
]
LIMITE = 10
alertas = []
for r in registros:
if r["acessos"] > LIMITE:
alertas.append(r["usuario"])

print(len(alertas), alertas)
```

Considere que o script foi executado com sucesso. A saída exibida na tela é:

A. 2 ['bruno', 'carla', 'diego']

B. 4 ['ana', 'bruno', 'carla', 'diego']

C. ['bruno', 'diego'] 2

D. 2 ['bruno', 'diego']

E. 2 ['ana', 'carla']

Pergunta 30 | escolha única

Um bioinformata mantém, em um repositório Git, os scripts de coleta de dados de um projeto de pesquisa. O repositório local está sincronizado com o remoto (origin), e a branch main local aponta para o mesmo commit de origin/main. Em seguida, um colega envia um novo commit para a branch main do remoto. Depois disso, o analista executa, com sucesso e nesta ordem, os comandos abaixo: git checkout -b ajuste-logs git add coleta.sh git commit -m "Ajusta o formato dos logs" git fetch origin Sobre o estado dos repositórios após a execução desses comandos, é correto afirmar que:

A. A branch ajuste-logs existe apenas no repositório local, e o fetch atualizou origin/main sem alterar a branch main local.

B. A branch ajuste-logs foi criada automaticamente no repositório remoto assim que o commit foi realizado.

C. O git fetch incorporou o commit do colega à branch ajuste-logs, por meio de um merge automático.

D. O git fetch atualizou a branch main local, que agora aponta para o mesmo commit de origin/main.

E. O commit realizado em ajuste-logs já está disponível para o colega, pois o git commit grava as alterações no repositório remoto.

Pergunta 31 | escolha única

Um bioinformata precisa enviar, no corpo de uma requisição a uma API, as informações de um projeto de pesquisa no formato JavaScript Object Notation (JSON). Segundo a especificação do formato, o trecho sintaticamente válido é:

A. {'projeto': 'Clima', 'participantes': 24}

B. {projeto: "Clima", participantes: 24}

C. {"projeto": "Clima", "participantes": 24, "ativo": true}

D. {"projeto": "Clima", "participantes": 24, "ativo": True}

E. {"projeto": "Clima", "participantes": 24,}

Pergunta 32 | escolha única

Uma instituição de ciência e tecnologia vai disponibilizar um novo serviço de processamento de dados para seus pesquisadores. Para isso, precisa adquirir servidores e licenças de software e disponibilizar esses componentes, com as especificações acordadas, quando e onde forem necessários. De acordo com o ITIL 4, a atividade da cadeia de valor de serviço responsável por essa ação é:

A. Melhorar.
B. Obter/construir.
C. Engajar.
D. Projetar e fazer a transição.
E. Entregar e dar suporte.

Pergunta 33 | escolha única

O ITIL 4 apresenta princípios orientadores e dimensões que auxiliam as organizações na adoção e na adaptação das práticas de gestão de serviços. Considere as sentenças abaixo, relativas a esses elementos do ITIL 4.
(01) As quatro dimensões da gestão de serviços são pessoas, processos, produtos e parceiros.
(02) O princípio "otimizar e automatizar" recomenda automatizar as atividades antes de simplificá-las, para obter ganhos imediatos.
(04) O princípio "comece de onde você está" orienta a avaliar e reaproveitar serviços, processos e recursos existentes antes de criar algo novo.
(08) A dimensão "informação e tecnologia" abrange, além das tecnologias de apoio, a gestão da informação, do conhecimento e da segurança.

Assinale a alternativa que representa a soma dos números dos itens corretos:

A. 5
B. 6
C. 10
D. 12
E. 15

Pergunta 34 | escolha única

O sistema de acompanhamento de fluxo laboratorial de um projeto de pesquisa ficou fora do ar por causa de um processo travado. Considere as ações abaixo, realizadas pela equipe de TI.
I. A equipe reiniciou o processo e restabeleceu o serviço o mais rápido possível.
II. Como a falha se repetiu três vezes no mês, a equipe investigou a causa raiz e registrou uma solução de contorno.
III. A correção definitiva exigiu a atualização do servidor de aplicação, que foi submetida à avaliação de riscos e à autorização antes de ser implantada.

De acordo com o ITIL 4, as ações I, II e III correspondem, respectivamente, às práticas de gerenciamento de:

A. Problemas, incidentes e mudanças.
B. Incidentes, mudanças e problemas.
C. Incidentes, problemas e mudanças.
D. Requisições, problemas e mudanças.
E. Incidentes, problemas e requisições.

Pergunta 35 | escolha única

O Departamento de Tecnologia da Informação e um laboratório, ambos de uma universidade, firmaram um acordo de nível de serviço (Service Level Agreement, SLA) para o portal de dados do laboratório. O acordo prevê disponibilidade mínima mensal de 99,5%, medida sobre as 24 horas de todos os dias do mês, e determina que as manutenções programadas previamente acordadas não sejam contabilizadas como indisponibilidade. Em um mês de 30 dias, ocorreram uma manutenção programada de 2 horas e duas falhas, de 1 hora e 40 minutos e de 1 hora e 30 minutos. Com relação ao cumprimento do SLA nesse mês, é correto afirmar que:

A. O SLA foi descumprido, pois a indisponibilidade total, incluindo a manutenção, foi de 310 minutos, superior ao limite de 216 minutos.

B. O SLA foi descumprido, pois o limite de indisponibilidade mensal para 99,5% é de 36 minutos.

C. O SLA foi descumprido, pois a indisponibilidade contabilizada, de 190 minutos, supera o limite de 150 minutos.

D. O SLA foi cumprido, pois a indisponibilidade contabilizada, de 190 minutos, é inferior ao limite de 216 minutos.

E. O SLA não pode ser avaliado sem um acordo de nível operacional (Operational Level Agreement, OLA) com a equipe de infraestrutura.